SHA-3 submission – Updated version: 2009-01-15

SIMD Is a Message Digest

Principal submitter:

Gaëtan Leurent

École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

Gaetan.Leurent@ens.fr
Tel: +33.1.44.32.20.47
Fax: +33.1.44.32.21.51

Auxiliary submitters:

Charles Bouillaguet, Pierre-Alain Fouque

Algorithm inventors/developers:

Gaëtan Leurent, Charles Bouillaguet, Pierre-Alain Fouque

Backup contact:

Pierre-Alain Fouque
École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

Pierre-Alain.Fouque@ens.fr
Tel: +33.1.44.32.20.48
Fax: +33.1.44.32.21.51

Signature:

About this version

This version is an updated version of the original submission, sent to NIST on January 15th.

The main difference with the original submission comes from the fact that there was a typo is the specification and in the implementation, which led an incorrect description of the hash function. The documentation and the implementation have been fixed, and the test vectors have been regenerated.

More precisely, here is a list of the modifications included in this version:

- Technical typos that leads to an incorrect description of the hash function:
  - In Section 1.2.2, we define the inner codes I_{185} and I_{233}, that gives an optimal minimal distance. However, in the following sections of the initial document, the codes used were I_{185} and I_{223}. The reference ans optimized implementations also used I_{223} in place of I_{233}. In this updated document, we have corrected this typo by using I_{233} everywhere, because it offers better properties. We also had to update the implementations, which means that the test vectors the Known Answer Tests, the Monte-Carlo Tests and the IV's had to be recomputed. This updated document contains the correct values.
  - In Section 1.2.3, we define four permutations p_0, p_1, p_2, p_3 to be used in SIMD-512. However, in our implementations, we used these permutations in a different order. This inconstancy between the code and the documentation has been resolved in favor of the code, because it has no security impact. This document has been modified to define the correct permutations.
- Performance fix:
  - The speed of the vectorized implementation of SIMD on the ARM architecture was based on an implementation of a early design, and an updated implementation actually showed that the performance are not as good as expected. The throughput as been corrected from ~~13 MB/s~~ to 9 MB/s an this platform. This does not affect other measurement.
- Additional material to clarify ambiguities
  - In Section 1.1.3, we added a paragraph to define the rotation.
  - In Section 1.2.2 we added a table with the parameters of the message expansion as a code.
  - In Section 1.2.3, we added a table to detail the step parameters used in a round.
  - In Section 1.2.5, we tried to clarify how to understand `"SIMD-`$\langle i \rangle$` v1.0"`: "the string is written in ASCII and padded with zeros, $\langle i \rangle$ is the decimal representation of n in ASCII without any extra zero, and there is a single space between the last digit of $\langle i \rangle$ and the `"v"`." instead of "~~the string is written in ASCII and padded with zeros, and $\langle i \rangle$ is the decimal representation of n in ASCII, without any trailing zero or space.~~"
  - In Section 1.2.6, we explained how to interpret the message and the IV as matrices.
  - In Chapter 6, we added a table with the hash output on some test vectors.
- Small improvements of the security analysis
  - In Section 1.2.2, paragraph *first layer* we added a paragraph on the minimal weight of the *affine* code which complements the results on the underlying *linear* code.

  - In Section 1.2.2, paragraph *second layer*, we added a paragraph about the minimal distance of the code in terms of NAF.
  - Rephrased the security proof against differential cryptanalysis (Section 4.2.1).

- Change of notations:
  - The expanded message use in the j-th Feistel ladder at round i was sometimes denoted by W_i^j and sometimes by $W_j^{(i)}$. To make the notations more uniform, we chose to denote round index with $X^{(i)}$ for any variable X. Thus, r_i become $r^{(i)}$; s_i become $s^{(i)}$; ϕ_i become $\phi^{(i)}$; p_i become $p^{(i)}$. Section 1.1.4 as been added to explain this convention.
  - There was conflict between the rotation constant r of the round i and the elements of the set r that is a parameter of a the round. We renamed the round parameter to π.

- Small technical typos:
  - In Section 1.2.2, when defining the first layer of the message expansion, the bounds of the sums were wrong. The sum is over the message words x_j, and go up to 63 for SIMD-256 (instead of ~~127~~), and 127 for SIMD-512 (instead of ~~255~~). The ~~x_i~~'s have been renamed to x_j to make this more clear (this also affects Section 1.1.2).
  - In some places, $\to$ and $\mapsto$ were used instead of each other. We now use $\to$ to define the domain and codomain of a function, and $\mapsto$ to define the rule of correspondence. In section 1.3.2 we now use $\rightsquigarrow$ to denote differential trails.
  - The message length is taken modulo 2^m and not modulo ~~2^{2^m}~~, since m is the size of a message block in bits, and we want to use this length as a message block. Note that this has hardly any practical significance...

    This typo was present in Section 1.2.1, 1.2.4, and 1.2.6.
  - In Section 1.2.2, "points of the field $\mathbb{F}_{257}$~~$[X]$~~" should be "points of the field $\mathbb{F}_{257}$".
  - In Section 1.2.2, changed ~~$I(x) = C \boxtimes x$~~ to $I_C : x \mapsto C \boxtimes x$.

- Small editorial changes and typos:
  - Some titles were not properly capitalized.
  - Section 1.1.1: "~~This field is interesting~~ because" changed to "We chose this field because"; changed $P = \sum_{j=0}^{n-1} x_j X^j$ to $P(X) = \sum_{j=0}^{n-1} x_j X^j$
  - Section 1.1.2: "This transform is identical to the DFT [...]. It is a bijection of $\mathbb{F}_{257}^n$.".
  - Section 1.1.3: "The Rings $\mathbb{Z}_{2^{16}}$ and $\mathbb{Z}_{2^{32}}$"; Changed "~~Since an element of $\mathbb{Z}_{2^{16}}$ can be seen as a 16-bit word, and an element of $\mathbb{Z}_{2^{32}}$ can be seen as a 32-bit word, we can apply bit-wise boolean functions to them. We will use the following functions:~~" to "We can represent elements of $\mathbb{Z}_{2^{16}}$ by 16-bit words, and elements of $\mathbb{Z}_{2^{32}}$ by 32-bit words. Thus, we define the following bit-wise boolean functions on 32-bit words:"
  - Section 1.2: "~~The~~ SIMD ~~hash~~ is..."; "Many hash functions use a custom block cipher [...], and a Feistel ladder."
  - Section 1.2.1: added "we use a truncation T to compute the hash value from the last internal state", and changed ~~D~~ to T in Figure 1.1; added "as well as the partial inverses $x \mapsto y$ s.t. $P(x, y) = z$ and $y \mapsto x$ s.t. $P(x, y) = z$ for all z's"

- Section 1.2.2: changed "~~member of the MD/SHA family~~" to "hash functions of the MD/SHA family"; In paragraph *First Layer*: corrected "~~expansive~~" to "expensive"; added a footnote about the NTT; "it has an optimal minimal distance"; In paragraph *Second Layer*: "We ~~choose to~~ use"; "we found ~~two~~ values [...] $C = 185$ and $C = 233$ (and their opposites)" changed to "we found four values [...] $C = 185$, $C = 233$, and their opposites"; "where $\widetilde{x}$ is x lifted to the integers, with $-128 \leq \widetilde{x} \leq 128$ (lifting to $\{-128, ...128\}$ is easier than to $\{0, ...257\}$)" changed to "x is lifted to the integers with $-128 \leq \widetilde{x} \leq 128$ because lifting to $\{-128, ...128\}$ is easier than to $\{0, ...257\}$"; "two copies of $O(M)$ coded differently" changed to "two copies of $O(M)$ encoded through two different inner codes".
- In section 1.2.3: changed "prevent ~~the possibility of a weak bit~~" to "prevent differential trails active only on the most-significant bit"; "a new value is computed in each Feistel ladder, and this new value is sent to another Feistel ladder"; changed "The whole compression function is made of 4 rounds, plus ~~one final round~~" to "The whole compression function is made of 4 rounds, plus four final steps", changed "the ~~choice of~~ constants" to "the chosen constants".
- Section 1.2.4: changed "~~is~~ needed" to "if needed"; changed "~~the first message word will be the low order byte of the counter~~" to "the low order byte of the counter will be the first message byte"; changed "~~so that the expanded message is prefix-free~~" to "Alternatively, we can consider that the compression function takes an extra input bit, and that the message is encoded in a prefix-free way."
- Section 1.2.5: IV $-n = \mathsf{SIMD\text{-}Compress}(0, \texttt{"SIMD-}\langle i \rangle\ \texttt{v1.0"}, \theta)$; changed "The ~~values for~~" to "The IV of"
- Section 1.2.6: "the reference implementation only keeps"
- Section 1.3.1: changed "the Merkle-Damgård iteration ~~without a finalization function D~~" to "the Merkle-Damgård iteration with no finalization function"; added "(which is equivalent to a prefix-free encoding of the message)".
- Section 1.3.2: "the feed-forward makes".
- Section 1.3.3: "~~and~~ an attack [...] translates" changed to "since an attack [...] translates"; "~~use the fact that the message expansion is weak~~" changed to "take advantage of the weak message expansion"; "~~which allows a quite~~ efficient software implementation" changed to "for an efficient software implementation"; "using concatenated codes"; "with ~~a~~ different inner code" changed to "with two different inner codes".
- Section 2.1.1: "~~ans~~" corrected to "and can"; "~~it's~~" corrected to "its"' added "The NTT can also be computed mostly inside the registers.".
- In Section 2.1.2: changed "~~For instance, one can use o cores for the message expansion, and one core for the Feistel part. In this case~~, we gain a factor 1.8 on the performance." to "When using two cores, we gain a factor 1.8 on the performance.".
- Section 3: "preimage or second preimage attack has a complexity of 2^n" changed to "a preimage or second preimage attack has a complexity of 2^n"
- Section 4.1.1: "~~we can hope there is~~ no generic attack [...] ~~as long as the compression function is good~~" changed to "there are no generic attack [...] ".
- Section 4.2.2: fixed "some differential pattern [...] ~~than~~ can be cancelled" to "some differential pattern [...] that can be cancelled"
- Section 5.2: title has been changed from "~~Strong Message Expansion~~" to "Security"; "a block cipher used to encrypt"; "~~expansive~~" corrected to "expensive".

Introduction

The SIMD hash function is quite similar to members of the MD/SHA family. It is based on a familiar Merkle-Damgård design, where the compression function is built from a Feistel-like cipher in Davies-Meyer mode. However there are some innovations in this design: the internal state is twice as big as the output size, we use a strong message expansion, and we use a modified feed-forward in the compression function. The main design criteria was to follow the MD/SHA designs principle which are quite well understood, and to add some elements to avoid all known attacks.

SIMD is particularly efficient on platforms with vector instructions (SIMD) which are available on many processors. Such instructions have been proposed since 1997 and are now widely deployed. Moreover, it is also possible to use two cores on multicore processors to boost the performance with a factor 1.8 by splitting the message expansion function and the hashing process.

Contents

Chapter 1

Algorithm Specification and Rationale

This document defines the SIMD family of hash functions. This family is based on two functions SIMD-256 and SIMD-512; we define SIMD-n with $n \leq 256$ as a truncation of SIMD-256, and SIMD-n with $256 < n \leq 512$ as a truncation of SIMD-512.

Each function SIMD-n takes as input a message of arbitrary size, and outputs a digest of n bits.

1.1 Mathematical Preliminaries and Notations

The design of SIMD uses a number of different operations with useful mathematical properties. In this section, we introduce the operations that will be used through this document, and detail their properties.

1.1.1 The Field $\mathbb{F}_{257}$

Since 257 is a prime, the field $\mathbb{F}_{257}$ is only the ring $\mathbb{Z}_{257}$ of the integers modulo 257. The operations in this field are indicated with $\pmod{257}$. We chose this field because we can map a byte to an element of the field, and the operations in $\mathbb{F}_{257}$ can be computed efficiently in software and in hardware.

1.1.2 The Number-Theoretic Transform

The Number-theoretic transform of size n in $\mathbb{F}_{257}$ is defined as:

$$\begin{aligned} &\mathsf{NTT}_n : \mathbb{F}_{257}^n \to \mathbb{F}_{257}^n \\ &\qquad (x_j)_{j=0}^{n-1} \mapsto (y_i)_{i=0}^{n-1} : \quad y_i = \sum_{j=0}^{n-1} x_j \omega^{ij} \pmod{257}. \end{aligned}$$

where $n \leq 256$, and ω is a n-th root of unity in $\mathbb{F}_{257}$. We can see it as a polynomial evaluation: if the sequence $(x_j)_{j=0}^{n-1}$ is interpreted as a polynomial $P(X) = \sum_{j=0}^{n-1} x_j X^j$, then we have $y_i = P(\omega^i)$.

This transform is identical to the Discrete Fourier Transform but it operates on a finite field instead of the field of complex numbers. It is a bijection of $\mathbb{F}_{257}^n$. It can be computed efficiently by the same algorithm as the Fast Fourier Transform, which has a complexity of $\mathcal{O}(n \log n)$ field operations.

1.1.3 The Rings $\mathbb{Z}_{2^{16}}$ and $\mathbb{Z}_{2^{32}}$

$\mathbb{Z}_{2^{16}}$ denotes the ring of integers modulo 2^{16}, and $\mathbb{Z}_{2^{32}}$ denotes the ring of the integers modulo 2^{32}. We use $\boxplus$ and $\boxtimes$ to represent the modular addition and multiplication in these rings. (Actually, we only use $\boxplus$ in $\mathbb{Z}_{2^{32}}$ and $\boxtimes$ in $\mathbb{Z}_{2^{16}}$).

We can represent elements of $\mathbb{Z}_{2^{16}}$ by 16-bit words, and elements of $\mathbb{Z}_{2^{32}}$ by 32-bit words. Thus, we define the following bit-wise boolean functions on 32-bit words:

$$\mathsf{IF}(A, B, C) = (A \wedge B) \ \vee (\neg A \wedge C)$$
$$\mathsf{MAJ}(A, B, C) = (A \wedge B) \ \vee (A \wedge C) \vee (B \wedge C)$$

where $\vee$ denotes the boolean OR, $\wedge$ denotes AND, and $\neg$ denotes NOT. We also use $\oplus$ for the exclusive or. IF acts as a conditional, and MAJ is the majority function. These function are already used in some hash functions because they have good properties: the output is unbiased, and no input bit has a linear effect on the output.

We also use bit-wise rotations on 32-bit words: x rotated to the left by s bits is denoted by $x^{\lll s}$.

1.1.4 Index and Exponent

In this document, we use $X^{(i)}$ to denote the variable X associated with round i. Many variable can be seen as vectors, to we use $X_{[0..k]}$ to denote the vector $[X_0, X_1, ...X_k]$ (or its transpose, depending on the context).

1.2 Description of the Algorithm

SIMD is an iterative hash function that follows the Merkle-Damgård design. The main component of a Merkle-Damgård hash function h is a compression function $C : \{0,1\}^p \times \{0,1\}^m \to \{0,1\}^p$. To compute $h(M)$, the message M is first divided into k chunks M_i's of m bits. Then the compression function is used to compress the message chunks and the internal state: $H_{i+1} = C(H_i, M_i)$. There is a padding rule to fill the last m-bit blocks, and the padding usually includes the message size (this is known as the Merkle-Damgård strengthening). The initial value of the internal state is called IV and is fixed in the description of the hash function. The output of the hash function is given by computing a finalization function $D : \{0,1\}^p \to \{0,1\}^n$ on the last internal state H_{k-1}.

The Davies-Meyer mode is a common way to build a compression function C from a block cipher E: it is defined as $C(h, m) = E_m(h) \oplus h$. Many hash functions use a custom block cipher, designed with a message expansion step, and a Feistel ladder.

The SIMD family uses a similar design, and the size parameters are as follows:

	Output size n	Message block size m	Internal state size p
SIMD-256	256	512	512
SIMD-512	512	1024	1024

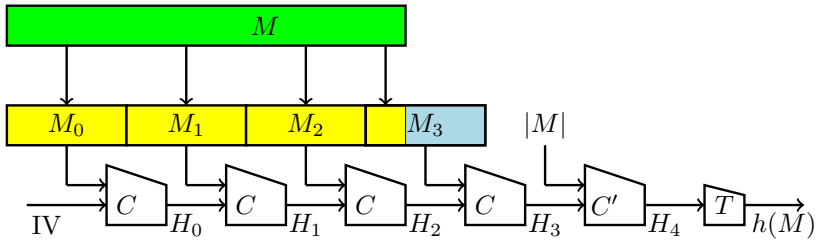

Figure 1.1: The iteration used in SIMD

The inner state is represented as a matrix of 32-bit words. For SIMD-256, it is a 4×4 matrix, while SIMD-512 has a 8×4 inner state:

$$\mathcal{S}_{256} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix} \qquad \mathcal{S}_{512} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}$$

In this section, we will describe more precisely the operating mode of SIMD, and the inside of the compression function: the message expansion and the Feistel ladder.

1.2.1 Mode of Operation

Iteration

Our mode of operation is similar to the wide-pipe construction of Lucks [16] and to Chop-MD [6]. The internal state is twice as large as the output, and we use a truncation T to compute the hash value from the last internal state. The padding rule is quite simple: the last message block is filled with zeros if it is smaller than m bits, and an extra block containing the size of the message in bits is added. This extra block is compressed with a slightly modified compression function C', and the output is truncated. This is described by Figure 1.1.

The size of the message input to SIMD is not limited, and the number of bits of the message included in the last block is taken modulo 2^m. We believe that it is not necessary to limit the message size in the description of the algorithm, but for all practical purpose it can be considered to be below 2^{64}. Therefore, the message input in the last message block is quite constrained. The last compression function C' acts as kind of blank round, and makes it harder to use the truncation to find a collision.

Modified Davies-Meyer

To build our compression from a Feistel-like block cipher, we will use a technique similar to the well known Davies-Meyer construction, but with a few variations.

First, we have a message block size that is equal to the internal state size, so we can use $C(h, m) = E_m(h \oplus m) \oplus h$ instead of $C(h, m) = E_m(h) \oplus h$. This is construction 8 from [4] (and construction 41 from [21]). It enjoys the same provable security guarantees than the original

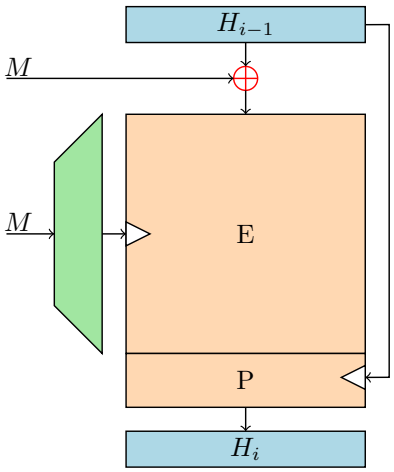

Figure 1.2: Modified Davies-Meyer

Davies-Meyer construction. Note that this is natural, because the former can be seen as a special case of the later, with a block cipher E' defined as $E'_k(x) = E_k(x \oplus k)$. The fact that $h \oplus m$ goes into the block cipher means that the adversary has to "commit" to a given value of m before starting to evaluate $E_m(h \oplus m)$. This prevents, for example, to construct the message m "on the fly", and complicates message modification techniques.

Second, instead of using a simple XOR to combine $E_m(h \oplus m)$ and h, we will use a few extra Feistel rounds, with h entering as the key. This makes a function $P : \{0,1\}^p \times \{0,1\}^p \to \{0,1\}^p$, and the compression function is defined as $P(h, E_m(h \oplus m))$. The good property of P is that the partial functions $x \mapsto P(x, y)$ that for all y's, and the partial functions $y \mapsto P(x, y)$ that for all x's, as well as the partial inverses $x \mapsto y$ s.t. $P(x, y) = z$ and $y \mapsto x$ s.t. $P(x, y) = z$ for all z's, are bijective. This is sufficient to prove the same security results as the original Davies-Meyer mode. Moreover, this modified mode prevents some kind of multi-block attacks, and does not allow to find trivial fixed points useful in many second preimage attacks [15]. Our modified Davies-Meyer mode is described in Figure 1.2.

1.2.2 The Message Expansion

The message expansion is a very important part of our design. It seems that all the attacks against hash functions of the MD/SHA family use the fact that in order to modify a small part of the expanded message, one can modify the original message block without too much effect on other parts of the full expanded message. Therefore, we choose to view the message expansion as an error correcting code, and we try to build a code with a high minimal distance. This is similar to the approach of [14], but our message expansion is very different from the MD/SHA one.

The message expansion is composed of three layers, which can each be considered as a code in some vector space. For SIMD-256 (resp. SIMD-512), it expands a 512-bit (resp. 1024-bit) message block into a 4096-bit (resp. 8192) expanded message, with a minimal distance of 520

(resp. 1032).

	Message block	Expanded message	Minimal distance
SIMD-256	512 bits	4096 bits	520 bits
SIMD-512	1024 bits	8192 bits	1032 bits

First Layer: Number-Theoretic Transform

The first layer of the message expansion is computationally expensive, but it a very important part of our design. The basic idea is to consider the message as a polynomial P of degree 63 (resp. 127) in $\mathbb{F}_{257}[X]$, and to evaluate this polynomial over 128 (resp. 256) points of the field $\mathbb{F}_{257}$ using a Number-Theoretic Transform[1]. This is essentially a truncated Reed-Solomon code, and it has an optimal minimal distance: two different polynomials will match on at most 63 (resp. 127) points. It reaches the Singleton bound, and therefore is a linear MDS code.

However, this code has some unwanted properties, that would allow to build very specific expanded messages:

- The Reed-Solomon code is cyclic: for any polynomial P, if $(y_i) = \mathsf{NTT}(P(X))$ and $(z_i) = \mathsf{NTT}(P(\omega X))$ with ω a n-th root of the unity, then $z_i = y_{i+1 \pmod n}$.
- The NTT of a constant polynomial k is uniform ($\forall i,\ y_i = k$). In particular, $\mathsf{NTT}(0) = 0$.

To avoid those properties, we will actually compute the NTT of the polynomial $P + X^{127}$ (resp. $P + X^{255}$). This is equivalent to adding some constants (actually the NTT of X^{127} or X^{255}) to the NTT of P. This makes the code affine, instead of just linear.

More precisely, the first message expansion step of SIMD-256 is defined as:

$$O : (\mathbb{Z}_{2^8})^{64} \to (\mathbb{F}_{257})^{128}$$
$$(x_j)_{j=0}^{63} \mapsto (y_i)_{i=0}^{127} : \quad y_i = \sum_{j=0}^{63} x_j \alpha^{ij} + \alpha^{127i} \pmod{257}.$$

where $\alpha = 139$ is a 128th root of unity in $\mathbb{F}_{257}$.

For SIMD-512, the first message expansion step is defined as:

$$O : (\mathbb{Z}_{2^8})^{128} \to (\mathbb{F}_{257})^{256}$$
$$(x_j)_{j=0}^{127} \mapsto (y_i)_{i=0}^{255} : \quad y_i = \sum_{j=0}^{127} x_j \beta^{ij} + \beta^{255i} \pmod{257}.$$

where $\beta = 41$ is a 256th root of unity in $\mathbb{F}_{257}$, and a square root of α.

This affine code has the same *differential* properties than the Reed-Solomon code: two different messages will match on at most 63 (resp. 127) y_i's. Moreover, we still have a good number of non-zero *values*. Let us consider SIMD-256, and an i such that $y_i = 0$. Then we have

$$y_i = 0 = P(\alpha^i) + \alpha^{127i}$$
$$0 = \alpha^i P(\alpha^i) + 1.$$

α^i is a root of $X.P + 1$, which is a polynomial of degree 64. Thus there are at least 64 non-zero y_i's in SIMD-256. Similarly, we can show there are at least 128 non-zero y_i's in SIMD-512

To map the x_j's from $\mathbb{Z}_{2^8}$ to $\mathbb{F}_{257}$, we take them as integers between 0 and 255.

[1]The NTT is a bijection, but we use it with half of the input set to zero, which makes it an injection.

Second Layer: Concatenated Code

In order to output a sequence of bytes (rather than elements of $\mathbb{F}_{257}$) and to increase the minimal distance of our message expansion, each symbol of $O(M)$ will be encoded through an inner code $I : \mathbb{F}_{257} \to \mathbb{Z}_{2^{16}}$. We use a class of very efficient codes, implemented with only a single multiplication modulo 2^{16}: $I_C : x \mapsto C \boxtimes x$ for some constant C. We ran an exhaustive search over the constant C, and we found four values that give a minimal Hamming distance of 4 bits: $C = 185$, $C = 233$, and their opposites. Thus, we will use the two following inner codes:

$$\begin{aligned} I_{185} &: \mathbb{F}_{257} \to \mathbb{Z}_{2^{16}} \\ &\quad x \mapsto 185 \boxtimes \widetilde{x} \qquad \text{where } -128 \leq \widetilde{x} \leq 128 \text{ and } \widetilde{x} = x \pmod{257} \\ I_{233} &: \mathbb{F}_{257} \to \mathbb{Z}_{2^{16}} \\ &\quad x \mapsto 233 \boxtimes \widetilde{x} \qquad \text{where } -128 \leq \widetilde{x} \leq 128 \text{ and } \widetilde{x} = x \pmod{257} \end{aligned}$$

x is lifted to the integers with $-128 \leq \widetilde{x} \leq 128$ because lifting to $\{-128, ...128\}$ is easier than to $\{0, ...257\}$. We will use both $I_{185}(O(M))$ and $I_{233}(O(M))$ in the expanded message (*i.e.*, we will have two copies of $O(M)$ encoded through two different inner codes).

Theses codes also have a minimal distance of 4 when we measure the weigh of the Non Adjacent Form (NAF) of the modular difference. The NAF is an optimal signed binary representation, so this means that from modular difference point of view, the code also has a distance of 4. We cannot express the 4 Hamming difference with less than 4 modular differences.

Third Layer : Permutation

The expanded message will be used as a sequence of 32-bit words, so we have to pack two 16-bit words together. The 32-bit word with $I_C(x)$ in his lower 16 bits and $I_C(y)$ in its higher 16 bits is denoted by $I_C(x, y)$. If $I_C(x)$ and $I_C(y)$ are seen as integers between 0 and $2^{16} - 1$, we have $I_C(x, y) = I_C(x) + 2^{16} I_C(y)$.

To make the message expansion stronger we permute the message words so that if an attacker wants to cancel some expanded message words, he will have to choose them quite far away. We first define an intermediate 32×4 (resp. 32×8) matrix of 32-bit words. For SIMD-256, we have (with $0 \leq j \leq 3$):

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[8i + 2j], & y[8i + 2j + 1]\big) & \text{when } 0 \leq i \leq 15 \\ I_{233}\big(y[8i + 2j - 128], & y[8i + 2j - 64]\big) & \text{when } 16 \leq i \leq 23 \\ I_{233}\big(y[8i + 2j - 191], & y[8i + 2j - 127]\big) & \text{when } 24 \leq i \leq 31 \end{cases}$$

For SIMD-512, we have (with $0 \leq j \leq 7$):

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[16i + 2j], & y[16i + 2j + 1]\big) & \text{when } 0 \leq i \leq 15 \\ I_{233}\big(y[16i + 2j - 256], & y[16i + 2j - 128]\big) & \text{when } 16 \leq i \leq 23 \\ I_{233}\big(y[16i + 2j - 383], & y[16i + 2j - 255]\big) & \text{when } 24 \leq i \leq 31 \end{cases}$$

Lastly, we permute the lines of the matrix Z. Let $W_j^{(i)} = Z_j^{(P(i))}$ with the following permutation:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	4	6	0	2	7	5	3	1	15	11	12	8	9	13	10	14
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	17	18	23	20	22	21	16	19	30	24	25	31	27	29	28	26

The full message expansion for SIMD-256 is given in Table 1.1.

i	$W_0^{(i)}$	$W_1^{(i)}$	$W_2^{(i)}$	$W_3^{(i)}$
0	$I_{185}(y_{32}, y_{33})$	$I_{185}(y_{34}, y_{35})$	$I_{185}(y_{36}, y_{37})$	$I_{185}(y_{38}, y_{39})$
1	$I_{185}(y_{48}, y_{49})$	$I_{185}(y_{50}, y_{51})$	$I_{185}(y_{52}, y_{53})$	$I_{185}(y_{54}, y_{55})$
2	$I_{185}(y_0, y_1)$	$I_{185}(y_2, y_3)$	$I_{185}(y_4, y_5)$	$I_{185}(y_6, y_7)$
3	$I_{185}(y_{16}, y_{17})$	$I_{185}(y_{18}, y_{19})$	$I_{185}(y_{20}, y_{21})$	$I_{185}(y_{22}, y_{23})$
4	$I_{185}(y_{56}, y_{57})$	$I_{185}(y_{58}, y_{59})$	$I_{185}(y_{60}, y_{61})$	$I_{185}(y_{62}, y_{63})$
5	$I_{185}(y_{40}, y_{41})$	$I_{185}(y_{42}, y_{43})$	$I_{185}(y_{44}, y_{45})$	$I_{185}(y_{46}, y_{47})$
6	$I_{185}(y_{24}, y_{25})$	$I_{185}(y_{26}, y_{27})$	$I_{185}(y_{28}, y_{29})$	$I_{185}(y_{30}, y_{31})$
7	$I_{185}(y_8, y_9)$	$I_{185}(y_{10}, y_{11})$	$I_{185}(y_{12}, y_{13})$	$I_{185}(y_{14}, y_{15})$
8	$I_{185}(y_{120}, y_{121})$	$I_{185}(y_{122}, y_{123})$	$I_{185}(y_{124}, y_{125})$	$I_{185}(y_{126}, y_{127})$
9	$I_{185}(y_{88}, y_{89})$	$I_{185}(y_{90}, y_{91})$	$I_{185}(y_{92}, y_{93})$	$I_{185}(y_{94}, y_{95})$
10	$I_{185}(y_{96}, y_{97})$	$I_{185}(y_{98}, y_{99})$	$I_{185}(y_{100}, y_{101})$	$I_{185}(y_{102}, y_{103})$
11	$I_{185}(y_{64}, y_{65})$	$I_{185}(y_{66}, y_{67})$	$I_{185}(y_{68}, y_{69})$	$I_{185}(y_{70}, y_{71})$
12	$I_{185}(y_{72}, y_{73})$	$I_{185}(y_{74}, y_{75})$	$I_{185}(y_{76}, y_{77})$	$I_{185}(y_{78}, y_{79})$
13	$I_{185}(y_{104}, y_{105})$	$I_{185}(y_{106}, y_{107})$	$I_{185}(y_{108}, y_{109})$	$I_{185}(y_{110}, y_{111})$
14	$I_{185}(y_{80}, y_{81})$	$I_{185}(y_{82}, y_{83})$	$I_{185}(y_{84}, y_{85})$	$I_{185}(y_{86}, y_{87})$
15	$I_{185}(y_{112}, y_{113})$	$I_{185}(y_{114}, y_{115})$	$I_{185}(y_{116}, y_{117})$	$I_{185}(y_{118}, y_{119})$
16	$I_{233}(y_8, y_{72})$	$I_{233}(y_{10}, y_{74})$	$I_{233}(y_{12}, y_{76})$	$I_{233}(y_{14}, y_{78})$
17	$I_{233}(y_{16}, y_{80})$	$I_{233}(y_{18}, y_{82})$	$I_{233}(y_{20}, y_{84})$	$I_{233}(y_{22}, y_{86})$
18	$I_{233}(y_{56}, y_{120})$	$I_{233}(y_{58}, y_{122})$	$I_{233}(y_{60}, y_{124})$	$I_{233}(y_{62}, y_{126})$
19	$I_{233}(y_{32}, y_{96})$	$I_{233}(y_{34}, y_{98})$	$I_{233}(y_{36}, y_{100})$	$I_{233}(y_{38}, y_{102})$
20	$I_{233}(y_{48}, y_{112})$	$I_{233}(y_{50}, y_{114})$	$I_{233}(y_{52}, y_{116})$	$I_{233}(y_{54}, y_{118})$
21	$I_{233}(y_{40}, y_{104})$	$I_{233}(y_{42}, y_{106})$	$I_{233}(y_{44}, y_{108})$	$I_{233}(y_{46}, y_{110})$
22	$I_{233}(y_0, y_{64})$	$I_{233}(y_2, y_{66})$	$I_{233}(y_4, y_{68})$	$I_{233}(y_6, y_{70})$
23	$I_{233}(y_{24}, y_{88})$	$I_{233}(y_{26}, y_{90})$	$I_{233}(y_{28}, y_{92})$	$I_{233}(y_{30}, y_{94})$
24	$I_{233}(y_{49}, y_{113})$	$I_{233}(y_{51}, y_{115})$	$I_{233}(y_{53}, y_{117})$	$I_{233}(y_{55}, y_{119})$
25	$I_{233}(y_1, y_{65})$	$I_{233}(y_3, y_{67})$	$I_{233}(y_5, y_{69})$	$I_{233}(y_7, y_{71})$
26	$I_{233}(y_9, y_{73})$	$I_{233}(y_{11}, y_{75})$	$I_{233}(y_{13}, y_{77})$	$I_{233}(y_{15}, y_{79})$
27	$I_{233}(y_{57}, y_{121})$	$I_{233}(y_{59}, y_{123})$	$I_{233}(y_{61}, y_{125})$	$I_{233}(y_{63}, y_{127})$
28	$I_{233}(y_{25}, y_{89})$	$I_{233}(y_{27}, y_{91})$	$I_{233}(y_{29}, y_{93})$	$I_{233}(y_{31}, y_{95})$
29	$I_{233}(y_{41}, y_{105})$	$I_{233}(y_{43}, y_{107})$	$I_{233}(y_{45}, y_{109})$	$I_{233}(y_{47}, y_{111})$
30	$I_{233}(y_{33}, y_{97})$	$I_{233}(y_{35}, y_{99})$	$I_{233}(y_{37}, y_{101})$	$I_{233}(y_{39}, y_{103})$
31	$I_{233}(y_{17}, y_{81})$	$I_{233}(y_{19}, y_{83})$	$I_{233}(y_{21}, y_{85})$	$I_{233}(y_{23}, y_{87})$

Table 1.1: Full Message Expansion for SIMD-256

1.2.3 The Feistel Ladder

The compression function is based on a Feistel structure, with a step function similar to the step functions of the MD/SHA family:

$$
\begin{aligned}
A_j^{(i)} &= \left(D_j^{(i-1)} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, B_j^{(i-1)}, C_j^{(i-1)})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)\lll r^{(i)}} \\
B_j^{(i)} &= A_j^{(i-1)\lll r^{(i)}} \\
C_j^{(i)} &= B_j^{(i-1)} \\
D_j^{(i)} &= C_j^{(i-1)}
\end{aligned}
$$

where $\phi^{(i)}$ is a boolean function, $\boxplus$ is the addition modulo 2^{32} and $\lll s^{(i)}$ denotes rotation to the left by an amount of $s^{(i)}$ bits. This step function is shown in Figure 1.3. Note that all the values used to compute the new $A_j^{(i+1)}$'s go through a rotation. That should prevent differential trails active only on the most-significant bit, as was found in MD5 [9].

Alternatively, we can write an equivalent description of the step update involving only the A_j registers:

$$
\begin{aligned}
B_j^{(i)} &= A_j^{(i-1)\lll r_{i-1}} \\
C_j^{(i)} &= A_j^{(i-2)\lll r_{i-2}} \\
D_j^{(i)} &= A_j^{(i-3)\lll r_{i-3}} \\
A_j^{(i)} &= \left(A_j^{(i-4)\lll r_{i-4}} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, A_j^{(i-2)\lll r_{i-2}}, A_j^{(i-3)\lll r_{i-3}})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)\lll r^{(i)}}
\end{aligned}
$$

We basically have 4 parallel Feistel ladders for SIMD-256 (resp. 8 for SIMD-512), and they interact together because of the permutations $p^{(i)}$'s. At each round, a new value is computed in each Feistel ladder, and this new value is sent to another Feistel ladder at the following round. The $p^{(i)}$'s are chosen to ensure a good diffusion. For SIMD-256, we define

$$
p^{(i)}(x) = \begin{cases} x+1 \pmod 4 & \text{if } i \text{ is even} \\ x+2 \pmod 4 & \text{if } i \text{ is odd} \end{cases}
$$

If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+2$. For SIMD-512, we define four permutations:

$$
\begin{aligned}
p^{(0)}(x) &= \begin{cases} x+1 \pmod 8 & \text{if } x = 0 \pmod 2 \\ x-1 \pmod 8 & \text{otherwise} \end{cases} \\
p^{(1)}(x) &= \begin{cases} x+2 \pmod 8 & \text{if } x = 0 \pmod 4 \text{ or } x = 1 \pmod 4 \\ x-2 \pmod 8 & \text{otherwise} \end{cases} \\
p^{(2)}(x) &= 7 - x \pmod 8 \\
p^{(3)}(x) &= x + 4 \pmod 8
\end{aligned}
$$

The permutation used at step i is $p^{(i \bmod 4)}$. If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+3$.

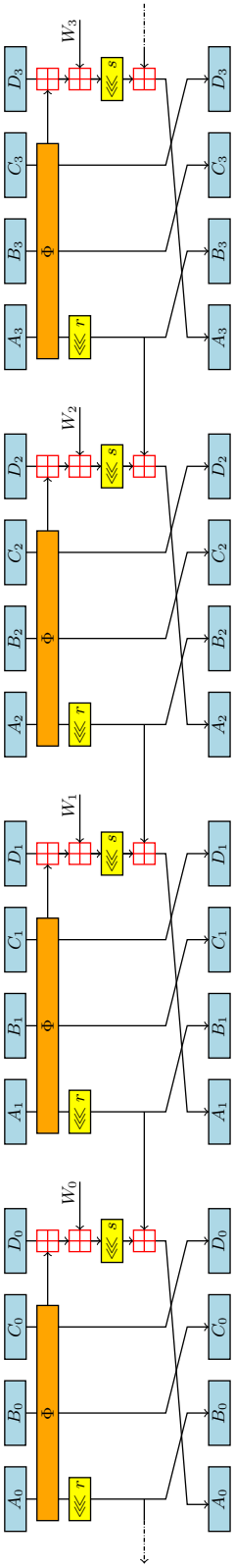

Figure 1.3: Step update of SIMD-256, with $p^{(i)}(x) = x + 1$

More precisely, the step update function of SIMD-256 is:

$$\text{(1.1)}\quad \mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{bmatrix}, \phi, r, s, p\right)$$
$$= \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0, B_0, C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1, B_1, C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2, B_2, C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3, B_3, C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \end{bmatrix}$$

and the step update function of SIMD-512 is:

$$\text{(1.2)}\quad \mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \\ W_4 \\ W_5 \\ W_6 \\ W_7 \end{bmatrix}, \phi, r, s, p\right)$$
$$= \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0, B_0, C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1, B_1, C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2, B_2, C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3, B_3, C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \\ (D_4 \boxplus W_4 \boxplus \phi(A_4, B_4, C_4))^{\lll s} \boxplus A_{p(4)}^{\lll r} & A_4^{\lll r} & B_4 & C_4 \\ (D_5 \boxplus W_5 \boxplus \phi(A_5, B_5, C_5))^{\lll s} \boxplus A_{p(5)}^{\lll r} & A_5^{\lll r} & B_5 & C_5 \\ (D_6 \boxplus W_6 \boxplus \phi(A_6, B_6, C_6))^{\lll s} \boxplus A_{p(6)}^{\lll r} & A_6^{\lll r} & B_6 & C_6 \\ (D_7 \boxplus W_7 \boxplus \phi(A_7, B_7, C_7))^{\lll s} \boxplus A_{p(7)}^{\lll r} & A_7^{\lll r} & B_7 & C_7 \end{bmatrix}$$

A block of eight steps, is called rounds, and it is parametrized by a set of rotation constants $\pi_{[0..3]}$. The boolean functions and the rotation constants are used as follows:

$\phi^{(i)}$	$r^{(i)}$	$s^{(i)}$
IF	π_0	π_1
IF	π_1	π_2
IF	π_2	π_3
IF	π_3	π_0
MAJ	π_0	π_1
MAJ	π_1	π_2
MAJ	π_2	π_3
MAJ	π_3	π_0

The whole compression function is made of 4 rounds, plus four final steps to mix the initial chaining value to the initial state (this is our feed-forward). A graphical representation of the compression function is given in Figure 1.4, and Algorithm 1 gives a pseudo-code description of the full SIMD hash function, with the chosen of constants and boolean functions.

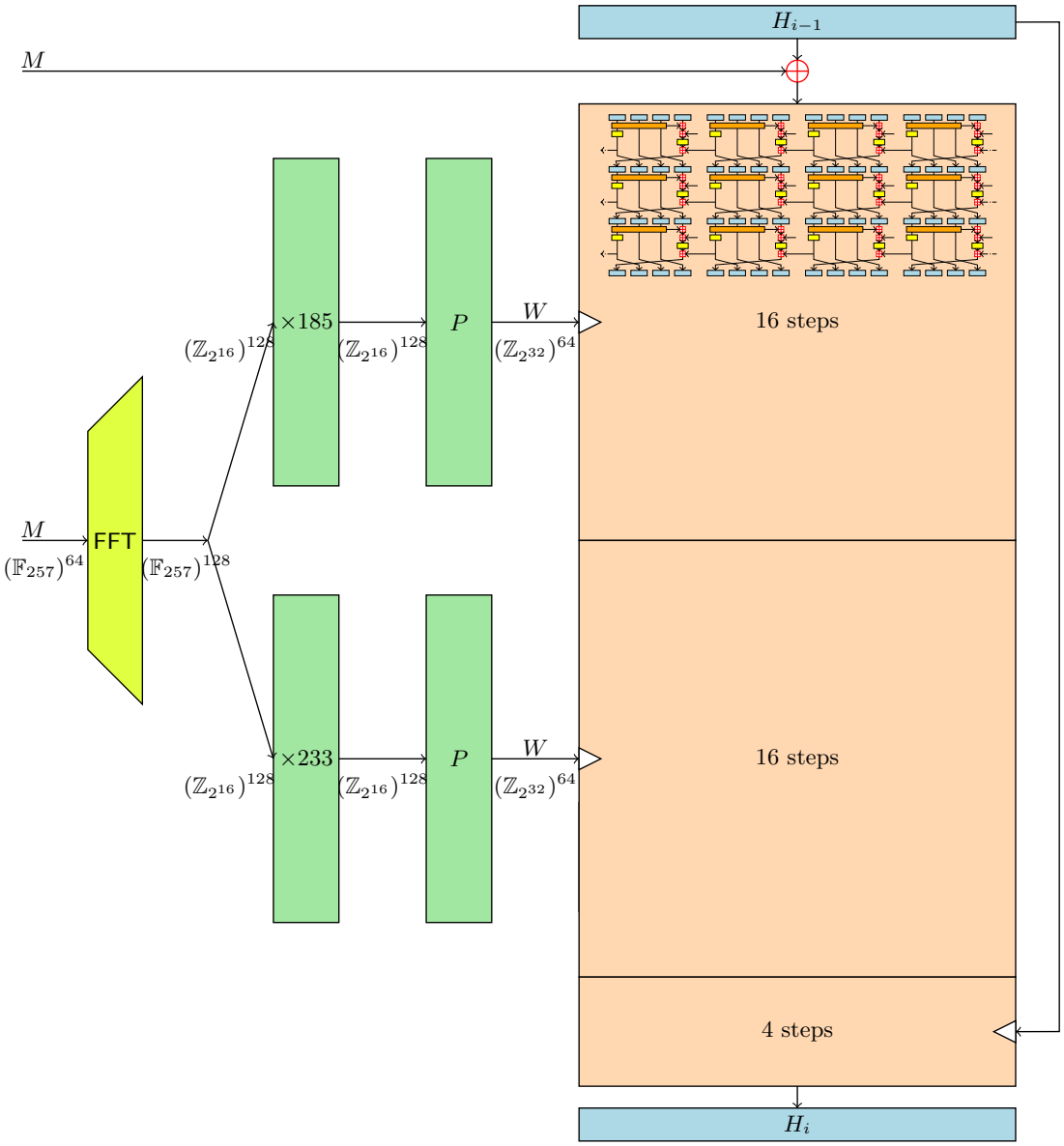

Figure 1.4: Compression function of SIMD-256

1.2.4 The Final Compression Function

After all the message blocks have been compressed, there is an extra call to the compression function, with the message length as input. The message length is counted in bits, modulo 2^m if needed. It is written as a sequence of bytes using the little endian convention, *i.e.* the low order byte of the counter will be the first message byte.

For this final compression function, we use a slightly different message expansion, with a tweaked outer code. In SIMD-256, instead of using $O(M) = \mathsf{NTT}_{128}(M+X^{127})$, we use $O'(M) = \mathsf{NTT}_{128}(M + X^{127} + X^{125})$. In SIMD-512, instead of using $O(M) = \mathsf{NTT}_{256}(M + X^{255})$, we use $O'(M) = \mathsf{NTT}_{256}(M + X^{255} + X^{253})$. The range of this modified message expansion is distinct from the range of the main message expansion. Alternatively, we can consider that the compression function takes an extra input bit, and that the message is encoded in a prefix-free way.

After that step, the output is defined as follows:

- For SIMD-256, output the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3.
- For SIMD-n with $n \leq 256$, output the n-bit prefix of the SIMD-256 output. For instance, SIMD-224's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2.
- For SIMD-512, output the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7.
- For SIMD-n with $256 < n \leq 512$, output the n-bit prefix of the SIMD-512 output. For instance, SIMD-384's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3.

1.2.5 Initialization Vector

Each SIMD-n function will use a distinct Initialization Vector, so as to avoid relations between the outputs of different members of the family. The IV of SIMD-n is defined as

$$\text{IV} - n = \mathsf{SIMD\text{-}Compress}(0, \texttt{"SIMD-}\langle i \rangle\ \texttt{v1.0"})$$

where the string is written in ASCII and padded with zeros, $\langle i \rangle$ is the decimal representation of n in ASCII without any extra zero, and there is a single space between the last digit of $\langle i \rangle$ and the `"v"`. The IV of SIMD-224, SIMD-256, SIMD-384 and SIMD-512 are given in Table 1.2.

1.2.6 Input and Output

To defines the set of function SIMD-$n : \{0,1\}^* \rightarrow \{0,1\}^n$, we still have to define how to map a bit-string to the input of SIMD, and how to map the output of SIMD to a bit-string. We will use a little-endian mapping, following the convention of MD4.

Input mapping

The input sequence of bits is interpreted in a natural manner as a sequence of bytes, where each consecutive group of eight bits is interpreted as a byte with the high-order (most significant) bit of each byte listed first.

Algorithm 1 Pseudo-code description of SIMD.

function MessageExpansion(M, f) ▷ f marks the final compression function
  if $f = 0$ **then**
    $(y_i) \leftarrow \mathsf{NTT}_{128}(M + X^{127})$ ▷ resp. X^{255} for SIMD-512
  else
    $(y_i) \leftarrow \mathsf{NTT}_{128}(M + X^{127} + X^{125})$ ▷ resp. $X^{255} + X^{253}$ for SIMD-512
  end if
  Compute the $Z_j^{(i)}$'s by applying the inner codes I_{185} and I_{233} to the y_i's.
  Compute the $W_j^{(i)}$'s by permuting the $Z_i^{(j)}$'s.
  return the $W_j^{(i)}$'s.
end function

function Round($\mathcal{S}$, i, $\pi_{[0..3]}$)
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+0)}, \mathsf{IF}, \pi_0, \pi_1)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+1)}, \mathsf{IF}, \pi_1, \pi_2)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+2)}, \mathsf{IF}, \pi_2, \pi_3)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+3)}, \mathsf{IF}, \pi_3, \pi_0)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+4)}, \mathsf{MAJ}, \pi_0, \pi_1)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+5)}, \mathsf{MAJ}, \pi_1, \pi_2)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+6)}, \mathsf{MAJ}, \pi_2, \pi_3)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+7)}, \mathsf{MAJ}, \pi_3, \pi_0)$
  return $\mathcal{S}$
end function

function SIMD-Compress(IV, M, f)
  $W \leftarrow \mathsf{MessageExpansion}(M, f)$
  $\mathcal{S} \leftarrow \mathrm{IV} \oplus M$
  $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 0, [\ 3, 20, 14, 27])$
  $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 1, [26,\ 4, 23, 11])$
  $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 2, [19, 28,\ 7, 22])$
  $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 3, [15,\ 5, 29,\ 9])$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_{[0..3]}^{(0)}, \mathsf{IF}, 15,\ 5)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_{[0..3]}^{(1)}, \mathsf{IF},\ 5, 29)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_{[0..3]}^{(2)}, \mathsf{IF}, 29,\ 9)$
  $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_{[0..3]}^{(3)}, \mathsf{IF},\ 9, 15)$
  return $\mathcal{S}$
end function

function SIMD(M)
  Split the message M into chunks $M_i, 0 \leq i < k$.
  M_{k-1} is padded with zeros.
  $\mathcal{S} \leftarrow \mathrm{IV}$
  for $0 \leq i < k$ **do**
    $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, M_i, 0)$
  end for
  $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, |M|, 1)$
  return $\mathsf{Truncate}(\mathcal{S})$
end function

SIMD-224 IV				
$A_{0..3}$	2bcc3476	64dce6a3	babf841b	cf1bb3a2
$B_{0..3}$	1389afa5	8818544b	83140916	9525c82b
$C_{0..3}$	42b233fc	f332c0dc	597129f0	7c8f6a8d
$D_{0..3}$	fe2c7137	3385203b	841742af	bcfe0e48

SIMD-256 IV				
$A_{0..3}$	96301f14	64f69407	8450cc02	42c538e3
$B_{0..3}$	75ad94b4	8b618939	5a13cb35	26141ded
$C_{0..3}$	2d83bbab	0c195501	cc0782ba	356688a2
$D_{0..3}$	5731b59d	abff7dd4	db4cd0f5	7240ec03

SIMD-384 IV				
$A_{0..3}$	0d14da0d	95c2d7d5	a95b8260	b4722c01
$A_{4..7}$	e4be208b	12cb4873	67773662	56a66d24
$B_{0..3}$	fba71944	6e1b3ca0	7d0b1a7c	b506d742
$B_{4..7}$	c417ab0b	eb34f21c	bab7945b	d1ed927e
$C_{0..3}$	e65ced88	b0667012	916393e6	4b0643ce
$C_{4..7}$	4fbed3f1	9627d2bc	eb96513b	9aa6c3e3
$D_{0..3}$	f8773176	4c45a87d	c3280609	e6996ca4
$D_{4..7}$	694e541f	0e3dcf80	042ab187	71fb0b87

SIMD-512 IV				
$A_{0..3}$	c2956828	3da33320	4149c566	c49d9244
$A_{4..7}$	04a3f1aa	0220c98b	7246bebf	e51d9d96
$B_{0..3}$	39369835	b7b6f593	956d5c2e	2e4e80c8
$B_{4..7}$	1e9fc449	84ca34e9	17d45ec5	27db1b31
$C_{0..3}$	d9ca7181	cf8e8183	e2f28feb	e9aa51c5
$C_{4..7}$	c5c2d649	37c0b473	07eef0a5	dd23d692
$D_{0..3}$	4d6185f6	bbdcbc6e	753b2bf6	7aac68ac
$D_{4..7}$	eb672a56	ed8a5dcd	b072020d	b07cf71f

Table 1.2: Initialization Vector for common versions of SIMD.

Each byte represents an integer between 0 and 255, and we use the canonical mapping from $\mathbb{Z}$ to $\mathbb{Z}_{257} = \mathbb{F}_{257}$ to construct the inputs of the NTT step of the message expansion. Note that the NTT will never receive the input value 256.

The message also needs to be interpreted as a matrix of 32-bit words to compute IV $\oplus M$. Each consecutive group of four bytes is interpreted as a word with the low-order (least significant) byte given first. The first word of IV and the first word of M are xored together to produce A_0, the second words are xored to compute A_1, and so on.

In the feed-forward, we need to see the IV as four vectors. The first vector IV_0 corresponds to the A vector of the state, IV_1 to the B vector, IV_2 to the C vector, and IV_3 to the D vector.

In the final compression function, we use a counter as the message input. The counter is taken modulo 2^m, so that it fits in one message block. The counter is converted to a sequence of bit using the same little endian convention: the first byte is the low-order byte. Note that the reference implementation only keeps a counter modulo 2^{64}, and is therefore unable to compute the hash of a message of more than 2^{64} bits, but this not a limitation of the algorithm.

Output Mapping

The output of SIMD is made of 32-bit words, which will be converted to bytes in a little-endian fashion: the first output byte is the low-order byte.

1.3 Rationale

The SIMD hash function follows the spirit of the MD/SHA family, but it should be protected against known attacks on members of this family.

1.3.1 Iteration Mode

We believe that Merkle-Damgård construction is now well understood, thanks to all previous attacks which have shown where weaknesses can be found. In particular the Merkle-Damgård iteration without no finalization function is sensible to some generic attacks:

- the extension attack;
- the second preimage attack on long messages [15];
- the multi-collision attack [13];
- various meet-in-the-middle attacks: building expandable messages from fixed point[8], preimages.

Those weakness can be tolerated, but we believe it is better to avoid them. This is why we use an internal state larger than the output size, and a modified compression function for the last block, (which is equivalent to a prefix-free encoding of the message).

1.3.2 Davies-Meyer

The Davies-Meyer mode is also well studied, and suffers the following problems:

- It is easy to find fixed-points, which can be used to build expandable messages. If we choose a message M, then $E_M^{-1}(0)$ is a fixed point as seen in Figure 1.5.

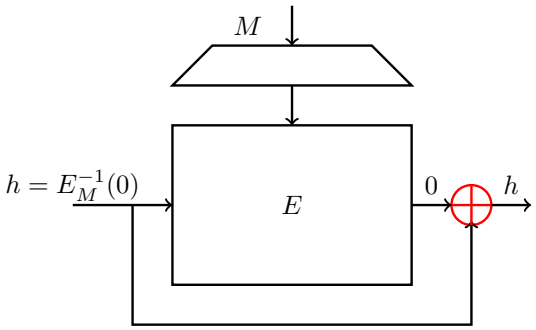

Figure 1.5: Finding fixed points in a Devies-Meyer compression function

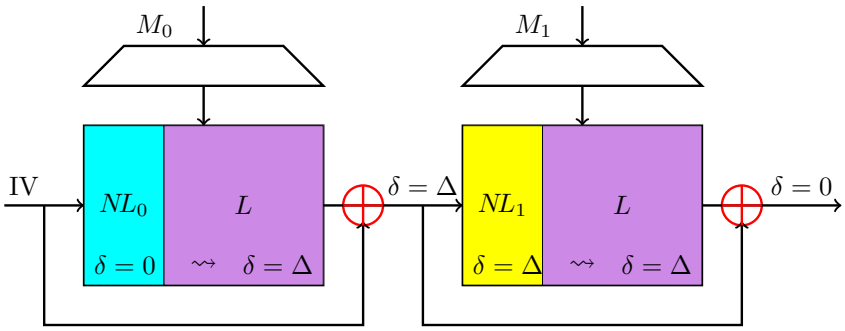

Figure 1.6: Multi-block attack using the Davies-Meyer feed-forward.

- In collision attacks, the feed-forward makes it quite easy to transform pseudo-collision into collisions. If we have a linear characteristic that gives a message difference Δ, we can use two non-linear characteristic to build a differential path $0 \rightsquigarrow \Delta$ and $\Delta \rightsquigarrow \Delta$ in the Feistel part. Figure 1.6 shows that this allows to find a collision when the input difference Δ cancels the output difference Δ in the feed-forward. This property was used to break MD5 [24] and SHA-1 [23].

Our non-linear feedback should avoid these attacks.

1.3.3 The Message Expansion

When a block cipher is used to build hash function in Davies-Meyer mode, the key of the block cipher is under control of the attacker. This setting is quite different from the regular use of a block cipher, since an attack against the hash function usually translates to a related-key attack on the block cipher. Therefore, the block cipher should be designed with a strong key expansion (the key expansion of the block cipher become the message expansion of the hash function).

Indeed, most attacks against Davies-Meyer based hash functions take advantage of the weak message expansion. For the members of the MD/SHA family, the message expansion can be seen as a linear code and the minimal distance of this code seems to play a very important role. This minimal distance is only 3 and 4 for MD4 and MD5, so the attacker has a lot of control. In SHA-1, the minimal distance is no more than 44, and is exactly 25 in the last 60 words [14]. Additionally, it is easy to shift a differential pattern one round down. This allows to build local collisions.

In our design, we follow the approach of Jutla and Patthak [14], who designed a better message expansion for SHA-1 with a minimal distance of 82, and 75 on the last 60 words. In [14], the authors used a code with a structure similar to the code of SHA-1 for efficiency reasons, and ruled out various algebraic codes. They consider Reed-Solomon codes over $\mathbb{F}_{2^8}$ which have a very good minimal distance, but they conclude they are unsuitable for a software implementation. In SIMD, we do use a Reed-Solomon code, but we use the field $\mathbb{F}_{257}$ for an efficient software implementation. This field was already used in the design of SWIFFT [17] for the same reason. Finally using concatenated codes, we can increase the minimal distance without adding much computations.

Our message expansion is designed to avoid related key attacks on the block cipher. It has a provable minimal distance of 520 for SIMD-256, and 1032 for SIMD-512. After the NTT layer of SIMD-256, any pair of distinct message are mapped to a sequence of 128 elements in $\mathbb{F}_{257}$, with at least 65 distinct components (resp. 256 elements with 129 distinct elements). The concatenated code maps the elements of $\mathbb{F}_{257}$ to 16-bit words, so that two distinct elements are mapped to words with a Hamming distance of at least 4. We have two copies of the concatenated code (with two different inner codes), so this makes a minimal hamming distance of $2 \times 4 \times 65 = 520$ for the message expansion of SIMD-256 (resp. $2 \times 4 \times 129 = 1032$ for SIMD-512).

Chapter 2

Implementation Aspect and Performances

The design of SIMD is highly parallellisable due to the choice of the components: the NTT and the parallel Feistel ladders. This should allow efficient hardware implementations. As far as software is concerned, we can use SIMD instructions (Single Instructions, Multiple Data) to compute some operations in parallel.

2.1 Software Implementation

2.1.1 SIMD Instructions

SIMD instructions allow to compute a given operation on multiple data in parallel. Processors that supports SIMD instructions usually come with a set of dedicated registers, which can contain a vector of integers or floating point data. For instance the SSE registers in x86 processors are 128-bit wide and can be used to store 16 8-bit values, 8 16-bit values, 4 32-bit values, or 2 64-bit values. The SIMD instruction set allows to compute in parallel some arithmetic operations on those vectors: addition, multiplication, bit-wise operations, ...

SIMD instructions were introduced in personal computers to improve the efficiency of multimedia computations, and are now very widely available. The x86 family offers MMX since 1997 and SSE since 1999 and the PPC family has AltiVec since 1998. For embedded systems, Intel has introduced IwMMXt to its PXA family of ARM processors, and is now promoting the Atom, an x86 processor which supports SSE. We believe that SIMD support will become even more widespread in the future. We also note that the efficiency of SIMD implementations is constantly improving: the SSE units of Intel Core micro-architecture based processors is much faster than in the older NetBurst micro-architecture. Similarly, the new AMD K10 processors feature a much better SSE units than AMD K8 ones.

Another advantage of SIMD instructions is that they usually come with a relatively large set of registers, even on CISC processors. The x86 architecture has only 8 general purpose 32-bit registers but SSE instructions comes with 8 extra 128-bit registers (on x86-64 we have 16 general purpose 64-bit registers, and 16 128-bit SSE registers). In most cases, the full state of the Feistel ladder can be kept inside those registers, which is good for performances. The NTT can also be computed mostly inside the registers.

Architecture		SHA-1	SHA-256	SHA-512	Scalar		Vector
					SIMD-256	SIMD-512	SIMD-256
Core2	32 bits	261	140	45	31	24	245
	64 bits	323	176	223	45	33	270
K10	32 bits	207	135	39	30	20	145
	64 bits	301	147	193	38	29	160
P4	32 bits	147	89	19	16	13	85
K8	32 bits	174	107	31	23	15	80
	64 bits	238	111	148	30	22	78
Atom	32 bits	66	35	12	7.2	5.7	64
G4	32 bits	102	55	16	10	7.5	78
ARM		19	11	3.0	2.1	1.6	9

Table 2.1: Performances of SIMD compared to the SHA family. The figures are in megabyte per second (MB/s).

2.1.2 Multi-core

Our design can also exploit multi-core processors: the most expensive part of the algorithm is the message expansion, and it can be done in parallel for different message blocks. When using two cores, we gain a factor 1.8 on the performance.

2.1.3 Performance

SIMD-512 and SIMD-256 offer comparable performances: one SIMD-512 compression function need roughly twice the number of operations of one SIMD-256 compression function, but it also take a message block twice as big. SIMD-512 is still somewhat slower because of the higher memory requirement, and the slightly more expensive NTT (because of the $\log n$ factor). As a general rule, the message expansion of SIMD takes half of the computing time.

The memory requirement of SIMD is essentially the internal state (64 bytes for SIMD-256 and 128 bytes for SIMD-512) and the output of the NTT ($4 \times 64 = 256$ bytes for SIMD-256 and $4 \times 128 = 256$ bytes for SIMD-512).

The performance for SHA-1, SHA-256 and SHA-512 have been obtained using the implementation from sphlib [22]. We used the same compiler for SHA and SIMD.

We stress that the *optimized* versions are not really optimized since they are written in pure C, and only use scalar instructions. The natural way to write an optimized version of SIMD is to write a vectorized implementation using SIMD instructions, which are available on many platforms.

Performances on a range of computers are given in Table 2.1 and Table 2.2. We compare two implementations of SIMD, a scalar one written in pure C and a vectorized one written in C using compiler extensions to access the SIMD instructions. Our vector implementation runs on x86 with SSE2, on PowerPC with Altivec, and on ARM with IwMMXt.

Software Platforms

Here is a brief description of the test platforms:
Core2: Intel Xeon E5440 running at 2.83 GHz; compiled with gcc 4.1.2.
K10: AMD Phenom 9850 running at 2.5 GHz; compiled with gcc 4.2.4.

Architecture		SHA-1	SHA-256	SHA-512	Scalar		Vector
					SIMD-256	SIMD-512	SIMD-256
Core2	32 bits	11	21	63	90	118	12
	64 bits	9	16	13	63	85	11
K10	32 bits	12	18	64	80	125	17
	64 bits	9	17	13	65	85	16
P4	32 bits	19	89	147	170	210	32
K8	32 bits	12	19	65	90	135	25
	64 bits	9	18	14	66	88	26
Atom	32 bits	24	46	133	220	280	25
G4	32 bits	12	23	78	125	166	16
ARM		22	38	138	200	260	46

Table 2.2: Performances of SIMD compared to the SHA family. The figures are in cycles per byte (c/B).

P4: Intel Pentium 4 running at 2.8 GHz; compiled with gcc 4.1.2.
K8: AMD Athlon64 X2 3800+ running at 2 GHz; compiled with gcc 4.2.3.
Atom: Intel Atom N270 running at 1.6 GHz; compiled with gcc 4.1.3.
G4: PowerPC 7447 running at 1.25 GHz; compiled with gcc 4.1.2.
ARM: Intel XScale PXA270 running at 416 MHz; compiled with gcc 4.1.3.

2.2 8-bit Implementation

We also tested SIMD on a 8-bit platform. We used gcc to compile the optimized code to an Atmel AVR AtMega8, and we ran it in the simularv simulator. We optimized some part of the code with inline assembly to handle the 8-bit architecture. Our code ran at 1300 cycles/byte.

2.3 Hardware Implementation

We did a preliminary study to implement SIMD on a FPGA. The Feistel part of SIMD can be implemented in the same way as the Feistel part of other hash functions of the MD/SHA family, and we would include the hardware to compute the four Feistels in parallel. Since SIMD has less steps than SHA-1 and SHA-2, this part will run faster, but requires more gates to computes the four Feistels. To compute the NTT, we propose to include the hardware to compute a size 8 NTT, which will be called 32 times to compute the size 128 NTT of SIMD-256. It should run at about the same speed as the Feistel part.

Chapter 3

Expected Strength

We conjecture that no non-random properties of an instance of SIMD-224 or SIMD-256 (indexed by the IV) can be identified with less than 2^{256} calls to the compression function.

Similarly we conjecture that no non-random properties of an instance of SIMD-384 or SIMD-512 can be identified with less than 2^{512} calls to the compression function.

In particular this means that we believe that a collision attack on SIMD-n has a complexity of $2^{n/2}$, and a preimage or second preimage attack has a complexity of 2^n. There should be neither shortcut multi-collision attack nor shortcut second preimage against long messages.

Chapter 4

Security Analysis

4.1 Mode of Operation

4.1.1 Mode of Operation for the Hash Function

Since we use a modified message expansion for the final compression function, the expanded message will be prefix free. This allow better security proofs of the iteration mode. Alternatively, we can model the compression function C and the final compression C' as two independent random oracles and see our construction as an instance of the wide-pipe design of Lucks [16].

Thus, following proofs from [5, 18, 16], our iteration mode is indifferentiable from a random oracle if the compression function is a random oracle. These proofs show that there is no generic attack against the mode of operation. Moreover, the security proved is up to 2^n queries, where n is the length of the hash function. Consequently, there are no generic attack against collision, second-preimage attack or preimage attack.

4.1.2 Security Results for Some Hash Based Constructions

The security proof for ChopMD has been provided in [5] by Chang and Nandi at FSE 2008 and the security proof for ChopMD with prefix-free message by Maurer and Tessaro at Crypto 2007 in [18] in the indifferentiablity framework. Such results show that there is no generic attack against the mode of operation. Moreover, since the security is above the birthday barrier and in 2^n if n is the hash length, then there is no better collision, second or preimage attack.

Moreover, the fact that messages are *prefix-free* allows to prove that the cascade construction of a PRF function is also a PRF [2]. This can also be used to prove the security of MAC function.

MAC Function

We propose two distinct ways to build a Message Authentication Code from the SIMD hash function.

First, as any Merkle-Damgård based hash function, SIMD can be used with the HMAC construction. The security proof of Bellare in [1] can be used to prove the security of HMAC-SIMD.

Second, we can simply compute $\mathrm{MAC}_k(M) = \mathsf{SIMD}(k\|M)$ where $\|$ denotes the concatenation. Thanks to the security proof in the indifferentiability framework, there are not generic shortcut attack on this construction. This means that one has to find a weakness in the compression in order to break this MAC.

Key Derivation

If SIMD is a PRF assuming that the compression function is a good PRF, then it is easy to prove that SIMD is a good randomness extractor that can be plugged in a key derivation function. Such results have been provided in [11]. The important point to construct a good randomness extractor already pointed out in [10] is the fact that we need to truncate the output of the function.

4.1.3 Mode of Operation for the Compression Function

The mode of operation for the compression function does not follow directly from the Davies-Meyer mode of operation. This mode presents some weaknesses we want to avoid : fix points can be easily found for example. The mode we used can be seen as a variant of the construction 8 of paper [4] (and construction 41 from [21]). Finally, the proofs provided in [4] can be extended to our construction in the ideal cipher model.

4.2 Security of the Compression Function

4.2.1 Resistance to Differential Cryptanalysis

The SIMD-family is provably secure against a class of differential attacks. This is based on the fact that the message expansion has a high minimal distance: any pair of distinct messages gives expanded messages with a least 520 bit differences for SIMD-256, resp. 1032 for SIMD-512.

If we assume that the attacker does not control the positions of the differences in the expanded message, each difference in the expanded message will introduce a difference in the state, and the attacker has to control its propagation. The attacker must at least control the effect of the carry, which will be good with a probability of 2^{-1}. As a comparison, in SHA-1, it is quite easy to control the error propagation because the perturbation vector can shifted to correct the errors, but the success probability is only $2^{-2.5}$. We expect that it will actually be more difficult to control the propagation of differences in SIMD.

Even if the adversary can use message-modification techniques to control the non-linearity in one half of the hash function for free, he still has to deal with 260 differences, resp. 516 for SIMD-512. Note that our compression function construction forces the adversary to choose the message from the beginning, so we do not expect message modification techniques to work.

4.2.2 The Step Update Function

The step update function of SIMD is defined as:

$$A_j^{(i)} = \left(A_j^{(i-4)\lll r_{i-4}} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, A_j^{(i-2)\lll r_{i-2}}, A_j^{(i-3)\lll r_{i-3}})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)\ \lll r^{(i)}}$$

It is quite similar to the step update functions of members of the MD/SHA family, and has been built with previous attacks on these functions in mind.

Our function is of form $A^{(i)} = F(A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}) \boxplus A^{(i-1)}$, like in MD5. This gives a good avalanche effect, since a difference in $A^{(i-1)}$ will most likely be propagated to $A^{(i)}$ and can not be easily absorbed. Most attacks on MD4 are based on the fact that the step update allows to easily absorb a difference in the internal state.

Den Boer and Bosselaers discovered an other kind of weakness in the step update function of MD5 [9]. If there is some differential pattern in $A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}$, that can be cancelled through F, then the addition of $A^{(i-1)}$ will reintroduce this pattern and it will propagate

in the compression function. To avoid this kind of attack, we added a rotation on $A^{(i-1)}$ in the design of SIMD.

4.3 Reduced Versions

We define two sets of reduced version of SIMD for security analysis, with a reduced number of steps, and a weaker message expansion. We encourage cryptographers to try and break them.

4.3.1 SIMD-$n/2.k$

We let SIMD-$n/2.k$ be a reduced version of SIMD-n with $2k$ steps in the main part of the Feistel instead of 2×16. The steps of SIMD-$n/2.k$ are the steps 0, 1, ... $k-1$, and 16, 17, ... $15+k$ of SIMD-n, plus the feed-forward steps. For SIMD-256/$2.k$, the reduced message expansion is defined as:

$$W_j^{(i)} = \begin{cases} I_{185}\big(y[8i+2j], & y[8i+2j+1]\big) & \text{when } 0 \le i < k \\ I_{233}\big(y[8i+2j-128], & y[8i+2j-127]\big) & \text{when } 16 \le i < 16+k \end{cases}$$

and for SIMD-512/k:

$$W_j^{(i)} = \begin{cases} I_{185}\big(y[16i+2j], & y[16i+2j+1]\big) & \text{when } 0 \le i < k \\ I_{233}\big(y[16i+2j-256], & y[16i+2j-255]\big) & \text{when } 16 \le i < 16+k \end{cases}$$

SIMD-$n/2.k$ is defined for k between 8 and 16.

4.3.2 SIMD-n/k

We let SIMD-n/k be a reduced version of SIMD-n with only k steps in the main part of the Feistel. The steps of SIMD-n/k are the steps 0, 1, ... $k-1$ of SIMD-n. For SIMD-256/k, the reduced message expansion is defined as:

$$W_j^{(i)} = I_{185}\big(y[8i+2j], y[8i+2j+1]\big)$$

and for SIMD-512/k:

$$W_j^{(i)} = I_{185}\big(y[16i+2j], y[16i+2j+1]\big)$$

SIMD-n/k is defined for k between 8 and 16.

There are no permutations is these reduced versions, and the message expansion of SIMD-256/$2.k$ and SIMD-256/k only uses $8k$ outputs of the NTT ($16k$ for SIMD-512/k). SIMD-$n/2.16$ and SIMD-$n/16$ uses the full NTT, while in SIMD-$n/8$ SIMD-$n/2.8$, the NTT does not expand the message at all, which should greatly reduce the security.

Note that SIMD-$n/2.8$ and SIMD-$n/16$ both have 16 steps, but the message expansion of SIMD-$n/2.8$ is much weaker than the message expansion of SIMD-$n/16$.

Chapter 5

Advantages and Limitations

5.1 Parallelism

SIMD features a small scale parallelism. The compression function itself can be parallelized to some extend. This can be used to improve hardware efficiency, and allows an efficient software implementation using SIMD instructions. The fact that about half the time required to compute the hash function is spent in the message expansion also allows a second level of parallelism: the message expansion of the message block $i + 1$ can be computed while the Feistel part is compressing the message block i.

We believe that this level of parallelism is sufficient for a general purpose hash function. If a specific application require an extremely fast hash function, it can use SIMD in a custom parallel mode. For instance, given a parallelization parameter k, one can split the message into k independent parts, hash the k parts with SIMD, and use an extra call to SIMD to rehash the concatenation of the k hash values.

5.2 Security

We believe that the internal block cipher in a hash function does not have the same security requirement than a block cipher used to encrypt a message. In particular, the block cipher inside a Davies-Meyer hash function should be secure under related key attacks. This is why the message expansion of SIMD is very strong. The security of the hash function is mainly based on its very high minimal distance. Of course, this also means that the message expansion is quite expensive: it accounts for about half the time spent in the hash function. However, there are some cases where we can reduce this cost and improve the efficiency of SIMD. If there is only a small of the message block that is variable, we can precompute the NTT of the fixed part, and add the variable part when it is known. This trick can be used to speed up the hashing of small messages (the counter in the final compression function has at most two active byte), or when SIMD is used in counter mode.

5.3 Performance

The performances of SIMD are very good on high-end desktop computers. SIMD-256 only needs 11 cycles per byte on one core of a Core2 processor, and we can go down to 6 cycles per byte if

we use two cores. More generally, SIMD is efficient on architectures which include a set of SIMD instructions.

On the other hand, it should also be noted than a fast implementation of the SIMD hash function has to use SIMD instructions, and can not be written in pure C. Similarly, the performances are not very good if there is no SIMD support on the target platform.

Chapter 6

Test Vectors

In this section we give test vectors and intermediate value during the computations. This should help implementors to make a correct implementation.

The hash values of the test-vectors are:

M	SIMD-224(M)
Empty message	3a6b867e2fb0c448370e2855f3794b557124c81077373311103d0c64
0x00, 0x01, 0x02, ...0x3f	498400626586837320 7d24517deaf957ac8177a2f19debe79aa9a013
700 1 bits	d1327309f6fc947e55c795823e052644e4314486c59a3be9faec146d

M	SIMD-256(M)
Empty message	1a53c82220377d3e9a783b106210995a0f3931b6d002f99c243accd15dac587d
0x00, 0x01, 0x02, ...0x3f	ece2b12117b808f0cce860e699c00973e70992a5ff18bbeb816ce86aee6001a9
700 1 bits	44e3eedcd4c0bbfca67593579559889b70b8089c3d7f8f1fb41ccc7d3f354f9f

M	SIMD-384(M)
Empty message	c5f08c18d50448edf6924ec71616a3626687db426a99c160 6f36918913a83b59411b58a6033447f005dc5153d7af0482
0x00, 0x01, 0x02, ...0x7f	7635e077d9de6005d6c82604ec9957afb58fe78fe8206456 81822c759e68aceefc08e7e0b1918db2ea9db2bd64724a15
1079 1 bits	e74ae8cb5652b03edb794e481356acfebbf712508f5f8236 e31da59eb1ed78e02949a53bb428449db81cc9cc8de60181

M	SIMD-512(M)
Empty message	426ab39fe63816339e65d100e34ddd593038852edc60e5eb166f3173b35a5124 587c1d8bcc29b0cbb0930cf6eccac44a40f21895bb1bb7dd89c67e1f77010243
0x00, 0x01, 0x02, ...0x7f	faab72f817727d7ab67cabeaa11c4dbdb42de233eff4495f8f39777fb598c831 c52260e101392f1a77ed7c7656bef378273f49afc199af8cd886458c4cf903f1
1079 1 bits	f8c0727a9918e81b83dd6909129f6ba695c1c5dc6b57710dce204ba789755ddc be9f6b8e7b0df37643731db5f7838f115b50327e8aac769bf452791d09a83a78

6.1 SIMD-224

6.1.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
y[ 24.. 31] =   96  176  161   47  189   61  248  107
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
```

```
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe2e01d2  949a6b66  d70b28f5  9af96507
Z[17] = a7b75849  29ded622  d3672c99  607a9f86
Z[18] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
Z[19] = a8a05760  5760a8a0  3de4c21c  0831f7cf
Z[20] = 00000000  70dc8f24  f0870f79  f5140aec
Z[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
Z[22] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
Z[23] = 091af6e6  6a7d9583  b9eb4615  ece3131d
Z[24] = 5beda413  9e9d6163  28f5d70b  5677a989
Z[25] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
Z[26] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
Z[27] = 49b9b647  d5392ac7  c87b3785  9e9d6163
Z[28] = 72ae8d52  992766d9  e1f71e09  9af96507
Z[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
Z[30] = f8b80748  1893e76d  607a9f86  1b4ee4b2
Z[31] = 9af96507  fa8a0576  f6e6091a  624c9db4
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = a7b75849  29ded622  d3672c99  607a9f86
W[17] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
W[18] = 091af6e6  6a7d9583  b9eb4615  ece3131d
W[19] = 00000000  70dc8f24  f0870f79  f5140aec
W[20] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
W[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
W[22] = fe2e01d2  949a6b66  d70b28f5  9af96507
W[23] = a8a05760  5760a8a0  3de4c21c  0831f7cf
W[24] = f8b80748  1893e76d  607a9f86  1b4ee4b2
```

```
W[25] = 5beda413  9e9d6163  28f5d70b  5677a989
W[26] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
W[27] = 9af96507  fa8a0576  f6e6091a  624c9db4
W[28] = 49b9b647  d5392ac7  c87b3785  9e9d6163
W[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
W[30] = 72ae8d52  992766d9  e1f71e09  9af96507
W[31] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
```

Feistel Steps

```
IV :
A[0]=2bcc3476  B[0]=1389afa5  C[0]=42b233fc  D[0]=fe2c7137
A[1]=64dce6a3  B[1]=8818544b  C[1]=f332c0dc  D[1]=3385203b
A[2]=babf841b  B[2]=83140916  C[2]=597129f0  D[2]=841742af
A[3]=cf1bb3a2  B[3]=9525c82b  C[3]=7c8f6a8d  D[3]=bcfe0e48

IV XOR M :
A[0]=2bcc3476  B[0]=1389afa5  C[0]=42b233fc  D[0]=fe2c7137
A[1]=64dce6a3  B[1]=8818544b  C[1]=f332c0dc  D[1]=3385203b
A[2]=babf841b  B[2]=83140916  C[2]=597129f0  D[2]=841742af
A[3]=cf1bb3a2  B[3]=9525c82b  C[3]=7c8f6a8d  D[3]=bcfe0e48

Step  0: (r= 3, s=20)
A[0]=b525a2a4  B[0]=5e61a3b1  C[0]=1389afa5  D[0]=42b233fc
A[1]=85dda76d  B[1]=26e7351b  C[1]=8818544b  D[1]=f332c0dc
A[2]=0783915d  B[2]=d5fc20dd  C[2]=83140916  D[2]=597129f0
A[3]=509dcf5e  B[3]=78dd9d16  C[3]=9525c82b  D[3]=7c8f6a8d

Step  1: (r=20, s=14)
A[0]=426ed002  B[0]=2a4b525a  C[0]=5e61a3b1  D[0]=1389afa5
A[1]=79cbc4f9  B[1]=76d85dda  C[1]=26e7351b  D[1]=8818544b
A[2]=2d7a36f5  B[2]=15d07839  C[2]=d5fc20dd  D[2]=83140916
A[3]=6823ed01  B[3]=f5e509dc  C[3]=78dd9d16  D[3]=9525c82b

Step  2: (r=14, s=27)
A[0]=48851f98  B[0]=b400909b  C[0]=2a4b525a  D[0]=5e61a3b1
A[1]=e8200c59  B[1]=f13e5e72  C[1]=76d85dda  D[1]=26e7351b
A[2]=9d0374d6  B[2]=8dbd4b5e  C[2]=15d07839  D[2]=d5fc20dd
A[3]=7a0c7226  B[3]=fb405a08  C[3]=f5e509dc  D[3]=78dd9d16

Step  3: (r=27, s= 3)
A[0]=f19636e0  B[0]=c24428fc  C[0]=b400909b  D[0]=2a4b525a
A[1]=f06ce3e0  B[1]=cf410062  C[1]=f13e5e72  D[1]=76d85dda
A[2]=bac12b40  B[2]=b4e81ba6  C[2]=8dbd4b5e  D[2]=15d07839
A[3]=0d08374f  B[3]=33d06391  C[3]=fb405a08  D[3]=f5e509dc

Step  4: (r= 3, s=20)
A[0]=44edc77e  B[0]=8cb1b707  C[0]=c24428fc  D[0]=b400909b
A[1]=910023b9  B[1]=83671f07  C[1]=cf410062  D[1]=f13e5e72
```

```
A[2]=1a8f59b3  B[2]=d6095a05  C[2]=b4e81ba6  D[2]=8dbd4b5e
A[3]=4ddfe89f  B[3]=6841ba78  C[3]=33d06391  D[3]=fb405a08

Step  5: (r=20, s=14)
A[0]=282299ca  B[0]=77e44edc  C[0]=8cb1b707  D[0]=c24428fc
A[1]=2ca6676c  B[1]=3b991002  C[1]=83671f07  D[1]=cf410062
A[2]=6a2363ab  B[2]=9b31a8f5  C[2]=d6095a05  D[2]=b4e81ba6
A[3]=8b4f54ae  B[3]=89f4ddfe  C[3]=6841ba78  D[3]=33d06391

Step  6: (r=14, s=27)
A[0]=ef7deb9a  B[0]=a6728a08  C[0]=77e44edc  D[0]=8cb1b707
A[1]=19d1d918  B[1]=99db0b29  C[1]=3b991002  D[1]=83671f07
A[2]=13049d7c  B[2]=d8eada88  C[2]=9b31a8f5  D[2]=d6095a05
A[3]=16c5dbd8  B[3]=d52ba2d3  C[3]=89f4ddfe  D[3]=6841ba78

Step  7: (r=27, s= 3)
A[0]=538e62ae  B[0]=d77bef5c  C[0]=a6728a08  D[0]=77e44edc
A[1]=bc16e56a  B[1]=c0ce8ec8  C[1]=99db0b29  D[1]=3b991002
A[2]=a8b4a2b1  B[2]=e09824eb  C[2]=d8eada88  D[2]=9b31a8f5
A[3]=ed80dc8f  B[3]=c0b62ede  C[3]=d52ba2d3  D[3]=89f4ddfe

Step  8: (r=26, s= 4)
A[0]=9d745db6  B[0]=b94e398a  C[0]=d77bef5c  D[0]=a6728a08
A[1]=57d20015  B[1]=aaf05b95  C[1]=c0ce8ec8  D[1]=99db0b29
A[2]=8ce4a30a  B[2]=c6a2d28a  C[2]=e09824eb  D[2]=d8eada88
A[3]=441e1484  B[3]=3fb60372  C[3]=c0b62ede  D[3]=d52ba2d3

Step  9: (r= 4, s=23)
A[0]=07a856a8  B[0]=d745db69  C[0]=b94e398a  D[0]=d77bef5c
A[1]=f55ea8b3  B[1]=7d200155  C[1]=aaf05b95  D[1]=c0ce8ec8
A[2]=230ea2b2  B[2]=ce4a30a8  C[2]=c6a2d28a  D[2]=e09824eb
A[3]=542648be  B[3]=41e14844  C[3]=3fb60372  D[3]=c0b62ede

Step 10: (r=23, s=11)
A[0]=dd4ee6e2  B[0]=5403d42b  C[0]=d745db69  D[0]=b94e398a
A[1]=8aed56c7  B[1]=59faaf54  C[1]=7d200155  D[1]=aaf05b95
A[2]=b374679f  B[2]=59118751  C[2]=ce4a30a8  D[2]=c6a2d28a
A[3]=d78f8b0c  B[3]=5f2a1324  C[3]=41e14844  D[3]=3fb60372

Step 11: (r=11, s=26)
A[0]=b09e3df0  B[0]=773716ea  C[0]=5403d42b  D[0]=d745db69
A[1]=0bc67ef2  B[1]=6ab63c57  C[1]=59faaf54  D[1]=7d200155
A[2]=5048220e  B[2]=a33cfd9b  C[2]=59118751  D[2]=ce4a30a8
A[3]=6a255c30  B[3]=7c5866bc  C[3]=5f2a1324  D[3]=41e14844

Step 12: (r=26, s= 4)
A[0]=da89bda0  B[0]=c2c278f7  C[0]=773716ea  D[0]=5403d42b
A[1]=a7f72f24  B[1]=c82f19fb  C[1]=6ab63c57  D[1]=59faaf54
A[2]=2813db1d  B[2]=39412088  C[2]=a33cfd9b  D[2]=59118751
```

```
A[3]=4c812a24  B[3]=c1a89570  C[3]=7c5866bc  D[3]=5f2a1324

Step 13: (r= 4, s=23)
A[0]=332bbddc  B[0]=a89bda0d  C[0]=c2c278f7  D[0]=773716ea
A[1]=955c5e25  B[1]=7f72f24a  C[1]=c82f19fb  D[1]=6ab63c57
A[2]=22456fbc  B[2]=813db1d2  C[2]=39412088  D[2]=a33cfd9b
A[3]=0ff1fc69  B[3]=c812a244  C[3]=c1a89570  D[3]=7c5866bc

Step 14: (r=23, s=11)
A[0]=e4d208c5  B[0]=ee1995de  C[0]=a89bda0d  D[0]=c2c278f7
A[1]=eade562b  B[1]=12caae2f  C[1]=7f72f24a  D[1]=c82f19fb
A[2]=3bca3548  B[2]=de1122b7  C[2]=813db1d2  D[2]=39412088
A[3]=6f82fe96  B[3]=3487f8fe  C[3]=c812a244  D[3]=c1a89570

Step 15: (r=11, s=26)
A[0]=f4509ae9  B[0]=90462f26  C[0]=ee1995de  D[0]=a89bda0d
A[1]=e54ee855  B[1]=f2b15f56  C[1]=12caae2f  D[1]=7f72f24a
A[2]=48ca0105  B[2]=51aa41de  C[2]=de1122b7  D[2]=813db1d2
A[3]=63c0c661  B[3]=17f4b37c  C[3]=3487f8fe  D[3]=c812a244

Step 16: (r=19, s=28)
A[0]=1158ee8f  B[0]=d74fa284  C[0]=90462f26  D[0]=ee1995de
A[1]=b1e767be  B[1]=42af2a77  C[1]=f2b15f56  D[1]=12caae2f
A[2]=45bf1e28  B[2]=082a4650  C[2]=51aa41de  D[2]=de1122b7
A[3]=5b54f250  B[3]=330b1e06  C[3]=17f4b37c  D[3]=3487f8fe

Step 17: (r=28, s= 7)
A[0]=2ad9c140  B[0]=f1158ee8  C[0]=d74fa284  D[0]=90462f26
A[1]=9927cfd1  B[1]=eb1e767b  C[1]=42af2a77  D[1]=f2b15f56
A[2]=78ed6bbc  B[2]=845bf1e2  C[2]=082a4650  D[2]=51aa41de
A[3]=60192b2c  B[3]=05b54f25  C[3]=330b1e06  D[3]=17f4b37c

Step 18: (r= 7, s=22)
A[0]=c80b86fe  B[0]=6ce0a015  C[0]=f1158ee8  D[0]=d74fa284
A[1]=4ac00d92  B[1]=93e7e8cc  C[1]=eb1e767b  D[1]=42af2a77
A[2]=81588e6b  B[2]=76b5de3c  C[2]=845bf1e2  D[2]=082a4650
A[3]=dca69ace  B[3]=0c959630  C[3]=05b54f25  D[3]=330b1e06

Step 19: (r=22, s=19)
A[0]=efa2d944  B[0]=bfb202e1  C[0]=6ce0a015  D[0]=f1158ee8
A[1]=57d9e4f7  B[1]=6492b003  C[1]=93e7e8cc  D[1]=eb1e767b
A[2]=6b41e90b  B[2]=9ae05623  C[2]=76b5de3c  D[2]=845bf1e2
A[3]=652c5dab  B[3]=b3b729a6  C[3]=0c959630  D[3]=05b54f25

Step 20: (r=19, s=28)
A[0]=b9a48be3  B[0]=ca277d16  C[0]=bfb202e1  D[0]=6ce0a015
A[1]=9f8e5c7f  B[1]=27babecf  C[1]=6492b003  D[1]=93e7e8cc
A[2]=8044536d  B[2]=485b5a0f  C[2]=9ae05623  D[2]=76b5de3c
A[3]=e0d98fe7  B[3]=ed5b2962  C[3]=b3b729a6  D[3]=0c959630
```

```
Step 21: (r=28, s= 7)
A[0]=d6d7864c  B[0]=3b9a48be  C[0]=ca277d16  D[0]=bfb202e1
A[1]=4efa1741  B[1]=f9f8e5c7  C[1]=27babecf  D[1]=6492b003
A[2]=5347e228  B[2]=d8044536  C[2]=485b5a0f  D[2]=9ae05623
A[3]=d6d54d41  B[3]=7e0d98fe  C[3]=ed5b2962  D[3]=b3b729a6

Step 22: (r= 7, s=22)
A[0]=b171be7b  B[0]=6bc3266b  C[0]=3b9a48be  D[0]=ca277d16
A[1]=700b5e1d  B[1]=7d0ba0a7  C[1]=f9f8e5c7  D[1]=27babecf
A[2]=bc592d9b  B[2]=a3f11429  C[2]=d8044536  D[2]=485b5a0f
A[3]=6f9669d1  B[3]=6aa6a0eb  C[3]=7e0d98fe  D[3]=ed5b2962

Step 23: (r=22, s=19)
A[0]=7e7c8b23  B[0]=9eec5c6f  C[0]=6bc3266b  D[0]=3b9a48be
A[1]=d413a6d4  B[1]=875c02d7  C[1]=7d0ba0a7  D[1]=f9f8e5c7
A[2]=aa1e50f8  B[2]=66ef164b  C[2]=a3f11429  D[2]=d8044536
A[3]=d8bf2375  B[3]=745be59a  C[3]=6aa6a0eb  D[3]=7e0d98fe

Step 24: (r=15, s= 5)
A[0]=5b99f833  B[0]=4591bf3e  C[0]=9eec5c6f  D[0]=6bc3266b
A[1]=1d165a86  B[1]=d36a6a09  C[1]=875c02d7  D[1]=7d0ba0a7
A[2]=1f7a0d0a  B[2]=287c550f  C[2]=66ef164b  D[2]=a3f11429
A[3]=b495a87f  B[3]=91baec5f  C[3]=745be59a  D[3]=6aa6a0eb

Step 25: (r= 5, s=29)
A[0]=80f67222  B[0]=733f066b  C[0]=4591bf3e  D[0]=9eec5c6f
A[1]=08937981  B[1]=a2cb50c3  C[1]=d36a6a09  D[1]=875c02d7
A[2]=59fb86ba  B[2]=ef41a143  C[2]=287c550f  D[2]=66ef164b
A[3]=150a77cd  B[3]=92b50ff6  C[3]=91baec5f  D[3]=745be59a

Step 26: (r=29, s= 9)
A[0]=fadb3b06  B[0]=501ece44  C[0]=733f066b  D[0]=4591bf3e
A[1]=63efa788  B[1]=21126f30  C[1]=a2cb50c3  D[1]=d36a6a09
A[2]=3327cde1  B[2]=4b3f70d7  C[2]=ef41a143  D[2]=287c550f
A[3]=4ecbca8b  B[3]=a2a14ef9  C[3]=92b50ff6  D[3]=91baec5f

Step 27: (r= 9, s=15)
A[0]=e8f4db4a  B[0]=b6760df5  C[0]=501ece44  D[0]=733f066b
A[1]=0af64e18  B[1]=df4f10c7  C[1]=21126f30  D[1]=a2cb50c3
A[2]=95ec8559  B[2]=4f9bc266  C[2]=4b3f70d7  D[2]=ef41a143
A[3]=4c575425  B[3]=9795169d  C[3]=a2a14ef9  D[3]=92b50ff6

Step 28: (r=15, s= 5)
A[0]=d4fd8450  B[0]=6da5747a  C[0]=b6760df5  D[0]=501ece44
A[1]=ae05fe46  B[1]=270c057b  C[1]=df4f10c7  D[1]=21126f30
A[2]=99a5ca0b  B[2]=42accaf6  C[2]=4f9bc266  D[2]=4b3f70d7
A[3]=6a9e7750  B[3]=aa12a62b  C[3]=9795169d  D[3]=a2a14ef9
```

```
Step 29: (r= 5, s=29)
A[0]=b1a3e781  B[0]=9fb08a1a  C[0]=6da5747a  D[0]=b6760df5
A[1]=9a398e15  B[1]=c0bfc8d5  C[1]=270c057b  D[1]=df4f10c7
A[2]=6b2918e6  B[2]=34b94173  C[2]=42accaf6  D[2]=4f9bc266
A[3]=d75f0c7f  B[3]=53ceea0d  C[3]=aa12a62b  D[3]=9795169d

Step 30: (r=29, s= 9)
A[0]=4049f58f  B[0]=36347cf0  C[0]=9fb08a1a  D[0]=6da5747a
A[1]=356d0f11  B[1]=b34731c2  C[1]=c0bfc8d5  D[1]=270c057b
A[2]=733eacb7  B[2]=cd65231c  C[2]=34b94173  D[2]=42accaf6
A[3]=108822fb  B[3]=faebe18f  C[3]=53ceea0d  D[3]=aa12a62b

Step 31: (r= 9, s=15)
A[0]=91f054c5  B[0]=93eb1e80  C[0]=36347cf0  D[0]=9fb08a1a
A[1]=7fcd7a7d  B[1]=da1e226a  C[1]=b34731c2  D[1]=c0bfc8d5
A[2]=af52d524  B[2]=7d596ee6  C[2]=cd65231c  D[2]=34b94173
A[3]=3c100344  B[3]=1045f621  C[3]=faebe18f  D[3]=53ceea0d

Feistel Step 0: (r=15, s= 5)
A[0]=295e27f6  B[0]=2a62c8f8  C[0]=93eb1e80  D[0]=36347cf0
A[1]=5fecc408  B[1]=bd3ebfe6  C[1]=da1e226a  D[1]=b34731c2
A[2]=9f679753  B[2]=6a9257a9  C[2]=7d596ee6  D[2]=cd65231c
A[3]=e532d056  B[3]=01a21e08  C[3]=1045f621  D[3]=faebe18f

Feistel Step 1: (r= 5, s=29)
A[0]=8d871323  B[0]=2bc4fec5  C[0]=2a62c8f8  D[0]=93eb1e80
A[1]=a16dd069  B[1]=fd98810b  C[1]=bd3ebfe6  D[1]=da1e226a
A[2]=2317743f  B[2]=ecf2ea73  C[2]=6a9257a9  D[2]=7d596ee6
A[3]=71c79d06  B[3]=a65a0adc  C[3]=01a21e08  D[3]=1045f621

Feistel Step 2: (r=29, s= 9)
A[0]=38886412  B[0]=71b0e264  C[0]=2bc4fec5  D[0]=2a62c8f8
A[1]=bb88999b  B[1]=342dba0d  C[1]=fd98810b  D[1]=bd3ebfe6
A[2]=8832061e  B[2]=e462ee87  C[2]=ecf2ea73  D[2]=6a9257a9
A[3]=e08657be  B[3]=ce38f3a0  C[3]=a65a0adc  D[3]=01a21e08

Feistel Step 3: (r= 9, s=15)
A[0]=7e866b3a  B[0]=10c82471  C[0]=71b0e264  D[0]=2bc4fec5
A[1]=48c4b02f  B[1]=11333777  C[1]=342dba0d  D[1]=fd98810b
A[2]=55280e37  B[2]=640c3d10  C[2]=e462ee87  D[2]=ecf2ea73
A[3]=554b79f3  B[3]=0caf7dc1  C[3]=ce38f3a0  D[3]=a65a0adc
```

Compression Function Output

```
A[0]=7e866b3a  B[0]=10c82471  C[0]=71b0e264  D[0]=2bc4fec5
A[1]=48c4b02f  B[1]=11333777  C[1]=342dba0d  D[1]=fd98810b
A[2]=55280e37  B[2]=640c3d10  C[2]=e462ee87  D[2]=ecf2ea73
A[3]=554b79f3  B[3]=0caf7dc1  C[3]=ce38f3a0  D[3]=a65a0adc
```

Hash Function Output

```
3a6b867e2fb0c448370e2855f3794b557124c81077373311103d0c64
```

6.1.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
y[ 24.. 31] =  124   92  110  120  191  202  211   82
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
```

```
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
Z[17] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
Z[18] = a2412723  e4b2ea28  71c5a8a0  9755ece3
Z[19] = 4aa270dc  949a641e  a06fc3ee  0f79d622
Z[20] = ef9ed622  fb73aa72  20c4065f  eeb5a413
Z[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
Z[22] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
Z[23] = 8d522551  05769e9d  cfc33126  f8b8237f
Z[24] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
Z[25] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
Z[26] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
Z[27] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
Z[28] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
Z[29] = ece3e025  39573ecd  edcc320f  0831d70b
Z[30] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
Z[31] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
W[17] = a2412723  e4b2ea28  71c5a8a0  9755ece3
W[18] = 8d522551  05769e9d  cfc33126  f8b8237f
W[19] = ef9ed622  fb73aa72  20c4065f  eeb5a413
W[20] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
W[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
W[22] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
W[23] = 4aa270dc  949a641e  a06fc3ee  0f79d622
```

```
W[24] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
W[25] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
W[26] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
W[27] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
W[28] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
W[29] = ece3e025  39573ecd  edcc320f  0831d70b
W[30] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
W[31] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
```

Feistel Steps

```
IV :
A[0]=2bcc3476  B[0]=1389afa5  C[0]=42b233fc  D[0]=fe2c7137
A[1]=64dce6a3  B[1]=8818544b  C[1]=f332c0dc  D[1]=3385203b
A[2]=babf841b  B[2]=83140916  C[2]=597129f0  D[2]=841742af
A[3]=cf1bb3a2  B[3]=9525c82b  C[3]=7c8f6a8d  D[3]=bcfe0e48

IV XOR M :
A[0]=28ce3576  B[0]=009bbeb5  C[0]=619012dc  D[0]=cd1e4007
A[1]=63dae3a7  B[1]=9f0e415f  C[1]=d414e5f8  D[1]=04b3150f
A[2]=b1b58d13  B[2]=980e100e  C[2]=725b00d8  D[2]=bf2d7b97
A[3]=c015beae  B[3]=8a3bd537  C[3]=53a147a1  D[3]=83c03374

Step  0: (r= 3, s=20)
A[0]=77362330  B[0]=4671abb1  C[0]=009bbeb5  D[0]=619012dc
A[1]=f5b7b96e  B[1]=1ed71d3b  C[1]=9f0e415f  D[1]=d414e5f8
A[2]=17b88abe  B[2]=8dac689d  C[2]=980e100e  D[2]=725b00d8
A[3]=40611a8c  B[3]=00adf576  C[3]=8a3bd537  D[3]=53a147a1

Step  1: (r=20, s=14)
A[0]=f268b552  B[0]=33077362  C[0]=4671abb1  D[0]=009bbeb5
A[1]=68d91472  B[1]=96ef5b7b  C[1]=1ed71d3b  D[1]=9f0e415f
A[2]=62fda6ed  B[2]=abe17b88  C[2]=8dac689d  D[2]=980e100e
A[3]=e987447e  B[3]=a8c40611  C[3]=00adf576  D[3]=8a3bd537

Step  2: (r=14, s=27)
A[0]=8f685929  B[0]=2d54bc9a  C[0]=33077362  D[0]=4671abb1
A[1]=a637dd81  B[1]=451c9a36  C[1]=96ef5b7b  D[1]=1ed71d3b
A[2]=c086c7fe  B[2]=69bb58bf  C[2]=abe17b88  D[2]=8dac689d
A[3]=58c61659  B[3]=d11fba61  C[3]=a8c40611  D[3]=00adf576

Step  3: (r=27, s= 3)
A[0]=47d45eb3  B[0]=4c7b42c9  C[0]=2d54bc9a  D[0]=33077362
A[1]=0e73639d  B[1]=0d31beec  C[1]=451c9a36  D[1]=96ef5b7b
A[2]=f7f022a7  B[2]=f604363f  C[2]=69bb58bf  D[2]=abe17b88
A[3]=45298341  B[3]=cac630b2  C[3]=d11fba61  D[3]=a8c40611

Step  4: (r= 3, s=20)
A[0]=6d8564c6  B[0]=3ea2f59a  C[0]=4c7b42c9  D[0]=2d54bc9a
```

```
A[1]=4dccbdcb  B[1]=739b1ce8  C[1]=0d31beec  D[1]=451c9a36
A[2]=7e23ee57  B[2]=bf81153f  C[2]=f604363f  D[2]=69bb58bf
A[3]=88b7e707  B[3]=294c1a0a  C[3]=cac630b2  D[3]=d11fba61

Step  5: (r=20, s=14)
A[0]=57c68269  B[0]=4c66d856  C[0]=3ea2f59a  D[0]=4c7b42c9
A[1]=84ce3ca3  B[1]=dcb4dccb  C[1]=739b1ce8  D[1]=0d31beec
A[2]=66efbc35  B[2]=e577e23e  C[2]=bf81153f  D[2]=f604363f
A[3]=4ef36b23  B[3]=70788b7e  C[3]=294c1a0a  D[3]=cac630b2

Step  6: (r=14, s=27)
A[0]=8e97d498  B[0]=a09a55f1  C[0]=4c66d856  D[0]=3ea2f59a
A[1]=98d19b15  B[1]=8f28e133  C[1]=dcb4dccb  D[1]=739b1ce8
A[2]=407a4192  B[2]=ef0d59bb  C[2]=e577e23e  D[2]=bf81153f
A[3]=940e5ec5  B[3]=dac8d3bc  C[3]=70788b7e  D[3]=294c1a0a

Step  7: (r=27, s= 3)
A[0]=1930b35f  B[0]=c474bea4  C[0]=a09a55f1  D[0]=4c66d856
A[1]=dabe93ec  B[1]=acc68cd8  C[1]=8f28e133  D[1]=dcb4dccb
A[2]=f3e49838  B[2]=9203d20c  C[2]=ef0d59bb  D[2]=e577e23e
A[3]=aaf59b2d  B[3]=2ca072f6  C[3]=dac8d3bc  D[3]=70788b7e

Step  8: (r=26, s= 4)
A[0]=9122391d  B[0]=7c64c2cd  C[0]=c474bea4  D[0]=a09a55f1
A[1]=01abb223  B[1]=b36afa4f  C[1]=acc68cd8  D[1]=8f28e133
A[2]=3ab4ae30  B[2]=e3cf9260  C[2]=9203d20c  D[2]=ef0d59bb
A[3]=95d24977  B[3]=b6abd66c  C[3]=2ca072f6  D[3]=dac8d3bc

Step  9: (r= 4, s=23)
A[0]=9b66a88e  B[0]=122391d9  C[0]=7c64c2cd  D[0]=c474bea4
A[1]=c12f041e  B[1]=1abb2230  C[1]=b36afa4f  D[1]=acc68cd8
A[2]=158b1349  B[2]=ab4ae303  C[2]=e3cf9260  D[2]=9203d20c
A[3]=8f7ba459  B[3]=5d249779  C[3]=b6abd66c  D[3]=2ca072f6

Step 10: (r=23, s=11)
A[0]=8b03f266  B[0]=474db354  C[0]=122391d9  D[0]=7c64c2cd
A[1]=28a72b2d  B[1]=0f609782  C[1]=1abb2230  D[1]=b36afa4f
A[2]=c84149b0  B[2]=a48ac589  C[2]=ab4ae303  D[2]=e3cf9260
A[3]=312b765a  B[3]=2cc7bdd2  C[3]=5d249779  D[3]=b6abd66c

Step 11: (r=11, s=26)
A[0]=509fdfbd  B[0]=1f933458  C[0]=474db354  D[0]=122391d9
A[1]=6bd381a4  B[1]=39596945  C[1]=0f609782  D[1]=1abb2230
A[2]=50963abd  B[2]=0a4d8642  C[2]=a48ac589  D[2]=ab4ae303
A[3]=31e1546f  B[3]=5bb2d189  C[3]=2cc7bdd2  D[3]=5d249779

Step 12: (r=26, s= 4)
A[0]=0144d42b  B[0]=f5427f7e  C[0]=1f933458  D[0]=474db354
A[1]=5af1f41b  B[1]=91af4e06  C[1]=39596945  D[1]=0f609782
```

```
A[2]=06cabaeb  B[2]=f54258ea  C[2]=0a4d8642  D[2]=a48ac589
A[3]=a47a1854  B[3]=bcc78551  C[3]=5bb2d189  D[3]=2cc7bdd2

Step 13: (r= 4, s=23)
A[0]=96526054  B[0]=144d42b0  C[0]=f5427f7e  D[0]=1f933458
A[1]=d44cf5d1  B[1]=af1f41b5  C[1]=91af4e06  D[1]=39596945
A[2]=011b73b9  B[2]=6cabaeb0  C[2]=f54258ea  D[2]=0a4d8642
A[3]=38975fd3  B[3]=47a1854a  C[3]=bcc78551  D[3]=5bb2d189

Step 14: (r=23, s=11)
A[0]=2b4d14dd  B[0]=2a4b2930  C[0]=144d42b0  D[0]=f5427f7e
A[1]=0149f553  B[1]=e8ea267a  C[1]=af1f41b5  D[1]=91af4e06
A[2]=7c76c44b  B[2]=dc808db9  C[2]=6cabaeb0  D[2]=f54258ea
A[3]=a2693381  B[3]=e99c4baf  C[3]=47a1854a  D[3]=bcc78551

Step 15: (r=11, s=26)
A[0]=97a4c2e7  B[0]=68a6e95a  C[0]=2a4b2930  D[0]=144d42b0
A[1]=7659bb8a  B[1]=4faa980a  C[1]=e8ea267a  D[1]=af1f41b5
A[2]=69c9bc46  B[2]=b6225be3  C[2]=dc808db9  D[2]=6cabaeb0
A[3]=038fe65b  B[3]=499c0d13  C[3]=e99c4baf  D[3]=47a1854a

Step 16: (r=19, s=28)
A[0]=015961e9  B[0]=173cbd26  C[0]=68a6e95a  D[0]=2a4b2930
A[1]=10d4e843  B[1]=dc53b2cd  C[1]=4faa980a  D[1]=e8ea267a
A[2]=809eb1d0  B[2]=e2334e4d  C[2]=b6225be3  D[2]=dc808db9
A[3]=6b4834be  B[3]=32d81c7f  C[3]=499c0d13  D[3]=e99c4baf

Step 17: (r=28, s= 7)
A[0]=2d86adb8  B[0]=9015961e  C[0]=173cbd26  D[0]=68a6e95a
A[1]=7294f8e1  B[1]=310d4e84  C[1]=dc53b2cd  D[1]=4faa980a
A[2]=cc55f420  B[2]=0809eb1d  C[2]=e2334e4d  D[2]=b6225be3
A[3]=18383755  B[3]=e6b4834b  C[3]=32d81c7f  D[3]=499c0d13

Step 18: (r= 7, s=22)
A[0]=fcbe7e21  B[0]=c356dc16  C[0]=9015961e  D[0]=173cbd26
A[1]=77be6a86  B[1]=4a7c70b9  C[1]=310d4e84  D[1]=dc53b2cd
A[2]=f1c7ace9  B[2]=2afa1066  C[2]=0809eb1d  D[2]=e2334e4d
A[3]=c2b02d24  B[3]=1c1baa8c  C[3]=e6b4834b  D[3]=32d81c7f

Step 19: (r=22, s=19)
A[0]=b5b2a986  B[0]=887f2f9f  C[0]=c356dc16  D[0]=9015961e
A[1]=57297c31  B[1]=a19def9a  C[1]=4a7c70b9  D[1]=310d4e84
A[2]=49808dab  B[2]=3a7c71eb  C[2]=2afa1066  D[2]=0809eb1d
A[3]=f8a81cad  B[3]=4930ac0b  C[3]=1c1baa8c  D[3]=e6b4834b

Step 20: (r=19, s=28)
A[0]=d7c22327  B[0]=4c35ad95  C[0]=887f2f9f  D[0]=c356dc16
A[1]=52ea23c4  B[1]=e18ab94b  C[1]=a19def9a  D[1]=4a7c70b9
A[2]=b544be02  B[2]=6d5a4c04  C[2]=3a7c71eb  D[2]=2afa1066
```

```
A[3]=410d8427  B[3]=e56fc540  C[3]=4930ac0b  D[3]=1c1baa8c

Step 21: (r=28, s= 7)
A[0]=8d229dbc  B[0]=7d7c2232  C[0]=4c35ad95  D[0]=887f2f9f
A[1]=c01b75df  B[1]=452ea23c  C[1]=e18ab94b  D[1]=a19def9a
A[2]=6c2b20b5  B[2]=2b544be0  C[2]=6d5a4c04  D[2]=3a7c71eb
A[3]=89af9d5f  B[3]=7410d842  C[3]=e56fc540  D[3]=4930ac0b

Step 22: (r= 7, s=22)
A[0]=82e8dace  B[0]=914ede46  C[0]=7d7c2232  D[0]=4c35ad95
A[1]=ab2bfa31  B[1]=0dbaefe0  C[1]=452ea23c  D[1]=e18ab94b
A[2]=7583cbc4  B[2]=15905ab6  C[2]=2b544be0  D[2]=6d5a4c04
A[3]=f42e424e  B[3]=d7ceafc4  C[3]=7410d842  D[3]=e56fc540

Step 23: (r=22, s=19)
A[0]=b6d6a319  B[0]=b3a0ba36  C[0]=914ede46  D[0]=7d7c2232
A[1]=d0892610  B[1]=8c6acafe  C[1]=0dbaefe0  D[1]=452ea23c
A[2]=9252d508  B[2]=f11d60f2  C[2]=15905ab6  D[2]=2b544be0
A[3]=b9b212c1  B[3]=93bd0b90  C[3]=d7ceafc4  D[3]=7410d842

Step 24: (r=15, s= 5)
A[0]=f0f65f34  B[0]=518cdb6b  C[0]=b3a0ba36  D[0]=914ede46
A[1]=e5bd3501  B[1]=93086844  C[1]=8c6acafe  D[1]=0dbaefe0
A[2]=a9ebd60a  B[2]=6a844929  C[2]=f11d60f2  D[2]=15905ab6
A[3]=d1b4ba42  B[3]=0960dcd9  C[3]=93bd0b90  D[3]=d7ceafc4

Step 25: (r= 5, s=29)
A[0]=9ae11f77  B[0]=1ecbe69e  C[0]=518cdb6b  D[0]=b3a0ba36
A[1]=72af3dae  B[1]=b7a6a03c  C[1]=93086844  D[1]=8c6acafe
A[2]=25876fbe  B[2]=3d7ac155  C[2]=6a844929  D[2]=f11d60f2
A[3]=92e892c2  B[3]=3697485a  C[3]=0960dcd9  D[3]=93bd0b90

Step 26: (r=29, s= 9)
A[0]=587307a4  B[0]=f35c23ee  C[0]=1ecbe69e  D[0]=518cdb6b
A[1]=c4744ffe  B[1]=ce55e7b5  C[1]=b7a6a03c  D[1]=93086844
A[2]=5f52db06  B[2]=c4b0edf7  C[2]=3d7ac155  D[2]=6a844929
A[3]=657a5add  B[3]=525d1258  C[3]=3697485a  D[3]=0960dcd9

Step 27: (r= 9, s=15)
A[0]=1c0be165  B[0]=e60f48b0  C[0]=f35c23ee  D[0]=1ecbe69e
A[1]=aacd5cba  B[1]=e89ffd88  C[1]=ce55e7b5  D[1]=b7a6a03c
A[2]=d7310abd  B[2]=a5b60cbe  C[2]=c4b0edf7  D[2]=3d7ac155
A[3]=cf62fe99  B[3]=f4b5baca  C[3]=525d1258  D[3]=3697485a

Step 28: (r=15, s= 5)
A[0]=c150dd33  B[0]=f0b28e05  C[0]=e60f48b0  D[0]=f35c23ee
A[1]=94205126  B[1]=ae5d5566  C[1]=e89ffd88  D[1]=ce55e7b5
A[2]=9060685b  B[2]=855eeb98  C[2]=a5b60cbe  D[2]=c4b0edf7
A[3]=0b7c48a3  B[3]=7f4ce7b1  C[3]=f4b5baca  D[3]=525d1258
```

```
Step 29: (r= 5, s=29)
A[0]=a417657a  B[0]=2a1ba678  C[0]=f0b28e05  D[0]=e60f48b0
A[1]=860263d6  B[1]=840a24d2  C[1]=ae5d5566  D[1]=e89ffd88
A[2]=311a178c  B[2]=0c0d0b72  C[2]=855eeb98  D[2]=a5b60cbe
A[3]=5f4b9f52  B[3]=6f891461  C[3]=7f4ce7b1  D[3]=f4b5baca

Step 30: (r=29, s= 9)
A[0]=a65229db  B[0]=5482ecaf  C[0]=2a1ba678  D[0]=f0b28e05
A[1]=7529b562  B[1]=d0c04c7a  C[1]=840a24d2  D[1]=ae5d5566
A[2]=56563350  B[2]=862342f1  C[2]=0c0d0b72  D[2]=855eeb98
A[3]=aad5797f  B[3]=4be973ea  C[3]=6f891461  D[3]=7f4ce7b1

Step 31: (r= 9, s=15)
A[0]=4dff3b87  B[0]=a453b74c  C[0]=5482ecaf  D[0]=2a1ba678
A[1]=0917d7bd  B[1]=536ac4ea  C[1]=d0c04c7a  D[1]=840a24d2
A[2]=8516c333  B[2]=ac66a0ac  C[2]=862342f1  D[2]=0c0d0b72
A[3]=d18e094f  B[3]=aaf2ff55  C[3]=4be973ea  D[3]=6f891461

Feistel Step 0: (r=15, s= 5)
A[0]=3358c7d8  B[0]=9dc3a6ff  C[0]=a453b74c  D[0]=5482ecaf
A[1]=b6d4ce82  B[1]=ebde848b  C[1]=536ac4ea  D[1]=d0c04c7a
A[2]=a329f670  B[2]=6199c28b  C[2]=ac66a0ac  D[2]=862342f1
A[3]=cecc2418  B[3]=04a7e8c7  C[3]=aaf2ff55  D[3]=4be973ea

Feistel Step 1: (r= 5, s=29)
A[0]=84e8d87a  B[0]=6b18fb06  C[0]=9dc3a6ff  D[0]=a453b74c
A[1]=c11f67ce  B[1]=da99d056  C[1]=ebde848b  D[1]=536ac4ea
A[2]=d1e9dcd8  B[2]=653ece14  C[2]=6199c28b  D[2]=ac66a0ac
A[3]=1b529741  B[3]=d9848319  C[3]=04a7e8c7  D[3]=aaf2ff55

Feistel Step 2: (r=29, s= 9)
A[0]=fbf78af9  B[0]=509d1b0f  C[0]=6b18fb06  D[0]=9dc3a6ff
A[1]=08c955fd  B[1]=d823ecf9  C[1]=da99d056  D[1]=ebde848b
A[2]=449bb1b6  B[2]=1a3d3b9b  C[2]=653ece14  D[2]=6199c28b
A[3]=a147ed99  B[3]=236a52e8  C[3]=d9848319  D[3]=04a7e8c7

Feistel Step 3: (r= 9, s=15)
A[0]=010662cf  B[0]=ef15f3f7  C[0]=509d1b0f  D[0]=6b18fb06
A[1]=44bc2ffc  B[1]=92abfa11  C[1]=d823ecf9  D[1]=da99d056
A[2]=317bf76e  B[2]=37636c89  C[2]=1a3d3b9b  D[2]=653ece14
A[3]=af7797c5  B[3]=8fdb3342  C[3]=236a52e8  D[3]=d9848319
```

Compression Function Output

```
A[0]=010662cf  B[0]=ef15f3f7  C[0]=509d1b0f  D[0]=6b18fb06
A[1]=44bc2ffc  B[1]=92abfa11  C[1]=d823ecf9  D[1]=da99d056
A[2]=317bf76e  B[2]=37636c89  C[2]=1a3d3b9b  D[2]=653ece14
A[3]=af7797c5  B[3]=8fdb3342  C[3]=236a52e8  D[3]=d9848319
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
y[ 88.. 95] =  145  170  131  192  136  139   53   98
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc5c03a4  2ac7d539  53bcac44  14efeb11
Z[17] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
```

```
Z[18] = 369cc964  9e9d6163  d9c6263a  2ac7d539
Z[19] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
Z[20] = e2e01d20  c6a93957  6c4f93b1  452cbad4
Z[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
Z[22] = c964369c  452cbad4  4aa2b55e  ac4453bc
Z[23] = 0a03f5fd  aa72558e  f0870f79  afe85018
Z[24] = 48d0b730  d70b28f5  3fb6c04a  db982468
Z[25] = e10e1ef2  6e2191df  d1952e6b  131dece3
Z[26] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
Z[27] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
Z[28] = 2ac7d539  624c9db4  641e9be2  263ad9c6
Z[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
Z[30] = c3053cfb  95836a7d  ab5b54a5  74808b80
Z[31] = 197ce684  de5321ad  607a9f86  2ac7d539
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
W[17] = 369cc964  9e9d6163  d9c6263a  2ac7d539
W[18] = 0a03f5fd  aa72558e  f0870f79  afe85018
W[19] = e2e01d20  c6a93957  6c4f93b1  452cbad4
W[20] = c964369c  452cbad4  4aa2b55e  ac4453bc
W[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
W[22] = fc5c03a4  2ac7d539  53bcac44  14efeb11
W[23] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
W[24] = c3053cfb  95836a7d  ab5b54a5  74808b80
W[25] = 48d0b730  d70b28f5  3fb6c04a  db982468
W[26] = e10e1ef2  6e2191df  d1952e6b  131dece3
W[27] = 197ce684  de5321ad  607a9f86  2ac7d539
W[28] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
W[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
W[30] = 2ac7d539  624c9db4  641e9be2  263ad9c6
W[31] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
```

Feistel Steps

```
IV :
A[0]=010662cf  B[0]=ef15f3f7  C[0]=509d1b0f  D[0]=6b18fb06
A[1]=44bc2ffc  B[1]=92abfa11  C[1]=d823ecf9  D[1]=da99d056
A[2]=317bf76e  B[2]=37636c89  C[2]=1a3d3b9b  D[2]=653ece14
A[3]=af7797c5  B[3]=8fdb3342  C[3]=236a52e8  D[3]=d9848319

IV XOR M :
A[0]=010660cf  B[0]=ef15f3f7  C[0]=509d1b0f  D[0]=6b18fb06
A[1]=44bc2ffc  B[1]=92abfa11  C[1]=d823ecf9  D[1]=da99d056
A[2]=317bf76e  B[2]=37636c89  C[2]=1a3d3b9b  D[2]=653ece14
A[3]=af7797c5  B[3]=8fdb3342  C[3]=236a52e8  D[3]=d9848319

Step  0: (r= 3, s=20)
A[0]=04bb2bda  B[0]=08330678  C[0]=ef15f3f7  D[0]=509d1b0f
A[1]=0ac20f0f  B[1]=25e17fe2  C[1]=92abfa11  D[1]=d823ecf9
A[2]=c6a1d0bb  B[2]=8bdfbb71  C[2]=37636c89  D[2]=1a3d3b9b
A[3]=0187aee1  B[3]=7bbcbe2d  C[3]=8fdb3342  D[3]=236a52e8

Step  1: (r=20, s=14)
A[0]=11f6852d  B[0]=bda04bb2  C[0]=08330678  D[0]=ef15f3f7
A[1]=db5807e0  B[1]=f0f0ac20  C[1]=25e17fe2  D[1]=92abfa11
A[2]=6cc2cfff  B[2]=0bbc6a1d  C[2]=8bdfbb71  D[2]=37636c89
A[3]=c61281d1  B[3]=ee10187a  C[3]=7bbcbe2d  D[3]=8fdb3342

Step  2: (r=14, s=27)
A[0]=606f6ea8  B[0]=a14b447d  C[0]=bda04bb2  D[0]=08330678
A[1]=9940f5d1  B[1]=01f836d6  C[1]=f0f0ac20  D[1]=25e17fe2
A[2]=f4f7cea5  B[2]=b3ffdb30  C[2]=0bbc6a1d  D[2]=8bdfbb71
A[3]=9eaf4785  B[3]=a0747184  C[3]=ee10187a  D[3]=7bbcbe2d

Step  3: (r=27, s= 3)
A[0]=7c88c12b  B[0]=43037b75  C[0]=a14b447d  D[0]=bda04bb2
A[1]=6d25cb67  B[1]=8cca07ae  C[1]=01f836d6  D[1]=f0f0ac20
A[2]=19f19b8e  B[2]=2fa7be75  C[2]=b3ffdb30  D[2]=0bbc6a1d
A[3]=7a71b952  B[3]=2cf57a3c  C[3]=a0747184  D[3]=ee10187a

Step  4: (r= 3, s=20)
A[0]=bcef0243  B[0]=e446095b  C[0]=43037b75  D[0]=a14b447d
A[1]=4ece75cf  B[1]=692e5b3b  C[1]=8cca07ae  D[1]=01f836d6
A[2]=ed3d7c34  B[2]=cf8cdc70  C[2]=2fa7be75  D[2]=b3ffdb30
A[3]=f6b55248  B[3]=d38dca93  C[3]=2cf57a3c  D[3]=a0747184

Step  5: (r=20, s=14)
A[0]=61bd75f4  B[0]=243bcef0  C[0]=e446095b  D[0]=43037b75
A[1]=b931f857  B[1]=5cf4ece7  C[1]=692e5b3b  D[1]=8cca07ae
A[2]=9fecfe5c  B[2]=c34ed3d7  C[2]=cf8cdc70  D[2]=2fa7be75
A[3]=5d0c63ad  B[3]=248f6b55  C[3]=d38dca93  D[3]=2cf57a3c
```

```
Step  6: (r=14, s=27)
A[0]=2d46ff1e  B[0]=5d7d186f  C[0]=243bcef0  D[0]=e446095b
A[1]=d93eead4  B[1]=7e15ee4c  C[1]=5cf4ece7  D[1]=692e5b3b
A[2]=eb912ee4  B[2]=3f9727fb  C[2]=c34ed3d7  D[2]=cf8cdc70
A[3]=7f5aa66b  B[3]=18eb5743  C[3]=248f6b55  D[3]=d38dca93

Step  7: (r=27, s= 3)
A[0]=7a1e1028  B[0]=f16a37f8  C[0]=5d7d186f  D[0]=243bcef0
A[1]=cb927536  B[1]=a6c9f756  C[1]=7e15ee4c  D[1]=5cf4ece7
A[2]=f1631436  B[2]=275c8977  C[2]=3f9727fb  D[2]=c34ed3d7
A[3]=b030e19e  B[3]=5bfad533  C[3]=18eb5743  D[3]=248f6b55

Step  8: (r=26, s= 4)
A[0]=b95d3efe  B[0]=a1e87840  C[0]=f16a37f8  D[0]=5d7d186f
A[1]=67b011cf  B[1]=db2e49d4  C[1]=a6c9f756  D[1]=7e15ee4c
A[2]=769f7c59  B[2]=dbc58c50  C[2]=275c8977  D[2]=3f9727fb
A[3]=9a18a945  B[3]=7ac0c386  C[3]=5bfad533  D[3]=18eb5743

Step  9: (r= 4, s=23)
A[0]=c977ca17  B[0]=95d3efeb  C[0]=a1e87840  D[0]=f16a37f8
A[1]=2a93d816  B[1]=7b011cf6  C[1]=db2e49d4  D[1]=a6c9f756
A[2]=95f2fb9a  B[2]=69f7c597  C[2]=dbc58c50  D[2]=275c8977
A[3]=de5eed1f  B[3]=a18a9459  C[3]=7ac0c386  D[3]=5bfad533

Step 10: (r=23, s=11)
A[0]=fbee2795  B[0]=0be4bbe5  C[0]=95d3efeb  D[0]=a1e87840
A[1]=ec6828fd  B[1]=0b1549ec  C[1]=7b011cf6  D[1]=db2e49d4
A[2]=2519758c  B[2]=cd4af97d  C[2]=69f7c597  D[2]=dbc58c50
A[3]=087a7cbb  B[3]=8fef2f76  C[3]=a18a9459  D[3]=7ac0c386

Step 11: (r=11, s=26)
A[0]=fb5b1ead  B[0]=713cafdf  C[0]=0be4bbe5  D[0]=95d3efeb
A[1]=bb3c8265  B[1]=4147ef63  C[1]=0b1549ec  D[1]=7b011cf6
A[2]=1eaddade  B[2]=cbac6128  C[2]=cd4af97d  D[2]=69f7c597
A[3]=9d66fd65  B[3]=d3e5d843  C[3]=8fef2f76  D[3]=a18a9459

Step 12: (r=26, s= 4)
A[0]=22e35fc8  B[0]=b7ed6c7a  C[0]=713cafdf  D[0]=0be4bbe5
A[1]=50fe9d18  B[1]=96ecf209  C[1]=4147ef63  D[1]=0b1549ec
A[2]=e3201b26  B[2]=787ab76b  C[2]=cbac6128  D[2]=cd4af97d
A[3]=c1ebd14f  B[3]=96759bf5  C[3]=d3e5d843  D[3]=8fef2f76

Step 13: (r= 4, s=23)
A[0]=1ca029ee  B[0]=2e35fc82  C[0]=b7ed6c7a  D[0]=713cafdf
A[1]=96f875be  B[1]=0fe9d185  C[1]=96ecf209  D[1]=4147ef63
A[2]=f205348c  B[2]=3201b26e  C[2]=787ab76b  D[2]=cbac6128
A[3]=0df9c56e  B[3]=1ebd14fc  C[3]=96759bf5  D[3]=d3e5d843

Step 14: (r=23, s=11)
```

```
A[0]=098ca99c  B[0]=f70e5014  C[0]=2e35fc82  D[0]=b7ed6c7a
A[1]=3315f259  B[1]=df4b7c3a  C[1]=0fe9d185  D[1]=96ecf209
A[2]=3ed0df37  B[2]=4679029a  C[2]=3201b26e  D[2]=787ab76b
A[3]=fb90059d  B[3]=b706fce2  C[3]=1ebd14fc  D[3]=96759bf5

Step 15: (r=11, s=26)
A[0]=51d3fadc  B[0]=654ce04c  C[0]=f70e5014  D[0]=2e35fc82
A[1]=b9b39840  B[1]=af92c998  C[1]=df4b7c3a  D[1]=0fe9d185
A[2]=12fb3e5f  B[2]=86f9b9f6  C[2]=4679029a  D[2]=3201b26e
A[3]=865cf351  B[3]=802cefdc  C[3]=b706fce2  D[3]=1ebd14fc

Step 16: (r=19, s=28)
A[0]=7d9f3127  B[0]=d6e28e9f  C[0]=654ce04c  D[0]=f70e5014
A[1]=f9b9dcf0  B[1]=c205cd9c  C[1]=af92c998  D[1]=df4b7c3a
A[2]=e049e36d  B[2]=f2f897d9  C[2]=86f9b9f6  D[2]=4679029a
A[3]=ea872846  B[3]=9a8c32e7  C[3]=802cefdc  D[3]=b706fce2

Step 17: (r=28, s= 7)
A[0]=14f181f7  B[0]=77d9f312  C[0]=d6e28e9f  D[0]=654ce04c
A[1]=64fe0d25  B[1]=0f9b9dcf  C[1]=c205cd9c  D[1]=af92c998
A[2]=13bc4a95  B[2]=de049e36  C[2]=f2f897d9  D[2]=86f9b9f6
A[3]=4d789a85  B[3]=6ea87284  C[3]=9a8c32e7  D[3]=802cefdc

Step 18: (r= 7, s=22)
A[0]=d7d81bcb  B[0]=78c0fb8a  C[0]=77d9f312  D[0]=d6e28e9f
A[1]=0f1d72c4  B[1]=7f0692b2  C[1]=0f9b9dcf  D[1]=c205cd9c
A[2]=ef27b400  B[2]=de254a89  C[2]=de049e36  D[2]=f2f897d9
A[3]=2f44abe6  B[3]=bc4d42a6  C[3]=6ea87284  D[3]=9a8c32e7

Step 19: (r=22, s=19)
A[0]=3b051e12  B[0]=f2f5f606  C[0]=78c0fb8a  D[0]=77d9f312
A[1]=2d8092d7  B[1]=b103c75c  C[1]=7f0692b2  D[1]=0f9b9dcf
A[2]=a0f7e16f  B[2]=003bc9ed  C[2]=de254a89  D[2]=de049e36
A[3]=b40e2c86  B[3]=f98bd12a  C[3]=bc4d42a6  D[3]=6ea87284

Step 20: (r=19, s=28)
A[0]=a279ae7f  B[0]=f091d828  C[0]=f2f5f606  D[0]=78c0fb8a
A[1]=a499b676  B[1]=96b96c04  C[1]=b103c75c  D[1]=7f0692b2
A[2]=7ec39249  B[2]=0b7d07bf  C[2]=003bc9ed  D[2]=de254a89
A[3]=5e019896  B[3]=6435a071  C[3]=f98bd12a  D[3]=bc4d42a6

Step 21: (r=28, s= 7)
A[0]=0c837a3f  B[0]=fa279ae7  C[0]=f091d828  D[0]=f2f5f606
A[1]=fbf6d748  B[1]=6a499b67  C[1]=96b96c04  D[1]=b103c75c
A[2]=ba9d664c  B[2]=97ec3924  C[2]=0b7d07bf  D[2]=003bc9ed
A[3]=59544061  B[3]=65e01989  C[3]=6435a071  D[3]=f98bd12a

Step 22: (r= 7, s=22)
A[0]=f1e599f1  B[0]=41bd1f86  C[0]=fa279ae7  D[0]=f091d828
```

```
A[1]=4528d7bb  B[1]=fb6ba47d  C[1]=6a499b67  D[1]=96b96c04
A[2]=019c2e13  B[2]=4eb3265d  C[2]=97ec3924  D[2]=0b7d07bf
A[3]=68da1b75  B[3]=aa2030ac  C[3]=65e01989  D[3]=6435a071

Step 23: (r=22, s=19)
A[0]=54bc4949  B[0]=7c7c7966  C[0]=41bd1f86  D[0]=fa279ae7
A[1]=8ee6b231  B[1]=eed14a35  C[1]=fb6ba47d  D[1]=6a499b67
A[2]=9c29a22b  B[2]=84c0670b  C[2]=4eb3265d  D[2]=97ec3924
A[3]=3de134d1  B[3]=dd5a3686  C[3]=aa2030ac  D[3]=65e01989

Step 24: (r=15, s= 5)
A[0]=a65fbc75  B[0]=24a4aa5e  C[0]=7c7c7966  D[0]=41bd1f86
A[1]=c3d75a53  B[1]=5918c773  C[1]=eed14a35  D[1]=fb6ba47d
A[2]=d59f23f1  B[2]=d115ce14  C[2]=84c0670b  D[2]=4eb3265d
A[3]=58bfe10d  B[3]=9a689ef0  C[3]=dd5a3686  D[3]=aa2030ac

Step 25: (r= 5, s=29)
A[0]=34bad63b  B[0]=cbf78eb4  C[0]=24a4aa5e  D[0]=7c7c7966
A[1]=3fed03a8  B[1]=7aeb4a78  C[1]=5918c773  D[1]=eed14a35
A[2]=f7ef744c  B[2]=b3e47e3a  C[2]=d115ce14  D[2]=84c0670b
A[3]=3f4f67ea  B[3]=17fc21ab  C[3]=9a689ef0  D[3]=dd5a3686

Step 26: (r=29, s= 9)
A[0]=8a8b3931  B[0]=66975ac7  C[0]=cbf78eb4  D[0]=24a4aa5e
A[1]=78430e38  B[1]=07fda075  C[1]=7aeb4a78  D[1]=5918c773
A[2]=dd110911  B[2]=9efdee89  C[2]=b3e47e3a  D[2]=d115ce14
A[3]=3051a1d6  B[3]=47e9ecfd  C[3]=17fc21ab  D[3]=9a689ef0

Step 27: (r= 9, s=15)
A[0]=b9c5e4c6  B[0]=16726315  C[0]=66975ac7  D[0]=cbf78eb4
A[1]=380bc98a  B[1]=861c70f0  C[1]=07fda075  D[1]=7aeb4a78
A[2]=0c555b57  B[2]=221223ba  C[2]=9efdee89  D[2]=b3e47e3a
A[3]=90afd77f  B[3]=a343ac60  C[3]=47e9ecfd  D[3]=17fc21ab

Step 28: (r=15, s= 5)
A[0]=58cd315b  B[0]=f2635ce2  C[0]=16726315  D[0]=66975ac7
A[1]=69b85852  B[1]=e4c51c05  C[1]=861c70f0  D[1]=07fda075
A[2]=c64a6fc1  B[2]=adab862a  C[2]=221223ba  D[2]=9efdee89
A[3]=95b9fbc0  B[3]=ebbfc857  C[3]=a343ac60  D[3]=47e9ecfd

Step 29: (r= 5, s=29)
A[0]=9ff8d22f  B[0]=19a62b6b  C[0]=f2635ce2  D[0]=16726315
A[1]=b90872f5  B[1]=370b0a4d  C[1]=e4c51c05  D[1]=861c70f0
A[2]=fe2eb249  B[2]=c94df838  C[2]=adab862a  D[2]=221223ba
A[3]=a9ce0fa6  B[3]=b73f7812  C[3]=ebbfc857  D[3]=a343ac60

Step 30: (r=29, s= 9)
A[0]=f0468218  B[0]=f3ff1a45  C[0]=19a62b6b  D[0]=f2635ce2
A[1]=2417a983  B[1]=b7210e5e  C[1]=370b0a4d  D[1]=e4c51c05
```

```
A[2]=961d4ada  B[2]=3fc5d649  C[2]=c94df838  D[2]=adab862a
A[3]=6f9b932f  B[3]=d539c1f4  C[3]=b73f7812  D[3]=ebbfc857

Step 31: (r= 9, s=15)
A[0]=7072250a  B[0]=8d0431e0  C[0]=f3ff1a45  D[0]=19a62b6b
A[1]=b64a80c9  B[1]=2f530648  C[1]=b7210e5e  D[1]=370b0a4d
A[2]=b514608e  B[2]=3a95b52c  C[2]=3fc5d649  D[2]=c94df838
A[3]=a5834e5c  B[3]=37265edf  C[3]=d539c1f4  D[3]=b73f7812

Feistel Step 0: (r=15, s= 5)
A[0]=079e0b18  B[0]=12853839  C[0]=8d0431e0  D[0]=f3ff1a45
A[1]=95906f7e  B[1]=4064db25  C[1]=2f530648  D[1]=b7210e5e
A[2]=5b231127  B[2]=30475a8a  C[2]=3a95b52c  D[2]=3fc5d649
A[3]=90c132b4  B[3]=a72e52c1  C[3]=37265edf  D[3]=d539c1f4

Feistel Step 1: (r= 5, s=29)
A[0]=f2154dd1  B[0]=f3c16300  C[0]=12853839  D[0]=8d0431e0
A[1]=86a86104  B[1]=b20defd2  C[1]=4064db25  D[1]=2f530648
A[2]=88b981db  B[2]=646224eb  C[2]=30475a8a  D[2]=3a95b52c
A[3]=d3955a52  B[3]=18265692  C[3]=a72e52c1  D[3]=37265edf

Feistel Step 2: (r=29, s= 9)
A[0]=d6513bc0  B[0]=3e42a9ba  C[0]=f3c16300  D[0]=12853839
A[1]=f8f3f5ce  B[1]=90d50c20  C[1]=b20defd2  D[1]=4064db25
A[2]=cd09d054  B[2]=7117303b  C[2]=646224eb  D[2]=30475a8a
A[3]=bc4b5ed7  B[3]=5a72ab4a  C[3]=18265692  D[3]=a72e52c1

Feistel Step 3: (r= 9, s=15)
A[0]=62008449  B[0]=a27781ac  C[0]=3e42a9ba  D[0]=f3c16300
A[1]=73838665  B[1]=e7eb9df1  C[1]=90d50c20  D[1]=b20defd2
A[2]=51247d20  B[2]=13a0a99a  C[2]=7117303b  D[2]=646224eb
A[3]=57f9ea7d  B[3]=96bdaf78  C[3]=5a72ab4a  D[3]=18265692
```

Compression Function Output

```
A[0]=62008449  B[0]=a27781ac  C[0]=3e42a9ba  D[0]=f3c16300
A[1]=73838665  B[1]=e7eb9df1  C[1]=90d50c20  D[1]=b20defd2
A[2]=51247d20  B[2]=13a0a99a  C[2]=7117303b  D[2]=646224eb
A[3]=57f9ea7d  B[3]=96bdaf78  C[3]=5a72ab4a  D[3]=18265692
```

Hash Function Output

```
498400626586837320 7d24517deaf957ac8177a2f19debe79aa9a013
```

6.1.3 Two-block Message

We use the message made of 700 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
y[ 88.. 95] =   32   58  213  108  189   44  222  244
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff178c69  a9895677  e4b21b4e  eb1114ef
Z[17] = 74808b80  49b9b647  f2590da7  6a7d9583
```

```
Z[18] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
Z[19] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
Z[20] = 0e90f170  ebfa1406  e10e1ef2  65079af9
Z[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
Z[22] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
Z[23] = 01d2fe2e  c3053cfb  369cc964  29ded622
Z[24] = bad4949a  bbbd51ea  6f0a0748  b90233e1
Z[25] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
Z[26] = 48d01ef2  a7b71ef2  6d38e856  263a065f
Z[27] = 34ca4443  624c4188  280c7397  f42b6d38
Z[28] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
Z[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
Z[30] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
Z[31] = 452cc6a9  db98a6ce  c305280c  558e53bc
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 74808b80  49b9b647  f2590da7  6a7d9583
W[17] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
W[18] = 01d2fe2e  c3053cfb  369cc964  29ded622
W[19] = 0e90f170  ebfa1406  e10e1ef2  65079af9
W[20] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
W[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
W[22] = ff178c69  a9895677  e4b21b4e  eb1114ef
W[23] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
W[24] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
W[25] = bad4949a  bbbd51ea  6f0a0748  b90233e1
W[26] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
W[27] = 452cc6a9  db98a6ce  c305280c  558e53bc
W[28] = 34ca4443  624c4188  280c7397  f42b6d38
W[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
W[30] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
W[31] = 48d01ef2  a7b71ef2  6d38e856  263a065f
```

Feistel Steps

```
IV :
A[0]=2bcc3476  B[0]=1389afa5  C[0]=42b233fc  D[0]=fe2c7137
A[1]=64dce6a3  B[1]=8818544b  C[1]=f332c0dc  D[1]=3385203b
A[2]=babf841b  B[2]=83140916  C[2]=597129f0  D[2]=841742af
A[3]=cf1bb3a2  B[3]=9525c82b  C[3]=7c8f6a8d  D[3]=bcfe0e48

IV XOR M :
A[0]=d433cb89  B[0]=ec76505a  C[0]=bd4dcc03  D[0]=01d38ec8
A[1]=9b23195c  B[1]=77e7abb4  C[1]=0ccd3f23  D[1]=cc7adfc4
A[2]=45407be4  B[2]=7cebf6e9  C[2]=a68ed60f  D[2]=7be8bd50
A[3]=30e44c5d  B[3]=6ada37d4  C[3]=83709572  D[3]=4301f1b7

Step  0: (r= 3, s=20)
A[0]=4d42f670  B[0]=a19e5c4e  C[0]=ec76505a  D[0]=bd4dcc03
A[1]=18154f23  B[1]=d918cae4  C[1]=77e7abb4  D[1]=0ccd3f23
A[2]=53f5aa65  B[2]=2a03df22  C[2]=7cebf6e9  D[2]=a68ed60f
A[3]=11088aa1  B[3]=872262e9  C[3]=6ada37d4  D[3]=83709572

Step  1: (r=20, s=14)
A[0]=6dafa003  B[0]=6704d42f  C[0]=a19e5c4e  D[0]=ec76505a
A[1]=5e4e2fbe  B[1]=f2318154  C[1]=d918cae4  D[1]=77e7abb4
A[2]=fe84979b  B[2]=a6553f5a  C[2]=2a03df22  D[2]=7cebf6e9
A[3]=d4ec4dc3  B[3]=aa111088  C[3]=872262e9  D[3]=6ada37d4

Step  2: (r=14, s=27)
A[0]=9fd1c61a  B[0]=e800db6b  C[0]=6704d42f  D[0]=a19e5c4e
A[1]=a247152e  B[1]=8bef9793  C[1]=f2318154  D[1]=d918cae4
A[2]=9cb6d099  B[2]=25e6ffa1  C[2]=a6553f5a  D[2]=2a03df22
A[3]=c0b946c3  B[3]=1370f53b  C[3]=aa111088  D[3]=872262e9

Step  3: (r=27, s= 3)
A[0]=de95b871  B[0]=d4fe8e30  C[0]=e800db6b  D[0]=6704d42f
A[1]=3f1ac8ac  B[1]=751238a9  C[1]=8bef9793  D[1]=f2318154
A[2]=c612c9d1  B[2]=cce5b684  C[2]=25e6ffa1  D[2]=a6553f5a
A[3]=282184fe  B[3]=1e05ca36  C[3]=1370f53b  D[3]=aa111088

Step  4: (r= 3, s=20)
A[0]=cbb7a697  B[0]=f4adc38e  C[0]=d4fe8e30  D[0]=e800db6b
A[1]=d724f632  B[1]=f8d64561  C[1]=751238a9  D[1]=8bef9793
A[2]=7904d882  B[2]=30964e8e  C[2]=cce5b684  D[2]=25e6ffa1
A[3]=2d2e2e89  B[3]=410c27f1  C[3]=1e05ca36  D[3]=1370f53b

Step  5: (r=20, s=14)
A[0]=df36031a  B[0]=697cbb7a  C[0]=f4adc38e  D[0]=d4fe8e30
A[1]=ed7cac46  B[1]=632d724f  C[1]=f8d64561  D[1]=751238a9
A[2]=e418f073  B[2]=8827904d  C[2]=30964e8e  D[2]=cce5b684
A[3]=3958b674  B[3]=e892d2e2  C[3]=410c27f1  D[3]=1e05ca36
```

```
Step  6: (r=14, s=27)
A[0]=7b553330  B[0]=80c6b7cd  C[0]=697cbb7a  D[0]=f4adc38e
A[1]=20b1aeeb  B[1]=2b11bb5f  C[1]=632d724f  D[1]=f8d64561
A[2]=ebe32c15  B[2]=3c1cf906  C[2]=8827904d  D[2]=30964e8e
A[3]=0fb56ca0  B[3]=2d9d0e56  C[3]=e892d2e2  D[3]=410c27f1

Step  7: (r=27, s= 3)
A[0]=406fed90  B[0]=83daa999  C[0]=80c6b7cd  D[0]=697cbb7a
A[1]=1f73d4a3  B[1]=59058d77  C[1]=2b11bb5f  D[1]=632d724f
A[2]=3afb34e9  B[2]=af5f1960  C[2]=3c1cf906  D[2]=8827904d
A[3]=007e9fab  B[3]=007dab65  C[3]=2d9d0e56  D[3]=e892d2e2

Step  8: (r=26, s= 4)
A[0]=9fb55be4  B[0]=4101bfb6  C[0]=83daa999  D[0]=80c6b7cd
A[1]=996b030a  B[1]=8c7dcf52  C[1]=59058d77  D[1]=2b11bb5f
A[2]=0dcb4b76  B[2]=a4ebecd3  C[2]=af5f1960  D[2]=3c1cf906
A[3]=e8e9b90b  B[3]=ac01fa7e  C[3]=007dab65  D[3]=2d9d0e56

Step  9: (r= 4, s=23)
A[0]=320ab5a5  B[0]=fb55be49  C[0]=4101bfb6  D[0]=83daa999
A[1]=13bc56d3  B[1]=96b030a9  C[1]=8c7dcf52  D[1]=59058d77
A[2]=155722d9  B[2]=dcb4b760  C[2]=a4ebecd3  D[2]=af5f1960
A[3]=53965800  B[3]=8e9b90be  C[3]=ac01fa7e  D[3]=007dab65

Step 10: (r=23, s=11)
A[0]=4523c5ad  B[0]=d299055a  C[0]=fb55be49  D[0]=4101bfb6
A[1]=6d43437f  B[1]=6989de2b  C[1]=96b030a9  D[1]=8c7dcf52
A[2]=07a24b80  B[2]=6c8aab91  C[2]=dcb4b760  D[2]=a4ebecd3
A[3]=a809d9c2  B[3]=0029cb2c  C[3]=8e9b90be  D[3]=ac01fa7e

Step 11: (r=11, s=26)
A[0]=266db036  B[0]=1e2d6a29  C[0]=d299055a  D[0]=fb55be49
A[1]=a8160935  B[1]=1a1bfb6a  C[1]=6989de2b  D[1]=96b030a9
A[2]=35942085  B[2]=125c003d  C[2]=6c8aab91  D[2]=dcb4b760
A[3]=8804fe36  B[3]=4ece1540  C[3]=0029cb2c  D[3]=8e9b90be

Step 12: (r=26, s= 4)
A[0]=0b040859  B[0]=d899b6c0  C[0]=1e2d6a29  D[0]=d299055a
A[1]=bf7ab65b  B[1]=d6a05824  C[1]=1a1bfb6a  D[1]=6989de2b
A[2]=20ece5de  B[2]=14d65082  C[2]=125c003d  D[2]=6c8aab91
A[3]=dcb5fdb8  B[3]=da2013f8  C[3]=4ece1540  D[3]=0029cb2c

Step 13: (r= 4, s=23)
A[0]=c4a8de7c  B[0]=b0408590  C[0]=d899b6c0  D[0]=1e2d6a29
A[1]=1ccc9e75  B[1]=f7ab65bb  C[1]=d6a05824  D[1]=1a1bfb6a
A[2]=a3785bff  B[2]=0ece5de2  C[2]=14d65082  D[2]=125c003d
A[3]=2976ab11  B[3]=cb5fdb8d  C[3]=da2013f8  D[3]=4ece1540

Step 14: (r=23, s=11)
```

```
A[0]=6c082f93  B[0]=3e62546f  C[0]=b0408590  D[0]=d899b6c0
A[1]=6091f982  B[1]=3a8e664f  C[1]=f7ab65bb  D[1]=d6a05824
A[2]=1e213ed4  B[2]=ffd1bc2d  C[2]=0ece5de2  D[2]=14d65082
A[3]=3a546e33  B[3]=8894bb55  C[3]=cb5fdb8d  D[3]=da2013f8

Step 15: (r=11, s=26)
A[0]=e962c7ed  B[0]=417c9b60  C[0]=3e62546f  D[0]=b0408590
A[1]=ed60a22c  B[1]=8fcc1304  C[1]=3a8e664f  D[1]=f7ab65bb
A[2]=bb40aef0  B[2]=09f6a0f1  C[2]=ffd1bc2d  D[2]=0ece5de2
A[3]=b465504a  B[3]=a37199d2  C[3]=8894bb55  D[3]=cb5fdb8d

Step 16: (r=19, s=28)
A[0]=3929854c  B[0]=3f6f4b16  C[0]=417c9b60  D[0]=3e62546f
A[1]=15991029  B[1]=11676b05  C[1]=8fcc1304  D[1]=3a8e664f
A[2]=e74534f2  B[2]=7785da05  C[2]=09f6a0f1  D[2]=ffd1bc2d
A[3]=bd5c3ddc  B[3]=8255a32a  C[3]=a37199d2  D[3]=8894bb55

Step 17: (r=28, s= 7)
A[0]=3e8efd48  B[0]=c3929854  C[0]=3f6f4b16  D[0]=417c9b60
A[1]=a9b27a1f  B[1]=91599102  C[1]=11676b05  D[1]=8fcc1304
A[2]=99019f42  B[2]=2e74534f  C[2]=7785da05  D[2]=09f6a0f1
A[3]=3ba79be7  B[3]=cbd5c3dd  C[3]=8255a32a  D[3]=a37199d2

Step 18: (r= 7, s=22)
A[0]=d24edca0  B[0]=477ea41f  C[0]=c3929854  D[0]=3f6f4b16
A[1]=c148aae4  B[1]=d93d0fd4  C[1]=91599102  D[1]=11676b05
A[2]=3af9b98c  B[2]=80cfa14c  C[2]=2e74534f  D[2]=7785da05
A[3]=37d4eda3  B[3]=d3cdf39d  C[3]=cbd5c3dd  D[3]=8255a32a

Step 19: (r=22, s=19)
A[0]=69e34d64  B[0]=283493b7  C[0]=477ea41f  D[0]=c3929854
A[1]=3f5c690f  B[1]=b930522a  C[1]=d93d0fd4  D[1]=91599102
A[2]=0a677ec5  B[2]=630ebe6e  C[2]=80cfa14c  D[2]=2e74534f
A[3]=c9366b43  B[3]=68cdf53b  C[3]=d3cdf39d  D[3]=cbd5c3dd

Step 20: (r=19, s=28)
A[0]=bb84dc81  B[0]=6b234f1a  C[0]=283493b7  D[0]=477ea41f
A[1]=d1d0e9fc  B[1]=4879fae3  C[1]=b930522a  D[1]=d93d0fd4
A[2]=93fe13f9  B[2]=f628533b  C[2]=630ebe6e  D[2]=80cfa14c
A[3]=39b9554d  B[3]=5a1e49b3  C[3]=68cdf53b  D[3]=d3cdf39d

Step 21: (r=28, s= 7)
A[0]=8f7e167b  B[0]=1bb84dc8  C[0]=6b234f1a  D[0]=283493b7
A[1]=2925f628  B[1]=cd1d0e9f  C[1]=4879fae3  D[1]=b930522a
A[2]=5e1a6dfa  B[2]=993fe13f  C[2]=f628533b  D[2]=630ebe6e
A[3]=ca62b323  B[3]=d39b9554  C[3]=5a1e49b3  D[3]=68cdf53b

Step 22: (r= 7, s=22)
A[0]=7187b5af  B[0]=bf0b3dc7  C[0]=1bb84dc8  D[0]=6b234f1a
```

```
A[1]=e061fb18  B[1]=92fb1414  C[1]=cd1d0e9f  D[1]=4879fae3
A[2]=ef2310b3  B[2]=0d36fd2f  C[2]=993fe13f  D[2]=f628533b
A[3]=9656bc2d  B[3]=315991e5  C[3]=d39b9554  D[3]=5a1e49b3

Step 23: (r=22, s=19)
A[0]=ab49e73f  B[0]=6bdc61ed  C[0]=bf0b3dc7  D[0]=1bb84dc8
A[1]=13c49ce9  B[1]=c638187e  C[1]=92fb1414  D[1]=cd1d0e9f
A[2]=7ece8dd1  B[2]=2cfbc8c4  C[2]=0d36fd2f  D[2]=993fe13f
A[3]=bdd68575  B[3]=0b6595af  C[3]=315991e5  D[3]=d39b9554

Step 24: (r=15, s= 5)
A[0]=94d330c4  B[0]=f39fd5a4  C[0]=6bdc61ed  D[0]=bf0b3dc7
A[1]=28cb2218  B[1]=4e7489e2  C[1]=c638187e  D[1]=92fb1414
A[2]=d5bf216d  B[2]=46e8bf67  C[2]=2cfbc8c4  D[2]=0d36fd2f
A[3]=c80fac55  B[3]=42badeeb  C[3]=0b6595af  D[3]=315991e5

Step 25: (r= 5, s=29)
A[0]=8694123b  B[0]=9a661892  C[0]=f39fd5a4  D[0]=6bdc61ed
A[1]=859a9a85  B[1]=19644305  C[1]=4e7489e2  D[1]=c638187e
A[2]=378b565d  B[2]=b7e42dba  C[2]=46e8bf67  D[2]=2cfbc8c4
A[3]=3f1d0f7b  B[3]=01f58ab9  C[3]=42badeeb  D[3]=0b6595af

Step 26: (r=29, s= 9)
A[0]=306338b3  B[0]=70d28247  C[0]=9a661892  D[0]=f39fd5a4
A[1]=dc4b2293  B[1]=b0b35350  C[1]=19644305  D[1]=4e7489e2
A[2]=776c2a0a  B[2]=a6f16acb  C[2]=b7e42dba  D[2]=46e8bf67
A[3]=3e13cca8  B[3]=67e3a1ef  C[3]=01f58ab9  D[3]=42badeeb

Step 27: (r= 9, s=15)
A[0]=267c8e77  B[0]=c6716660  C[0]=70d28247  D[0]=9a661892
A[1]=617bae16  B[1]=964527b8  C[1]=b0b35350  D[1]=19644305
A[2]=d2083ec7  B[2]=d85414ee  C[2]=a6f16acb  D[2]=b7e42dba
A[3]=f0f587d0  B[3]=2799507c  C[3]=67e3a1ef  D[3]=01f58ab9

Step 28: (r=15, s= 5)
A[0]=8b279843  B[0]=473b933e  C[0]=c6716660  D[0]=70d28247
A[1]=a3d95ca9  B[1]=d70b30bd  C[1]=964527b8  D[1]=b0b35350
A[2]=0c047c90  B[2]=1f63e904  C[2]=d85414ee  D[2]=a6f16acb
A[3]=098ad0e9  B[3]=c3e8787a  C[3]=2799507c  D[3]=67e3a1ef

Step 29: (r= 5, s=29)
A[0]=3ecdb6dc  B[0]=64f30871  C[0]=473b933e  D[0]=c6716660
A[1]=9311c9cf  B[1]=7b2b9534  C[1]=d70b30bd  D[1]=964527b8
A[2]=9b306dc6  B[2]=808f9201  C[2]=1f63e904  D[2]=d85414ee
A[3]=9d38b100  B[3]=315a1d21  C[3]=c3e8787a  D[3]=2799507c

Step 30: (r=29, s= 9)
A[0]=6b92fd83  B[0]=87d9b6db  C[0]=64f30871  D[0]=473b933e
A[1]=05586499  B[1]=f2623939  C[1]=7b2b9534  D[1]=d70b30bd
```

```
A[2]=4d2e7a25  B[2]=d3660db8  C[2]=808f9201  D[2]=1f63e904
A[3]=1e41d3f7  B[3]=13a71620  C[3]=315a1d21  D[3]=c3e8787a

Step 31: (r= 9, s=15)
A[0]=14764689  B[0]=25fb06d7  C[0]=87d9b6db  D[0]=64f30871
A[1]=c61c6752  B[1]=b0c9320a  C[1]=f2623939  D[1]=7b2b9534
A[2]=9bb8adbc  B[2]=5cf44a9a  C[2]=d3660db8  D[2]=808f9201
A[3]=7bc6b0bc  B[3]=83a7ee3c  C[3]=13a71620  D[3]=315a1d21

Feistel Step 0: (r=15, s= 5)
A[0]=4b07da51  B[0]=23448a3b  C[0]=25fb06d7  D[0]=87d9b6db
A[1]=65350e2e  B[1]=33a9630e  C[1]=b0c9320a  D[1]=f2623939
A[2]=e1021475  B[2]=56de4ddc  C[2]=5cf44a9a  D[2]=d3660db8
A[3]=a6f36a1b  B[3]=585e3de3  C[3]=83a7ee3c  D[3]=13a71620

Feistel Step 1: (r= 5, s=29)
A[0]=18ae8d5e  B[0]=60fb4a29  C[0]=23448a3b  D[0]=25fb06d7
A[1]=23f9bb66  B[1]=a6a1c5cc  C[1]=33a9630e  D[1]=b0c9320a
A[2]=f76956de  B[2]=20428ebc  C[2]=56de4ddc  D[2]=5cf44a9a
A[3]=fbe6371a  B[3]=de6d4374  C[3]=585e3de3  D[3]=83a7ee3c

Feistel Step 2: (r=29, s= 9)
A[0]=f3093085  B[0]=c315d1ab  C[0]=60fb4a29  D[0]=23448a3b
A[1]=1a559088  B[1]=c47f376c  C[1]=a6a1c5cc  D[1]=33a9630e
A[2]=d6851491  B[2]=deed2adb  C[2]=20428ebc  D[2]=56de4ddc
A[3]=29df4760  B[3]=5f7cc6e3  C[3]=de6d4374  D[3]=585e3de3

Feistel Step 3: (r= 9, s=15)
A[0]=3537165f  B[0]=12610be6  C[0]=c315d1ab  D[0]=60fb4a29
A[1]=aad94664  B[1]=ab211034  C[1]=c47f376c  D[1]=a6a1c5cc
A[2]=a00574c4  B[2]=0a2923ad  C[2]=deed2adb  D[2]=20428ebc
A[3]=f4710aa0  B[3]=be8ec053  C[3]=5f7cc6e3  D[3]=de6d4374
```

Compression Function Output

```
A[0]=3537165f  B[0]=12610be6  C[0]=c315d1ab  D[0]=60fb4a29
A[1]=aad94664  B[1]=ab211034  C[1]=c47f376c  D[1]=a6a1c5cc
A[2]=a00574c4  B[2]=0a2923ad  C[2]=deed2adb  D[2]=20428ebc
A[3]=f4710aa0  B[3]=be8ec053  C[3]=5f7cc6e3  D[3]=de6d4374
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0cbec792  4443e76d  0e902f54  9755eeb5
Z[17] = a9890aec  ff17d9c6  f087c4d7  4e465849
Z[18] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
Z[19] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
Z[20] = 1e09e1f7  6507624c  114b280c  58496163
Z[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
Z[22] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
Z[23] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
Z[24] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
Z[25] = 59325760  d450900d  3c129db4  12344e46
Z[26] = 280c409f  048d1a65  280c624c  72ae0cbe
Z[27] = 9f86386e  f8b8b55e  280c1234  47e70e90
Z[28] = f1701e09  9af9e59b  5bed6335  daaf263a
```

```
Z[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
Z[30] = ece372ae  091a386e  f6e62e6b  d450d70b
Z[31] = 29de966c  320f0cbe  5677d450  c87b29de
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = a9890aec  ff17d9c6  f087c4d7  4e465849
W[17] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
W[18] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
W[19] = 1e09e1f7  6507624c  114b280c  58496163
W[20] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
W[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
W[22] = 0cbec792  4443e76d  0e902f54  9755eeb5
W[23] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
W[24] = ece372ae  091a386e  f6e62e6b  d450d70b
W[25] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
W[26] = 59325760  d450900d  3c129db4  12344e46
W[27] = 29de966c  320f0cbe  5677d450  c87b29de
W[28] = 9f86386e  f8b8b55e  280c1234  47e70e90
W[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
W[30] = f1701e09  9af9e59b  5bed6335  daaf263a
W[31] = 280c409f  048d1a65  280c624c  72ae0cbe
```

Feistel Steps

```
IV :
A[0]=3537165f  B[0]=12610be6  C[0]=c315d1ab  D[0]=60fb4a29
A[1]=aad94664  B[1]=ab211034  C[1]=c47f376c  D[1]=a6a1c5cc
A[2]=a00574c4  B[2]=0a2923ad  C[2]=deed2adb  D[2]=20428ebc
A[3]=f4710aa0  B[3]=be8ec053  C[3]=5f7cc6e3  D[3]=de6d4374

IV XOR M :
A[0]=cac8e9a0  B[0]=ed9ef419  C[0]=c315d1ab  D[0]=60fb4a29
A[1]=5526b99b  B[1]=5bdeefcb  C[1]=c47f376c  D[1]=a6a1c5cc
```

```
A[2]=5ffa8b3b  B[2]=0a2923ad  C[2]=deed2adb  D[2]=20428ebc
A[3]=0b8ef55f  B[3]=be8ec053  C[3]=5f7cc6e3  D[3]=de6d4374

Step  0: (r= 3, s=20)
A[0]=cee9f40c  B[0]=56474d06  C[0]=ed9ef419  D[0]=c315d1ab
A[1]=3c4a8aa6  B[1]=a935ccda  C[1]=5bdeefcb  D[1]=c47f376c
A[2]=83973e45  B[2]=ffd459da  C[2]=0a2923ad  D[2]=deed2adb
A[3]=91ed096b  B[3]=5c77aaf8  C[3]=be8ec053  D[3]=5f7cc6e3

Step  1: (r=20, s=14)
A[0]=b3e65ad1  B[0]=40ccee9f  C[0]=56474d06  D[0]=ed9ef419
A[1]=4c55b608  B[1]=aa63c4a8  C[1]=a935ccda  D[1]=5bdeefcb
A[2]=7ed75280  B[2]=e4583973  C[2]=ffd459da  D[2]=0a2923ad
A[3]=bb70a400  B[3]=96b91ed0  C[3]=5c77aaf8  D[3]=be8ec053

Step  2: (r=14, s=27)
A[0]=848dbbcc  B[0]=96b46cf9  C[0]=40ccee9f  D[0]=56474d06
A[1]=e5d9e4fe  B[1]=6d821315  C[1]=aa63c4a8  D[1]=a935ccda
A[2]=0743c9f0  B[2]=d4a01fb5  C[2]=e4583973  D[2]=ffd459da
A[3]=1b2c6305  B[3]=29002edc  C[3]=96b91ed0  D[3]=5c77aaf8

Step  3: (r=27, s= 3)
A[0]=f312c001  B[0]=64246dde  C[0]=96b46cf9  D[0]=40ccee9f
A[1]=9747b369  B[1]=f72ecf27  C[1]=6d821315  D[1]=aa63c4a8
A[2]=f3eacd37  B[2]=803a1e4f  C[2]=d4a01fb5  D[2]=e4583973
A[3]=98689f46  B[3]=28d96318  C[3]=29002edc  D[3]=96b91ed0

Step  4: (r= 3, s=20)
A[0]=bf7bce24  B[0]=9896000f  C[0]=64246dde  D[0]=96b46cf9
A[1]=69b1224f  B[1]=ba3d9b4c  C[1]=f72ecf27  D[1]=6d821315
A[2]=9ede1f59  B[2]=9f5669bf  C[2]=803a1e4f  D[2]=d4a01fb5
A[3]=c4040412  B[3]=c344fa34  C[3]=28d96318  D[3]=29002edc

Step  5: (r=20, s=14)
A[0]=1140009f  B[0]=e24bf7bc  C[0]=9896000f  D[0]=64246dde
A[1]=15140493  B[1]=24f69b12  C[1]=ba3d9b4c  D[1]=f72ecf27
A[2]=c67b699e  B[2]=f599ede1  C[2]=9f5669bf  D[2]=803a1e4f
A[3]=97d40664  B[3]=412c4040  C[3]=c344fa34  D[3]=28d96318

Step  6: (r=14, s=27)
A[0]=4a2e6a70  B[0]=0027c450  C[0]=e24bf7bc  D[0]=9896000f
A[1]=51e8c4de  B[1]=0124c545  C[1]=24f69b12  D[1]=ba3d9b4c
A[2]=84c97356  B[2]=da67b19e  C[2]=f599ede1  D[2]=9f5669bf
A[3]=b7e538fc  B[3]=019925f5  C[3]=412c4040  D[3]=c344fa34

Step  7: (r=27, s= 3)
A[0]=b555c4f3  B[0]=82517353  C[0]=0027c450  D[0]=e24bf7bc
A[1]=ffc13c0a  B[1]=f28f4626  C[1]=0124c545  D[1]=24f69b12
A[2]=b2fad834  B[2]=b4264b9a  C[2]=da67b19e  D[2]=f599ede1
```

```
A[3]=0b52502e  B[3]=e5bf29c7  C[3]=019925f5  D[3]=412c4040

Step  8: (r=26, s= 4)
A[0]=6bd39b68  B[0]=ced55713  C[0]=82517353  D[0]=0027c450
A[1]=c88f2fa3  B[1]=2bff04f0  C[1]=f28f4626  D[1]=0124c545
A[2]=deb7db83  B[2]=d2cbeb60  C[2]=b4264b9a  D[2]=da67b19e
A[3]=39ff7834  B[3]=b82d4940  C[3]=e5bf29c7  D[3]=019925f5

Step  9: (r= 4, s=23)
A[0]=69bce84d  B[0]=bd39b686  C[0]=ced55713  D[0]=82517353
A[1]=0212795a  B[1]=88f2fa3c  C[1]=2bff04f0  D[1]=f28f4626
A[2]=7bb012c0  B[2]=eb7db83d  C[2]=d2cbeb60  D[2]=b4264b9a
A[3]=2d8e694e  B[3]=9ff78343  C[3]=b82d4940  D[3]=e5bf29c7

Step 10: (r=23, s=11)
A[0]=87131a6d  B[0]=26b4de74  C[0]=bd39b686  D[0]=ced55713
A[1]=20d6866b  B[1]=ad01093c  C[1]=88f2fa3c  D[1]=2bff04f0
A[2]=a1aa7678  B[2]=603dd809  C[2]=eb7db83d  D[2]=d2cbeb60
A[3]=523df1a2  B[3]=a716c734  C[3]=9ff78343  D[3]=b82d4940

Step 11: (r=11, s=26)
A[0]=b021cd8d  B[0]=98d36c38  C[0]=26b4de74  D[0]=bd39b686
A[1]=6c0a315e  B[1]=b4335906  C[1]=ad01093c  D[1]=88f2fa3c
A[2]=8d4f2b73  B[2]=53b3c50d  C[2]=603dd809  D[2]=eb7db83d
A[3]=ccbd1bec  B[3]=ef8d1291  C[3]=a716c734  D[3]=9ff78343

Step 12: (r=26, s= 4)
A[0]=c5940a80  B[0]=36c08736  C[0]=98d36c38  D[0]=26b4de74
A[1]=f2a666be  B[1]=79b028c5  C[1]=b4335906  D[1]=ad01093c
A[2]=7a3a4444  B[2]=ce353cad  C[2]=53b3c50d  D[2]=603dd809
A[3]=174dd90f  B[3]=b332f46f  C[3]=ef8d1291  D[3]=a716c734

Step 13: (r= 4, s=23)
A[0]=06d7c04f  B[0]=5940a80c  C[0]=36c08736  D[0]=98d36c38
A[1]=608db43f  B[1]=2a666bef  C[1]=79b028c5  D[1]=b4335906
A[2]=e0c82731  B[2]=a3a44447  C[2]=ce353cad  D[2]=53b3c50d
A[3]=9643054d  B[3]=74dd90f1  C[3]=b332f46f  D[3]=ef8d1291

Step 14: (r=23, s=11)
A[0]=243fd555  B[0]=27836be0  C[0]=5940a80c  D[0]=36c08736
A[1]=3dad7d16  B[1]=1fb046da  C[1]=2a666bef  D[1]=79b028c5
A[2]=c81d0433  B[2]=98f06413  C[2]=a3a44447  D[2]=ce353cad
A[3]=a3f6cbe7  B[3]=a6cb2182  C[3]=74dd90f1  D[3]=b332f46f

Step 15: (r=11, s=26)
A[0]=f153ff60  B[0]=feaaa921  C[0]=27836be0  D[0]=5940a80c
A[1]=ed617b70  B[1]=6be8b1ed  C[1]=1fb046da  D[1]=2a666bef
A[2]=e3e967df  B[2]=e8219e40  C[2]=98f06413  D[2]=a3a44447
A[3]=d4c63f24  B[3]=b65f3d1f  C[3]=a6cb2182  D[3]=74dd90f1
```

```
Step 16: (r=19, s=28)
A[0]=6b1c30d4  B[0]=fb078a9f  C[0]=feaaa921  D[0]=27836be0
A[1]=39560704  B[1]=db876b0b  C[1]=6be8b1ed  D[1]=1fb046da
A[2]=e1ec7726  B[2]=3eff1f4b  C[2]=e8219e40  D[2]=98f06413
A[3]=029ebd0b  B[3]=f926a631  C[3]=b65f3d1f  D[3]=a6cb2182

Step 17: (r=28, s= 7)
A[0]=20d274cc  B[0]=46b1c30d  C[0]=fb078a9f  D[0]=feaaa921
A[1]=07257b9b  B[1]=43956070  C[1]=db876b0b  D[1]=6be8b1ed
A[2]=2ad6ec96  B[2]=6e1ec772  C[2]=3eff1f4b  D[2]=e8219e40
A[3]=542aaf8e  B[3]=b029ebd0  C[3]=f926a631  D[3]=b65f3d1f

Step 18: (r= 7, s=22)
A[0]=fdb9d3ab  B[0]=693a6610  C[0]=46b1c30d  D[0]=fb078a9f
A[1]=40ba4601  B[1]=92bdcd83  C[1]=43956070  D[1]=db876b0b
A[2]=13fb15c8  B[2]=6b764b15  C[2]=6e1ec772  D[2]=3eff1f4b
A[3]=f7e92c01  B[3]=1557c72a  C[3]=b029ebd0  D[3]=f926a631

Step 19: (r=22, s=19)
A[0]=e6d92112  B[0]=eaff6e74  C[0]=693a6610  D[0]=46b1c30d
A[1]=8ec01cac  B[1]=80502e91  C[1]=92bdcd83  D[1]=43956070
A[2]=3f4d6c7c  B[2]=7204fec5  C[2]=6b764b15  D[2]=6e1ec772
A[3]=fb73641f  B[3]=007dfa4b  C[3]=1557c72a  D[3]=b029ebd0

Step 20: (r=19, s=28)
A[0]=454fcbc1  B[0]=089736c9  C[0]=eaff6e74  D[0]=693a6610
A[1]=2ff0fb06  B[1]=e5647600  C[1]=80502e91  D[1]=92bdcd83
A[2]=f348a8ef  B[2]=63e1fa6b  C[2]=7204fec5  D[2]=6b764b15
A[3]=4181ddfc  B[3]=20ffdb9b  C[3]=007dfa4b  D[3]=1557c72a

Step 21: (r=28, s= 7)
A[0]=cd7013fd  B[0]=1454fcbc  C[0]=089736c9  D[0]=eaff6e74
A[1]=9e0c4516  B[1]=62ff0fb0  C[1]=e5647600  D[1]=80502e91
A[2]=04ab6b48  B[2]=ff348a8e  C[2]=63e1fa6b  D[2]=7204fec5
A[3]=37f56ed2  B[3]=c4181ddf  C[3]=20ffdb9b  D[3]=007dfa4b

Step 22: (r= 7, s=22)
A[0]=46e38fea  B[0]=b809fee6  C[0]=1454fcbc  D[0]=089736c9
A[1]=99606419  B[1]=06228b4f  C[1]=62ff0fb0  D[1]=e5647600
A[2]=13b176e1  B[2]=55b5a402  C[2]=ff348a8e  D[2]=63e1fa6b
A[3]=eef93338  B[3]=fab7691b  C[3]=c4181ddf  D[3]=20ffdb9b

Step 23: (r=22, s=19)
A[0]=8f5cf170  B[0]=fa91b8e3  C[0]=b809fee6  D[0]=1454fcbc
A[1]=e12c6fe0  B[1]=06665819  C[1]=06228b4f  D[1]=62ff0fb0
A[2]=6e0f4cd1  B[2]=b844ec5d  C[2]=55b5a402  D[2]=ff348a8e
A[3]=0bebe7f1  B[3]=ce3bbe4c  C[3]=fab7691b  D[3]=c4181ddf
```

```
Step 24: (r=15, s= 5)
A[0]=a1363aad  B[0]=78b847ae  C[0]=fa91b8e3  D[0]=b809fee6
A[1]=ee6abcb5  B[1]=37f07096  C[1]=06665819  D[1]=06228b4f
A[2]=eded2f7a  B[2]=a668b707  C[2]=b844ec5d  D[2]=55b5a402
A[3]=cdccae40  B[3]=f3f885f5  C[3]=ce3bbe4c  D[3]=fab7691b

Step 25: (r= 5, s=29)
A[0]=4643f2d9  B[0]=26c755b4  C[0]=78b847ae  D[0]=fa91b8e3
A[1]=0afbacef  B[1]=cd5796bd  C[1]=37f07096  D[1]=06665819
A[2]=a34400f0  B[2]=bda5ef5d  C[2]=a668b707  D[2]=b844ec5d
A[3]=bf439580  B[3]=b995c819  C[3]=f3f885f5  D[3]=ce3bbe4c

Step 26: (r=29, s= 9)
A[0]=602b68c2  B[0]=28c87e5b  C[0]=26c755b4  D[0]=78b847ae
A[1]=29e2464e  B[1]=e15f759d  C[1]=cd5796bd  D[1]=37f07096
A[2]=206b43e3  B[2]=1468801e  C[2]=bda5ef5d  D[2]=a668b707
A[3]=7be28e0f  B[3]=17e872b0  C[3]=b995c819  D[3]=f3f885f5

Step 27: (r= 9, s=15)
A[0]=84502af1  B[0]=56d184c0  C[0]=28c87e5b  D[0]=26c755b4
A[1]=6e24c6a2  B[1]=c48c9c53  C[1]=e15f759d  D[1]=cd5796bd
A[2]=f28c5226  B[2]=d687c640  C[2]=1468801e  D[2]=bda5ef5d
A[3]=3d7e4487  B[3]=c51c1ef7  C[3]=17e872b0  D[3]=b995c819

Step 28: (r=15, s= 5)
A[0]=c708d58b  B[0]=1578c228  C[0]=56d184c0  D[0]=28c87e5b
A[1]=6cb78f1b  B[1]=63513712  C[1]=c48c9c53  D[1]=e15f759d
A[2]=aa1c11b6  B[2]=29137946  C[2]=d687c640  D[2]=1468801e
A[3]=f49e6e2a  B[3]=22439ebf  C[3]=c51c1ef7  D[3]=17e872b0

Step 29: (r= 5, s=29)
A[0]=4636ddf1  B[0]=e11ab178  C[0]=1578c228  D[0]=56d184c0
A[1]=92e0da2f  B[1]=96f1e36d  C[1]=63513712  D[1]=c48c9c53
A[2]=063a58f4  B[2]=438236d5  C[2]=29137946  D[2]=d687c640
A[3]=24c88c29  B[3]=93cdc55e  C[3]=22439ebf  D[3]=c51c1ef7

Step 30: (r=29, s= 9)
A[0]=eb449e5f  B[0]=28c6dbbe  C[0]=e11ab178  D[0]=1578c228
A[1]=71b18702  B[1]=f25c1b45  C[1]=96f1e36d  D[1]=63513712
A[2]=33dda3f0  B[2]=80c74b1e  C[2]=438236d5  D[2]=29137946
A[3]=5269bd43  B[3]=24991185  C[3]=93cdc55e  D[3]=22439ebf

Step 31: (r= 9, s=15)
A[0]=8a6a73cc  B[0]=893cbfd6  C[0]=28c6dbbe  D[0]=e11ab178
A[1]=bdd8b40b  B[1]=630e04e3  C[1]=f25c1b45  D[1]=96f1e36d
A[2]=08efea49  B[2]=bb47e067  C[2]=80c74b1e  D[2]=438236d5
A[3]=037058c0  B[3]=d37a86a4  C[3]=24991185  D[3]=93cdc55e

Feistel Step 0: (r=15, s= 5)
```

```
A[0]=39d658a3  B[0]=39e64535  C[0]=893cbfd6  D[0]=28c6dbbe
A[1]=900ba78b  B[1]=5a05deec  C[1]=630e04e3  D[1]=f25c1b45
A[2]=a6519fc5  B[2]=f5248477  C[2]=bb47e067  D[2]=80c74b1e
A[3]=40e075ab  B[3]=2c6001b8  C[3]=d37a86a4  D[3]=24991185

Feistel Step 1: (r= 5, s=29)
A[0]=08d6d297  B[0]=3acb1467  C[0]=39e64535  D[0]=893cbfd6
A[1]=3e1f0bb4  B[1]=0174f172  C[1]=5a05deec  D[1]=630e04e3
A[2]=83c9fecd  B[2]=ca33f8b4  C[2]=f5248477  D[2]=bb47e067
A[3]=90493c22  B[3]=1c0eb568  C[3]=2c6001b8  D[3]=d37a86a4

Feistel Step 2: (r=29, s= 9)
A[0]=f1113282  B[0]=e11ada52  C[0]=3acb1467  D[0]=39e64535
A[1]=f49ccea8  B[1]=87c3e176  C[1]=0174f172  D[1]=5a05deec
A[2]=081118a4  B[2]=b0793fd9  C[2]=ca33f8b4  D[2]=f5248477
A[3]=20215930  B[3]=52092784  C[3]=1c0eb568  D[3]=2c6001b8

Feistel Step 3: (r= 9, s=15)
A[0]=f5140b6d  B[0]=226505e2  C[0]=e11ada52  D[0]=3acb1467
A[1]=8dc7a384  B[1]=399d51e9  C[1]=87c3e176  D[1]=0174f172
A[2]=a846f1af  B[2]=22314810  C[2]=b0793fd9  D[2]=ca33f8b4
A[3]=aed76557  B[3]=42b26040  C[3]=52092784  D[3]=1c0eb568
```

Compression Function Output

```
A[0]=f5140b6d  B[0]=226505e2  C[0]=e11ada52  D[0]=3acb1467
A[1]=8dc7a384  B[1]=399d51e9  C[1]=87c3e176  D[1]=0174f172
A[2]=a846f1af  B[2]=22314810  C[2]=b0793fd9  D[2]=ca33f8b4
A[3]=aed76557  B[3]=42b26040  C[3]=52092784  D[3]=1c0eb568
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
```

```
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
Z[17] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
Z[18] = f7cf7480  49b92296  9af9e76d  ebfa966c
Z[19] = 452c2723  386e33e1  3cfb2f54  f17090f6
Z[20] = a413de53  71c5fa8a  2d823ecd  065f65f0
Z[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
Z[22] = 7480f7cf  065f65f0  0bd5607a  576014ef
Z[23] = cb36b730  558e16c1  b1bad0ac  5b04114b
Z[24] = 0a03624c  983eea28  00e96b66  9ccbe59b
Z[25] = a241e025  2f543cfb  92c8ef9e  d450ae16
Z[26] = bca6c5c0  e93f9927  d195b0d1  58491406
Z[27] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
Z[28] = ebfa966c  237f48d0  255146fe  e76d9af9
Z[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
Z[30] = 6e21fe2e  409f2bb0  567715d8  35b3369c
Z[31] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
```

```
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
W[17] = f7cf7480  49b92296  9af9e76d  ebfa966c
W[18] = cb36b730  558e16c1  b1bad0ac  5b04114b
W[19] = a413de53  71c5fa8a  2d823ecd  065f65f0
W[20] = 7480f7cf  065f65f0  0bd5607a  576014ef
W[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
W[22] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
W[23] = 452c2723  386e33e1  3cfb2f54  f17090f6
W[24] = 6e21fe2e  409f2bb0  567715d8  35b3369c
W[25] = 0a03624c  983eea28  00e96b66  9ccbe59b
W[26] = a241e025  2f543cfb  92c8ef9e  d450ae16
W[27] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
W[28] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
W[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
W[30] = ebfa966c  237f48d0  255146fe  e76d9af9
W[31] = bca6c5c0  e93f9927  d195b0d1  58491406
```

Feistel Steps

```
IV :
A[0]=f5140b6d  B[0]=226505e2  C[0]=e11ada52  D[0]=3acb1467
A[1]=8dc7a384  B[1]=399d51e9  C[1]=87c3e176  D[1]=0174f172
A[2]=a846f1af  B[2]=22314810  C[2]=b0793fd9  D[2]=ca33f8b4
A[3]=aed76557  B[3]=42b26040  C[3]=52092784  D[3]=1c0eb568

IV XOR M :
A[0]=f51409d1  B[0]=226505e2  C[0]=e11ada52  D[0]=3acb1467
A[1]=8dc7a384  B[1]=399d51e9  C[1]=87c3e176  D[1]=0174f172
A[2]=a846f1af  B[2]=22314810  C[2]=b0793fd9  D[2]=ca33f8b4
A[3]=aed76557  B[3]=42b26040  C[3]=52092784  D[3]=1c0eb568

Step  0: (r= 3, s=20)
A[0]=44fd8c90  B[0]=a8a04e8f  C[0]=226505e2  D[0]=e11ada52
A[1]=331bfa2f  B[1]=6e3d1c24  C[1]=399d51e9  D[1]=87c3e176
A[2]=04ce5774  B[2]=42378d7d  C[2]=22314810  D[2]=b0793fd9
A[3]=3a2235b5  B[3]=76bb2abd  C[3]=42b26040  D[3]=52092784
```

```
Step  1: (r=20, s=14)
A[0]=efad0d77  B[0]=c9044fd8  C[0]=a8a04e8f  D[0]=226505e2
A[1]=ae665767  B[1]=a2f331bf  C[1]=6e3d1c24  D[1]=399d51e9
A[2]=ef7e48da  B[2]=77404ce5  C[2]=42378d7d  D[2]=22314810
A[3]=89396dc4  B[3]=5b53a223  C[3]=76bb2abd  D[3]=42b26040

Step  2: (r=14, s=27)
A[0]=9fa59ccf  B[0]=435dfbeb  C[0]=c9044fd8  D[0]=a8a04e8f
A[1]=728cc498  B[1]=95d9eb99  C[1]=a2f331bf  D[1]=6e3d1c24
A[2]=0a66ed28  B[2]=9236bbdf  C[2]=77404ce5  D[2]=42378d7d
A[3]=30c885ea  B[3]=5b71224e  C[3]=5b53a223  D[3]=76bb2abd

Step  3: (r=27, s= 3)
A[0]=2b876ebe  B[0]=7cfd2ce6  C[0]=435dfbeb  D[0]=c9044fd8
A[1]=be078efc  B[1]=c3946624  C[1]=95d9eb99  D[1]=a2f331bf
A[2]=50fe4b21  B[2]=40533769  C[2]=9236bbdf  D[2]=77404ce5
A[3]=d33c2fcb  B[3]=5186442f  C[3]=5b71224e  D[3]=5b53a223

Step  4: (r= 3, s=20)
A[0]=3fab647d  B[0]=5c3b75f1  C[0]=7cfd2ce6  D[0]=435dfbeb
A[1]=b0b48f9d  B[1]=f03c77e5  C[1]=c3946624  D[1]=95d9eb99
A[2]=c581adf4  B[2]=87f2590a  C[2]=40533769  D[2]=9236bbdf
A[3]=bf11212e  B[3]=99e17e5e  C[3]=5186442f  D[3]=5b71224e

Step  5: (r=20, s=14)
A[0]=3587bc62  B[0]=47d3fab6  C[0]=5c3b75f1  D[0]=7cfd2ce6
A[1]=3ab3bf8f  B[1]=f9db0b48  C[1]=f03c77e5  D[1]=c3946624
A[2]=bf768ac2  B[2]=df4c581a  C[2]=87f2590a  D[2]=40533769
A[3]=dc330d08  B[3]=12ebf112  C[3]=99e17e5e  D[3]=5186442f

Step  6: (r=14, s=27)
A[0]=4ee068f3  B[0]=ef188d61  C[0]=47d3fab6  D[0]=5c3b75f1
A[1]=b87c0e56  B[1]=efe3ceac  C[1]=f9db0b48  D[1]=f03c77e5
A[2]=fb5bccb4  B[2]=a2b0afdd  C[2]=df4c581a  D[2]=87f2590a
A[3]=e87430a9  B[3]=c342370c  C[3]=12ebf112  D[3]=99e17e5e

Step  7: (r=27, s= 3)
A[0]=3de68e89  B[0]=9a770347  C[0]=ef188d61  D[0]=47d3fab6
A[1]=245961f5  B[1]=b5c3e072  C[1]=efe3ceac  D[1]=f9db0b48
A[2]=4cc75a92  B[2]=a7dade65  C[2]=a2b0afdd  D[2]=df4c581a
A[3]=8f92f61a  B[3]=4f43a185  C[3]=c342370c  D[3]=12ebf112

Step  8: (r=26, s= 4)
A[0]=1faea857  B[0]=24f79a3a  C[0]=9a770347  D[0]=ef188d61
A[1]=1b86f853  B[1]=d4916587  C[1]=b5c3e072  D[1]=efe3ceac
A[2]=7a0fdff2  B[2]=49331d6a  C[2]=a7dade65  D[2]=a2b0afdd
A[3]=49853fdf  B[3]=6a3e4bd8  C[3]=4f43a185  D[3]=c342370c
```

```
Step  9: (r= 4, s=23)
A[0]=50dc85ce  B[0]=faea8571  C[0]=24f79a3a  D[0]=9a770347
A[1]=6752c221  B[1]=b86f8531  C[1]=d4916587  D[1]=b5c3e072
A[2]=d2bc126f  B[2]=a0fdff27  C[2]=49331d6a  D[2]=a7dade65
A[3]=6282c48c  B[3]=9853fdf4  C[3]=6a3e4bd8  D[3]=4f43a185

Step 10: (r=23, s=11)
A[0]=fb81815c  B[0]=e7286e42  C[0]=faea8571  D[0]=24f79a3a
A[1]=eeecd21e  B[1]=10b3a961  C[1]=b86f8531  D[1]=d4916587
A[2]=1f3eb3db  B[2]=37e95e09  C[2]=a0fdff27  D[2]=49331d6a
A[3]=e2dbb061  B[3]=46314162  C[3]=9853fdf4  D[3]=6a3e4bd8

Step 11: (r=11, s=26)
A[0]=5de02ea0  B[0]=0c0ae7dc  C[0]=e7286e42  D[0]=faea8571
A[1]=e7ce5e81  B[1]=6690f777  C[1]=10b3a961  D[1]=b86f8531
A[2]=e4123e0c  B[2]=f59ed8f9  C[2]=37e95e09  D[2]=a0fdff27
A[3]=a0672559  B[3]=dd830f16  C[3]=46314162  D[3]=9853fdf4

Step 12: (r=26, s= 4)
A[0]=e1e26a89  B[0]=817780ba  C[0]=0c0ae7dc  D[0]=e7286e42
A[1]=7cfad43c  B[1]=079f397a  C[1]=6690f777  D[1]=10b3a961
A[2]=6492dfc8  B[2]=339048f8  C[2]=f59ed8f9  D[2]=37e95e09
A[3]=1de9e01d  B[3]=66819c95  C[3]=dd830f16  D[3]=46314162

Step 13: (r= 4, s=23)
A[0]=d2c7e200  B[0]=1e26a89e  C[0]=817780ba  D[0]=0c0ae7dc
A[1]=5d4e1925  B[1]=cfad43c7  C[1]=079f397a  D[1]=6690f777
A[2]=20577695  B[2]=492dfc86  C[2]=339048f8  D[2]=f59ed8f9
A[3]=19211457  B[3]=de9e01d1  C[3]=66819c95  D[3]=dd830f16

Step 14: (r=23, s=11)
A[0]=5ebe5253  B[0]=006963f1  C[0]=1e26a89e  D[0]=817780ba
A[1]=c4eb68db  B[1]=92aea70c  C[1]=cfad43c7  D[1]=079f397a
A[2]=fbb74818  B[2]=4a902bbb  C[2]=492dfc86  D[2]=339048f8
A[3]=f1099001  B[3]=2b8c908a  C[3]=de9e01d1  D[3]=66819c95

Step 15: (r=11, s=26)
A[0]=f21d24dd  B[0]=f2929af5  C[0]=006963f1  D[0]=1e26a89e
A[1]=ac868611  B[1]=5b46de27  C[1]=92aea70c  D[1]=cfad43c7
A[2]=d1a24de0  B[2]=ba40c7dd  C[2]=4a902bbb  D[2]=492dfc86
A[3]=3579a3f0  B[3]=4c800f88  C[3]=2b8c908a  D[3]=de9e01d1

Step 16: (r=19, s=28)
A[0]=6689c4cf  B[0]=26ef90e9  C[0]=f2929af5  D[0]=006963f1
A[1]=807c6fac  B[1]=308d6434  C[1]=5b46de27  D[1]=92aea70c
A[2]=67f6cff8  B[2]=6f068d12  C[2]=ba40c7dd  D[2]=4a902bbb
A[3]=c87cb648  B[3]=1f81abcd  C[3]=4c800f88  D[3]=2b8c908a

Step 17: (r=28, s= 7)
```

```
A[0]=f0b92256  B[0]=f6689c4c  C[0]=26ef90e9  D[0]=f2929af5
A[1]=47e6afff  B[1]=c807c6fa  C[1]=308d6434  D[1]=5b46de27
A[2]=3eb8bb3e  B[2]=867f6cff  C[2]=6f068d12  D[2]=ba40c7dd
A[3]=cbf1260c  B[3]=8c87cb64  C[3]=1f81abcd  D[3]=4c800f88

Step 18: (r= 7, s=22)
A[0]=b8050d9b  B[0]=5c912b78  C[0]=f6689c4c  D[0]=26ef90e9
A[1]=54e5d84d  B[1]=f357ffa3  C[1]=c807c6fa  D[1]=308d6434
A[2]=2a7fd4d6  B[2]=5c5d9f1f  C[2]=867f6cff  D[2]=6f068d12
A[3]=82a22ce3  B[3]=f8930665  C[3]=8c87cb64  D[3]=1f81abcd

Step 19: (r=22, s=19)
A[0]=7a4beb5d  B[0]=66ee0143  C[0]=5c912b78  D[0]=f6689c4c
A[1]=246c7d64  B[1]=13553976  C[1]=f357ffa3  D[1]=c807c6fa
A[2]=a7df4877  B[2]=358a9ff5  C[2]=5c5d9f1f  D[2]=867f6cff
A[3]=dc6accbc  B[3]=38e0a88b  C[3]=f8930665  D[3]=8c87cb64

Step 20: (r=19, s=28)
A[0]=39bc6f5a  B[0]=5aebd25f  C[0]=66ee0143  D[0]=5c912b78
A[1]=43d9099f  B[1]=eb212363  C[1]=13553976  D[1]=f357ffa3
A[2]=726a2a25  B[2]=43bd3efa  C[2]=358a9ff5  D[2]=5c5d9f1f
A[3]=68b8792f  B[3]=65e6e356  C[3]=38e0a88b  D[3]=f8930665

Step 21: (r=28, s= 7)
A[0]=4bd90ad3  B[0]=a39bc6f5  C[0]=5aebd25f  D[0]=66ee0143
A[1]=aa4fdd33  B[1]=f43d9099  C[1]=eb212363  D[1]=13553976
A[2]=b179faaf  B[2]=5726a2a2  C[2]=43bd3efa  D[2]=358a9ff5
A[3]=03b71cfe  B[3]=f68b8792  C[3]=65e6e356  D[3]=38e0a88b

Step 22: (r= 7, s=22)
A[0]=644ab037  B[0]=ec8569a5  C[0]=a39bc6f5  D[0]=5aebd25f
A[1]=0277b730  B[1]=27ee99d5  C[1]=f43d9099  D[1]=eb212363
A[2]=5b75eced  B[2]=bcfd57d8  C[2]=5726a2a2  D[2]=43bd3efa
A[3]=15e3145c  B[3]=db8e7f01  C[3]=f68b8792  D[3]=65e6e356

Step 23: (r=22, s=19)
A[0]=0d130299  B[0]=0dd912ac  C[0]=ec8569a5  D[0]=a39bc6f5
A[1]=5dafc93c  B[1]=cc009ded  C[1]=27ee99d5  D[1]=f43d9099
A[2]=b790141e  B[2]=3b56dd7b  C[2]=bcfd57d8  D[2]=5726a2a2
A[3]=26e21501  B[3]=170578c5  C[3]=db8e7f01  D[3]=f68b8792

Step 24: (r=15, s= 5)
A[0]=cf0448d6  B[0]=814c8689  C[0]=0dd912ac  D[0]=ec8569a5
A[1]=6dba229c  B[1]=e49e2ed7  C[1]=cc009ded  D[1]=27ee99d5
A[2]=2de29e0e  B[2]=0a0f5bc8  C[2]=3b56dd7b  D[2]=bcfd57d8
A[3]=eab38c6a  B[3]=0a809371  C[3]=170578c5  D[3]=db8e7f01

Step 25: (r= 5, s=29)
A[0]=eb607d98  B[0]=e0891ad9  C[0]=814c8689  D[0]=0dd912ac
```

```
A[1]=ab0a95db  B[1]=b744538d  C[1]=e49e2ed7  D[1]=cc009ded
A[2]=db88beaf  B[2]=bc53c1c5  C[2]=0a0f5bc8  D[2]=3b56dd7b
A[3]=ea403e3d  B[3]=56718d5d  C[3]=0a809371  D[3]=170578c5

Step 26: (r=29, s= 9)
A[0]=c47c27db  B[0]=1d6c0fb3  C[0]=e0891ad9  D[0]=814c8689
A[1]=cd9e039a  B[1]=756152bb  C[1]=b744538d  D[1]=e49e2ed7
A[2]=0c65c493  B[2]=fb7117d5  C[2]=bc53c1c5  D[2]=0a0f5bc8
A[3]=4ad4800f  B[3]=bd4807c7  C[3]=56718d5d  D[3]=0a809371

Step 27: (r= 9, s=15)
A[0]=7272e68c  B[0]=f84fb788  C[0]=1d6c0fb3  D[0]=e0891ad9
A[1]=5b2b9c47  B[1]=3c07359b  C[1]=756152bb  D[1]=b744538d
A[2]=ce6fa99f  B[2]=cb892618  C[2]=fb7117d5  D[2]=bc53c1c5
A[3]=57a13f09  B[3]=a9001e95  C[3]=bd4807c7  D[3]=56718d5d

Step 28: (r=15, s= 5)
A[0]=6abe060b  B[0]=73463939  C[0]=f84fb788  D[0]=1d6c0fb3
A[1]=603c77cb  B[1]=ce23ad95  C[1]=3c07359b  D[1]=756152bb
A[2]=8de76b48  B[2]=d4cfe737  C[2]=cb892618  D[2]=fb7117d5
A[3]=2e2612be  B[3]=9f84abd0  C[3]=a9001e95  D[3]=bd4807c7

Step 29: (r= 5, s=29)
A[0]=2796aa83  B[0]=57c0c16d  C[0]=73463939  D[0]=f84fb788
A[1]=5d4f7cc0  B[1]=078ef96c  C[1]=ce23ad95  D[1]=3c07359b
A[2]=e4f6cd89  B[2]=bced6911  C[2]=d4cfe737  D[2]=cb892618
A[3]=9fca408f  B[3]=c4c257c5  C[3]=9f84abd0  D[3]=a9001e95

Step 30: (r=29, s= 9)
A[0]=2d982a50  B[0]=64f2d550  C[0]=57c0c16d  D[0]=73463939
A[1]=6997390e  B[1]=0ba9ef98  C[1]=078ef96c  D[1]=ce23ad95
A[2]=88ad97dc  B[2]=3c9ed9b1  C[2]=bced6911  D[2]=d4cfe737
A[3]=c4ed7bb0  B[3]=f3f94811  C[3]=c4c257c5  D[3]=9f84abd0

Step 31: (r= 9, s=15)
A[0]=3b5483ef  B[0]=3054a05b  C[0]=64f2d550  D[0]=57c0c16d
A[1]=7adbc302  B[1]=2e721cd3  C[1]=0ba9ef98  D[1]=078ef96c
A[2]=e92151e4  B[2]=5b2fb911  C[2]=3c9ed9b1  D[2]=bced6911
A[3]=bc25fb2e  B[3]=daf76189  C[3]=f3f94811  D[3]=c4c257c5

Feistel Step 0: (r=15, s= 5)
A[0]=1af56425  B[0]=41f79daa  C[0]=3054a05b  D[0]=64f2d550
A[1]=c20ba5e8  B[1]=e1813d6d  C[1]=2e721cd3  D[1]=0ba9ef98
A[2]=5c15d84a  B[2]=a8f27490  C[2]=5b2fb911  D[2]=3c9ed9b1
A[3]=34db6453  B[3]=fd975e12  C[3]=daf76189  D[3]=f3f94811

Feistel Step 1: (r= 5, s=29)
A[0]=17c4b540  B[0]=5eac84a3  C[0]=41f79daa  D[0]=3054a05b
A[1]=21a39a45  B[1]=4174bd18  C[1]=e1813d6d  D[1]=2e721cd3
```

```
A[2]=abedd6fd  B[2]=82bb094b  C[2]=a8f27490  D[2]=5b2fb911
A[3]=a8211ad5  B[3]=9b6c8a66  C[3]=fd975e12  D[3]=daf76189

Feistel Step 2: (r=29, s= 9)
A[0]=f2432218  B[0]=02f896a8  C[0]=5eac84a3  D[0]=41f79daa
A[1]=62f49dcd  B[1]=a4347348  C[1]=4174bd18  D[1]=e1813d6d
A[2]=7d368a76  B[2]=b57dbadf  C[2]=82bb094b  D[2]=a8f27490
A[3]=70a73cbd  B[3]=b504235a  C[3]=9b6c8a66  D[3]=fd975e12

Feistel Step 3: (r= 9, s=15)
A[0]=097332d1  B[0]=864431e4  C[0]=02f896a8  D[0]=5eac84a3
A[1]=7e94fcf6  B[1]=e93b9ac5  C[1]=a4347348  D[1]=4174bd18
A[2]=8295c755  B[2]=6d14ecfa  C[2]=b57dbadf  D[2]=82bb094b
A[3]=4426053e  B[3]=4e797ae1  C[3]=b504235a  D[3]=9b6c8a66
```

Compression Function Output

```
Compression function output :
A[0]=097332d1  B[0]=864431e4  C[0]=02f896a8  D[0]=5eac84a3
A[1]=7e94fcf6  B[1]=e93b9ac5  C[1]=a4347348  D[1]=4174bd18
A[2]=8295c755  B[2]=6d14ecfa  C[2]=b57dbadf  D[2]=82bb094b
A[3]=4426053e  B[3]=4e797ae1  C[3]=b504235a  D[3]=9b6c8a66
```

Hash Function Output

```
d1327309f6fc947e55c795823e052644e4314486c59a3be9faec146d
```

6.2 SIMD-256

6.2.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
```

```
y[ 24.. 31] =   96  176  161   47  189   61  248  107
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe2e01d2  949a6b66  d70b28f5  9af96507
Z[17] = a7b75849  29ded622  d3672c99  607a9f86
Z[18] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
Z[19] = a8a05760  5760a8a0  3de4c21c  0831f7cf
Z[20] = 00000000  70dc8f24  f0870f79  f5140aec
Z[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
Z[22] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
Z[23] = 091af6e6  6a7d9583  b9eb4615  ece3131d
Z[24] = 5beda413  9e9d6163  28f5d70b  5677a989
Z[25] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
Z[26] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
Z[27] = 49b9b647  d5392ac7  c87b3785  9e9d6163
Z[28] = 72ae8d52  992766d9  e1f71e09  9af96507
Z[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
Z[30] = f8b80748  1893e76d  607a9f86  1b4ee4b2
Z[31] = 9af96507  fa8a0576  f6e6091a  624c9db4
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = a7b75849  29ded622  d3672c99  607a9f86
W[17] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
W[18] = 091af6e6  6a7d9583  b9eb4615  ece3131d
W[19] = 00000000  70dc8f24  f0870f79  f5140aec
W[20] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
W[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
W[22] = fe2e01d2  949a6b66  d70b28f5  9af96507
W[23] = a8a05760  5760a8a0  3de4c21c  0831f7cf
W[24] = f8b80748  1893e76d  607a9f86  1b4ee4b2
W[25] = 5beda413  9e9d6163  28f5d70b  5677a989
W[26] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
W[27] = 9af96507  fa8a0576  f6e6091a  624c9db4
W[28] = 49b9b647  d5392ac7  c87b3785  9e9d6163
W[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
W[30] = 72ae8d52  992766d9  e1f71e09  9af96507
W[31] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
```

Feistel Steps

```
IV :
A[0]=96301f14  B[0]=75ad94b4  C[0]=2d83bbab  D[0]=5731b59d
A[1]=64f69407  B[1]=8b618939  C[1]=0c195501  D[1]=abff7dd4
A[2]=8450cc02  B[2]=5a13cb35  C[2]=cc0782ba  D[2]=db4cd0f5
A[3]=42c538e3  B[3]=26141ded  C[3]=356688a2  D[3]=7240ec03

IV XOR M :
A[0]=96301f14  B[0]=75ad94b4  C[0]=2d83bbab  D[0]=5731b59d
A[1]=64f69407  B[1]=8b618939  C[1]=0c195501  D[1]=abff7dd4
A[2]=8450cc02  B[2]=5a13cb35  C[2]=cc0782ba  D[2]=db4cd0f5
A[3]=42c538e3  B[3]=26141ded  C[3]=356688a2  D[3]=7240ec03

Step  0: (r= 3, s=20)
```

```
A[0]=cd783cb1  B[0]=b180f8a4  C[0]=75ad94b4  D[0]=2d83bbab
A[1]=7616c142  B[1]=27b4a03b  C[1]=8b618939  D[1]=0c195501
A[2]=958d7af4  B[2]=22866014  C[2]=5a13cb35  D[2]=cc0782ba
A[3]=8a90928c  B[3]=1629c71a  C[3]=26141ded  D[3]=356688a2

Step  1: (r=20, s=14)
A[0]=4014520b  B[0]=cb1cd783  C[0]=b180f8a4  D[0]=75ad94b4
A[1]=5684930c  B[1]=1427616c  C[1]=27b4a03b  D[1]=8b618939
A[2]=1aabca04  B[2]=af4958d7  C[2]=22866014  D[2]=5a13cb35
A[3]=8d84b2db  B[3]=28c8a909  C[3]=1629c71a  D[3]=26141ded

Step  2: (r=14, s=27)
A[0]=8db54227  B[0]=1482d005  C[0]=cb1cd783  D[0]=b180f8a4
A[1]=e2f04ea7  B[1]=24c315a1  C[1]=1427616c  D[1]=27b4a03b
A[2]=9fd3c5ff  B[2]=f28106aa  C[2]=af4958d7  D[2]=22866014
A[3]=84638a9e  B[3]=2cb6e361  C[3]=28c8a909  D[3]=1629c71a

Step  3: (r=27, s= 3)
A[0]=f49b865c  B[0]=3c6daa11  C[0]=1482d005  D[0]=cb1cd783
A[1]=a5a13655  B[1]=3f178275  C[1]=24c315a1  D[1]=1427616c
A[2]=befb4761  B[2]=fcfe9e2f  C[2]=f28106aa  D[2]=af4958d7
A[3]=cd8a42c8  B[3]=f4231c54  C[3]=2cb6e361  D[3]=28c8a909

Step  4: (r= 3, s=20)
A[0]=52eeb0b2  B[0]=a4dc32e7  C[0]=3c6daa11  D[0]=1482d005
A[1]=2d1e1b1f  B[1]=2d09b2ad  C[1]=3f178275  D[1]=24c315a1
A[2]=d6cd6e2f  B[2]=f7da3b0d  C[2]=fcfe9e2f  D[2]=f28106aa
A[3]=4c48a8d6  B[3]=6c521646  C[3]=f4231c54  D[3]=2cb6e361

Step  5: (r=20, s=14)
A[0]=c29611cd  B[0]=0b252eeb  C[0]=a4dc32e7  D[0]=3c6daa11
A[1]=01a88551  B[1]=b1f2d1e1  C[1]=2d09b2ad  D[1]=3f178275
A[2]=24d93501  B[2]=e2fd6cd6  C[2]=f7da3b0d  D[2]=fcfe9e2f
A[3]=b06ea386  B[3]=8d64c48a  C[3]=6c521646  D[3]=f4231c54

Step  6: (r=14, s=27)
A[0]=2578097d  B[0]=847370a5  C[0]=0b252eeb  D[0]=a4dc32e7
A[1]=015607ad  B[1]=2154406a  C[1]=b1f2d1e1  D[1]=2d09b2ad
A[2]=2961196b  B[2]=4d404936  C[2]=e2fd6cd6  D[2]=f7da3b0d
A[3]=53e25d87  B[3]=a8e1ac1b  C[3]=8d64c48a  D[3]=6c521646

Step  7: (r=27, s= 3)
A[0]=7d781838  B[0]=e92bc04b  C[0]=847370a5  D[0]=0b252eeb
A[1]=befdadae  B[1]=680ab03d  C[1]=2154406a  D[1]=b1f2d1e1
A[2]=3af0ffb0  B[2]=594b08cb  C[2]=4d404936  D[2]=e2fd6cd6
A[3]=551761fb  B[3]=3a9f12ec  C[3]=a8e1ac1b  D[3]=8d64c48a

Step  8: (r=26, s= 4)
A[0]=fc9561e0  B[0]=e1f5e060  C[0]=e92bc04b  D[0]=847370a5
```

```
A[1]=2b4c31ab  B[1]=bafbf6b6  C[1]=680ab03d  D[1]=2154406a
A[2]=7d9838fa  B[2]=c0ebc3fe  C[2]=594b08cb  D[2]=4d404936
A[3]=288a04b9  B[3]=ed545d87  C[3]=3a9f12ec  D[3]=a8e1ac1b

Step  9: (r= 4, s=23)
A[0]=b1d3ee2c  B[0]=c9561e0f  C[0]=e1f5e060  D[0]=e92bc04b
A[1]=c8d51fad  B[1]=b4c31ab2  C[1]=bafbf6b6  D[1]=680ab03d
A[2]=7407194c  B[2]=d9838fa7  C[2]=c0ebc3fe  D[2]=594b08cb
A[3]=658dec96  B[3]=88a04b92  C[3]=ed545d87  D[3]=3a9f12ec

Step 10: (r=23, s=11)
A[0]=555922bc  B[0]=1658e9f7  C[0]=c9561e0f  D[0]=e1f5e060
A[1]=165e61d6  B[1]=d6e46a8f  C[1]=b4c31ab2  D[1]=bafbf6b6
A[2]=41748788  B[2]=a63a038c  C[2]=d9838fa7  D[2]=c0ebc3fe
A[3]=e1778590  B[3]=4b32c6f6  C[3]=88a04b92  D[3]=ed545d87

Step 11: (r=11, s=26)
A[0]=3b598a79  B[0]=c915e2aa  C[0]=1658e9f7  D[0]=c9561e0f
A[1]=14be437b  B[1]=f30eb0b2  C[1]=d6e46a8f  D[1]=b4c31ab2
A[2]=6afe7566  B[2]=a43c420b  C[2]=a63a038c  D[2]=d9838fa7
A[3]=7cfd6c21  B[3]=bc2c870b  C[3]=4b32c6f6  D[3]=88a04b92

Step 12: (r=26, s= 4)
A[0]=93df282b  B[0]=e4ed6629  C[0]=c915e2aa  D[0]=1658e9f7
A[1]=2e15e48d  B[1]=ec52f90d  C[1]=f30eb0b2  D[1]=d6e46a8f
A[2]=f24eea73  B[2]=99abf9d5  C[2]=a43c420b  D[2]=a63a038c
A[3]=bbe34b1a  B[3]=85f3f5b0  C[3]=bc2c870b  D[3]=4b32c6f6

Step 13: (r= 4, s=23)
A[0]=61358ae7  B[0]=3df282b9  C[0]=e4ed6629  D[0]=c915e2aa
A[1]=b3be9243  B[1]=e15e48d2  C[1]=ec52f90d  D[1]=f30eb0b2
A[2]=32063b1e  B[2]=24eea73f  C[2]=99abf9d5  D[2]=a43c420b
A[3]=cd8c051b  B[3]=be34b1ab  C[3]=85f3f5b0  D[3]=bc2c870b

Step 14: (r=23, s=11)
A[0]=368d9a8a  B[0]=73b09ac5  C[0]=3df282b9  D[0]=e4ed6629
A[1]=6377d2f2  B[1]=21d9df49  C[1]=e15e48d2  D[1]=ec52f90d
A[2]=dc18bacf  B[2]=8f19031d  C[2]=24eea73f  D[2]=99abf9d5
A[3]=b627539c  B[3]=8de6c602  C[3]=be34b1ab  D[3]=85f3f5b0

Step 15: (r=11, s=26)
A[0]=1e31d7a7  B[0]=6cd451b4  C[0]=73b09ac5  D[0]=3df282b9
A[1]=ec21bd99  B[1]=be97931b  C[1]=21d9df49  D[1]=e15e48d2
A[2]=8e9dccbe  B[2]=c5d67ee0  C[2]=8f19031d  D[2]=24eea73f
A[3]=fffeb70a  B[3]=3a9ce5b1  C[3]=8de6c602  D[3]=be34b1ab

Step 16: (r=19, s=28)
A[0]=5203045b  B[0]=bd38f18e  C[0]=6cd451b4  D[0]=73b09ac5
A[1]=4185e412  B[1]=eccf610d  C[1]=be97931b  D[1]=21d9df49
```

```
A[2]=5036a22c  B[2]=65f474ee  C[2]=c5d67ee0  D[2]=8f19031d
A[3]=d2cdb4f1  B[3]=b857fff5  C[3]=3a9ce5b1  D[3]=8de6c602

Step 17: (r=28, s= 7)
A[0]=f9dab219  B[0]=b5203045  C[0]=bd38f18e  D[0]=6cd451b4
A[1]=28543261  B[1]=24185e41  C[1]=eccf610d  D[1]=be97931b
A[2]=a602cacc  B[2]=c5036a22  C[2]=65f474ee  D[2]=c5d67ee0
A[3]=a36af76f  B[3]=1d2cdb4f  C[3]=b857fff5  D[3]=3a9ce5b1

Step 18: (r= 7, s=22)
A[0]=b263f482  B[0]=ed590cfc  C[0]=b5203045  D[0]=bd38f18e
A[1]=fc28d271  B[1]=2a193094  C[1]=24185e41  D[1]=eccf610d
A[2]=7b4d25e1  B[2]=01656653  C[2]=c5036a22  D[2]=65f474ee
A[3]=18a93c71  B[3]=b57bb7d1  C[3]=1d2cdb4f  D[3]=b857fff5

Step 19: (r=22, s=19)
A[0]=2af9e718  B[0]=20ac98fd  C[0]=ed590cfc  D[0]=b5203045
A[1]=7e52586f  B[1]=9c7f0a34  C[1]=2a193094  D[1]=24185e41
A[2]=b6037714  B[2]=785ed349  C[2]=01656653  D[2]=c5036a22
A[3]=ae851f04  B[3]=1c462a4f  C[3]=b57bb7d1  D[3]=1d2cdb4f

Step 20: (r=19, s=28)
A[0]=953bda87  B[0]=38c157cf  C[0]=20ac98fd  D[0]=ed590cfc
A[1]=41d0c47e  B[1]=c37bf292  C[1]=9c7f0a34  D[1]=2a193094
A[2]=ea6f6f49  B[2]=b8a5b01b  C[2]=785ed349  D[2]=01656653
A[3]=1a54057c  B[3]=f8257428  C[3]=1c462a4f  D[3]=b57bb7d1

Step 21: (r=28, s= 7)
A[0]=5b982185  B[0]=7953bda8  C[0]=38c157cf  D[0]=20ac98fd
A[1]=9bb89632  B[1]=e41d0c47  C[1]=c37bf292  D[1]=9c7f0a34
A[2]=0095ef8f  B[2]=9ea6f6f4  C[2]=b8a5b01b  D[2]=785ed349
A[3]=68878731  B[3]=c1a54057  C[3]=f8257428  D[3]=1c462a4f

Step 22: (r= 7, s=22)
A[0]=f3714441  B[0]=cc10c2ad  C[0]=7953bda8  D[0]=38c157cf
A[1]=3634dc42  B[1]=dc4b194d  C[1]=e41d0c47  D[1]=c37bf292
A[2]=fb3d9cb0  B[2]=4af7c780  C[2]=9ea6f6f4  D[2]=b8a5b01b
A[3]=adf8bbe1  B[3]=43c398b4  C[3]=c1a54057  D[3]=f8257428

Step 23: (r=22, s=19)
A[0]=cb05a502  B[0]=107cdc51  C[0]=cc10c2ad  D[0]=7953bda8
A[1]=b433f5fb  B[1]=108d8d37  C[1]=dc4b194d  D[1]=e41d0c47
A[2]=57bb6663  B[2]=2c3ecf67  C[2]=4af7c780  D[2]=9ea6f6f4
A[3]=37f39eff  B[3]=f86b7e2e  C[3]=43c398b4  D[3]=c1a54057

Step 24: (r=15, s= 5)
A[0]=bf0f4dc7  B[0]=d2816582  C[0]=107cdc51  D[0]=cc10c2ad
A[1]=5281c947  B[1]=fafdda19  C[1]=108d8d37  D[1]=dc4b194d
A[2]=438b679a  B[2]=b331abdd  C[2]=2c3ecf67  D[2]=4af7c780
```

```
A[3]=7d69cc6b  B[3]=cf7f9bf9  C[3]=f86b7e2e  D[3]=43c398b4

Step 25: (r= 5, s=29)
A[0]=c8bafad2  B[0]=e1e9b8f7  C[0]=d2816582  D[0]=107cdc51
A[1]=e6e8564b  B[1]=503928ea  C[1]=fafdda19  D[1]=108d8d37
A[2]=f64e2248  B[2]=716cf348  C[2]=b331abdd  D[2]=2c3ecf67
A[3]=9d2e087f  B[3]=ad398d6f  C[3]=cf7f9bf9  D[3]=f86b7e2e

Step 26: (r=29, s= 9)
A[0]=5c02c29d  B[0]=59175f5a  C[0]=e1e9b8f7  D[0]=d2816582
A[1]=3efa5d15  B[1]=7cdd0ac9  C[1]=503928ea  D[1]=fafdda19
A[2]=93542392  B[2]=1ec9c449  C[2]=716cf348  D[2]=b331abdd
A[3]=090db727  B[3]=f3a5c10f  C[3]=ad398d6f  D[3]=cf7f9bf9

Step 27: (r= 9, s=15)
A[0]=cac8d8d9  B[0]=05853ab8  C[0]=59175f5a  D[0]=e1e9b8f7
A[1]=9fab8742  B[1]=f4ba2a7d  C[1]=7cdd0ac9  D[1]=503928ea
A[2]=4824c8f8  B[2]=a8472526  C[2]=1ec9c449  D[2]=716cf348
A[3]=d63895fd  B[3]=1b6e4e12  C[3]=f3a5c10f  D[3]=ad398d6f

Step 28: (r=15, s= 5)
A[0]=68ba92a3  B[0]=6c6ce564  C[0]=05853ab8  D[0]=59175f5a
A[1]=aa27e356  B[1]=c3a14fd5  C[1]=f4ba2a7d  D[1]=7cdd0ac9
A[2]=90bcd1c4  B[2]=647c2412  C[2]=a8472526  D[2]=1ec9c449
A[3]=4ce36387  B[3]=4afeeb1c  C[3]=1b6e4e12  D[3]=f3a5c10f

Step 29: (r= 5, s=29)
A[0]=449ae689  B[0]=1752546d  C[0]=6c6ce564  D[0]=05853ab8
A[1]=d4c33346  B[1]=44fc6ad5  C[1]=c3a14fd5  D[1]=f4ba2a7d
A[2]=27d5f8fc  B[2]=179a3892  C[2]=647c2412  D[2]=a8472526
A[3]=b9c74361  B[3]=9c6c70e9  C[3]=4afeeb1c  D[3]=1b6e4e12

Step 30: (r=29, s= 9)
A[0]=f7f155e1  B[0]=28935cd1  C[0]=1752546d  D[0]=6c6ce564
A[1]=0af515c4  B[1]=da986668  C[1]=44fc6ad5  D[1]=c3a14fd5
A[2]=6c306bd0  B[2]=84fabf1f  C[2]=179a3892  D[2]=647c2412
A[3]=d4c0616f  B[3]=3738e86c  C[3]=9c6c70e9  D[3]=4afeeb1c

Step 31: (r= 9, s=15)
A[0]=5a0716eb  B[0]=e2abc3ef  C[0]=28935cd1  D[0]=1752546d
A[1]=43f0ff16  B[1]=ea2b8815  C[1]=da986668  D[1]=44fc6ad5
A[2]=37ced339  B[2]=60d7a0d8  C[2]=84fabf1f  D[2]=179a3892
A[3]=2d84da34  B[3]=80c2dfa9  C[3]=3738e86c  D[3]=9c6c70e9

Feistel Step 0: (r=15, s= 5)
A[0]=8242f17a  B[0]=8b75ad03  C[0]=e2abc3ef  D[0]=28935cd1
A[1]=ed0d86f7  B[1]=7f8b21f8  C[1]=ea2b8815  D[1]=da986668
A[2]=09502d09  B[2]=699c9be7  C[2]=60d7a0d8  D[2]=84fabf1f
A[3]=c8ca33a1  B[3]=6d1a16c2  C[3]=80c2dfa9  D[3]=3738e86c
```

```
Feistel Step 1: (r= 5, s=29)
A[0]=ba2af3c2  B[0]=485e2f50  C[0]=8b75ad03  D[0]=e2abc3ef
A[1]=53eb134b  B[1]=a1b0defd  C[1]=7f8b21f8  D[1]=ea2b8815
A[2]=f172f1d4  B[2]=2a05a121  C[2]=699c9be7  D[2]=60d7a0d8
A[3]=d65bdb99  B[3]=19467439  C[3]=6d1a16c2  D[3]=80c2dfa9

Feistel Step 2: (r=29, s= 9)
A[0]=87db189c  B[0]=57455e78  C[0]=485e2f50  D[0]=8b75ad03
A[1]=684e7c81  B[1]=6a7d6269  C[1]=a1b0defd  D[1]=7f8b21f8
A[2]=1268e61d  B[2]=9e2e5e3a  C[2]=2a05a121  D[2]=699c9be7
A[3]=2ebeac56  B[3]=3acb7b73  C[3]=19467439  D[3]=6d1a16c2

Feistel Step 3: (r= 9, s=15)
A[0]=22c8531a  B[0]=b631390f  C[0]=57455e78  D[0]=485e2f50
A[1]=3e7d3720  B[1]=9cf902d0  C[1]=6a7d6269  D[1]=a1b0defd
A[2]=103b789a  B[2]=d1cc3a24  C[2]=9e2e5e3a  D[2]=2a05a121
A[3]=5a991062  B[3]=7d58ac5d  C[3]=3acb7b73  D[3]=19467439
```

Compression Function Output

```
A[0]=22c8531a  B[0]=b631390f  C[0]=57455e78  D[0]=485e2f50
A[1]=3e7d3720  B[1]=9cf902d0  C[1]=6a7d6269  D[1]=a1b0defd
A[2]=103b789a  B[2]=d1cc3a24  C[2]=9e2e5e3a  D[2]=2a05a121
A[3]=5a991062  B[3]=7d58ac5d  C[3]=3acb7b73  D[3]=19467439
```

Hash Function Output

```
1a53c82220377d3e9a783b106210995a0f3931b6d002f99c243accd15dac587d
```

6.2.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
```

```
y[ 24.. 31] =  124   92  110  120  191  202  211   82
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
Z[17] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
Z[18] = a2412723  e4b2ea28  71c5a8a0  9755ece3
Z[19] = 4aa270dc  949a641e  a06fc3ee  0f79d622
Z[20] = ef9ed622  fb73aa72  20c4065f  eeb5a413
Z[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
Z[22] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
Z[23] = 8d522551  05769e9d  cfc33126  f8b8237f
Z[24] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
Z[25] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
Z[26] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
Z[27] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
Z[28] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
Z[29] = ece3e025  39573ecd  edcc320f  0831d70b
Z[30] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
Z[31] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
W[17] = a2412723  e4b2ea28  71c5a8a0  9755ece3
W[18] = 8d522551  05769e9d  cfc33126  f8b8237f
W[19] = ef9ed622  fb73aa72  20c4065f  eeb5a413
W[20] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
W[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
W[22] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
W[23] = 4aa270dc  949a641e  a06fc3ee  0f79d622
W[24] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
W[25] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
W[26] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
W[27] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
W[28] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
W[29] = ece3e025  39573ecd  edcc320f  0831d70b
W[30] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
W[31] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
```

Feistel Steps

```
IV :
A[0]=96301f14  B[0]=75ad94b4  C[0]=2d83bbab  D[0]=5731b59d
A[1]=64f69407  B[1]=8b618939  C[1]=0c195501  D[1]=abff7dd4
A[2]=8450cc02  B[2]=5a13cb35  C[2]=cc0782ba  D[2]=db4cd0f5
A[3]=42c538e3  B[3]=26141ded  C[3]=356688a2  D[3]=7240ec03

IV XOR M :
A[0]=95321e14  B[0]=66bf85a4  C[0]=0ea19a8b  D[0]=640384ad
A[1]=63f09103  B[1]=9c779c2d  C[1]=2b3f7025  D[1]=9cc948e0
A[2]=8f5ac50a  B[2]=4109d22d  C[2]=e72dab92  D[2]=e076e9cd
A[3]=4dcb35ef  B[3]=390a00f1  C[3]=1a48a58e  D[3]=4d7ed13f

Step  0: (r= 3, s=20)
```

```
A[0]=9f69cdf9  B[0]=a990f0a4  C[0]=66bf85a4  D[0]=0ea19a8b
A[1]=cc5211a3  B[1]=1f84881b  C[1]=9c779c2d  D[1]=2b3f7025
A[2]=059f4757  B[2]=7ad62854  C[2]=4109d22d  D[2]=e72dab92
A[3]=3bc570f4  B[3]=6e59af7a  C[3]=390a00f1  D[3]=1a48a58e

Step  1: (r=20, s=14)
A[0]=5e1ee7b9  B[0]=df99f69c  C[0]=a990f0a4  D[0]=66bf85a4
A[1]=fe991fe4  B[1]=1a3cc521  C[1]=1f84881b  D[1]=9c779c2d
A[2]=d836b415  B[2]=757059f4  C[2]=7ad62854  D[2]=4109d22d
A[3]=171e47d1  B[3]=0f43bc57  C[3]=6e59af7a  D[3]=390a00f1

Step  2: (r=14, s=27)
A[0]=d3c25aa6  B[0]=b9ee5787  C[0]=df99f69c  D[0]=a990f0a4
A[1]=598fb103  B[1]=47f93fa6  C[1]=1a3cc521  D[1]=1f84881b
A[2]=54bba6e3  B[2]=ad05760d  C[2]=757059f4  D[2]=7ad62854
A[3]=110ada5f  B[3]=91f445c7  C[3]=0f43bc57  D[3]=6e59af7a

Step  3: (r=27, s= 3)
A[0]=8a160fe1  B[0]=369e12d5  C[0]=b9ee5787  D[0]=df99f69c
A[1]=b887b5fe  B[1]=1acc7d88  C[1]=47f93fa6  D[1]=1a3cc521
A[2]=16512320  B[2]=1aa5dd37  C[2]=ad05760d  D[2]=757059f4
A[3]=39fca22a  B[3]=f88856d2  C[3]=91f445c7  D[3]=0f43bc57

Step  4: (r= 3, s=20)
A[0]=84699597  B[0]=50b07f0c  C[0]=369e12d5  D[0]=b9ee5787
A[1]=0a4dd01b  B[1]=c43daff5  C[1]=1acc7d88  D[1]=47f93fa6
A[2]=51dbe3e0  B[2]=b2891900  C[2]=1aa5dd37  D[2]=ad05760d
A[3]=453b673d  B[3]=cfe51151  C[3]=f88856d2  D[3]=91f445c7

Step  5: (r=20, s=14)
A[0]=43c1cb15  B[0]=59784699  C[0]=50b07f0c  D[0]=369e12d5
A[1]=c1b234bf  B[1]=01b0a4dd  C[1]=c43daff5  D[1]=1acc7d88
A[2]=240d006c  B[2]=3e051dbe  C[2]=b2891900  D[2]=1aa5dd37
A[3]=601c74a3  B[3]=73d453b6  C[3]=cfe51151  D[3]=f88856d2

Step  6: (r=14, s=27)
A[0]=03884648  B[0]=72c550f0  C[0]=59784699  D[0]=50b07f0c
A[1]=59b4b493  B[1]=8d2ff06c  C[1]=01b0a4dd  D[1]=c43daff5
A[2]=a6707e3c  B[2]=401b0903  C[2]=3e051dbe  D[2]=b2891900
A[3]=af824d2a  B[3]=1d28d807  C[3]=73d453b6  D[3]=cfe51151

Step  7: (r=27, s= 3)
A[0]=36584113  B[0]=401c4232  C[0]=72c550f0  D[0]=59784699
A[1]=f0cdaa15  B[1]=9acda5a4  C[1]=8d2ff06c  D[1]=01b0a4dd
A[2]=0c5b15ef  B[2]=e53383f1  C[2]=401b0903  D[2]=3e051dbe
A[3]=47805782  B[3]=557c1269  C[3]=1d28d807  D[3]=73d453b6

Step  8: (r=26, s= 4)
A[0]=04b6fe81  B[0]=4cd96104  C[0]=401c4232  D[0]=72c550f0
```

```
A[1]=305b064d  B[1]=57c336a8  C[1]=9acda5a4  D[1]=8d2ff06c
A[2]=768e1682  B[2]=bc316c57  C[2]=e53383f1  D[2]=401b0903
A[3]=e407e03c  B[3]=091e015e  C[3]=557c1269  D[3]=1d28d807

Step  9: (r= 4, s=23)
A[0]=9b5e551d  B[0]=4b6fe810  C[0]=4cd96104  D[0]=401c4232
A[1]=a77e206f  B[1]=05b064d3  C[1]=57c336a8  D[1]=9acda5a4
A[2]=96094531  B[2]=68e16827  C[2]=bc316c57  D[2]=e53383f1
A[3]=5c3c84ce  B[3]=407e03ce  C[3]=091e015e  D[3]=557c1269

Step 10: (r=23, s=11)
A[0]=547dc49f  B[0]=8ecdaf2a  C[0]=4b6fe810  D[0]=4cd96104
A[1]=7f915ad0  B[1]=37d3bf10  C[1]=05b064d3  D[1]=57c336a8
A[2]=9760fee1  B[2]=98cb04a2  C[2]=68e16827  D[2]=bc316c57
A[3]=3f021394  B[3]=672e1e42  C[3]=407e03ce  D[3]=091e015e

Step 11: (r=11, s=26)
A[0]=dd7bf08f  B[0]=ee24faa3  C[0]=8ecdaf2a  D[0]=4b6fe810
A[1]=93c497f0  B[1]=8ad683fc  C[1]=37d3bf10  D[1]=05b064d3
A[2]=87e060f4  B[2]=07f70cbb  C[2]=98cb04a2  D[2]=68e16827
A[3]=a8961146  B[3]=109ca1f8  C[3]=672e1e42  D[3]=407e03ce

Step 12: (r=26, s= 4)
A[0]=338e30df  B[0]=3f75efc2  C[0]=ee24faa3  D[0]=8ecdaf2a
A[1]=6f74ada9  B[1]=c24f125f  C[1]=8ad683fc  D[1]=37d3bf10
A[2]=b355c2b3  B[2]=d21f8183  C[2]=07f70cbb  D[2]=98cb04a2
A[3]=8fe80555  B[3]=1aa25845  C[3]=109ca1f8  D[3]=672e1e42

Step 13: (r= 4, s=23)
A[0]=6ebb8e20  B[0]=38e30df3  C[0]=3f75efc2  D[0]=ee24faa3
A[1]=4d182dff  B[1]=f74ada96  C[1]=c24f125f  D[1]=8ad683fc
A[2]=9671e58f  B[2]=355c2b3b  C[2]=d21f8183  D[2]=07f70cbb
A[3]=ba8f069c  B[3]=fe805558  C[3]=1aa25845  D[3]=109ca1f8

Step 14: (r=23, s=11)
A[0]=59a73e43  B[0]=10375dc7  C[0]=38e30df3  D[0]=3f75efc2
A[1]=ac14a4a9  B[1]=ffa68c16  C[1]=f74ada96  D[1]=c24f125f
A[2]=bea22197  B[2]=c7cb38f2  C[2]=355c2b3b  D[2]=d21f8183
A[3]=ad5129af  B[3]=4e5d4783  C[3]=fe805558  D[3]=1aa25845

Step 15: (r=11, s=26)
A[0]=4f715b2f  B[0]=39f21acd  C[0]=10375dc7  D[0]=38e30df3
A[1]=a824978f  B[1]=a5254d60  C[1]=ffa68c16  D[1]=f74ada96
A[2]=877500cf  B[2]=110cbdf5  C[2]=c7cb38f2  D[2]=355c2b3b
A[3]=26aca805  B[3]=894d7d6a  C[3]=4e5d4783  D[3]=fe805558

Step 16: (r=19, s=28)
A[0]=c2d4b04c  B[0]=d97a7b8a  C[0]=39f21acd  D[0]=10375dc7
A[1]=9c304635  B[1]=bc7d4124  C[1]=a5254d60  D[1]=ffa68c16
```

```
A[2]=d353b46e  B[2]=067c3ba8  C[2]=110cbdf5  D[2]=c7cb38f2
A[3]=bedff63f  B[3]=40293565  C[3]=894d7d6a  D[3]=4e5d4783

Step 17: (r=28, s= 7)
A[0]=e294f51b  B[0]=cc2d4b04  C[0]=d97a7b8a  D[0]=39f21acd
A[1]=c34dd0b3  B[1]=59c30463  C[1]=bc7d4124  D[1]=a5254d60
A[2]=c2baf0a1  B[2]=ed353b46  C[2]=067c3ba8  D[2]=110cbdf5
A[3]=b7fbea56  B[3]=fbedff63  C[3]=40293565  D[3]=894d7d6a

Step 18: (r= 7, s=22)
A[0]=8e908683  B[0]=4a7a8df1  C[0]=cc2d4b04  D[0]=d97a7b8a
A[1]=a682541c  B[1]=a6e859e1  C[1]=59c30463  D[1]=bc7d4124
A[2]=86de7c65  B[2]=5d7850e1  C[2]=ed353b46  D[2]=067c3ba8
A[3]=5d9809d9  B[3]=fdf52b5b  C[3]=fbedff63  D[3]=40293565

Step 19: (r=22, s=19)
A[0]=12ea5257  B[0]=a0e3a421  C[0]=4a7a8df1  D[0]=cc2d4b04
A[1]=56252393  B[1]=0729a095  C[1]=a6e859e1  D[1]=59c30463
A[2]=4c3849ed  B[2]=1961b79f  C[2]=5d7850e1  D[2]=ed353b46
A[3]=cec3173b  B[3]=76576602  C[3]=fdf52b5b  D[3]=fbedff63

Step 20: (r=19, s=28)
A[0]=1eaad3c2  B[0]=92b89752  C[0]=a0e3a421  D[0]=4a7a8df1
A[1]=a3b44f2e  B[1]=1c9ab129  C[1]=0729a095  D[1]=a6e859e1
A[2]=2b2e27dd  B[2]=4f6a61c2  C[2]=1961b79f  D[2]=5d7850e1
A[3]=e34ded4f  B[3]=b9de7618  C[3]=76576602  D[3]=fdf52b5b

Step 21: (r=28, s= 7)
A[0]=e00df700  B[0]=21eaad3c  C[0]=92b89752  D[0]=a0e3a421
A[1]=972ec232  B[1]=ea3b44f2  C[1]=1c9ab129  D[1]=0729a095
A[2]=568fd7c0  B[2]=d2b2e27d  C[2]=4f6a61c2  D[2]=1961b79f
A[3]=346dab5f  B[3]=fe34ded4  C[3]=b9de7618  D[3]=76576602

Step 22: (r= 7, s=22)
A[0]=83e9fa58  B[0]=06fb8070  C[0]=21eaad3c  D[0]=92b89752
A[1]=d1182e96  B[1]=9761194b  C[1]=ea3b44f2  D[1]=1c9ab129
A[2]=087cd912  B[2]=47ebe02b  C[2]=d2b2e27d  D[2]=4f6a61c2
A[3]=2e1c016f  B[3]=36d5af9a  C[3]=fe34ded4  D[3]=b9de7618

Step 23: (r=22, s=19)
A[0]=c9b9296b  B[0]=9620fa7e  C[0]=06fb8070  D[0]=21eaad3c
A[1]=6c97aa71  B[1]=a5b4460b  C[1]=9761194b  D[1]=ea3b44f2
A[2]=c57a9126  B[2]=44821f36  C[2]=47ebe02b  D[2]=d2b2e27d
A[3]=86748171  B[3]=5bcb8700  C[3]=36d5af9a  D[3]=fe34ded4

Step 24: (r=15, s= 5)
A[0]=1c2d530a  B[0]=94b5e4dc  C[0]=9620fa7e  D[0]=06fb8070
A[1]=bc8988af  B[1]=d538b64b  C[1]=a5b4460b  D[1]=9761194b
A[2]=eb7b5f36  B[2]=489362bd  C[2]=44821f36  D[2]=47ebe02b
```

```
A[3]=b1fe96b0  B[3]=40b8c33a  C[3]=5bcb8700  D[3]=36d5af9a

Step 25: (r= 5, s=29)
A[0]=43dbf6ef  B[0]=85aa6143  C[0]=94b5e4dc  D[0]=9620fa7e
A[1]=6e9dcbf9  B[1]=913115f7  C[1]=d538b64b  D[1]=a5b4460b
A[2]=ad313739  B[2]=6f6be6dd  C[2]=489362bd  D[2]=44821f36
A[3]=2145e5a4  B[3]=3fd2d616  C[3]=40b8c33a  D[3]=5bcb8700

Step 26: (r=29, s= 9)
A[0]=79a5d1a7  B[0]=e87b7edd  C[0]=85aa6143  D[0]=94b5e4dc
A[1]=de0ab2dc  B[1]=2dd3b97f  C[1]=913115f7  D[1]=d538b64b
A[2]=9ce61e06  B[2]=35a626e7  C[2]=6f6be6dd  D[2]=489362bd
A[3]=68841be9  B[3]=8428bcb4  C[3]=3fd2d616  D[3]=40b8c33a

Step 27: (r= 9, s=15)
A[0]=0dcdce1e  B[0]=4ba34ef3  C[0]=e87b7edd  D[0]=85aa6143
A[1]=4c38a088  B[1]=1565b9bc  C[1]=2dd3b97f  D[1]=913115f7
A[2]=585309c4  B[2]=cc3c0d39  C[2]=35a626e7  D[2]=6f6be6dd
A[3]=d487b8b4  B[3]=0837d2d1  C[3]=8428bcb4  D[3]=3fd2d616

Step 28: (r=15, s= 5)
A[0]=ba84a1e0  B[0]=e70f06e6  C[0]=4ba34ef3  D[0]=e87b7edd
A[1]=1769c996  B[1]=5044261c  C[1]=1565b9bc  D[1]=2dd3b97f
A[2]=fc52c0a6  B[2]=84e22c29  C[2]=cc3c0d39  D[2]=35a626e7
A[3]=df8a347a  B[3]=dc5a6a43  C[3]=0837d2d1  D[3]=8428bcb4

Step 29: (r= 5, s=29)
A[0]=2274e19b  B[0]=50943c17  C[0]=e70f06e6  D[0]=4ba34ef3
A[1]=00d8a398  B[1]=ed3932c2  C[1]=5044261c  D[1]=1565b9bc
A[2]=4e90c8ba  B[2]=8a5814df  C[2]=84e22c29  D[2]=cc3c0d39
A[3]=3a47d384  B[3]=f1468f5b  C[3]=dc5a6a43  D[3]=0837d2d1

Step 30: (r=29, s= 9)
A[0]=feb5b623  B[0]=644e9c33  C[0]=50943c17  D[0]=e70f06e6
A[1]=5fca7757  B[1]=001b1473  C[1]=ed3932c2  D[1]=5044261c
A[2]=01b8f536  B[2]=49d21917  C[2]=8a5814df  D[2]=84e22c29
A[3]=b938dc1c  B[3]=8748fa70  C[3]=f1468f5b  D[3]=dc5a6a43

Step 31: (r= 9, s=15)
A[0]=578fa94d  B[0]=6b6c47fd  C[0]=644e9c33  D[0]=50943c17
A[1]=c1289f57  B[1]=94eeaebf  C[1]=001b1473  D[1]=ed3932c2
A[2]=754b558f  B[2]=71ea6c03  C[2]=49d21917  D[2]=8a5814df
A[3]=8ad1446a  B[3]=71b83972  C[3]=8748fa70  D[3]=f1468f5b

Feistel Step 0: (r=15, s= 5)
A[0]=91b9f5dd  B[0]=d4a6abc7  C[0]=6b6c47fd  D[0]=644e9c33
A[1]=f8325abf  B[1]=4fabe094  C[1]=94eeaebf  D[1]=001b1473
A[2]=b29ae3f9  B[2]=aac7baa5  C[2]=71ea6c03  D[2]=49d21917
A[3]=093701ce  B[3]=a2354568  C[3]=71b83972  D[3]=8748fa70
```

```
Feistel Step 1: (r= 5, s=29)
A[0]=edf899cf  B[0]=373ebbb2  C[0]=d4a6abc7  D[0]=6b6c47fd
A[1]=41edaa09  B[1]=064b57ff  C[1]=4fabe094  D[1]=94eeaebf
A[2]=2837ce0f  B[2]=535c7f36  C[2]=aac7baa5  D[2]=71ea6c03
A[3]=aa0ea239  B[3]=26e039c1  C[3]=a2354568  D[3]=71b83972

Feistel Step 2: (r=29, s= 9)
A[0]=85bc0add  B[0]=fdbf1339  C[0]=373ebbb2  D[0]=d4a6abc7
A[1]=8b93b51f  B[1]=283db541  C[1]=064b57ff  D[1]=4fabe094
A[2]=c21c9bc8  B[2]=e506f9c1  C[2]=535c7f36  D[2]=aac7baa5
A[3]=9e0dbecb  B[3]=3541d447  C[3]=26e039c1  D[3]=a2354568

Feistel Step 3: (r= 9, s=15)
A[0]=c387834f  B[0]=7815bb0b  C[0]=fdbf1339  D[0]=373ebbb2
A[1]=c6a21b3e  B[1]=276a3f17  C[1]=283db541  D[1]=064b57ff
A[2]=3cdde6b7  B[2]=39379184  C[2]=e506f9c1  D[2]=535c7f36
A[3]=0ac163c2  B[3]=1b7d973c  C[3]=3541d447  D[3]=26e039c1
```

Compression Function Output

```
A[0]=c387834f  B[0]=7815bb0b  C[0]=fdbf1339  D[0]=373ebbb2
A[1]=c6a21b3e  B[1]=276a3f17  C[1]=283db541  D[1]=064b57ff
A[2]=3cdde6b7  B[2]=39379184  C[2]=e506f9c1  D[2]=535c7f36
A[3]=0ac163c2  B[3]=1b7d973c  C[3]=3541d447  D[3]=26e039c1
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
```

```
y[ 88.. 95] =  145  170  131  192  136  139   53   98
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc5c03a4  2ac7d539  53bcac44  14efeb11
Z[17] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
Z[18] = 369cc964  9e9d6163  d9c6263a  2ac7d539
Z[19] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
Z[20] = e2e01d20  c6a93957  6c4f93b1  452cbad4
Z[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
Z[22] = c964369c  452cbad4  4aa2b55e  ac4453bc
Z[23] = 0a03f5fd  aa72558e  f0870f79  afe85018
Z[24] = 48d0b730  d70b28f5  3fb6c04a  db982468
Z[25] = e10e1ef2  6e2191df  d1952e6b  131dece3
Z[26] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
Z[27] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
Z[28] = 2ac7d539  624c9db4  641e9be2  263ad9c6
Z[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
Z[30] = c3053cfb  95836a7d  ab5b54a5  74808b80
Z[31] = 197ce684  de5321ad  607a9f86  2ac7d539
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
```

```
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
W[17] = 369cc964  9e9d6163  d9c6263a  2ac7d539
W[18] = 0a03f5fd  aa72558e  f0870f79  afe85018
W[19] = e2e01d20  c6a93957  6c4f93b1  452cbad4
W[20] = c964369c  452cbad4  4aa2b55e  ac4453bc
W[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
W[22] = fc5c03a4  2ac7d539  53bcac44  14efeb11
W[23] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
W[24] = c3053cfb  95836a7d  ab5b54a5  74808b80
W[25] = 48d0b730  d70b28f5  3fb6c04a  db982468
W[26] = e10e1ef2  6e2191df  d1952e6b  131dece3
W[27] = 197ce684  de5321ad  607a9f86  2ac7d539
W[28] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
W[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
W[30] = 2ac7d539  624c9db4  641e9be2  263ad9c6
W[31] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
```

Feistel Steps

```
IV :
A[0]=c387834f  B[0]=7815bb0b  C[0]=fdbf1339  D[0]=373ebbb2
A[1]=c6a21b3e  B[1]=276a3f17  C[1]=283db541  D[1]=064b57ff
A[2]=3cdde6b7  B[2]=39379184  C[2]=e506f9c1  D[2]=535c7f36
A[3]=0ac163c2  B[3]=1b7d973c  C[3]=3541d447  D[3]=26e039c1

IV XOR M :
A[0]=c387814f  B[0]=7815bb0b  C[0]=fdbf1339  D[0]=373ebbb2
A[1]=c6a21b3e  B[1]=276a3f17  C[1]=283db541  D[1]=064b57ff
A[2]=3cdde6b7  B[2]=39379184  C[2]=e506f9c1  D[2]=535c7f36
A[3]=0ac163c2  B[3]=1b7d973c  C[3]=3541d447  D[3]=26e039c1

Step  0: (r= 3, s=20)
A[0]=95e9f24c  B[0]=1c3c0a7e  C[0]=7815bb0b  D[0]=fdbf1339
A[1]=34cd9dad  B[1]=3510d9f6  C[1]=276a3f17  D[1]=283db541
A[2]=85caed7c  B[2]=e6ef35b9  C[2]=39379184  D[2]=e506f9c1
A[3]=b9e08707  B[3]=560b1e10  C[3]=1b7d973c  D[3]=3541d447

Step  1: (r=20, s=14)
A[0]=6a418747  B[0]=24c95e9f  C[0]=1c3c0a7e  D[0]=7815bb0b
A[1]=fefe8b03  B[1]=dad34cd9  C[1]=3510d9f6  D[1]=276a3f17
```

```
A[2]=21d757ed  B[2]=d7c85cae  C[2]=e6ef35b9  D[2]=39379184
A[3]=a6124790  B[3]=707b9e08  C[3]=560b1e10  D[3]=1b7d973c

Step  2: (r=14, s=27)
A[0]=16571620  B[0]=61d1da90  C[0]=24c95e9f  D[0]=1c3c0a7e
A[1]=7f195c25  B[1]=a2c0ffbf  C[1]=dad34cd9  D[1]=3510d9f6
A[2]=b8587fa2  B[2]=d5fb4875  C[2]=d7c85cae  D[2]=e6ef35b9
A[3]=4f15e7b4  B[3]=91e42984  C[3]=707b9e08  D[3]=560b1e10

Step  3: (r=27, s= 3)
A[0]=1b5c9207  B[0]=00b2b8b1  C[0]=61d1da90  D[0]=24c95e9f
A[1]=62b4d172  B[1]=2bf8cae1  C[1]=a2c0ffbf  D[1]=dad34cd9
A[2]=8edf9aae  B[2]=15c2c3fd  C[2]=d5fb4875  D[2]=d7c85cae
A[3]=75e2780f  B[3]=a278af3d  C[3]=91e42984  D[3]=707b9e08

Step  4: (r= 3, s=20)
A[0]=2977b182  B[0]=dae49038  C[0]=00b2b8b1  D[0]=61d1da90
A[1]=429e5d8a  B[1]=15a68b93  C[1]=2bf8cae1  D[1]=a2c0ffbf
A[2]=ee55d11e  B[2]=76fcd574  C[2]=15c2c3fd  D[2]=d5fb4875
A[3]=45b49688  B[3]=af13c07b  C[3]=a278af3d  D[3]=91e42984

Step  5: (r=20, s=14)
A[0]=3f3980c8  B[0]=1822977b  C[0]=dae49038  D[0]=00b2b8b1
A[1]=4c563e39  B[1]=d8a429e5  C[1]=15a68b93  D[1]=2bf8cae1
A[2]=2466f130  B[2]=11eee55d  C[2]=76fcd574  D[2]=15c2c3fd
A[3]=91c3c925  B[3]=68845b49  C[3]=af13c07b  D[3]=a278af3d

Step  6: (r=14, s=27)
A[0]=5a5be7e5  B[0]=60320fce  C[0]=1822977b  D[0]=dae49038
A[1]=c208cba6  B[1]=8f8e5315  C[1]=d8a429e5  D[1]=15a68b93
A[2]=074924f7  B[2]=bc4c0919  C[2]=11eee55d  D[2]=76fcd574
A[3]=285b6a60  B[3]=f2496470  C[3]=68845b49  D[3]=af13c07b

Step  7: (r=27, s= 3)
A[0]=15855249  B[0]=2ad2df3f  C[0]=60320fce  D[0]=1822977b
A[1]=4756e51f  B[1]=3610465d  C[1]=8f8e5315  D[1]=d8a429e5
A[2]=b3f36ecc  B[2]=b83a4927  C[2]=bc4c0919  D[2]=11eee55d
A[3]=7796f8cd  B[3]=0142db53  C[3]=f2496470  D[3]=68845b49

Step  8: (r=26, s= 4)
A[0]=4e2d4b6c  B[0]=24561549  C[0]=2ad2df3f  D[0]=60320fce
A[1]=fad38eff  B[1]=7d1d5b94  C[1]=3610465d  D[1]=8f8e5315
A[2]=e2607e74  B[2]=32cfcdbb  C[2]=b83a4927  D[2]=bc4c0919
A[3]=e0d59769  B[3]=35de5be3  C[3]=0142db53  D[3]=f2496470

Step  9: (r= 4, s=23)
A[0]=42aafc78  B[0]=e2d4b6c4  C[0]=24561549  D[0]=2ad2df3f
A[1]=5b47ca3f  B[1]=ad38efff  C[1]=7d1d5b94  D[1]=3610465d
A[2]=50a56743  B[2]=2607e74e  C[2]=32cfcdbb  D[2]=b83a4927
```

```
A[3]=c56668f2  B[3]=0d59769e  C[3]=35de5be3  D[3]=0142db53

Step 10: (r=23, s=11)
A[0]=1b98a981  B[0]=3c21557e  C[0]=e2d4b6c4  D[0]=24561549
A[1]=514d003c  B[1]=1fada3e5  C[1]=ad38efff  D[1]=7d1d5b94
A[2]=bddbb484  B[2]=a1a852b3  C[2]=2607e74e  D[2]=32cfcdbb
A[3]=e84fe829  B[3]=7962b334  C[3]=0d59769e  D[3]=35de5be3

Step 11: (r=11, s=26)
A[0]=82fdd294  B[0]=c54c08dc  C[0]=3c21557e  D[0]=e2d4b6c4
A[1]=47a8a8f7  B[1]=6801e28a  C[1]=1fada3e5  D[1]=ad38efff
A[2]=c96fd26c  B[2]=dda425ee  C[2]=a1a852b3  D[2]=2607e74e
A[3]=4a1b0716  B[3]=7f414f42  C[3]=7962b334  D[3]=0d59769e

Step 12: (r=26, s= 4)
A[0]=c82a8cd7  B[0]=520bf74a  C[0]=c54c08dc  D[0]=3c21557e
A[1]=f8644d9e  B[1]=dd1ea2a3  C[1]=6801e28a  D[1]=1fada3e5
A[2]=06ca9de8  B[2]=b325bf49  C[2]=dda425ee  D[2]=a1a852b3
A[3]=cea91b63  B[3]=59286c1c  C[3]=7f414f42  D[3]=7962b334

Step 13: (r= 4, s=23)
A[0]=a62682dc  B[0]=82a8cd7c  C[0]=520bf74a  D[0]=c54c08dc
A[1]=1faaee1d  B[1]=8644d9ef  C[1]=dd1ea2a3  D[1]=6801e28a
A[2]=40387278  B[2]=6ca9de80  C[2]=b325bf49  D[2]=dda425ee
A[3]=610f2955  B[3]=ea91b63c  C[3]=59286c1c  D[3]=7f414f42

Step 14: (r=23, s=11)
A[0]=de6c7795  B[0]=6e531341  C[0]=82a8cd7c  D[0]=520bf74a
A[1]=281f4d6f  B[1]=0e8fd577  C[1]=8644d9ef  D[1]=dd1ea2a3
A[2]=32df69ea  B[2]=3c201c39  C[2]=6ca9de80  D[2]=b325bf49
A[3]=ab3dc075  B[3]=aab08794  C[3]=ea91b63c  D[3]=59286c1c

Step 15: (r=11, s=26)
A[0]=0b0f7a23  B[0]=63bcaef3  C[0]=6e531341  D[0]=82a8cd7c
A[1]=e85e3434  B[1]=fa6b7940  C[1]=0e8fd577  D[1]=8644d9ef
A[2]=326f184f  B[2]=fb4f5196  C[2]=3c201c39  D[2]=6ca9de80
A[3]=4bece3ff  B[3]=ee03ad59  C[3]=aab08794  D[3]=ea91b63c

Step 16: (r=19, s=28)
A[0]=6a88c83d  B[0]=d118587b  C[0]=63bcaef3  D[0]=6e531341
A[1]=008f9966  B[1]=a1a742f1  C[1]=fa6b7940  D[1]=0e8fd577
A[2]=88d7f064  B[2]=c2799378  C[2]=fb4f5196  D[2]=3c201c39
A[3]=550a578c  B[3]=1ffa5f67  C[3]=ee03ad59  D[3]=aab08794

Step 17: (r=28, s= 7)
A[0]=5eb34f79  B[0]=d6a88c83  C[0]=d118587b  D[0]=63bcaef3
A[1]=cf9c42cc  B[1]=6008f996  C[1]=a1a742f1  D[1]=fa6b7940
A[2]=7692bf07  B[2]=488d7f06  C[2]=c2799378  D[2]=fb4f5196
A[3]=a2370ae0  B[3]=c550a578  C[3]=1ffa5f67  D[3]=ee03ad59
```

```
Step 18: (r= 7, s=22)
A[0]=0af2c097  B[0]=59a7bcaf  C[0]=d6a88c83  D[0]=d118587b
A[1]=2a20c5fe  B[1]=ce216667  C[1]=6008f996  D[1]=a1a742f1
A[2]=3ef0a039  B[2]=495f83bb  C[2]=488d7f06  D[2]=c2799378
A[3]=0fb6adc3  B[3]=1b857051  C[3]=c550a578  D[3]=1ffa5f67

Step 19: (r=22, s=19)
A[0]=1f644140  B[0]=25c2bcb0  C[0]=59a7bcaf  D[0]=d6a88c83
A[1]=36398172  B[1]=7f8a8831  C[1]=ce216667  D[1]=6008f996
A[2]=590675e8  B[2]=0e4fbc28  C[2]=495f83bb  D[2]=488d7f06
A[3]=552c0f8a  B[3]=70c3edab  C[3]=1b857051  D[3]=c550a578

Step 20: (r=19, s=28)
A[0]=0770e9c7  B[0]=0a00fb22  C[0]=25c2bcb0  D[0]=59a7bcaf
A[1]=8178bb80  B[1]=0b91b1cc  C[1]=7f8a8831  D[1]=ce216667
A[2]=4a1aa800  B[2]=af42c833  C[2]=0e4fbc28  D[2]=495f83bb
A[3]=0632a18d  B[3]=7c52a960  C[3]=70c3edab  D[3]=1b857051

Step 21: (r=28, s= 7)
A[0]=14173816  B[0]=70770e9c  C[0]=0a00fb22  D[0]=25c2bcb0
A[1]=734d582a  B[1]=08178bb8  C[1]=0b91b1cc  D[1]=7f8a8831
A[2]=b59b8c39  B[2]=04a1aa80  C[2]=af42c833  D[2]=0e4fbc28
A[3]=bbc5c15e  B[3]=d0632a18  C[3]=7c52a960  D[3]=70c3edab

Step 22: (r= 7, s=22)
A[0]=4138a2b7  B[0]=0b9c0b0a  C[0]=70770e9c  D[0]=0a00fb22
A[1]=927376d7  B[1]=a6ac1539  C[1]=08178bb8  D[1]=0b91b1cc
A[2]=0a229359  B[2]=cdc61cda  C[2]=04a1aa80  D[2]=af42c833
A[3]=90bb88ea  B[3]=e2e0af5d  C[3]=d0632a18  D[3]=7c52a960

Step 23: (r=22, s=19)
A[0]=33c9b30f  B[0]=add04e28  C[0]=0b9c0b0a  D[0]=70770e9c
A[1]=1c3d07bb  B[1]=b5e49cdd  C[1]=a6ac1539  D[1]=08178bb8
A[2]=3732bc4e  B[2]=d64288a4  C[2]=cdc61cda  D[2]=04a1aa80
A[3]=d1c0887e  B[3]=3aa42ee2  C[3]=e2e0af5d  D[3]=d0632a18

Step 24: (r=15, s= 5)
A[0]=2de84209  B[0]=d98799e4  C[0]=add04e28  D[0]=0b9c0b0a
A[1]=e6087563  B[1]=83dd8e1e  C[1]=b5e49cdd  D[1]=a6ac1539
A[2]=1cb06011  B[2]=5e271b99  C[2]=d64288a4  D[2]=cdc61cda
A[3]=ca043952  B[3]=443f68e0  C[3]=3aa42ee2  D[3]=e2e0af5d

Step 25: (r= 5, s=29)
A[0]=f1cb9bee  B[0]=bd084125  C[0]=d98799e4  D[0]=add04e28
A[1]=c2bba3b2  B[1]=c10eac7c  C[1]=83dd8e1e  D[1]=b5e49cdd
A[2]=fa842de0  B[2]=960c0223  C[2]=5e271b99  D[2]=d64288a4
A[3]=66f24cd0  B[3]=40872a59  C[3]=443f68e0  D[3]=3aa42ee2
```

```
Step 26: (r=29, s= 9)
A[0]=2d33f105  B[0]=de39737d  C[0]=bd084125  D[0]=d98799e4
A[1]=c9067786  B[1]=58577476  C[1]=c10eac7c  D[1]=83dd8e1e
A[2]=0a70da15  B[2]=1f5085bc  C[2]=960c0223  D[2]=5e271b99
A[3]=80c1de99  B[3]=0cde499a  C[3]=40872a59  D[3]=443f68e0

Step 27: (r= 9, s=15)
A[0]=da7af1b2  B[0]=67e20a5a  C[0]=de39737d  D[0]=bd084125
A[1]=59e20820  B[1]=0cef0d92  C[1]=58577476  D[1]=c10eac7c
A[2]=858cb8d9  B[2]=e1b42a14  C[2]=1f5085bc  D[2]=960c0223
A[3]=e067e578  B[3]=83bd3301  C[3]=0cde499a  D[3]=40872a59

Step 28: (r=15, s= 5)
A[0]=8e90a6ba  B[0]=78d96d3d  C[0]=67e20a5a  D[0]=de39737d
A[1]=360b3dc1  B[1]=04102cf1  C[1]=0cef0d92  D[1]=58577476
A[2]=fa1f34e9  B[2]=5c6cc2c6  C[2]=e1b42a14  D[2]=1f5085bc
A[3]=cfffb520  B[3]=f2bc7033  C[3]=83bd3301  D[3]=0cde499a

Step 29: (r= 5, s=29)
A[0]=ad1351ea  B[0]=d214d751  C[0]=78d96d3d  D[0]=67e20a5a
A[1]=4fb8b42c  B[1]=c167b826  C[1]=04102cf1  D[1]=0cef0d92
A[2]=70edf079  B[2]=43e69d3f  C[2]=5c6cc2c6  D[2]=e1b42a14
A[3]=f0c9722f  B[3]=fff6a419  C[3]=f2bc7033  D[3]=83bd3301

Step 30: (r=29, s= 9)
A[0]=00612f9a  B[0]=55a26a3d  C[0]=d214d751  D[0]=78d96d3d
A[1]=06ec9377  B[1]=89f71685  C[1]=c167b826  D[1]=04102cf1
A[2]=7d461972  B[2]=2e1dbe0f  C[2]=43e69d3f  D[2]=5c6cc2c6
A[3]=3e9c6f76  B[3]=fe192e45  C[3]=fff6a419  D[3]=f2bc7033

Step 31: (r= 9, s=15)
A[0]=fca4c730  B[0]=c25f3400  C[0]=55a26a3d  D[0]=d214d751
A[1]=8465437f  B[1]=d926ee0d  C[1]=89f71685  D[1]=c167b826
A[2]=ea31220b  B[2]=8c32e4fa  C[2]=2e1dbe0f  D[2]=43e69d3f
A[3]=d1d4bd4f  B[3]=38deec7d  C[3]=fe192e45  D[3]=fff6a419

Feistel Step 0: (r=15, s= 5)
A[0]=761097dc  B[0]=63987e52  C[0]=c25f3400  D[0]=55a26a3d
A[1]=c90b333a  B[1]=a1bfc232  C[1]=d926ee0d  D[1]=89f71685
A[2]=fecfe96b  B[2]=9105f518  C[2]=8c32e4fa  D[2]=2e1dbe0f
A[3]=964f435b  B[3]=5ea7e8ea  C[3]=38deec7d  D[3]=fe192e45

Feistel Step 1: (r= 5, s=29)
A[0]=f00018f2  B[0]=c212fb8e  C[0]=63987e52  D[0]=c25f3400
A[1]=323a8fec  B[1]=21666759  C[1]=a1bfc232  D[1]=d926ee0d
A[2]=41046233  B[2]=d9fd2d7f  C[2]=9105f518  D[2]=8c32e4fa
A[3]=0c6c3d96  B[3]=c9e86b72  C[3]=5ea7e8ea  D[3]=38deec7d

Feistel Step 2: (r=29, s= 9)
```

```
A[0]=f3d2c904  B[0]=5e00031e  C[0]=c212fb8e  D[0]=63987e52
A[1]=7ff5dd8c  B[1]=864751fd  C[1]=21666759  D[1]=a1bfc232
A[2]=40b57436  B[2]=68208c46  C[2]=d9fd2d7f  D[2]=9105f518
A[3]=775480b0  B[3]=c18d87b2  C[3]=c9e86b72  D[3]=5ea7e8ea

Feistel Step 3: (r= 9, s=15)
A[0]=21b1e2ec  B[0]=a59209e7  C[0]=5e00031e  D[0]=c212fb8e
A[1]=f008b817  B[1]=ebbb18ff  C[1]=864751fd  D[1]=21666759
A[2]=e660e8cc  B[2]=6ae86c81  C[2]=68208c46  D[2]=d9fd2d7f
A[3]=7309c099  B[3]=a90160ee  C[3]=c18d87b2  D[3]=c9e86b72
```

Compression Function Output

```
A[0]=21b1e2ec  B[0]=a59209e7  C[0]=5e00031e  D[0]=c212fb8e
A[1]=f008b817  B[1]=ebbb18ff  C[1]=864751fd  D[1]=21666759
A[2]=e660e8cc  B[2]=6ae86c81  C[2]=68208c46  D[2]=d9fd2d7f
A[3]=7309c099  B[3]=a90160ee  C[3]=c18d87b2  D[3]=c9e86b72
```

Hash Function Output

```
ece2b12117b808f0cce860e699c00973e70992a5ff18bbeb816ce86aee6001a9
```

6.2.3 Two-block Message

We use the message made of 700 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
```

```
y[ 88.. 95] =   32   58  213  108  189   44  222  244
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff178c69  a9895677  e4b21b4e  eb1114ef
Z[17] = 74808b80  49b9b647  f2590da7  6a7d9583
Z[18] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
Z[19] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
Z[20] = 0e90f170  ebfa1406  e10e1ef2  65079af9
Z[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
Z[22] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
Z[23] = 01d2fe2e  c3053cfb  369cc964  29ded622
Z[24] = bad4949a  bbbd51ea  6f0a0748  b90233e1
Z[25] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
Z[26] = 48d01ef2  a7b71ef2  6d38e856  263a065f
Z[27] = 34ca4443  624c4188  280c7397  f42b6d38
Z[28] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
Z[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
Z[30] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
Z[31] = 452cc6a9  db98a6ce  c305280c  558e53bc
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
```

```
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 74808b80  49b9b647  f2590da7  6a7d9583
W[17] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
W[18] = 01d2fe2e  c3053cfb  369cc964  29ded622
W[19] = 0e90f170  ebfa1406  e10e1ef2  65079af9
W[20] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
W[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
W[22] = ff178c69  a9895677  e4b21b4e  eb1114ef
W[23] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
W[24] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
W[25] = bad4949a  bbbd51ea  6f0a0748  b90233e1
W[26] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
W[27] = 452cc6a9  db98a6ce  c305280c  558e53bc
W[28] = 34ca4443  624c4188  280c7397  f42b6d38
W[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
W[30] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
W[31] = 48d01ef2  a7b71ef2  6d38e856  263a065f
```

Feistel Steps

```
IV :
A[0]=96301f14  B[0]=75ad94b4  C[0]=2d83bbab  D[0]=5731b59d
A[1]=64f69407  B[1]=8b618939  C[1]=0c195501  D[1]=abff7dd4
A[2]=8450cc02  B[2]=5a13cb35  C[2]=cc0782ba  D[2]=db4cd0f5
A[3]=42c538e3  B[3]=26141ded  C[3]=356688a2  D[3]=7240ec03

IV XOR M :
A[0]=69cfe0eb  B[0]=8a526b4b  C[0]=d27c4454  D[0]=a8ce4a62
A[1]=9b096bf8  B[1]=749e76c6  C[1]=f3e6aafe  D[1]=5400822b
A[2]=7baf33fd  B[2]=a5ec34ca  C[2]=33f87d45  D[2]=24b32f0a
A[3]=bd3ac71c  B[3]=d9ebe212  C[3]=ca99775d  D[3]=8dbf13fc

Step  0: (r= 3, s=20)
A[0]=0b6aca3e  B[0]=4e7f075b  C[0]=8a526b4b  D[0]=d27c4454
A[1]=2af91842  B[1]=d84b5fc4  C[1]=749e76c6  D[1]=f3e6aafe
A[2]=3017bfe1  B[2]=dd799feb  C[2]=a5ec34ca  D[2]=33f87d45
A[3]=afe15f36  B[3]=e9d638e5  C[3]=d9ebe212  D[3]=ca99775d

Step  1: (r=20, s=14)
A[0]=5745e1c1  B[0]=a3e0b6ac  C[0]=4e7f075b  D[0]=8a526b4b
A[1]=27a2ce29  B[1]=8422af91  C[1]=d84b5fc4  D[1]=749e76c6
```

```
A[2]=157eb76e  B[2]=fe13017b  C[2]=dd799feb  D[2]=a5ec34ca
A[3]=bf63f149  B[3]=f36afe15  C[3]=e9d638e5  D[3]=d9ebe212

Step  2: (r=14, s=27)
A[0]=a58e8798  B[0]=787055d1  C[0]=a3e0b6ac  D[0]=4e7f075b
A[1]=426c2838  B[1]=b38a49e8  C[1]=8422af91  D[1]=d84b5fc4
A[2]=1890aa7b  B[2]=addb855f  C[2]=fe13017b  D[2]=dd799feb
A[3]=3028f52b  B[3]=fc526fd8  C[3]=f36afe15  D[3]=e9d638e5

Step  3: (r=27, s= 3)
A[0]=2454fbcf  B[0]=c52c743c  C[0]=787055d1  D[0]=a3e0b6ac
A[1]=10c2bfd4  B[1]=c2136141  C[1]=b38a49e8  D[1]=8422af91
A[2]=8f4ac2e9  B[2]=d8c48553  C[2]=addb855f  D[2]=fe13017b
A[3]=d3523600  B[3]=598147a9  C[3]=fc526fd8  D[3]=f36afe15

Step  4: (r= 3, s=20)
A[0]=3793ab92  B[0]=22a7de79  C[0]=c52c743c  D[0]=787055d1
A[1]=16231480  B[1]=8615fea0  C[1]=c2136141  D[1]=b38a49e8
A[2]=523c6aab  B[2]=7a56174c  C[2]=d8c48553  D[2]=addb855f
A[3]=6898d21d  B[3]=9a91b006  C[3]=598147a9  D[3]=fc526fd8

Step  5: (r=20, s=14)
A[0]=fe458f69  B[0]=b923793a  C[0]=22a7de79  D[0]=c52c743c
A[1]=136d5116  B[1]=48016231  C[1]=8615fea0  D[1]=c2136141
A[2]=1f6048a4  B[2]=aab523c6  C[2]=7a56174c  D[2]=d8c48553
A[3]=e5aaf370  B[3]=21d6898d  C[3]=9a91b006  D[3]=598147a9

Step  6: (r=14, s=27)
A[0]=01f1c6bf  B[0]=63da7f91  C[0]=b923793a  D[0]=22a7de79
A[1]=01ea0f71  B[1]=544584db  C[1]=48016231  D[1]=8615fea0
A[2]=9854373b  B[2]=122907d8  C[2]=aab523c6  D[2]=7a56174c
A[3]=2668e020  B[3]=bcdc396a  C[3]=21d6898d  D[3]=9a91b006

Step  7: (r=27, s= 3)
A[0]=a29aaf60  B[0]=f80f8e35  C[0]=63da7f91  D[0]=b923793a
A[1]=72a19b44  B[1]=880f507b  C[1]=544584db  D[1]=48016231
A[2]=8d99de1f  B[2]=dcc2a1b9  C[2]=122907d8  D[2]=aab523c6
A[3]=b5ef758a  B[3]=01334701  C[3]=bcdc396a  D[3]=21d6898d

Step  8: (r=26, s= 4)
A[0]=27701c4a  B[0]=828a6abd  C[0]=f80f8e35  D[0]=63da7f91
A[1]=742ad18a  B[1]=11ca866d  C[1]=880f507b  D[1]=544584db
A[2]=b984cd87  B[2]=7e366778  C[2]=dcc2a1b9  D[2]=122907d8
A[3]=7209ed73  B[3]=2ad7bdd6  C[3]=01334701  D[3]=bcdc396a

Step  9: (r= 4, s=23)
A[0]=0f80c28b  B[0]=7701c4a2  C[0]=828a6abd  D[0]=f80f8e35
A[1]=e4bc0829  B[1]=42ad18a7  C[1]=11ca866d  D[1]=880f507b
A[2]=6d58e2bf  B[2]=984cd87b  C[2]=7e366778  D[2]=dcc2a1b9
```

```
A[3]=fb986e8e  B[3]=209ed737  C[3]=2ad7bdd6  D[3]=01334701

Step 10: (r=23, s=11)
A[0]=e10639c8  B[0]=4587c061  C[0]=7701c4a2  D[0]=828a6abd
A[1]=962e836f  B[1]=14f25e04  C[1]=42ad18a7  D[1]=11ca866d
A[2]=f9f2e123  B[2]=5fb6ac71  C[2]=984cd87b  D[2]=7e366778
A[3]=28fc3061  B[3]=477dcc37  C[3]=209ed737  D[3]=2ad7bdd6

Step 11: (r=11, s=26)
A[0]=3193bc88  B[0]=31ce4708  C[0]=4587c061  D[0]=7701c4a2
A[1]=0a43f6b8  B[1]=741b7cb1  C[1]=14f25e04  D[1]=42ad18a7
A[2]=3e8ec731  B[2]=97091fcf  C[2]=5fb6ac71  D[2]=984cd87b
A[3]=2fe76282  B[3]=e1830947  C[3]=477dcc37  D[3]=209ed737

Step 12: (r=26, s= 4)
A[0]=84f76288  B[0]=20c64ef2  C[0]=31ce4708  D[0]=4587c061
A[1]=f2e7591f  B[1]=e0290fda  C[1]=741b7cb1  D[1]=14f25e04
A[2]=b8356eda  B[2]=c4fa3b1c  C[2]=97091fcf  D[2]=5fb6ac71
A[3]=42bd8ba9  B[3]=08bf9d8a  C[3]=e1830947  D[3]=477dcc37

Step 13: (r= 4, s=23)
A[0]=dbee4231  B[0]=4f762888  C[0]=20c64ef2  D[0]=31ce4708
A[1]=024429ed  B[1]=2e7591ff  C[1]=e0290fda  D[1]=741b7cb1
A[2]=52e94378  B[2]=8356edab  C[2]=c4fa3b1c  D[2]=97091fcf
A[3]=af158f0f  B[3]=2bd8ba94  C[3]=08bf9d8a  D[3]=e1830947

Step 14: (r=23, s=11)
A[0]=1c80e7d0  B[0]=18edf721  C[0]=4f762888  D[0]=20c64ef2
A[1]=fe623724  B[1]=f6812214  C[1]=2e7591ff  D[1]=e0290fda
A[2]=66eb504c  B[2]=bc2974a1  C[2]=8356edab  D[2]=c4fa3b1c
A[3]=f49ff07c  B[3]=87d78ac7  C[3]=2bd8ba94  D[3]=08bf9d8a

Step 15: (r=11, s=26)
A[0]=b291d01c  B[0]=073e80e4  C[0]=18edf721  D[0]=4f762888
A[1]=c3c86a13  B[1]=11b927f3  C[1]=f6812214  D[1]=2e7591ff
A[2]=fde1ccfd  B[2]=5a826337  C[2]=bc2974a1  D[2]=8356edab
A[3]=7b830e5e  B[3]=ff83e7a4  C[3]=87d78ac7  D[3]=2bd8ba94

Step 16: (r=19, s=28)
A[0]=2d8553f5  B[0]=80e5948e  C[0]=073e80e4  D[0]=18edf721
A[1]=42cb75b3  B[1]=509e1e43  C[1]=11b927f3  D[1]=f6812214
A[2]=efd762d0  B[2]=67efef0e  C[2]=5a826337  D[2]=bc2974a1
A[3]=4a4871f7  B[3]=72f3dc18  C[3]=ff83e7a4  D[3]=87d78ac7

Step 17: (r=28, s= 7)
A[0]=062428d7  B[0]=52d8553f  C[0]=80e5948e  D[0]=073e80e4
A[1]=8668bf1b  B[1]=342cb75b  C[1]=509e1e43  D[1]=11b927f3
A[2]=5c0d2910  B[2]=0efd762d  C[2]=67efef0e  D[2]=5a826337
A[3]=26fcfdfa  B[3]=74a4871f  C[3]=72f3dc18  D[3]=ff83e7a4
```

```
Step 18: (r= 7, s=22)
A[0]=00c28287  B[0]=12146b83  C[0]=52d8553f  D[0]=80e5948e
A[1]=18dee775  B[1]=345f8dc3  C[1]=342cb75b  D[1]=509e1e43
A[2]=28ef40d7  B[2]=0694882e  C[2]=0efd762d  D[2]=67efef0e
A[3]=ca3bee13  B[3]=7e7efd13  C[3]=74a4871f  D[3]=72f3dc18

Step 19: (r=22, s=19)
A[0]=23994846  B[0]=a1c030a0  C[0]=12146b83  D[0]=52d8553f
A[1]=c19617b1  B[1]=dd4637b9  C[1]=345f8dc3  D[1]=342cb75b
A[2]=c332ad32  B[2]=35ca3bd0  C[2]=0694882e  D[2]=0efd762d
A[3]=fec8ed8c  B[3]=84f28efb  C[3]=7e7efd13  D[3]=74a4871f

Step 20: (r=19, s=28)
A[0]=952ee851  B[0]=42311cca  C[0]=a1c030a0  D[0]=12146b83
A[1]=012d7f86  B[1]=bd8e0cb0  C[1]=dd4637b9  D[1]=345f8dc3
A[2]=e4a48169  B[2]=69961995  C[2]=35ca3bd0  D[2]=0694882e
A[3]=2ea6ded9  B[3]=6c67f647  C[3]=84f28efb  D[3]=7e7efd13

Step 21: (r=28, s= 7)
A[0]=dd18c5e3  B[0]=1952ee85  C[0]=42311cca  D[0]=a1c030a0
A[1]=48562950  B[1]=6012d7f8  C[1]=bd8e0cb0  D[1]=dd4637b9
A[2]=6a2baab3  B[2]=9e4a4816  C[2]=69961995  D[2]=35ca3bd0
A[3]=daa207ac  B[3]=92ea6ded  C[3]=6c67f647  D[3]=84f28efb

Step 22: (r= 7, s=22)
A[0]=9e532246  B[0]=8c62f1ee  C[0]=1952ee85  D[0]=42311cca
A[1]=1e11131c  B[1]=2b14a824  C[1]=6012d7f8  D[1]=bd8e0cb0
A[2]=3e64f804  B[2]=15d559b5  C[2]=9e4a4816  D[2]=69961995
A[3]=8235ab70  B[3]=5103d66d  C[3]=92ea6ded  D[3]=6c67f647

Step 23: (r=22, s=19)
A[0]=14977665  B[0]=91a794c8  C[0]=8c62f1ee  D[0]=1952ee85
A[1]=1be68a00  B[1]=c7078444  C[1]=2b14a824  D[1]=6012d7f8
A[2]=0e11e47d  B[2]=010f993e  C[2]=15d559b5  D[2]=9e4a4816
A[3]=f38679cc  B[3]=dc208d6a  C[3]=5103d66d  D[3]=92ea6ded

Step 24: (r=15, s= 5)
A[0]=72564820  B[0]=bb328a4b  C[0]=91a794c8  D[0]=8c62f1ee
A[1]=4e4b09e0  B[1]=45000df3  C[1]=c7078444  D[1]=2b14a824
A[2]=ea8bb102  B[2]=f23e8708  C[2]=010f993e  D[2]=15d559b5
A[3]=4ffcac8d  B[3]=3ce679c3  C[3]=dc208d6a  D[3]=5103d66d

Step 25: (r= 5, s=29)
A[0]=70d384c7  B[0]=4ac9040e  C[0]=bb328a4b  D[0]=91a794c8
A[1]=551062a7  B[1]=c9613c09  C[1]=45000df3  D[1]=c7078444
A[2]=77c6c155  B[2]=5176205d  C[2]=f23e8708  D[2]=010f993e
A[3]=fe3e828f  B[3]=ff9591a9  C[3]=3ce679c3  D[3]=dc208d6a
```

```
Step 26: (r=29, s= 9)
A[0]=a32897b4  B[0]=ee1a7098  C[0]=4ac9040e  D[0]=bb328a4b
A[1]=bb7defdf  B[1]=eaa20c54  C[1]=c9613c09  D[1]=45000df3
A[2]=71a392c7  B[2]=aef8d82a  C[2]=5176205d  D[2]=f23e8708
A[3]=6b895215  B[3]=ffc7d051  C[3]=ff9591a9  D[3]=3ce679c3

Step 27: (r= 9, s=15)
A[0]=77ed0477  B[0]=512f6946  C[0]=ee1a7098  D[0]=4ac9040e
A[1]=7b2eb033  B[1]=fbdfbf76  C[1]=eaa20c54  D[1]=c9613c09
A[2]=80c6d462  B[2]=47258ee3  C[2]=aef8d82a  D[2]=5176205d
A[3]=4b7c087b  B[3]=12a42ad7  C[3]=ffc7d051  D[3]=ff9591a9

Step 28: (r=15, s= 5)
A[0]=306ed295  B[0]=823bbbf6  C[0]=512f6946  D[0]=ee1a7098
A[1]=55b88147  B[1]=5819bd97  C[1]=fbdfbf76  D[1]=eaa20c54
A[2]=112bb07e  B[2]=6a314063  C[2]=47258ee3  D[2]=aef8d82a
A[3]=76dca27f  B[3]=043da5be  C[3]=12a42ad7  D[3]=ffc7d051

Step 29: (r= 5, s=29)
A[0]=7c7cbf96  B[0]=0dda52a6  C[0]=823bbbf6  D[0]=512f6946
A[1]=7cd3e4d0  B[1]=b71028ea  C[1]=5819bd97  D[1]=fbdfbf76
A[2]=09f44622  B[2]=25760fc2  C[2]=6a314063  D[2]=47258ee3
A[3]=0e8054d3  B[3]=db944fee  C[3]=043da5be  D[3]=12a42ad7

Step 30: (r=29, s= 9)
A[0]=03238144  B[0]=cf8f97f2  C[0]=0dda52a6  D[0]=823bbbf6
A[1]=b49685c2  B[1]=0f9a7c9a  C[1]=b71028ea  D[1]=5819bd97
A[2]=df061699  B[2]=413e88c4  C[2]=25760fc2  D[2]=6a314063
A[3]=b3c627de  B[3]=61d00a9a  C[3]=db944fee  D[3]=043da5be

Step 31: (r= 9, s=15)
A[0]=c394a109  B[0]=47028806  C[0]=cf8f97f2  D[0]=0dda52a6
A[1]=10f99918  B[1]=2d0b8569  C[1]=0f9a7c9a  D[1]=b71028ea
A[2]=62bf1656  B[2]=0c2d33be  C[2]=413e88c4  D[2]=25760fc2
A[3]=0b09148e  B[3]=8c4fbd67  C[3]=61d00a9a  D[3]=db944fee

Feistel Step 0: (r=15, s= 5)
A[0]=2f4d1e1a  B[0]=5084e1ca  C[0]=47028806  D[0]=cf8f97f2
A[1]=ed7f80c4  B[1]=cc8c087c  C[1]=2d0b8569  D[1]=0f9a7c9a
A[2]=e8d5d0d9  B[2]=8b2b315f  C[2]=0c2d33be  D[2]=413e88c4
A[3]=36d9beba  B[3]=8a470584  C[3]=8c4fbd67  D[3]=61d00a9a

Feistel Step 1: (r= 5, s=29)
A[0]=ab6290d3  B[0]=e9a3c345  C[0]=5084e1ca  D[0]=47028806
A[1]=e818d8ae  B[1]=aff0189d  C[1]=cc8c087c  D[1]=2d0b8569
A[2]=ee933434  B[2]=1aba1b3d  C[2]=8b2b315f  D[2]=0c2d33be
A[3]=32357e66  B[3]=db37d746  C[3]=8a470584  D[3]=8c4fbd67

Feistel Step 2: (r=29, s= 9)
```

```
A[0]=374d0ff1  B[0]=756c521a  C[0]=e9a3c345  D[0]=5084e1ca
A[1]=0fb8f451  B[1]=dd031b15  C[1]=aff0189d  D[1]=cc8c087c
A[2]=a3d69f93  B[2]=9dd26686  C[2]=1aba1b3d  D[2]=8b2b315f
A[3]=d0a7f0d2  B[3]=c646afcc  C[3]=db37d746  D[3]=8a470584

Feistel Step 3: (r= 9, s=15)
A[0]=59fcfa19  B[0]=9a1fe26e  C[0]=756c521a  D[0]=e9a3c345
A[1]=1f583886  B[1]=71e8a21f  C[1]=dd031b15  D[1]=aff0189d
A[2]=9ea0e2a7  B[2]=ad3f2747  C[2]=9dd26686  D[2]=1aba1b3d
A[3]=be8e85ee  B[3]=4fe1a5a1  C[3]=c646afcc  D[3]=db37d746
```

Compression Function Output

```
A[0]=59fcfa19  B[0]=9a1fe26e  C[0]=756c521a  D[0]=e9a3c345
A[1]=1f583886  B[1]=71e8a21f  C[1]=dd031b15  D[1]=aff0189d
A[2]=9ea0e2a7  B[2]=ad3f2747  C[2]=9dd26686  D[2]=1aba1b3d
A[3]=be8e85ee  B[3]=4fe1a5a1  C[3]=c646afcc  D[3]=db37d746
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0cbec792  4443e76d  0e902f54  9755eeb5
Z[17] = a9890aec  ff17d9c6  f087c4d7  4e465849
Z[18] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
Z[19] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
Z[20] = 1e09e1f7  6507624c  114b280c  58496163
Z[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
Z[22] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
Z[23] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
Z[24] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
Z[25] = 59325760  d450900d  3c129db4  12344e46
Z[26] = 280c409f  048d1a65  280c624c  72ae0cbe
Z[27] = 9f86386e  f8b8b55e  280c1234  47e70e90
Z[28] = f1701e09  9af9e59b  5bed6335  daaf263a
Z[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
Z[30] = ece372ae  091a386e  f6e62e6b  d450d70b
Z[31] = 29de966c  320f0cbe  5677d450  c87b29de
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
```

```
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = a9890aec  ff17d9c6  f087c4d7  4e465849
W[17] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
W[18] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
W[19] = 1e09e1f7  6507624c  114b280c  58496163
W[20] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
W[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
W[22] = 0cbec792  4443e76d  0e902f54  9755eeb5
W[23] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
W[24] = ece372ae  091a386e  f6e62e6b  d450d70b
W[25] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
W[26] = 59325760  d450900d  3c129db4  12344e46
W[27] = 29de966c  320f0cbe  5677d450  c87b29de
W[28] = 9f86386e  f8b8b55e  280c1234  47e70e90
W[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
W[30] = f1701e09  9af9e59b  5bed6335  daaf263a
W[31] = 280c409f  048d1a65  280c624c  72ae0cbe
```

Feistel Steps

```
IV :
A[0]=59fcfa19  B[0]=9a1fe26e  C[0]=756c521a  D[0]=e9a3c345
A[1]=1f583886  B[1]=71e8a21f  C[1]=dd031b15  D[1]=aff0189d
A[2]=9ea0e2a7  B[2]=ad3f2747  C[2]=9dd26686  D[2]=1aba1b3d
A[3]=be8e85ee  B[3]=4fe1a5a1  C[3]=c646afcc  D[3]=db37d746

IV XOR M :
A[0]=a60305e6  B[0]=65e01d91  C[0]=756c521a  D[0]=e9a3c345
A[1]=e0a7c779  B[1]=81175de0  C[1]=dd031b15  D[1]=aff0189d
A[2]=615f1d58  B[2]=ad3f2747  C[2]=9dd26686  D[2]=1aba1b3d
A[3]=41717a11  B[3]=4fe1a5a1  C[3]=c646afcc  D[3]=db37d746

Step  0: (r= 3, s=20)
A[0]=3585aa6f  B[0]=30182f35  C[0]=65e01d91  D[0]=756c521a
A[1]=4bcc6aef  B[1]=053e3bcf  C[1]=81175de0  D[1]=dd031b15
A[2]=387e4274  B[2]=0af8eac3  C[2]=ad3f2747  D[2]=9dd26686
A[3]=d6843ed1  B[3]=0b8bd08a  C[3]=4fe1a5a1  D[3]=c646afcc

Step  1: (r=20, s=14)
A[0]=d5d5581a  B[0]=a6f3585a  C[0]=30182f35  D[0]=65e01d91
A[1]=30254aff  B[1]=aef4bcc6  C[1]=053e3bcf  D[1]=81175de0
A[2]=873f2c63  B[2]=274387e4  C[2]=0af8eac3  D[2]=ad3f2747
A[3]=ac85e92e  B[3]=ed1d6843  C[3]=0b8bd08a  D[3]=4fe1a5a1

Step  2: (r=14, s=27)
A[0]=688e1f89  B[0]=5606b575  C[0]=a6f3585a  D[0]=30182f35
A[1]=e95b4df0  B[1]=52bfcc09  C[1]=aef4bcc6  D[1]=053e3bcf
```

```
A[2]=56fb93be  B[2]=cb18e1cf  C[2]=274387e4  D[2]=0af8eac3
A[3]=9dd005f8  B[3]=7a4bab21  C[3]=ed1d6843  D[3]=0b8bd08a

Step  3: (r=27, s= 3)
A[0]=41aed386  B[0]=4b4470fc  C[0]=5606b575  D[0]=a6f3585a
A[1]=cc9027ba  B[1]=874ada6f  C[1]=52bfcc09  D[1]=aef4bcc6
A[2]=2c31b879  B[2]=f2b7dc9d  C[2]=cb18e1cf  D[2]=274387e4
A[3]=f7072993  B[3]=c4ee802f  C[3]=7a4bab21  D[3]=ed1d6843

Step  4: (r= 3, s=20)
A[0]=571aa03c  B[0]=0d769c32  C[0]=4b4470fc  D[0]=5606b575
A[1]=5e25beac  B[1]=64813dd6  C[1]=874ada6f  D[1]=52bfcc09
A[2]=154838f7  B[2]=618dc3c9  C[2]=f2b7dc9d  D[2]=cb18e1cf
A[3]=6c76e6f1  B[3]=b8394c9f  C[3]=c4ee802f  D[3]=7a4bab21

Step  5: (r=20, s=14)
A[0]=5641fbdd  B[0]=03c571aa  C[0]=0d769c32  D[0]=4b4470fc
A[1]=be2357c2  B[1]=eac5e25b  C[1]=64813dd6  D[1]=874ada6f
A[2]=06dad5f7  B[2]=8f715483  C[2]=618dc3c9  D[2]=f2b7dc9d
A[3]=d5602d0e  B[3]=6f16c76e  C[3]=b8394c9f  D[3]=c4ee802f

Step  6: (r=14, s=27)
A[0]=e9eb7495  B[0]=7ef75590  C[0]=03c571aa  D[0]=0d769c32
A[1]=67521c36  B[1]=d5f0af88  C[1]=eac5e25b  D[1]=64813dd6
A[2]=1b8be40c  B[2]=b57dc1b6  C[2]=8f715483  D[2]=618dc3c9
A[3]=3d64d37a  B[3]=0b43b558  C[3]=6f16c76e  D[3]=b8394c9f

Step  7: (r=27, s= 3)
A[0]=56cd3295  B[0]=af4f5ba4  C[0]=7ef75590  D[0]=03c571aa
A[1]=6d699352  B[1]=b33a90e1  C[1]=d5f0af88  D[1]=eac5e25b
A[2]=47322659  B[2]=60dc5f20  C[2]=b57dc1b6  D[2]=8f715483
A[3]=e06de272  B[3]=d1eb269b  C[3]=0b43b558  D[3]=6f16c76e

Step  8: (r=26, s= 4)
A[0]=81e34eb2  B[0]=555b34ca  C[0]=af4f5ba4  D[0]=7ef75590
A[1]=a903f985  B[1]=49b5a64d  C[1]=b33a90e1  D[1]=d5f0af88
A[2]=12e894b5  B[2]=651cc899  C[2]=60dc5f20  D[2]=b57dc1b6
A[3]=3c2edcfa  B[3]=cb81b789  C[3]=d1eb269b  D[3]=0b43b558

Step  9: (r= 4, s=23)
A[0]=863a21fb  B[0]=1e34eb28  C[0]=555b34ca  D[0]=af4f5ba4
A[1]=276380dd  B[1]=903f985a  C[1]=49b5a64d  D[1]=b33a90e1
A[2]=24cf9eeb  B[2]=2e894b51  C[2]=651cc899  D[2]=60dc5f20
A[3]=4946a6ea  B[3]=c2edcfa3  C[3]=cb81b789  D[3]=d1eb269b

Step 10: (r=23, s=11)
A[0]=f3d8e199  B[0]=fdc31d10  C[0]=1e34eb28  D[0]=555b34ca
A[1]=51cded2c  B[1]=6e93b1c0  C[1]=903f985a  D[1]=49b5a64d
A[2]=0ade03ce  B[2]=759267cf  C[2]=2e894b51  D[2]=651cc899
```

```
A[3]=7de5d8c8  B[3]=7524a353  C[3]=c2edcfa3  D[3]=cb81b789

Step 11: (r=11, s=26)
A[0]=51a53d7e  B[0]=c70ccf9e  C[0]=fdc31d10  D[0]=1e34eb28
A[1]=781c8a26  B[1]=6f69628e  C[1]=6e93b1c0  D[1]=903f985a
A[2]=e8ba281e  B[2]=f01e7056  C[2]=759267cf  D[2]=2e894b51
A[3]=b5ddce3d  B[3]=2ec643ef  C[3]=7524a353  D[3]=c2edcfa3

Step 12: (r=26, s= 4)
A[0]=42acac1b  B[0]=f94694f5  C[0]=c70ccf9e  D[0]=fdc31d10
A[1]=36468b1d  B[1]=99e07228  C[1]=6f69628e  D[1]=6e93b1c0
A[2]=e4416d9c  B[2]=7ba2e8a0  C[2]=f01e7056  D[2]=759267cf
A[3]=6bb3a975  B[3]=f6d77738  C[3]=2ec643ef  D[3]=7524a353

Step 13: (r= 4, s=23)
A[0]=2cccfb34  B[0]=2acac1b4  C[0]=f94694f5  D[0]=c70ccf9e
A[1]=abf2daf5  B[1]=6468b1d3  C[1]=99e07228  D[1]=6f69628e
A[2]=d927d2b3  B[2]=4416d9ce  C[2]=7ba2e8a0  D[2]=f01e7056
A[3]=968836e9  B[3]=bb3a9756  C[3]=f6d77738  D[3]=2ec643ef

Step 14: (r=23, s=11)
A[0]=bd0de1ea  B[0]=9a16667d  C[0]=2acac1b4  D[0]=f94694f5
A[1]=9545fcd0  B[1]=7ad5f96d  C[1]=6468b1d3  D[1]=99e07228
A[2]=011b5763  B[2]=59ec93e9  C[2]=4416d9ce  D[2]=7ba2e8a0
A[3]=152d1080  B[3]=74cb441b  C[3]=bb3a9756  D[3]=f6d77738

Step 15: (r=11, s=26)
A[0]=c14bbd41  B[0]=6f0f55e8  C[0]=9a16667d  D[0]=2acac1b4
A[1]=f4d98647  B[1]=2fe684aa  C[1]=7ad5f96d  D[1]=6468b1d3
A[2]=81e57596  B[2]=dabb1808  C[2]=59ec93e9  D[2]=4416d9ce
A[3]=780bd235  B[3]=688400a9  C[3]=74cb441b  D[3]=bb3a9756

Step 16: (r=19, s=28)
A[0]=f536d90d  B[0]=ea0e0a5d  C[0]=6f0f55e8  D[0]=9a16667d
A[1]=e5d867b7  B[1]=323fa6cc  C[1]=2fe684aa  D[1]=7ad5f96d
A[2]=7280436e  B[2]=acb40f2b  C[2]=dabb1808  D[2]=59ec93e9
A[3]=91721999  B[3]=91abc05e  C[3]=688400a9  D[3]=74cb441b

Step 17: (r=28, s= 7)
A[0]=179a9bbf  B[0]=df536d90  C[0]=ea0e0a5d  D[0]=6f0f55e8
A[1]=cae54c79  B[1]=7e5d867b  C[1]=323fa6cc  D[1]=2fe684aa
A[2]=284e763a  B[2]=e7280436  C[2]=acb40f2b  D[2]=dabb1808
A[3]=3e3233a2  B[3]=99172199  C[3]=91abc05e  D[3]=688400a9

Step 18: (r= 7, s=22)
A[0]=fb873c48  B[0]=cd4ddf8b  C[0]=df536d90  D[0]=ea0e0a5d
A[1]=6717cd87  B[1]=72a63ce5  C[1]=7e5d867b  D[1]=323fa6cc
A[2]=ffd36429  B[2]=273b1d14  C[2]=e7280436  D[2]=acb40f2b
A[3]=c9214a7a  B[3]=1919d11f  C[3]=99172199  D[3]=91abc05e
```

```
Step 19: (r=22, s=19)
A[0]=59e6a043  B[0]=123ee1cf  C[0]=cd4ddf8b  D[0]=df536d90
A[1]=5f5ad4fa  B[1]=61d9c5f3  C[1]=72a63ce5  D[1]=7e5d867b
A[2]=ecae0ba0  B[2]=0a7ff4d9  C[2]=273b1d14  D[2]=e7280436
A[3]=7cb9de57  B[3]=9eb24852  C[3]=1919d11f  D[3]=99172199

Step 20: (r=19, s=28)
A[0]=d82fa2fb  B[0]=021acf35  C[0]=123ee1cf  D[0]=cd4ddf8b
A[1]=fbd394f3  B[1]=a7d2fad6  C[1]=61d9c5f3  D[1]=72a63ce5
A[2]=b7c4f1e2  B[2]=5d076570  C[2]=0a7ff4d9  D[2]=273b1d14
A[3]=8a4868e9  B[3]=f2bbe5ce  C[3]=9eb24852  D[3]=1919d11f

Step 21: (r=28, s= 7)
A[0]=b32f34a4  B[0]=bd82fa2f  C[0]=021acf35  D[0]=123ee1cf
A[1]=987bd854  B[1]=3fbd394f  C[1]=a7d2fad6  D[1]=61d9c5f3
A[2]=93bfe8ef  B[2]=2b7c4f1e  C[2]=5d076570  D[2]=0a7ff4d9
A[3]=d3ff0ac0  B[3]=98a4868e  C[3]=f2bbe5ce  D[3]=9eb24852

Step 22: (r= 7, s=22)
A[0]=1fa0ac75  B[0]=979a5259  C[0]=bd82fa2f  D[0]=021acf35
A[1]=4d8dfe32  B[1]=3dec2a4c  C[1]=3fbd394f  D[1]=a7d2fad6
A[2]=6a52744d  B[2]=dff477c9  C[2]=2b7c4f1e  D[2]=5d076570
A[3]=0cdc8448  B[3]=ff856069  C[3]=98a4868e  D[3]=f2bbe5ce

Step 23: (r=22, s=19)
A[0]=8a4ebfd5  B[0]=1d47e82b  C[0]=979a5259  D[0]=bd82fa2f
A[1]=a54bd682  B[1]=8c93637f  C[1]=3dec2a4c  D[1]=3fbd394f
A[2]=6f45e33b  B[2]=135a949d  C[2]=dff477c9  D[2]=2b7c4f1e
A[3]=3d14ef91  B[3]=12033721  C[3]=ff856069  D[3]=98a4868e

Step 24: (r=15, s= 5)
A[0]=f2ebef7e  B[0]=5feac527  C[0]=1d47e82b  D[0]=979a5259
A[1]=a179391e  B[1]=eb4152a5  C[1]=8c93637f  D[1]=3dec2a4c
A[2]=422aeae0  B[2]=f19db7a2  C[2]=135a949d  D[2]=dff477c9
A[3]=4ebb656e  B[3]=77c89e8a  C[3]=12033721  D[3]=ff856069

Step 25: (r= 5, s=29)
A[0]=4695123a  B[0]=5d7defde  C[0]=5feac527  D[0]=1d47e82b
A[1]=e0b7a2b8  B[1]=2f2723d4  C[1]=eb4152a5  D[1]=8c93637f
A[2]=5ee06f8a  B[2]=455d5c08  C[2]=f19db7a2  D[2]=135a949d
A[3]=b3fe71b9  B[3]=d76cadc9  C[3]=77c89e8a  D[3]=12033721

Step 26: (r=29, s= 9)
A[0]=102449fe  B[0]=48d2a247  C[0]=5d7defde  D[0]=5feac527
A[1]=e2a85109  B[1]=1c16f457  C[1]=2f2723d4  D[1]=eb4152a5
A[2]=cc9cc0a0  B[2]=4bdc0df1  C[2]=455d5c08  D[2]=f19db7a2
A[3]=913c883e  B[3]=367fce37  C[3]=d76cadc9  D[3]=77c89e8a
```

```
Step 27: (r= 9, s=15)
A[0]=ba6e2d2a  B[0]=4893fc20  C[0]=48d2a247  D[0]=5d7defde
A[1]=622c924d  B[1]=50a213c5  C[1]=1c16f457  D[1]=2f2723d4
A[2]=9ce14519  B[2]=39814199  C[2]=4bdc0df1  D[2]=455d5c08
A[3]=8bd1df25  B[3]=79107d22  C[3]=367fce37  D[3]=d76cadc9

Step 28: (r=15, s= 5)
A[0]=04013ede  B[0]=16955d37  C[0]=4893fc20  D[0]=48d2a247
A[1]=a35a3d5f  B[1]=4926b116  C[1]=50a213c5  D[1]=1c16f457
A[2]=d4e94098  B[2]=a28cce70  C[2]=39814199  D[2]=4bdc0df1
A[3]=6b48cd42  B[3]=ef92c5e8  C[3]=79107d22  D[3]=367fce37

Step 29: (r= 5, s=29)
A[0]=f98515a9  B[0]=8027dbc0  C[0]=16955d37  D[0]=4893fc20
A[1]=0b153f3e  B[1]=6b47abf4  C[1]=4926b116  D[1]=50a213c5
A[2]=4d0432e0  B[2]=9d28131a  C[2]=a28cce70  D[2]=39814199
A[3]=2dcf95f5  B[3]=6919a84d  C[3]=ef92c5e8  D[3]=79107d22

Step 30: (r=29, s= 9)
A[0]=d4523d7c  B[0]=3f30a2b5  C[0]=8027dbc0  D[0]=16955d37
A[1]=5109b2c9  B[1]=c162a7e7  C[1]=6b47abf4  D[1]=4926b116
A[2]=9b286f02  B[2]=09a0865c  C[2]=9d28131a  D[2]=a28cce70
A[3]=f5833637  B[3]=a5b9f2be  C[3]=6919a84d  D[3]=ef92c5e8

Step 31: (r= 9, s=15)
A[0]=7dc36ea0  B[0]=a47af9a8  C[0]=3f30a2b5  D[0]=8027dbc0
A[1]=be1cb766  B[1]=136592a2  C[1]=c162a7e7  D[1]=6b47abf4
A[2]=40662b88  B[2]=50de0536  C[2]=09a0865c  D[2]=9d28131a
A[3]=55d8368f  B[3]=066c6feb  C[3]=a5b9f2be  D[3]=6919a84d

Feistel Step 0: (r=15, s= 5)
A[0]=6eab30ce  B[0]=b7503ee1  C[0]=a47af9a8  D[0]=3f30a2b5
A[1]=d69303ee  B[1]=5bb35f0e  C[1]=136592a2  D[1]=c162a7e7
A[2]=cd370d9c  B[2]=15c42033  C[2]=50de0536  D[2]=09a0865c
A[3]=3992ddba  B[3]=1b47aaec  C[3]=066c6feb  D[3]=a5b9f2be

Feistel Step 1: (r= 5, s=29)
A[0]=16d5e379  B[0]=d56619cd  C[0]=b7503ee1  D[0]=a47af9a8
A[1]=c34412e9  B[1]=d2607dda  C[1]=5bb35f0e  D[1]=136592a2
A[2]=8efb8f87  B[2]=a6e1b399  C[2]=15c42033  D[2]=50de0536
A[3]=d501c643  B[3]=325bb747  C[3]=1b47aaec  D[3]=066c6feb

Feistel Step 2: (r=29, s= 9)
A[0]=8f3b99fb  B[0]=22dabc6f  C[0]=d56619cd  D[0]=b7503ee1
A[1]=a9f67d86  B[1]=3868825d  C[1]=d2607dda  D[1]=5bb35f0e
A[2]=a6bf13d5  B[2]=f1df71f0  C[2]=a6e1b399  D[2]=15c42033
A[3]=18780a3c  B[3]=7aa038c8  C[3]=325bb747  D[3]=1b47aaec

Feistel Step 3: (r= 9, s=15)
```

```
A[0]=cb72a4f6  B[0]=7733f71e  C[0]=22dabc6f  D[0]=d56619cd
A[1]=ac183b31  B[1]=ecfb0d53  C[1]=3868825d  D[1]=d2607dda
A[2]=6dd85fcc  B[2]=7e27ab4d  C[2]=f1df71f0  D[2]=a6e1b399
A[3]=8cb9a5a4  B[3]=f0147830  C[3]=7aa038c8  D[3]=325bb747
```

Compression Function Output

```
A[0]=cb72a4f6  B[0]=7733f71e  C[0]=22dabc6f  D[0]=d56619cd
A[1]=ac183b31  B[1]=ecfb0d53  C[1]=3868825d  D[1]=d2607dda
A[2]=6dd85fcc  B[2]=7e27ab4d  C[2]=f1df71f0  D[2]=a6e1b399
A[3]=8cb9a5a4  B[3]=f0147830  C[3]=7aa038c8  D[3]=325bb747
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
```

```
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
Z[17] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
Z[18] = f7cf7480  49b92296  9af9e76d  ebfa966c
Z[19] = 452c2723  386e33e1  3cfb2f54  f17090f6
Z[20] = a413de53  71c5fa8a  2d823ecd  065f65f0
Z[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
Z[22] = 7480f7cf  065f65f0  0bd5607a  576014ef
Z[23] = cb36b730  558e16c1  b1bad0ac  5b04114b
Z[24] = 0a03624c  983eea28  00e96b66  9ccbe59b
Z[25] = a241e025  2f543cfb  92c8ef9e  d450ae16
Z[26] = bca6c5c0  e93f9927  d195b0d1  58491406
Z[27] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
Z[28] = ebfa966c  237f48d0  255146fe  e76d9af9
Z[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
Z[30] = 6e21fe2e  409f2bb0  567715d8  35b3369c
Z[31] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
W[17] = f7cf7480  49b92296  9af9e76d  ebfa966c
W[18] = cb36b730  558e16c1  b1bad0ac  5b04114b
W[19] = a413de53  71c5fa8a  2d823ecd  065f65f0
```

```
W[20] = 7480f7cf  065f65f0  0bd5607a  576014ef
W[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
W[22] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
W[23] = 452c2723  386e33e1  3cfb2f54  f17090f6
W[24] = 6e21fe2e  409f2bb0  567715d8  35b3369c
W[25] = 0a03624c  983eea28  00e96b66  9ccbe59b
W[26] = a241e025  2f543cfb  92c8ef9e  d450ae16
W[27] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
W[28] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
W[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
W[30] = ebfa966c  237f48d0  255146fe  e76d9af9
W[31] = bca6c5c0  e93f9927  d195b0d1  58491406
```

Feistel Steps

```
IV :
A[0]=cb72a4f6  B[0]=7733f71e  C[0]=22dabc6f  D[0]=d56619cd
A[1]=ac183b31  B[1]=ecfb0d53  C[1]=3868825d  D[1]=d2607dda
A[2]=6dd85fcc  B[2]=7e27ab4d  C[2]=f1df71f0  D[2]=a6e1b399
A[3]=8cb9a5a4  B[3]=f0147830  C[3]=7aa038c8  D[3]=325bb747

IV XOR M :
A[0]=cb72a64a  B[0]=7733f71e  C[0]=22dabc6f  D[0]=d56619cd
A[1]=ac183b31  B[1]=ecfb0d53  C[1]=3868825d  D[1]=d2607dda
A[2]=6dd85fcc  B[2]=7e27ab4d  C[2]=f1df71f0  D[2]=a6e1b399
A[3]=8cb9a5a4  B[3]=f0147830  C[3]=7aa038c8  D[3]=325bb747

Step  0: (r= 3, s=20)
A[0]=34c02e68  B[0]=5b953256  C[0]=7733f71e  D[0]=22dabc6f
A[1]=9cdf8903  B[1]=60c1d98d  C[1]=ecfb0d53  D[1]=3868825d
A[2]=74fae195  B[2]=6ec2fe63  C[2]=7e27ab4d  D[2]=f1df71f0
A[3]=659275aa  B[3]=65cd2d24  C[3]=f0147830  D[3]=7aa038c8

Step  1: (r=20, s=14)
A[0]=83a86cf5  B[0]=e6834c02  C[0]=5b953256  D[0]=7733f71e
A[1]=f2ce0825  B[1]=9039cdf8  C[1]=60c1d98d  D[1]=ecfb0d53
A[2]=d0b82881  B[2]=19574fae  C[2]=6ec2fe63  D[2]=7e27ab4d
A[3]=addfb4d8  B[3]=5aa65927  C[3]=65cd2d24  D[3]=f0147830

Step  2: (r=14, s=27)
A[0]=bf082de4  B[0]=1b3d60ea  C[0]=e6834c02  D[0]=5b953256
A[1]=457de0c7  B[1]=82097cb3  C[1]=9039cdf8  D[1]=60c1d98d
A[2]=65c431f3  B[2]=0a20742e  C[2]=19574fae  D[2]=6ec2fe63
A[3]=dc5a9360  B[3]=ed362b77  C[3]=5aa65927  D[3]=65cd2d24

Step  3: (r=27, s= 3)
A[0]=e2359f53  B[0]=25f8416f  C[0]=1b3d60ea  D[0]=e6834c02
A[1]=fff5ea8f  B[1]=3a2bef06  C[1]=82097cb3  D[1]=9039cdf8
A[2]=65bb89e1  B[2]=9b2e218f  C[2]=0a20742e  D[2]=19574fae
```

```
A[3]=5d7d14c0  B[3]=06e2d49b  C[3]=ed362b77  D[3]=5aa65927

Step  4: (r= 3, s=20)
A[0]=398b8f04  B[0]=11acfa9f  C[0]=25f8416f  D[0]=1b3d60ea
A[1]=16df8347  B[1]=ffaf547f  C[1]=3a2bef06  D[1]=82097cb3
A[2]=a87ea246  B[2]=2ddc4f0b  C[2]=9b2e218f  D[2]=0a20742e
A[3]=cd023f26  B[3]=ebe8a602  C[3]=06e2d49b  D[3]=ed362b77

Step  5: (r=20, s=14)
A[0]=ad6c0f65  B[0]=f04398b8  C[0]=11acfa9f  D[0]=25f8416f
A[1]=d663ad2a  B[1]=34716df8  C[1]=ffaf547f  D[1]=3a2bef06
A[2]=8f63bfa9  B[2]=246a87ea  C[2]=2ddc4f0b  D[2]=9b2e218f
A[3]=ad88e1c2  B[3]=f26cd023  C[3]=ebe8a602  D[3]=06e2d49b

Step  6: (r=14, s=27)
A[0]=ea6ded71  B[0]=03d96b5b  C[0]=f04398b8  D[0]=11acfa9f
A[1]=7957c005  B[1]=eb4ab598  C[1]=34716df8  D[1]=ffaf547f
A[2]=afd0ba18  B[2]=efea63d8  C[2]=246a87ea  D[2]=2ddc4f0b
A[3]=9d781e3e  B[3]=3870ab62  C[3]=f26cd023  D[3]=ebe8a602

Step  7: (r=27, s= 3)
A[0]=9ade5f96  B[0]=8f536f6b  C[0]=03d96b5b  D[0]=f04398b8
A[1]=405f2096  B[1]=2bcabe00  C[1]=eb4ab598  D[1]=34716df8
A[2]=158230a1  B[2]=c57e85d0  C[2]=efea63d8  D[2]=246a87ea
A[3]=4686599b  B[3]=f4ebc0f1  C[3]=3870ab62  D[3]=f26cd023

Step  8: (r=26, s= 4)
A[0]=386f5e17  B[0]=5a6b797e  C[0]=8f536f6b  D[0]=03d96b5b
A[1]=b67c77ab  B[1]=59017c82  C[1]=2bcabe00  D[1]=eb4ab598
A[2]=5642f328  B[2]=845608c2  C[2]=c57e85d0  D[2]=efea63d8
A[3]=520b2f03  B[3]=6d1a1966  C[3]=f4ebc0f1  D[3]=3870ab62

Step  9: (r= 4, s=23)
A[0]=47255b92  B[0]=86f5e173  C[0]=5a6b797e  D[0]=8f536f6b
A[1]=94e1c8a4  B[1]=67c77abb  C[1]=59017c82  D[1]=2bcabe00
A[2]=10c9e0bf  B[2]=642f3285  C[2]=845608c2  D[2]=c57e85d0
A[3]=49e0a36f  B[3]=20b2f035  C[3]=6d1a1966  D[3]=f4ebc0f1

Step 10: (r=23, s=11)
A[0]=3e89d5d2  B[0]=c92392ad  C[0]=86f5e173  D[0]=5a6b797e
A[1]=3c30219d  B[1]=524a70e4  C[1]=67c77abb  D[1]=59017c82
A[2]=ae3aab8a  B[2]=5f8864f0  C[2]=642f3285  D[2]=845608c2
A[3]=e514bade  B[3]=b7a4f051  C[3]=20b2f035  D[3]=6d1a1966

Step 11: (r=11, s=26)
A[0]=5107a946  B[0]=4eae91f4  C[0]=c92392ad  D[0]=86f5e173
A[1]=af4096c5  B[1]=810ce9e1  C[1]=524a70e4  D[1]=67c77abb
A[2]=e9fb031b  B[2]=d55c5571  C[2]=5f8864f0  D[2]=642f3285
A[3]=e81cdd83  B[3]=a5d6f728  C[3]=b7a4f051  D[3]=20b2f035
```

```
Step 12: (r=26, s= 4)
A[0]=71a825c3  B[0]=19441ea5  C[0]=4eae91f4  D[0]=c92392ad
A[1]=79f0e82d  B[1]=16bd025b  C[1]=810ce9e1  D[1]=524a70e4
A[2]=c4a36314  B[2]=6fa7ec0c  C[2]=d55c5571  D[2]=5f8864f0
A[3]=52c49d0f  B[3]=0fa07376  C[3]=a5d6f728  D[3]=b7a4f051

Step 13: (r= 4, s=23)
A[0]=b02d38f2  B[0]=1a825c37  C[0]=19441ea5  D[0]=4eae91f4
A[1]=e1f044a6  B[1]=9f0e82d7  C[1]=16bd025b  D[1]=810ce9e1
A[2]=9e6f03f7  B[2]=4a36314c  C[2]=6fa7ec0c  D[2]=d55c5571
A[3]=ec102ef4  B[3]=2c49d0f5  C[3]=0fa07376  D[3]=a5d6f728

Step 14: (r=23, s=11)
A[0]=20b249ab  B[0]=7958169c  C[0]=1a825c37  D[0]=19441ea5
A[1]=bd093fb6  B[1]=5370f822  C[1]=9f0e82d7  D[1]=16bd025b
A[2]=c3aa400c  B[2]=fbcf3781  C[2]=4a36314c  D[2]=6fa7ec0c
A[3]=0429c75b  B[3]=7a760817  C[3]=2c49d0f5  D[3]=0fa07376

Step 15: (r=11, s=26)
A[0]=e4a5857c  B[0]=924d5905  C[0]=7958169c  D[0]=1a825c37
A[1]=d1df2b29  B[1]=49fdb5e8  C[1]=5370f822  D[1]=9f0e82d7
A[2]=884d4d9e  B[2]=5200661d  C[2]=fbcf3781  D[2]=4a36314c
A[3]=ff986bcc  B[3]=4e3ad821  C[3]=7a760817  D[3]=2c49d0f5

Step 16: (r=19, s=28)
A[0]=097f77c6  B[0]=2be7252c  C[0]=924d5905  D[0]=7958169c
A[1]=4dfd2d96  B[1]=594e8ef9  C[1]=49fdb5e8  D[1]=5370f822
A[2]=2484c51e  B[2]=6cf4426a  C[2]=5200661d  D[2]=fbcf3781
A[3]=a64eaac6  B[3]=5e67fcc3  C[3]=4e3ad821  D[3]=7a760817

Step 17: (r=28, s= 7)
A[0]=29a45cd7  B[0]=6097f77c  C[0]=2be7252c  D[0]=924d5905
A[1]=a5c0c31f  B[1]=64dfd2d9  C[1]=594e8ef9  D[1]=49fdb5e8
A[2]=07587402  B[2]=e2484c51  C[2]=6cf4426a  D[2]=5200661d
A[3]=d8ab8633  B[3]=6a64eaac  C[3]=5e67fcc3  D[3]=4e3ad821

Step 18: (r= 7, s=22)
A[0]=4cc1a2b3  B[0]=d22e6b94  C[0]=6097f77c  D[0]=2be7252c
A[1]=94c117a9  B[1]=e0618fd2  C[1]=64dfd2d9  D[1]=594e8ef9
A[2]=a21ec3cb  B[2]=ac3a0103  C[2]=e2484c51  D[2]=6cf4426a
A[3]=e56c548d  B[3]=55c319ec  C[3]=6a64eaac  D[3]=5e67fcc3

Step 19: (r=22, s=19)
A[0]=cdc2083b  B[0]=acd33068  C[0]=d22e6b94  D[0]=6097f77c
A[1]=ae16b6b7  B[1]=ea653045  C[1]=e0618fd2  D[1]=64dfd2d9
A[2]=1f2706ec  B[2]=f2e887b0  C[2]=ac3a0103  D[2]=e2484c51
A[3]=d562d085  B[3]=23795b15  C[3]=55c319ec  D[3]=6a64eaac
```

```
Step 20: (r=19, s=28)
A[0]=efdb222d  B[0]=41de6e10  C[0]=acd33068  D[0]=d22e6b94
A[1]=3cbb4832  B[1]=b5bd70b5  C[1]=ea653045  D[1]=e0618fd2
A[2]=3ef3265c  B[2]=3760f938  C[2]=f2e887b0  D[2]=ac3a0103
A[3]=4350f3a2  B[3]=842eab16  C[3]=23795b15  D[3]=55c319ec

Step 21: (r=28, s= 7)
A[0]=fdb10f0b  B[0]=defdb222  C[0]=41de6e10  D[0]=acd33068
A[1]=12e4db8e  B[1]=23cbb483  C[1]=b5bd70b5  D[1]=ea653045
A[2]=7640f965  B[2]=c3ef3265  C[2]=3760f938  D[2]=f2e887b0
A[3]=175807e3  B[3]=24350f3a  C[3]=842eab16  D[3]=23795b15

Step 22: (r= 7, s=22)
A[0]=42bfdf11  B[0]=d88785fe  C[0]=defdb222  D[0]=41de6e10
A[1]=ee7f4628  B[1]=726dc709  C[1]=23cbb483  D[1]=b5bd70b5
A[2]=c963bfc1  B[2]=207cb2bb  C[2]=c3ef3265  D[2]=3760f938
A[3]=7b86fc03  B[3]=ac03f18b  C[3]=24350f3a  D[3]=842eab16

Step 23: (r=22, s=19)
A[0]=539d6740  B[0]=c450aff7  C[0]=d88785fe  D[0]=defdb222
A[1]=55d9669a  B[1]=8a3b9fd1  C[1]=726dc709  D[1]=23cbb483
A[2]=9fba5e55  B[2]=f07258ef  C[2]=207cb2bb  D[2]=c3ef3265
A[3]=52f8ad0a  B[3]=00dee1bf  C[3]=ac03f18b  D[3]=24350f3a

Step 24: (r=15, s= 5)
A[0]=599834ae  B[0]=b3a029ce  C[0]=c450aff7  D[0]=d88785fe
A[1]=0437c86d  B[1]=b34d2aec  C[1]=8a3b9fd1  D[1]=726dc709
A[2]=b22d4f15  B[2]=2f2acfdd  C[2]=f07258ef  D[2]=207cb2bb
A[3]=8c2715ee  B[3]=5685297c  C[3]=00dee1bf  D[3]=ac03f18b

Step 25: (r= 5, s=29)
A[0]=74b3553b  B[0]=330695cb  C[0]=b3a029ce  D[0]=c450aff7
A[1]=3779f7f6  B[1]=86f90da0  C[1]=b34d2aec  D[1]=8a3b9fd1
A[2]=4382a58f  B[2]=45a9e2b6  C[2]=2f2acfdd  D[2]=f07258ef
A[3]=f0aec4b4  B[3]=84e2bdd1  C[3]=5685297c  D[3]=00dee1bf

Step 26: (r=29, s= 9)
A[0]=f08b1531  B[0]=6e966aa7  C[0]=330695cb  D[0]=b3a029ce
A[1]=02453d31  B[1]=c6ef3efe  C[1]=86f90da0  D[1]=b34d2aec
A[2]=667ca077  B[2]=e87054b1  C[2]=45a9e2b6  D[2]=2f2acfdd
A[3]=1511c55e  B[3]=9e15d896  C[3]=84e2bdd1  D[3]=5685297c

Step 27: (r= 9, s=15)
A[0]=227967b7  B[0]=162a63e1  C[0]=6e966aa7  D[0]=330695cb
A[1]=c8c92912  B[1]=8a7a6204  C[1]=c6ef3efe  D[1]=86f90da0
A[2]=c4c2bd45  B[2]=f940eecc  C[2]=e87054b1  D[2]=45a9e2b6
A[3]=66ba4dbd  B[3]=238abc2a  C[3]=9e15d896  D[3]=84e2bdd1

Step 28: (r=15, s= 5)
```

```
A[0]=3a4a9efa  B[0]=b3db913c  C[0]=162a63e1  D[0]=6e966aa7
A[1]=99a964b9  B[1]=94896464  C[1]=8a7a6204  D[1]=c6ef3efe
A[2]=db0035ea  B[2]=5ea2e261  C[2]=f940eecc  D[2]=e87054b1
A[3]=70392074  B[3]=26deb35d  C[3]=238abc2a  D[3]=9e15d896

Step 29: (r= 5, s=29)
A[0]=2bd4d5c9  B[0]=4953df47  C[0]=b3db913c  D[0]=162a63e1
A[1]=0f7336e3  B[1]=352c9733  C[1]=94896464  D[1]=8a7a6204
A[2]=55d002f9  B[2]=6006bd5b  C[2]=5ea2e261  D[2]=f940eecc
A[3]=97f46b2d  B[3]=07240e8e  C[3]=26deb35d  D[3]=238abc2a

Step 30: (r=29, s= 9)
A[0]=538d9b37  B[0]=257a9ab9  C[0]=4953df47  D[0]=b3db913c
A[1]=707c6fe5  B[1]=61ee66dc  C[1]=352c9733  D[1]=94896464
A[2]=dcaf144b  B[2]=2aba005f  C[2]=6006bd5b  D[2]=5ea2e261
A[3]=fe7efade  B[3]=b2fe8d65  C[3]=07240e8e  D[3]=26deb35d

Step 31: (r= 9, s=15)
A[0]=574270a7  B[0]=1b366ea7  C[0]=257a9ab9  D[0]=4953df47
A[1]=b0b63596  B[1]=f8dfcae0  C[1]=61ee66dc  D[1]=352c9733
A[2]=6efd3b1a  B[2]=5e2897b9  C[2]=2aba005f  D[2]=6006bd5b
A[3]=23f865b3  B[3]=fdf5bdfc  C[3]=b2fe8d65  D[3]=07240e8e

Feistel Step 0: (r=15, s= 5)
A[0]=1af937e4  B[0]=3853aba1  C[0]=1b366ea7  D[0]=257a9ab9
A[1]=01efdd18  B[1]=1acb585b  C[1]=f8dfcae0  D[1]=61ee66dc
A[2]=b3ffa27f  B[2]=9d8d377e  C[2]=5e2897b9  D[2]=2aba005f
A[3]=f2dff069  B[3]=32d991fc  C[3]=fdf5bdfc  D[3]=b2fe8d65

Feistel Step 1: (r= 5, s=29)
A[0]=d6b50fa5  B[0]=5f26fc83  C[0]=3853aba1  D[0]=1b366ea7
A[1]=44f6a722  B[1]=3dfba300  C[1]=1acb585b  D[1]=f8dfcae0
A[2]=aff4d8f8  B[2]=7ff44ff6  C[2]=9d8d377e  D[2]=5e2897b9
A[3]=7a5d3772  B[3]=5bfe0d3e  C[3]=32d991fc  D[3]=fdf5bdfc

Feistel Step 2: (r=29, s= 9)
A[0]=384e045c  B[0]=bad6a1f4  C[0]=5f26fc83  D[0]=3853aba1
A[1]=9e8fc7bf  B[1]=489ed4e4  C[1]=3dfba300  D[1]=1acb585b
A[2]=5a3ee60e  B[2]=15fe9b1f  C[2]=7ff44ff6  D[2]=9d8d377e
A[3]=9fcfa79a  B[3]=4f4ba6ee  C[3]=5bfe0d3e  D[3]=32d991fc

Feistel Step 3: (r= 9, s=15)
A[0]=dceee344  B[0]=9c08b870  C[0]=bad6a1f4  D[0]=5f26fc83
A[1]=fcbbc0d4  B[1]=1f8f7f3d  C[1]=489ed4e4  D[1]=3dfba300
A[2]=579375a6  B[2]=7dcc1cb4  C[2]=15fe9b1f  D[2]=7ff44ff6
A[3]=9b885995  B[3]=9f4f353f  C[3]=4f4ba6ee  D[3]=5bfe0d3e
```

Compression Function Output

```
A[0]=dceee344  B[0]=9c08b870  C[0]=bad6a1f4  D[0]=5f26fc83
```

```
A[1]=fcbbc0d4  B[1]=1f8f7f3d  C[1]=489ed4e4  D[1]=3dfba300
A[2]=579375a6  B[2]=7dcc1cb4  C[2]=15fe9b1f  D[2]=7ff44ff6
A[3]=9b885995  B[3]=9f4f353f  C[3]=4f4ba6ee  D[3]=5bfe0d3e
```

Hash Function Output

```
44e3eedcd4c0bbfca67593579559889b70b8089c3d7f8f1fb41ccc7d3f354f9f
```

6.3 SIMD-384

6.3.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  203  156   47  118  214  107  106
y[  8.. 15] =   45   93  212   20  111   73  162  251
y[ 16.. 23] =   97  215  249   53  211   19    3   89
y[ 24.. 31] =   49  207  101   67  151  130  223   23
y[ 32.. 39] =  189  202  178  239  253  127  204   49
y[ 40.. 47] =   76  236   82  137  232  157   65   79
y[ 48.. 55] =   96  161  176  130  161   30   47    9
y[ 56.. 63] =  189  247   61  226  248   90  107   64
y[ 64.. 71] =    0   88  131  243  133   59  113  115
y[ 72.. 79] =   17  236   33  213   12  191  111   19
y[ 80.. 87] =  251   61  103  208   57   35  148  248
y[ 88.. 95] =   47  116   65  119  249  178  143   40
y[ 96..103] =  189  129    8  163  204  227  230  196
y[104..111] =  205  122  151   45  187   19  227   72
```

```
y[112..119] =  247  125  111  121  140  220    6  107
y[120..127] =   77   69   10  101   21   65  149  171
y[128..135] =  255   54  101  210  139   43  150  151
y[136..143] =  212  164   45  237  146  184   95    6
y[144..151] =  160   42    8  204   46  238  254  168
y[152..159] =  208   50  156  190  106  127   34  234
y[160..167] =   68   55   79   18    4  130   53  208
y[168..175] =  181   21  175  120   25  100  192  178
y[176..183] =  161   96   81  127   96  227  210  248
y[184..191] =   68   10  196   31    9  167  150  193
y[192..199] =    0  169  126   14  124  198  144  142
y[200..207] =  240   21  224   44  245   66  146  238
y[208..215] =    6  196  154   49  200  222  109    9
y[216..223] =  210  141  192  138    8   79  114  217
y[224..231] =   68  128  249   94   53   30   27   61
y[232..239] =   52  135  106  212   70  238   30  185
y[240..247] =   10  132  146  136  117   37  251  150
y[248..255] =  180  188  247  156  236  192  108   86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
```

```
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
Z[17] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
Z[18] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
Z[19] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
Z[20] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
Z[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
Z[22] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
Z[23] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
Z[24] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
Z[25] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
Z[26] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
Z[27] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
Z[28] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
Z[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
        966c6994  93b16c4f  47e7b819  db982468
Z[30] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
Z[31] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
```

Expanded Message

```
W[ 0] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
W[ 3] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
```

```
W[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
W[ 8] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
W[17] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
W[18] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
W[19] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
W[20] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
W[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
W[22] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
W[23] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
W[24] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
W[25] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
W[26] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
W[27] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
W[28] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
W[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
```

```
        966c6994  93b16c4f  47e7b819  db982468
W[30] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
W[31] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
```

Feistel Steps

```
IV :
A[0]=0d14da0d  B[0]=fba71944  C[0]=e65ced88  D[0]=f8773176
A[1]=95c2d7d5  B[1]=6e1b3ca0  C[1]=b0667012  D[1]=4c45a87d
A[2]=a95b8260  B[2]=7d0b1a7c  C[2]=916393e6  D[2]=c3280609
A[3]=b4722c01  B[3]=b506d742  C[3]=4b0643ce  D[3]=e6996ca4
A[4]=e4be208b  B[4]=c417ab0b  C[4]=4fbed3f1  D[4]=694e541f
A[5]=12cb4873  B[5]=eb34f21c  C[5]=9627d2bc  D[5]=0e3dcf80
A[6]=67773662  B[6]=bab7945b  C[6]=eb96513b  D[6]=042ab187
A[7]=56a66d24  B[7]=d1ed927e  C[7]=9aa6c3e3  D[7]=71fb0b87

IV XOR M :
A[0]=0d14da0d  B[0]=fba71944  C[0]=e65ced88  D[0]=f8773176
A[1]=95c2d7d5  B[1]=6e1b3ca0  C[1]=b0667012  D[1]=4c45a87d
A[2]=a95b8260  B[2]=7d0b1a7c  C[2]=916393e6  D[2]=c3280609
A[3]=b4722c01  B[3]=b506d742  C[3]=4b0643ce  D[3]=e6996ca4
A[4]=e4be208b  B[4]=c417ab0b  C[4]=4fbed3f1  D[4]=694e541f
A[5]=12cb4873  B[5]=eb34f21c  C[5]=9627d2bc  D[5]=0e3dcf80
A[6]=67773662  B[6]=bab7945b  C[6]=eb96513b  D[6]=042ab187
A[7]=56a66d24  B[7]=d1ed927e  C[7]=9aa6c3e3  D[7]=71fb0b87

Step  0: (r= 3, s=20)
A[0]=9db8f462  B[0]=68a6d068  C[0]=fba71944  D[0]=e65ced88
A[1]=87bd3550  B[1]=ae16beac  C[1]=6e1b3ca0  D[1]=b0667012
A[2]=a8c3cf79  B[2]=4adc1305  C[2]=7d0b1a7c  D[2]=916393e6
A[3]=ac8f9eb5  B[3]=a391600d  C[3]=b506d742  D[3]=4b0643ce
A[4]=d48cd71d  B[4]=25f1045f  C[4]=c417ab0b  D[4]=4fbed3f1
A[5]=c5484dca  B[5]=965a4398  C[5]=eb34f21c  D[5]=9627d2bc
A[6]=ae1b5c22  B[6]=3bb9b313  C[6]=bab7945b  D[6]=eb96513b
A[7]=260f38c0  B[7]=b5336922  C[7]=d1ed927e  D[7]=9aa6c3e3

Step  1: (r=20, s=14)
A[0]=5d0cc95d  B[0]=4629db8f  C[0]=68a6d068  D[0]=fba71944
A[1]=97f95f9c  B[1]=55087bd3  C[1]=ae16beac  D[1]=6e1b3ca0
A[2]=e65191ee  B[2]=f79a8c3c  C[2]=4adc1305  D[2]=7d0b1a7c
A[3]=316d2fef  B[3]=eb5ac8f9  C[3]=a391600d  D[3]=b506d742
A[4]=f8ca0cd4  B[4]=71dd48cd  C[4]=25f1045f  D[4]=c417ab0b
A[5]=2a71fa3d  B[5]=dcac5484  C[5]=965a4398  D[5]=eb34f21c
A[6]=5d9d55d0  B[6]=c22ae1b5  C[6]=3bb9b313  D[6]=bab7945b
A[7]=b2c945a8  B[7]=8c0260f3  C[7]=b5336922  D[7]=d1ed927e

Step  2: (r=14, s=27)
```

```
A[0]=6b348c51  B[0]=32575743  C[0]=4629db8f  D[0]=68a6d068
A[1]=f3dd26e1  B[1]=57e725fe  C[1]=55087bd3  D[1]=ae16beac
A[2]=f8f3f22b  B[2]=647bb994  C[2]=f79a8c3c  D[2]=4adc1305
A[3]=7861099d  B[3]=4bfbcc5b  C[3]=eb5ac8f9  D[3]=a391600d
A[4]=47e5fafd  B[4]=83353e32  C[4]=71dd48cd  D[4]=25f1045f
A[5]=412a5aac  B[5]=7e8f4a9c  C[5]=dcac5484  D[5]=965a4398
A[6]=8274343f  B[6]=55741767  C[6]=c22ae1b5  D[6]=3bb9b313
A[7]=fcedacf6  B[7]=516a2cb2  C[7]=8c0260f3  D[7]=b5336922

Step  3: (r=27, s= 3)
A[0]=226ee872  B[0]=8b59a462  C[0]=32575743  D[0]=4629db8f
A[1]=28e16f14  B[1]=0f9ee937  C[1]=57e725fe  D[1]=55087bd3
A[2]=6d120349  B[2]=5fc79f91  C[2]=647bb994  D[2]=f79a8c3c
A[3]=4b9f7f33  B[3]=ebc3084c  C[3]=4bfbcc5b  D[3]=eb5ac8f9
A[4]=db65503c  B[4]=ea3f2fd7  C[4]=83353e32  D[4]=71dd48cd
A[5]=f1255467  B[5]=620952d5  C[5]=7e8f4a9c  D[5]=dcac5484
A[6]=ff7354da  B[6]=fc13a1a1  C[6]=55741767  D[6]=c22ae1b5
A[7]=e16b2ebd  B[7]=b7e76d67  C[7]=516a2cb2  D[7]=8c0260f3

Step  4: (r= 3, s=20)
A[0]=d287a69c  B[0]=13774391  C[0]=8b59a462  D[0]=32575743
A[1]=a78309a4  B[1]=470b78a1  C[1]=0f9ee937  D[1]=57e725fe
A[2]=91009cb7  B[2]=68901a4b  C[2]=5fc79f91  D[2]=647bb994
A[3]=033862dc  B[3]=5cfbf99a  C[3]=ebc3084c  D[3]=4bfbcc5b
A[4]=73b1923a  B[4]=db2a81e6  C[4]=ea3f2fd7  D[4]=83353e32
A[5]=c463fd50  B[5]=892aa33f  C[5]=620952d5  D[5]=7e8f4a9c
A[6]=77b85f5f  B[6]=fb9aa6d7  C[6]=fc13a1a1  D[6]=55741767
A[7]=f57e9b5a  B[7]=0b5975ef  C[7]=b7e76d67  D[7]=516a2cb2

Step  5: (r=20, s=14)
A[0]=09d88c7a  B[0]=69cd287a  C[0]=13774391  D[0]=8b59a462
A[1]=a444c288  B[1]=9a4a7830  C[1]=470b78a1  D[1]=0f9ee937
A[2]=4a235e4b  B[2]=cb791009  C[2]=68901a4b  D[2]=5fc79f91
A[3]=53e71c8d  B[3]=2dc03386  C[3]=5cfbf99a  D[3]=ebc3084c
A[4]=2eff7016  B[4]=23a73b19  C[4]=db2a81e6  D[4]=ea3f2fd7
A[5]=50e9fd17  B[5]=d50c463f  C[5]=892aa33f  D[5]=620952d5
A[6]=5204c217  B[6]=f5f77b85  C[6]=fb9aa6d7  D[6]=fc13a1a1
A[7]=6afc0fb3  B[7]=b5af57e9  C[7]=0b5975ef  D[7]=b7e76d67

Step  6: (r=14, s=27)
A[0]=e66b9250  B[0]=231e8276  C[0]=69cd287a  D[0]=13774391
A[1]=a256edbb  B[1]=30a22911  C[1]=9a4a7830  D[1]=470b78a1
A[2]=65430fdd  B[2]=d792d288  C[2]=cb791009  D[2]=68901a4b
A[3]=6686c6dd  B[3]=c72354f9  C[3]=2dc03386  D[3]=5cfbf99a
A[4]=0f98fe77  B[4]=dc058bbf  C[4]=23a73b19  D[4]=db2a81e6
A[5]=20792db9  B[5]=7f45d43a  C[5]=d50c463f  D[5]=892aa33f
A[6]=ea27d4fe  B[6]=3085d481  C[6]=f5f77b85  D[6]=fb9aa6d7
A[7]=4bafab0b  B[7]=03ecdabf  C[7]=b5af57e9  D[7]=0b5975ef
```

```
Step  7: (r=27, s= 3)
A[0]=7be528d5  B[0]=87335c92  C[0]=231e8276  D[0]=69cd287a
A[1]=c5e2a9bd  B[1]=dd12b76d  C[1]=30a22911  D[1]=9a4a7830
A[2]=e4499b58  B[2]=eb2a187e  C[2]=d792d288  D[2]=cb791009
A[3]=80d81268  B[3]=eb343636  C[3]=c72354f9  D[3]=2dc03386
A[4]=bba66108  B[4]=b87cc7f3  C[4]=dc058bbf  D[4]=23a73b19
A[5]=542c3b26  B[5]=c903c96d  C[5]=7f45d43a  D[5]=d50c463f
A[6]=6f0b8e92  B[6]=f7513ea7  C[6]=3085d481  D[6]=f5f77b85
A[7]=e87dfe76  B[7]=5a5d7d58  C[7]=03ecdabf  D[7]=b5af57e9

Step  8: (r=26, s= 4)
A[0]=22533107  B[0]=55ef94a3  C[0]=87335c92  D[0]=231e8276
A[1]=d3bc2706  B[1]=f7178aa6  C[1]=dd12b76d  D[1]=30a22911
A[2]=3f0f3736  B[2]=6391266d  C[2]=eb2a187e  D[2]=d792d288
A[3]=dda98487  B[3]=a2036049  C[3]=eb343636  D[3]=c72354f9
A[4]=785da3aa  B[4]=22ee9984  C[4]=b87cc7f3  D[4]=dc058bbf
A[5]=980f5da3  B[5]=9950b0ec  C[5]=c903c96d  D[5]=7f45d43a
A[6]=c3eea5ac  B[6]=49bc2e3a  C[6]=f7513ea7  D[6]=3085d481
A[7]=44ee5b1d  B[7]=dba1f7f9  C[7]=5a5d7d58  D[7]=03ecdabf

Step  9: (r= 4, s=23)
A[0]=c5ea64af  B[0]=25331072  C[0]=55ef94a3  D[0]=87335c92
A[1]=df4e0878  B[1]=3bc2706d  C[1]=f7178aa6  D[1]=dd12b76d
A[2]=4f859395  B[2]=f0f37363  C[2]=6391266d  D[2]=eb2a187e
A[3]=d573cc9f  B[3]=da98487d  C[3]=a2036049  D[3]=eb343636
A[4]=992c310d  B[4]=85da3aa7  C[4]=22ee9984  D[4]=b87cc7f3
A[5]=d79d08f0  B[5]=80f5da39  C[5]=9950b0ec  D[5]=c903c96d
A[6]=1c8cd733  B[6]=3eea5acc  C[6]=49bc2e3a  D[6]=f7513ea7
A[7]=e38e09bb  B[7]=4ee5b1d4  C[7]=dba1f7f9  D[7]=5a5d7d58

Step 10: (r=23, s=11)
A[0]=f55769ea  B[0]=57e2f532  C[0]=25331072  D[0]=55ef94a3
A[1]=be398f7f  B[1]=3c6fa704  C[1]=3bc2706d  D[1]=f7178aa6
A[2]=3db7e78c  B[2]=caa7c2c9  C[2]=f0f37363  D[2]=6391266d
A[3]=d933ea69  B[3]=4feab9e6  C[3]=da98487d  D[3]=a2036049
A[4]=fb8c3541  B[4]=86cc9618  C[4]=85da3aa7  D[4]=22ee9984
A[5]=fdf64656  B[5]=786bce84  C[5]=80f5da39  D[5]=9950b0ec
A[6]=21efc329  B[6]=998e466b  C[6]=3eea5acc  D[6]=49bc2e3a
A[7]=a10a826c  B[7]=ddf1c704  C[7]=4ee5b1d4  D[7]=dba1f7f9

Step 11: (r=11, s=26)
A[0]=f0f373ed  B[0]=bb4f57aa  C[0]=57e2f532  D[0]=25331072
A[1]=4e7eeb19  B[1]=cc7bfdf1  C[1]=3c6fa704  D[1]=3bc2706d
A[2]=c7477b9f  B[2]=bf3c61ed  C[2]=caa7c2c9  D[2]=f0f37363
A[3]=fe97b7f5  B[3]=9f534ec9  C[3]=4feab9e6  D[3]=da98487d
A[4]=50e9ba08  B[4]=61aa0fdc  C[4]=86cc9618  D[4]=85da3aa7
A[5]=448900af  B[5]=b232b7ef  C[5]=786bce84  D[5]=80f5da39
A[6]=800e8ad0  B[6]=7e19490f  C[6]=998e466b  D[6]=3eea5acc
A[7]=7212c689  B[7]=54136508  C[7]=ddf1c704  D[7]=4ee5b1d4
```

```
Step 12: (r=26, s= 4)
A[0]=dc4e1bdf  B[0]=b7c3cdcf  C[0]=bb4f57aa  D[0]=57e2f532
A[1]=d71a2235  B[1]=6539fbac  C[1]=cc7bfdf1  D[1]=3c6fa704
A[2]=fdf9e5ca  B[2]=7f1d1dee  C[2]=bf3c61ed  D[2]=caa7c2c9
A[3]=20dd8165  B[3]=d7fa5edf  C[3]=9f534ec9  D[3]=4feab9e6
A[4]=6b6d7970  B[4]=2143a6e8  C[4]=61aa0fdc  D[4]=86cc9618
A[5]=2cb525a4  B[5]=bd122402  C[5]=b232b7ef  D[5]=786bce84
A[6]=51c7662d  B[6]=42003a2b  C[6]=7e19490f  D[6]=998e466b
A[7]=67a95114  B[7]=25c84b1a  C[7]=54136508  D[7]=ddf1c704

Step 13: (r= 4, s=23)
A[0]=8b93eb5b  B[0]=c4e1bdfd  C[0]=b7c3cdcf  D[0]=bb4f57aa
A[1]=32eaa0fe  B[1]=71a2235d  C[1]=6539fbac  D[1]=cc7bfdf1
A[2]=883a0b7c  B[2]=df9e5caf  C[2]=7f1d1dee  D[2]=bf3c61ed
A[3]=2e194708  B[3]=0dd81652  C[3]=d7fa5edf  D[3]=9f534ec9
A[4]=29409527  B[4]=b6d79706  C[4]=2143a6e8  D[4]=61aa0fdc
A[5]=13846128  B[5]=cb525a42  C[5]=bd122402  D[5]=b232b7ef
A[6]=e7e9ea61  B[6]=1c7662d5  C[6]=42003a2b  D[6]=7e19490f
A[7]=0a65a3ef  B[7]=7a951146  C[7]=25c84b1a  D[7]=54136508

Step 14: (r=23, s=11)
A[0]=8b3a9e27  B[0]=adc5c9f5  C[0]=c4e1bdfd  D[0]=b7c3cdcf
A[1]=77cc174e  B[1]=7f197550  C[1]=71a2235d  D[1]=6539fbac
A[2]=301fbc44  B[2]=be441d05  C[2]=df9e5caf  D[2]=7f1d1dee
A[3]=a9f024a8  B[3]=84170ca3  C[3]=0dd81652  D[3]=d7fa5edf
A[4]=5f97c133  B[4]=9394a04a  C[4]=b6d79706  D[4]=2143a6e8
A[5]=ad299a24  B[5]=9409c230  C[5]=cb525a42  D[5]=bd122402
A[6]=6d457db5  B[6]=30f3f4f5  C[6]=1c7662d5  D[6]=42003a2b
A[7]=bf90b423  B[7]=f78532d1  C[7]=7a951146  D[7]=25c84b1a

Step 15: (r=11, s=26)
A[0]=6092316f  B[0]=d4f13c59  C[0]=adc5c9f5  D[0]=c4e1bdfd
A[1]=4d53ea1e  B[1]=60ba73be  C[1]=7f197550  D[1]=71a2235d
A[2]=2d3950eb  B[2]=fde22180  C[2]=be441d05  D[2]=df9e5caf
A[3]=97e89bd8  B[3]=8125454f  C[3]=84170ca3  D[3]=0dd81652
A[4]=ce74018e  B[4]=be099afc  C[4]=9394a04a  D[4]=b6d79706
A[5]=5160d0e8  B[5]=4cd12569  C[5]=9409c230  D[5]=cb525a42
A[6]=d7a51506  B[6]=2bedab6a  C[6]=30f3f4f5  D[6]=1c7662d5
A[7]=b0ea9b93  B[7]=85a11dfc  C[7]=f78532d1  D[7]=7a951146

Step 16: (r=19, s=28)
A[0]=44995b90  B[0]=8b7b0491  C[0]=d4f13c59  D[0]=adc5c9f5
A[1]=ca2b5dc8  B[1]=50f26a9f  C[1]=60ba73be  D[1]=7f197550
A[2]=3b52d349  B[2]=875969ca  C[2]=fde22180  D[2]=be441d05
A[3]=101eabb1  B[3]=dec4bf44  C[3]=8125454f  D[3]=84170ca3
A[4]=39de814c  B[4]=0c7673a0  C[4]=be099afc  D[4]=9394a04a
A[5]=7fb15f2a  B[5]=87428b06  C[5]=4cd12569  D[5]=9409c230
A[6]=c6ac1598  B[6]=a836bd28  C[6]=2bedab6a  D[6]=30f3f4f5
```

```
A[7]=ee498fea  B[7]=dc9d8754  C[7]=85a11dfc  D[7]=f78532d1

Step 17: (r=28, s= 7)
A[0]=a58da272  B[0]=044995b9  C[0]=8b7b0491  D[0]=d4f13c59
A[1]=eacdfe4e  B[1]=8ca2b5dc  C[1]=50f26a9f  D[1]=60ba73be
A[2]=f1072a7d  B[2]=93b52d34  C[2]=875969ca  D[2]=fde22180
A[3]=4a088ffe  B[3]=1101eabb  C[3]=dec4bf44  D[3]=8125454f
A[4]=ec6b54c7  B[4]=c39de814  C[4]=0c7673a0  D[4]=be099afc
A[5]=0300a3a6  B[5]=a7fb15f2  C[5]=87428b06  D[5]=4cd12569
A[6]=516cb78c  B[6]=8c6ac159  C[6]=a836bd28  D[6]=2bedab6a
A[7]=aafdbd37  B[7]=aee498fe  C[7]=dc9d8754  D[7]=85a11dfc

Step 18: (r= 7, s=22)
A[0]=7b19bdc2  B[0]=c6d13952  C[0]=044995b9  D[0]=8b7b0491
A[1]=1f00dfcb  B[1]=66ff2775  C[1]=8ca2b5dc  D[1]=50f26a9f
A[2]=aed1c249  B[2]=83953ef8  C[2]=93b52d34  D[2]=875969ca
A[3]=956e80f7  B[3]=0447ff25  C[3]=1101eabb  D[3]=dec4bf44
A[4]=119603b6  B[4]=35aa63f6  C[4]=c39de814  D[4]=0c7673a0
A[5]=8d07fd46  B[5]=8051d301  C[5]=a7fb15f2  D[5]=87428b06
A[6]=52ef7a46  B[6]=b65bc628  C[6]=8c6ac159  D[6]=a836bd28
A[7]=508aede7  B[7]=7ede9bd5  C[7]=aee498fe  D[7]=dc9d8754

Step 19: (r=22, s=19)
A[0]=ddeaf3e1  B[0]=709ec66f  C[0]=c6d13952  D[0]=044995b9
A[1]=4bd59417  B[1]=f2c7c037  C[1]=66ff2775  D[1]=8ca2b5dc
A[2]=d4e91b37  B[2]=926bb470  C[2]=83953ef8  D[2]=93b52d34
A[3]=fc28045b  B[3]=3de55ba0  C[3]=0447ff25  D[3]=1101eabb
A[4]=e71d4aba  B[4]=ed846580  C[4]=35aa63f6  D[4]=c39de814
A[5]=c8c021d2  B[5]=51a341ff  C[5]=8051d301  D[5]=a7fb15f2
A[6]=ebd59124  B[6]=9194bbde  C[6]=b65bc628  D[6]=8c6ac159
A[7]=6fa90fcc  B[7]=79d422bb  C[7]=7ede9bd5  D[7]=aee498fe

Step 20: (r=19, s=28)
A[0]=222af35f  B[0]=9f0eef57  C[0]=709ec66f  D[0]=c6d13952
A[1]=5d92136c  B[1]=a0ba5eac  C[1]=f2c7c037  D[1]=66ff2775
A[2]=984da4f6  B[2]=d9bea748  C[2]=926bb470  D[2]=83953ef8
A[3]=701e5a5c  B[3]=22dfe140  C[3]=3de55ba0  D[3]=0447ff25
A[4]=3c1e37c8  B[4]=55d738ea  C[4]=ed846580  D[4]=35aa63f6
A[5]=126aa85e  B[5]=0e964601  C[5]=51a341ff  D[5]=8051d301
A[6]=7662ee94  B[6]=89275eac  C[6]=9194bbde  D[6]=b65bc628
A[7]=5dc85744  B[7]=7e637d48  C[7]=79d422bb  D[7]=7ede9bd5

Step 21: (r=28, s= 7)
A[0]=9512784e  B[0]=f222af35  C[0]=9f0eef57  D[0]=709ec66f
A[1]=b06d9621  B[1]=c5d92136  C[1]=a0ba5eac  D[1]=f2c7c037
A[2]=042e5429  B[2]=6984da4f  C[2]=d9bea748  D[2]=926bb470
A[3]=f454b982  B[3]=c701e5a5  C[3]=22dfe140  D[3]=3de55ba0
A[4]=844871ad  B[4]=83c1e37c  C[4]=55d738ea  D[4]=ed846580
A[5]=2b83ca1f  B[5]=e126aa85  C[5]=0e964601  D[5]=51a341ff
```

```
A[6]=e9a0a1a3  B[6]=47662ee9  C[6]=89275eac  D[6]=9194bbde
A[7]=11fc5837  B[7]=45dc8574  C[7]=7e637d48  D[7]=79d422bb

Step 22: (r= 7, s=22)
A[0]=e42d8f75  B[0]=893c274a  C[0]=f222af35  D[0]=9f0eef57
A[1]=6c0cbd92  B[1]=36cb10d8  C[1]=c5d92136  D[1]=a0ba5eac
A[2]=49c13cd2  B[2]=172a1482  C[2]=6984da4f  D[2]=d9bea748
A[3]=c5298ce9  B[3]=2a5cc17a  C[3]=c701e5a5  D[3]=22dfe140
A[4]=42af55ba  B[4]=2438d6c2  C[4]=83c1e37c  D[4]=55d738ea
A[5]=db139c7a  B[5]=c1e50f95  C[5]=e126aa85  D[5]=0e964601
A[6]=1a887deb  B[6]=d050d1f4  C[6]=47662ee9  D[6]=89275eac
A[7]=f745b954  B[7]=fe2c1b88  C[7]=45dc8574  D[7]=7e637d48

Step 23: (r=22, s=19)
A[0]=1ff1eab4  B[0]=dd790b63  C[0]=893c274a  D[0]=f222af35
A[1]=52e13ed1  B[1]=649b032f  C[1]=36cb10d8  D[1]=c5d92136
A[2]=e01a771a  B[2]=3492704f  C[2]=172a1482  D[2]=6984da4f
A[3]=e4c3ca84  B[3]=3a714a63  C[3]=2a5cc17a  D[3]=c701e5a5
A[4]=757dbe91  B[4]=6e90abd5  C[4]=2438d6c2  D[4]=83c1e37c
A[5]=c577c4f7  B[5]=1eb6c4e7  C[5]=c1e50f95  D[5]=e126aa85
A[6]=d7b98d1d  B[6]=7ac6a21f  C[6]=d050d1f4  D[6]=47662ee9
A[7]=fa69ecce  B[7]=553dd16e  C[7]=fe2c1b88  D[7]=45dc8574

Step 24: (r=15, s= 5)
A[0]=2371ed50  B[0]=f55a0ff8  C[0]=dd790b63  D[0]=893c274a
A[1]=f3b3c627  B[1]=9f68a970  C[1]=649b032f  D[1]=36cb10d8
A[2]=660863d8  B[2]=3b8d700d  C[2]=3492704f  D[2]=172a1482
A[3]=582ca352  B[3]=e5427261  C[3]=3a714a63  D[3]=2a5cc17a
A[4]=fba38dea  B[4]=df48babe  C[4]=6e90abd5  D[4]=2438d6c2
A[5]=7c5d26f5  B[5]=e27be2bb  C[5]=1eb6c4e7  D[5]=c1e50f95
A[6]=11e9a365  B[6]=c68eebdc  C[6]=7ac6a21f  D[6]=d050d1f4
A[7]=d6e23527  B[7]=f6677d34  C[7]=553dd16e  D[7]=fe2c1b88

Step 25: (r= 5, s=29)
A[0]=b803dbbe  B[0]=6e3daa04  C[0]=f55a0ff8  D[0]=dd790b63
A[1]=f9fa01e3  B[1]=7678c4fe  C[1]=9f68a970  D[1]=649b032f
A[2]=3c5ab5b1  B[2]=c10c7b0c  C[2]=3b8d700d  D[2]=3492704f
A[3]=1bff5688  B[3]=05946a4b  C[3]=e5427261  D[3]=3a714a63
A[4]=13090766  B[4]=7471bd5f  C[4]=df48babe  D[4]=6e90abd5
A[5]=5e9c4589  B[5]=8ba4deaf  C[5]=e27be2bb  D[5]=1eb6c4e7
A[6]=f37f9457  B[6]=3d346ca2  C[6]=c68eebdc  D[6]=7ac6a21f
A[7]=6709401e  B[7]=dc46a4fa  C[7]=f6677d34  D[7]=553dd16e

Step 26: (r=29, s= 9)
A[0]=e7c802e5  B[0]=d7007b77  C[0]=6e3daa04  D[0]=f55a0ff8
A[1]=ac28afdf  B[1]=7f3f403c  C[1]=7678c4fe  D[1]=9f68a970
A[2]=d5b8d4fe  B[2]=278b56b6  C[2]=c10c7b0c  D[2]=3b8d700d
A[3]=cc5cbc8a  B[3]=037fead1  C[3]=05946a4b  D[3]=e5427261
A[4]=adf84dc1  B[4]=c26120ec  C[4]=7471bd5f  D[4]=df48babe
```

```
A[5]=6f5c91cf  B[5]=2bd388b1  C[5]=8ba4deaf  D[5]=e27be2bb
A[6]=a47b6484  B[6]=fe6ff28a  C[6]=3d346ca2  D[6]=c68eebdc
A[7]=4147a9a0  B[7]=cce12803  C[7]=dc46a4fa  D[7]=f6677d34

Step 27: (r= 9, s=15)
A[0]=86acacc0  B[0]=9005cbcf  C[0]=d7007b77  D[0]=6e3daa04
A[1]=e50a76be  B[1]=515fbf58  C[1]=7f3f403c  D[1]=7678c4fe
A[2]=ddd43aab  B[2]=71a9fdab  C[2]=278b56b6  D[2]=c10c7b0c
A[3]=ee960360  B[3]=b9791598  C[3]=037fead1  D[3]=05946a4b
A[4]=653a843d  B[4]=f09b835b  C[4]=c26120ec  D[4]=7471bd5f
A[5]=58045898  B[5]=b9239ede  C[5]=2bd388b1  D[5]=8ba4deaf
A[6]=397da215  B[6]=f6c90948  C[6]=fe6ff28a  D[6]=3d346ca2
A[7]=671d260f  B[7]=8f534082  C[7]=cce12803  D[7]=dc46a4fa

Step 28: (r=15, s= 5)
A[0]=afc73ff0  B[0]=56604356  C[0]=9005cbcf  D[0]=d7007b77
A[1]=3c5937c1  B[1]=3b5f7285  C[1]=515fbf58  D[1]=7f3f403c
A[2]=6ab317ee  B[2]=1d55eeea  C[2]=71a9fdab  D[2]=278b56b6
A[3]=39a4b87f  B[3]=01b0774b  C[3]=b9791598  D[3]=037fead1
A[4]=e552c44d  B[4]=421eb29d  C[4]=f09b835b  D[4]=c26120ec
A[5]=5e2a14b9  B[5]=2c4c2c02  C[5]=b9239ede  D[5]=2bd388b1
A[6]=ca13c62b  B[6]=d10a9cbe  C[6]=f6c90948  D[6]=fe6ff28a
A[7]=fc0a846c  B[7]=9307b38e  C[7]=8f534082  D[7]=cce12803

Step 29: (r= 5, s=29)
A[0]=9d1b1da7  B[0]=f8e7fe15  C[0]=56604356  D[0]=9005cbcf
A[1]=d13e1953  B[1]=8b26f827  C[1]=3b5f7285  D[1]=515fbf58
A[2]=69144ce4  B[2]=5662fdcd  C[2]=1d55eeea  D[2]=71a9fdab
A[3]=f3d33b26  B[3]=34970fe7  C[3]=01b0774b  D[3]=b9791598
A[4]=e995c714  B[4]=aa5889bc  C[4]=421eb29d  D[4]=f09b835b
A[5]=e0c66fd2  B[5]=c542972b  C[5]=2c4c2c02  D[5]=b9239ede
A[6]=4d64f095  B[6]=4278c579  C[6]=d10a9cbe  D[6]=f6c90948
A[7]=ee3230ca  B[7]=81508d9f  C[7]=9307b38e  D[7]=8f534082

Step 30: (r=29, s= 9)
A[0]=00bc4251  B[0]=f3a363b4  C[0]=f8e7fe15  D[0]=56604356
A[1]=6401e204  B[1]=7a27c32a  C[1]=8b26f827  D[1]=3b5f7285
A[2]=f459632c  B[2]=8d22899c  C[2]=5662fdcd  D[2]=1d55eeea
A[3]=60ae0de6  B[3]=de7a6764  C[3]=34970fe7  D[3]=01b0774b
A[4]=8a621d3f  B[4]=9d32b8e2  C[4]=aa5889bc  D[4]=421eb29d
A[5]=7a6e3326  B[5]=5c18cdfa  C[5]=c542972b  D[5]=2c4c2c02
A[6]=036baa12  B[6]=a9ac9e12  C[6]=4278c579  D[6]=d10a9cbe
A[7]=29aa19b6  B[7]=5dc64619  C[7]=81508d9f  D[7]=9307b38e

Step 31: (r= 9, s=15)
A[0]=7de8bb9f  B[0]=7884a201  C[0]=f3a363b4  D[0]=f8e7fe15
A[1]=fe8b27e9  B[1]=03c408c8  C[1]=7a27c32a  D[1]=8b26f827
A[2]=fd5ae317  B[2]=b2c659e8  C[2]=8d22899c  D[2]=5662fdcd
A[3]=2e18913d  B[3]=5c1bccc1  C[3]=de7a6764  D[3]=34970fe7
```

```
A[4]=152411d8  B[4]=c43a7f14  C[4]=9d32b8e2  D[4]=aa5889bc
A[5]=aebe83af  B[5]=dc664cf4  C[5]=5c18cdfa  D[5]=c542972b
A[6]=9aac71a3  B[6]=d7542406  C[6]=a9ac9e12  D[6]=4278c579
A[7]=e0a5f732  B[7]=54336c53  C[7]=5dc64619  D[7]=81508d9f

Feistel Step 0: (r=15, s= 5)
A[0]=a40c47a5  B[0]=5dcfbef4  C[0]=7884a201  D[0]=f3a363b4
A[1]=cfa1d7b8  B[1]=93f4ff45  C[1]=03c408c8  D[1]=7a27c32a
A[2]=4cb7cdc2  B[2]=718bfead  C[2]=b2c659e8  D[2]=8d22899c
A[3]=221043e5  B[3]=489e970c  C[3]=5c1bccc1  D[3]=de7a6764
A[4]=ab044682  B[4]=08ec0a92  C[4]=c43a7f14  D[4]=9d32b8e2
A[5]=8f719ce8  B[5]=41d7d75f  C[5]=dc664cf4  D[5]=5c18cdfa
A[6]=9a2eadfd  B[6]=38d1cd56  C[6]=d7542406  D[6]=a9ac9e12
A[7]=e41da91c  B[7]=fb997052  C[7]=54336c53  D[7]=5dc64619

Feistel Step 1: (r= 5, s=29)
A[0]=20749cbc  B[0]=8188f4b4  C[0]=5dcfbef4  D[0]=7884a201
A[1]=8f8d7885  B[1]=f43af719  C[1]=93f4ff45  D[1]=03c408c8
A[2]=a12724cc  B[2]=96f9b849  C[2]=718bfead  D[2]=b2c659e8
A[3]=522e90ce  B[3]=42087ca4  C[3]=489e970c  D[3]=5c1bccc1
A[4]=bb86d3a3  B[4]=6088d055  C[4]=08ec0a92  D[4]=c43a7f14
A[5]=d6c9d62a  B[5]=ee339d11  C[5]=41d7d75f  D[5]=dc664cf4
A[6]=d8bf684d  B[6]=45d5bfb3  C[6]=38d1cd56  D[6]=d7542406
A[7]=323184ae  B[7]=83b5239c  C[7]=fb997052  D[7]=54336c53

Feistel Step 2: (r=29, s= 9)
A[0]=a0d32c0d  B[0]=840e9397  C[0]=8188f4b4  D[0]=5dcfbef4
A[1]=01f8239a  B[1]=b1f1af10  C[1]=f43af719  D[1]=93f4ff45
A[2]=02a9a8ee  B[2]=9424e499  C[2]=96f9b849  D[2]=718bfead
A[3]=ebc10257  B[3]=ca45d219  C[3]=42087ca4  D[3]=489e970c
A[4]=8e9bfe82  B[4]=7770da74  C[4]=6088d055  D[4]=08ec0a92
A[5]=df8eef0c  B[5]=5ad93ac5  C[5]=ee339d11  D[5]=41d7d75f
A[6]=32365757  B[6]=bb17ed09  C[6]=45d5bfb3  D[6]=38d1cd56
A[7]=ab50b90c  B[7]=c6463095  C[7]=83b5239c  D[7]=fb997052

Feistel Step 3: (r= 9, s=15)
A[0]=188cf0c5  B[0]=a6581b41  C[0]=840e9397  D[0]=8188f4b4
A[1]=ed4804d5  B[1]=f0473403  C[1]=b1f1af10  D[1]=f43af719
A[2]=c74e92f6  B[2]=5351dc05  C[2]=9424e499  D[2]=96f9b849
A[3]=62a31616  B[3]=8204afd7  C[3]=ca45d219  D[3]=42087ca4
A[4]=42db8766  B[4]=37fd051d  C[4]=7770da74  D[4]=6088d055
A[5]=60c1996a  B[5]=1dde19bf  C[5]=5ad93ac5  D[5]=ee339d11
A[6]=8991366f  B[6]=6caeae64  C[6]=bb17ed09  D[6]=45d5bfb3
A[7]=593ba813  B[7]=a1721956  C[7]=c6463095  D[7]=83b5239c
```

Compression Function Output

```
A[0]=188cf0c5  B[0]=a6581b41  C[0]=840e9397  D[0]=8188f4b4
A[1]=ed4804d5  B[1]=f0473403  C[1]=b1f1af10  D[1]=f43af719
```

```
A[2]=c74e92f6  B[2]=5351dc05  C[2]=9424e499  D[2]=96f9b849
A[3]=62a31616  B[3]=8204afd7  C[3]=ca45d219  D[3]=42087ca4
A[4]=42db8766  B[4]=37fd051d  C[4]=7770da74  D[4]=6088d055
A[5]=60c1996a  B[5]=1dde19bf  C[5]=5ad93ac5  D[5]=ee339d11
A[6]=8991366f  B[6]=6caeae64  C[6]=bb17ed09  D[6]=45d5bfb3
A[7]=593ba813  B[7]=a1721956  C[7]=c6463095  D[7]=83b5239c
```

Hash Function Output

```
c5f08c18d50448edf6924ec71616a3626687db426a99c160
6f36918913a83b59411b58a6033447f005dc5153d7af0482
```

6.3.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
```

```
y[104..111] =  129  171   92   61  218   92  254   87
y[112..119] =   84  189  205  152  233    8  203  182
y[120..127] =  168  207  190  143  124  129   57   30
y[128..135] =  192  141   92  168  121  110  169   28
y[136..143] =  128  161  211  146  197   45   44  249
y[144..151] =  171  249   62   82  157  156   70   32
y[152..159] =  122  202  163   42  174   32   21  256
y[160..167] =  244   93  107    0   28  137   44  134
y[168..175] =  129  255  154   17   97  197  180   68
y[176..183] =  132  107  244   30   65  163  147  190
y[184..191] =  115  193   79   65   69  180   30   67
y[192..199] =  205    3  191  238   12   69   15  256
y[200..207] =  106   66  122   90  108  168    4   39
y[208..215] =   82  251  217  159   43   47   16  138
y[216..223] =   62   41  152   21   23  239  124  246
y[224..231] =  176   51  194   43   74   68  188  100
y[232..239] =   19  207   16  134  197   67  195   38
y[240..247] =    3  145  211  141   79   12    7  226
y[248..255] =   91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
Z[10] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
```

```
        1da12cce  0f2db41f  f2fe109f  f80d599c
Z[14] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
Z[16] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
Z[17] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
Z[18] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
Z[19] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
Z[20] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
Z[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
Z[22] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
Z[23] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
Z[24] = 966c4d5d  aeffa6ce  641edd6a  197c1406
        a8a0b1ba  9af9be78  28f5409f  f8b83957
Z[25] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
Z[26] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
Z[27] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
Z[28] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
Z[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
Z[30] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
Z[31] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
```

```
        dbdebfaf  ad9ecf95  a380599c  15ae2931
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
W[17] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
W[18] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
W[19] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
W[20] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
W[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
W[22] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
W[23] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
W[24] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
W[25] = 966c4d5d  aeffa6ce  641edd6a  197c1406
        a8a0b1ba  9af9be78  28f5409f  f8b83957
W[26] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
W[27] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
W[28] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
```

```
W[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
W[30] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
W[31] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
```

Feistel Steps

```
IV :
A[0]=0d14da0d  B[0]=fba71944  C[0]=e65ced88  D[0]=f8773176
A[1]=95c2d7d5  B[1]=6e1b3ca0  C[1]=b0667012  D[1]=4c45a87d
A[2]=a95b8260  B[2]=7d0b1a7c  C[2]=916393e6  D[2]=c3280609
A[3]=b4722c01  B[3]=b506d742  C[3]=4b0643ce  D[3]=e6996ca4
A[4]=e4be208b  B[4]=c417ab0b  C[4]=4fbed3f1  D[4]=694e541f
A[5]=12cb4873  B[5]=eb34f21c  C[5]=9627d2bc  D[5]=0e3dcf80
A[6]=67773662  B[6]=bab7945b  C[6]=eb96513b  D[6]=042ab187
A[7]=56a66d24  B[7]=d1ed927e  C[7]=9aa6c3e3  D[7]=71fb0b87

IV XOR M :
A[0]=0e16db0d  B[0]=d8853864  C[0]=a51eacc8  D[0]=9b155016
A[1]=92c4d2d1  B[1]=493d1984  C[1]=f7203556  D[1]=2b23cd19
A[2]=a2518b68  B[2]=56213354  C[2]=da29daae  D[2]=a8426f61
A[3]=bb7c210d  B[3]=9a28fa6e  C[3]=04480e82  D[3]=89f701c8
A[4]=f7ac319b  B[4]=f7259a3b  C[4]=1cec82a1  D[4]=1a3c256f
A[5]=05dd5d67  B[5]=dc02c728  C[5]=c17187e8  D[5]=794bbaf4
A[6]=7c6d2f7a  B[6]=818dad63  C[6]=b0cc0863  D[6]=7f50c8ff
A[7]=49b87038  B[7]=eed3af42  C[7]=c5f89ebf  D[7]=0e8576fb

Step  0: (r= 3, s=20)
A[0]=f5167721  B[0]=70b6d868  C[0]=d8853864  D[0]=a51eacc8
A[1]=e1b29e47  B[1]=9626968c  C[1]=493d1984  D[1]=f7203556
A[2]=2dd0f55b  B[2]=128c5b45  C[2]=56213354  D[2]=da29daae
A[3]=12dfad64  B[3]=dbe1086d  C[3]=9a28fa6e  D[3]=04480e82
A[4]=c24db1f2  B[4]=bd618cdf  C[4]=f7259a3b  D[4]=1cec82a1
A[5]=42063f58  B[5]=2eeaeb38  C[5]=dc02c728  D[5]=c17187e8
A[6]=97b44fcd  B[6]=e3697bd3  C[6]=818dad63  D[6]=b0cc0863
A[7]=336c4bca  B[7]=4dc381c2  C[7]=eed3af42  D[7]=c5f89ebf

Step  1: (r=20, s=14)
A[0]=4d0e2a72  B[0]=721f5167  C[0]=70b6d868  D[0]=d8853864
A[1]=32b463aa  B[1]=e47e1b29  C[1]=9626968c  D[1]=493d1984
A[2]=74659051  B[2]=55b2dd0f  C[2]=128c5b45  D[2]=56213354
A[3]=ca1c07a5  B[3]=d6412dfa  C[3]=dbe1086d  D[3]=9a28fa6e
A[4]=2918a04e  B[4]=1f2c24db  C[4]=bd618cdf  D[4]=f7259a3b
A[5]=2a0a59a6  B[5]=f5842063  C[5]=2eeaeb38  D[5]=dc02c728
A[6]=d5320277  B[6]=fcd97b44  C[6]=e3697bd3  D[6]=818dad63
A[7]=0619d50e  B[7]=bca336c4  C[7]=4dc381c2  D[7]=eed3af42
```

```
Step  2: (r=14, s=27)
A[0]=b1790fa7  B[0]=8a9c9343  C[0]=721f5167  D[0]=70b6d868
A[1]=add305a4  B[1]=18ea8cad  C[1]=e47e1b29  D[1]=9626968c
A[2]=faf42ca6  B[2]=64145d19  C[2]=55b2dd0f  D[2]=128c5b45
A[3]=0c030bc0  B[3]=01e97287  C[3]=d6412dfa  D[3]=dbe1086d
A[4]=b49cbba3  B[4]=28138a46  C[4]=1f2c24db  D[4]=bd618cdf
A[5]=ea7b3a83  B[5]=96698a82  C[5]=f5842063  D[5]=2eeaeb38
A[6]=06443e18  B[6]=809df54c  C[6]=fcd97b44  D[6]=e3697bd3
A[7]=b5ed82a1  B[7]=75438186  C[7]=bca336c4  D[7]=4dc381c2

Step  3: (r=27, s= 3)
A[0]=f673d8a0  B[0]=3d8bc87d  C[0]=8a9c9343  D[0]=721f5167
A[1]=06a83a1a  B[1]=256e982d  C[1]=18ea8cad  D[1]=e47e1b29
A[2]=30869fec  B[2]=37d7a165  C[2]=64145d19  D[2]=55b2dd0f
A[3]=fdf8ce32  B[3]=0060185e  C[3]=01e97287  D[3]=d6412dfa
A[4]=90f307d2  B[4]=1da4e5dd  C[4]=28138a46  D[4]=1f2c24db
A[5]=b146e51c  B[5]=1f53d9d4  C[5]=96698a82  D[5]=f5842063
A[6]=051ca2e4  B[6]=c03221f0  C[6]=809df54c  D[6]=fcd97b44
A[7]=8a1c2008  B[7]=0daf6c15  C[7]=75438186  D[7]=bca336c4

Step  4: (r= 3, s=20)
A[0]=9d11ca46  B[0]=b39ec507  C[0]=3d8bc87d  D[0]=8a9c9343
A[1]=8fc89d8f  B[1]=3541d0d0  C[1]=256e982d  D[1]=18ea8cad
A[2]=820f72bd  B[2]=8434ff61  C[2]=37d7a165  D[2]=64145d19
A[3]=94df1ed7  B[3]=efc67197  C[3]=0060185e  D[3]=01e97287
A[4]=503864cb  B[4]=87983e94  C[4]=1da4e5dd  D[4]=28138a46
A[5]=205be4ff  B[5]=8a3728e5  C[5]=1f53d9d4  D[5]=96698a82
A[6]=bd2307ab  B[6]=28e51720  C[6]=c03221f0  D[6]=809df54c
A[7]=28830d27  B[7]=50e10044  C[7]=0daf6c15  D[7]=75438186

Step  5: (r=20, s=14)
A[0]=0685eff2  B[0]=a469d11c  C[0]=b39ec507  D[0]=3d8bc87d
A[1]=797db019  B[1]=d8f8fc89  C[1]=3541d0d0  D[1]=256e982d
A[2]=f3a898a9  B[2]=2bd820f7  C[2]=8434ff61  D[2]=37d7a165
A[3]=06d5c96e  B[3]=ed794df1  C[3]=efc67197  D[3]=0060185e
A[4]=6104f722  B[4]=4cb50386  C[4]=87983e94  D[4]=1da4e5dd
A[5]=7b3cf880  B[5]=4ff205be  C[5]=8a3728e5  D[5]=1f53d9d4
A[6]=db7992f3  B[6]=7abbd230  C[6]=28e51720  D[6]=c03221f0
A[7]=8281e2b0  B[7]=d2728830  C[7]=50e10044  D[7]=0daf6c15

Step  6: (r=14, s=27)
A[0]=1006bd91  B[0]=7bfc81a1  C[0]=a469d11c  D[0]=b39ec507
A[1]=79d128e2  B[1]=6c065e5f  C[1]=d8f8fc89  D[1]=3541d0d0
A[2]=26e247cc  B[2]=262a7cea  C[2]=2bd820f7  D[2]=8434ff61
A[3]=df470a66  B[3]=725b81b5  C[3]=ed794df1  D[3]=efc67197
A[4]=15e8ebe9  B[4]=3dc89841  C[4]=4cb50386  D[4]=87983e94
A[5]=c9b2dce6  B[5]=3e201ecf  C[5]=4ff205be  D[5]=8a3728e5
A[6]=35d43121  B[6]=64bcf6de  C[6]=7abbd230  D[6]=28e51720
A[7]=0ce6aa35  B[7]=78ac20a0  C[7]=d2728830  D[7]=50e10044
```

```
Step  7: (r=27, s= 3)
A[0]=30d9fc24  B[0]=888035ec  C[0]=7bfc81a1  D[0]=a469d11c
A[1]=47d81ae2  B[1]=13ce8947  C[1]=6c065e5f  D[1]=d8f8fc89
A[2]=66d87a7f  B[2]=6137123e  C[2]=262a7cea  D[2]=2bd820f7
A[3]=5494e035  B[3]=36fa3853  C[3]=725b81b5  D[3]=ed794df1
A[4]=58f6433b  B[4]=48af475f  C[4]=3dc89841  D[4]=4cb50386
A[5]=8412ffcb  B[5]=364d96e7  C[5]=3e201ecf  D[5]=4ff205be
A[6]=0b70bd6c  B[6]=09aea189  C[6]=64bcf6de  D[6]=7abbd230
A[7]=e9257f37  B[7]=a8673551  C[7]=78ac20a0  D[7]=d2728830

Step  8: (r=26, s= 4)
A[0]=7affef34  B[0]=90c367f0  C[0]=888035ec  D[0]=7bfc81a1
A[1]=a005e29b  B[1]=891f606b  C[1]=13ce8947  D[1]=6c065e5f
A[2]=20b96049  B[2]=fd9b61e9  C[2]=6137123e  D[2]=262a7cea
A[3]=dc72aaf9  B[3]=d5525380  C[3]=36fa3853  D[3]=725b81b5
A[4]=ae62564c  B[4]=ed63d90c  C[4]=48af475f  D[4]=3dc89841
A[5]=bae23cc9  B[5]=2e104bff  C[5]=364d96e7  D[5]=3e201ecf
A[6]=f77d25c7  B[6]=b02dc2f5  C[6]=09aea189  D[6]=64bcf6de
A[7]=7618e60f  B[7]=dfa495fc  C[7]=a8673551  D[7]=78ac20a0

Step  9: (r= 4, s=23)
A[0]=adc30e61  B[0]=affef347  C[0]=90c367f0  D[0]=888035ec
A[1]=ebb571fc  B[1]=005e29ba  C[1]=891f606b  D[1]=13ce8947
A[2]=e120e156  B[2]=0b960492  C[2]=fd9b61e9  D[2]=6137123e
A[3]=5cfa8f5c  B[3]=c72aaf9d  C[3]=d5525380  D[3]=36fa3853
A[4]=b5d0989d  B[4]=e62564ca  C[4]=ed63d90c  D[4]=48af475f
A[5]=cc5bf468  B[5]=ae23cc9b  C[5]=2e104bff  D[5]=364d96e7
A[6]=aa98489e  B[6]=77d25c7f  C[6]=b02dc2f5  D[6]=09aea189
A[7]=83678c00  B[7]=618e60f7  C[7]=dfa495fc  D[7]=a8673551

Step 10: (r=23, s=11)
A[0]=73e2fe09  B[0]=30d6e187  C[0]=affef347  D[0]=90c367f0
A[1]=e32fcc55  B[1]=fe75dab8  C[1]=005e29ba  D[1]=891f606b
A[2]=ad435b7f  B[2]=ab709070  C[2]=0b960492  D[2]=fd9b61e9
A[3]=aff12027  B[3]=ae2e7d47  C[3]=c72aaf9d  D[3]=d5525380
A[4]=d4da886b  B[4]=4edae84c  C[4]=e62564ca  D[4]=ed63d90c
A[5]=8966119a  B[5]=34662dfa  C[5]=ae23cc9b  D[5]=2e104bff
A[6]=9c468298  B[6]=4f554c24  C[6]=77d25c7f  D[6]=b02dc2f5
A[7]=13286a97  B[7]=0041b3c6  C[7]=618e60f7  D[7]=dfa495fc

Step 11: (r=11, s=26)
A[0]=d02a9b0e  B[0]=17f04b9f  C[0]=30d6e187  D[0]=affef347
A[1]=b539e67d  B[1]=7e62af19  C[1]=fe75dab8  D[1]=005e29ba
A[2]=5ff87c1b  B[2]=1adbfd6a  C[2]=ab709070  D[2]=0b960492
A[3]=62b39fa7  B[3]=89013d7f  C[3]=ae2e7d47  D[3]=c72aaf9d
A[4]=682c5c28  B[4]=d4435ea6  C[4]=4edae84c  D[4]=e62564ca
A[5]=ee73b6fa  B[5]=308cd44b  C[5]=34662dfa  D[5]=ae23cc9b
A[6]=1bde1d3a  B[6]=3414c4e2  C[6]=4f554c24  D[6]=77d25c7f
```

```
A[7]=41eac8e1  B[7]=4354b899  C[7]=0041b3c6  D[7]=618e60f7

Step 12: (r=26, s= 4)
A[0]=a97cf2a4  B[0]=3b40aa6c  C[0]=17f04b9f  D[0]=30d6e187
A[1]=dc64f67f  B[1]=f6d4e799  C[1]=7e62af19  D[1]=fe75dab8
A[2]=86b65b0b  B[2]=6d7fe1f0  C[2]=1adbfd6a  D[2]=ab709070
A[3]=f461db98  B[3]=9d8ace7e  C[3]=89013d7f  D[3]=ae2e7d47
A[4]=96cb60db  B[4]=a1a0b170  C[4]=d4435ea6  D[4]=4edae84c
A[5]=aff48be0  B[5]=ebb9cedb  C[5]=308cd44b  D[5]=34662dfa
A[6]=697e758d  B[6]=e86f7874  C[6]=3414c4e2  D[6]=4f554c24
A[7]=09d206ce  B[7]=8507ab23  C[7]=4354b899  D[7]=0041b3c6

Step 13: (r= 4, s=23)
A[0]=2619a9bb  B[0]=97cf2a4a  C[0]=3b40aa6c  D[0]=17f04b9f
A[1]=baf8be61  B[1]=c64f67fd  C[1]=f6d4e799  D[1]=7e62af19
A[2]=0ebd5e1e  B[2]=6b65b0b8  C[2]=6d7fe1f0  D[2]=1adbfd6a
A[3]=f14a00b1  B[3]=461db98f  C[3]=9d8ace7e  D[3]=89013d7f
A[4]=9de7f899  B[4]=6cb60db9  C[4]=a1a0b170  D[4]=d4435ea6
A[5]=0f981538  B[5]=ff48be0a  C[5]=ebb9cedb  D[5]=308cd44b
A[6]=408b76a1  B[6]=97e758d6  C[6]=e86f7874  D[6]=3414c4e2
A[7]=f64590e5  B[7]=9d206ce0  C[7]=8507ab23  D[7]=4354b899

Step 14: (r=23, s=11)
A[0]=f260475b  B[0]=dd930cd4  C[0]=97cf2a4a  D[0]=3b40aa6c
A[1]=4fc37164  B[1]=30dd7c5f  C[1]=c64f67fd  D[1]=f6d4e799
A[2]=ac1abda7  B[2]=0f075eaf  C[2]=6b65b0b8  D[2]=6d7fe1f0
A[3]=93ff4425  B[3]=58f8a500  C[3]=461db98f  D[3]=9d8ace7e
A[4]=1ed7a103  B[4]=4ccef3fc  C[4]=6cb60db9  D[4]=a1a0b170
A[5]=88471012  B[5]=9c07cc0a  C[5]=ff48be0a  D[5]=ebb9cedb
A[6]=74fcfaac  B[6]=50a045bb  C[6]=97e758d6  D[6]=e86f7874
A[7]=d6e1b51f  B[7]=72fb22c8  C[7]=9d206ce0  D[7]=8507ab23

Step 15: (r=11, s=26)
A[0]=b1e796ee  B[0]=023adf93  C[0]=dd930cd4  D[0]=97cf2a4a
A[1]=75f37500  B[1]=1b8b227e  C[1]=30dd7c5f  D[1]=c64f67fd
A[2]=4f0c12f7  B[2]=d5ed3d60  C[2]=0f075eaf  D[2]=6b65b0b8
A[3]=a68c33bd  B[3]=fa212c9f  C[3]=58f8a500  D[3]=461db98f
A[4]=95643516  B[4]=bd0818f6  C[4]=4ccef3fc  D[4]=6cb60db9
A[5]=f0479c57  B[5]=38809442  C[5]=9c07cc0a  D[5]=ff48be0a
A[6]=2fa43bf7  B[6]=e7d563a7  C[6]=50a045bb  D[6]=97e758d6
A[7]=6ffeab2b  B[7]=0da8feb7  C[7]=72fb22c8  D[7]=9d206ce0

Step 16: (r=19, s=28)
A[0]=715f6c28  B[0]=b7758f3c  C[0]=023adf93  D[0]=dd930cd4
A[1]=b87a587c  B[1]=a803af9b  C[1]=1b8b227e  D[1]=30dd7c5f
A[2]=934451f4  B[2]=97ba7860  C[2]=d5ed3d60  D[2]=0f075eaf
A[3]=5fbec2cf  B[3]=9ded3461  C[3]=fa212c9f  D[3]=58f8a500
A[4]=9e543f98  B[4]=a8b4ab21  C[4]=bd0818f6  D[4]=4ccef3fc
A[5]=c7106a05  B[5]=e2bf823c  C[5]=38809442  D[5]=9c07cc0a
```

```
A[6]=05998f75  B[6]=dfb97d21  C[6]=e7d563a7  D[6]=50a045bb
A[7]=9c97f99b  B[7]=595b7ff5  C[7]=0da8feb7  D[7]=72fb22c8

Step 17: (r=28, s= 7)
A[0]=e359db21  B[0]=8715f6c2  C[0]=b7758f3c  D[0]=023adf93
A[1]=d835384a  B[1]=cb87a587  C[1]=a803af9b  D[1]=1b8b227e
A[2]=9dba8ec2  B[2]=4934451f  C[2]=97ba7860  D[2]=d5ed3d60
A[3]=24ee7c26  B[3]=f5fbec2c  C[3]=9ded3461  D[3]=fa212c9f
A[4]=0648fab7  B[4]=89e543f9  C[4]=a8b4ab21  D[4]=bd0818f6
A[5]=2686f135  B[5]=5c7106a0  C[5]=e2bf823c  D[5]=38809442
A[6]=ed8bfb41  B[6]=505998f7  C[6]=dfb97d21  D[6]=e7d563a7
A[7]=6d7124c3  B[7]=b9c97f99  C[7]=595b7ff5  D[7]=0da8feb7

Step 18: (r= 7, s=22)
A[0]=41796cb6  B[0]=aced90f1  C[0]=8715f6c2  D[0]=b7758f3c
A[1]=75740e5c  B[1]=1a9c256c  C[1]=cb87a587  D[1]=a803af9b
A[2]=2e02dbf9  B[2]=dd47614e  C[2]=4934451f  D[2]=97ba7860
A[3]=1c2cf69c  B[3]=773e1312  C[3]=f5fbec2c  D[3]=9ded3461
A[4]=60ec4714  B[4]=247d5b83  C[4]=89e543f9  D[4]=a8b4ab21
A[5]=391dc564  B[5]=43789a93  C[5]=5c7106a0  D[5]=e2bf823c
A[6]=539c8dc8  B[6]=c5fda0f6  C[6]=505998f7  D[6]=dfb97d21
A[7]=403baa1d  B[7]=b89261b6  C[7]=b9c97f99  D[7]=595b7ff5

Step 19: (r=22, s=19)
A[0]=ad18af8f  B[0]=2d905e5b  C[0]=aced90f1  D[0]=8715f6c2
A[1]=8fde7bc3  B[1]=971d5d03  C[1]=1a9c256c  D[1]=cb87a587
A[2]=b5c4660a  B[2]=fe4b80b6  C[2]=dd47614e  D[2]=4934451f
A[3]=73d51b89  B[3]=a7070b3d  C[3]=773e1312  D[3]=f5fbec2c
A[4]=1445f341  B[4]=c5183b11  C[4]=247d5b83  D[4]=89e543f9
A[5]=97721714  B[5]=590e4771  C[5]=43789a93  D[5]=5c7106a0
A[6]=d8779fd3  B[6]=7214e723  C[6]=c5fda0f6  D[6]=505998f7
A[7]=743fc1cf  B[7]=87500eea  C[7]=b89261b6  D[7]=b9c97f99

Step 20: (r=19, s=28)
A[0]=cccbe52b  B[0]=7c7d68c5  C[0]=2d905e5b  D[0]=aced90f1
A[1]=3f9a43c6  B[1]=de1c7ef3  C[1]=971d5d03  D[1]=1a9c256c
A[2]=04e90614  B[2]=3055ae23  C[2]=fe4b80b6  D[2]=dd47614e
A[3]=f33a122c  B[3]=dc4b9ea8  C[3]=a7070b3d  D[3]=773e1312
A[4]=629da037  B[4]=9a08a22f  C[4]=c5183b11  D[4]=247d5b83
A[5]=75f05945  B[5]=b8a4bb90  C[5]=590e4771  D[5]=43789a93
A[6]=cd1ee3d4  B[6]=fe9ec3bc  C[6]=7214e723  D[6]=c5fda0f6
A[7]=c1f5afa8  B[7]=0e7ba1fe  C[7]=87500eea  D[7]=b89261b6

Step 21: (r=28, s= 7)
A[0]=74d6bd13  B[0]=bcccbe52  C[0]=7c7d68c5  D[0]=2d905e5b
A[1]=777d0c6c  B[1]=63f9a43c  C[1]=de1c7ef3  D[1]=971d5d03
A[2]=173436ee  B[2]=404e9061  C[2]=3055ae23  D[2]=fe4b80b6
A[3]=d0ac05fa  B[3]=cf33a122  C[3]=dc4b9ea8  D[3]=a7070b3d
A[4]=cf1aa3cc  B[4]=7629da03  C[4]=9a08a22f  D[4]=c5183b11
```

```
A[5]=52385628  B[5]=575f0594  C[5]=b8a4bb90  D[5]=590e4771
A[6]=fc13526f  B[6]=4cd1ee3d  C[6]=fe9ec3bc  D[6]=7214e723
A[7]=c78e0fec  B[7]=8c1f5afa  C[7]=0e7ba1fe  D[7]=87500eea

Step 22: (r= 7, s=22)
A[0]=d4e3c794  B[0]=6b5e89ba  C[0]=bcccbe52  D[0]=7c7d68c5
A[1]=dac1cdbc  B[1]=be86363b  C[1]=63f9a43c  D[1]=de1c7ef3
A[2]=f34a4487  B[2]=9a1b770b  C[2]=404e9061  D[2]=3055ae23
A[3]=109ead17  B[3]=5602fd68  C[3]=cf33a122  D[3]=dc4b9ea8
A[4]=be08e5bc  B[4]=8d51e667  C[4]=7629da03  D[4]=9a08a22f
A[5]=bdfbd238  B[5]=1c2b1429  C[5]=575f0594  D[5]=b8a4bb90
A[6]=74143966  B[6]=09a937fe  C[6]=4cd1ee3d  D[6]=fe9ec3bc
A[7]=a92de88d  B[7]=c707f663  C[7]=8c1f5afa  D[7]=0e7ba1fe

Step 23: (r=22, s=19)
A[0]=d95fbe71  B[0]=e53538f1  C[0]=6b5e89ba  D[0]=bcccbe52
A[1]=cf8de742  B[1]=6f36b073  C[1]=be86363b  D[1]=63f9a43c
A[2]=1d06f35b  B[2]=21fcd291  C[2]=9a1b770b  D[2]=404e9061
A[3]=5738bd83  B[3]=45c427ab  C[3]=5602fd68  D[3]=cf33a122
A[4]=c6f33ede  B[4]=6f2f8239  C[4]=8d51e667  D[4]=7629da03
A[5]=d057a0b1  B[5]=8e2f7ef4  C[5]=1c2b1429  D[5]=575f0594
A[6]=9f19227d  B[6]=599d050e  C[6]=09a937fe  D[6]=4cd1ee3d
A[7]=aef9de79  B[7]=236a4b7a  C[7]=c707f663  D[7]=8c1f5afa

Step 24: (r=15, s= 5)
A[0]=bd44329f  B[0]=df38ecaf  C[0]=e53538f1  D[0]=6b5e89ba
A[1]=23b147b0  B[1]=f3a167c6  C[1]=6f36b073  D[1]=be86363b
A[2]=88e6bd5c  B[2]=79ad8e83  C[2]=21fcd291  D[2]=9a1b770b
A[3]=60f16570  B[3]=5ec1ab9c  C[3]=45c427ab  D[3]=5602fd68
A[4]=c9e2a6fd  B[4]=9f6f6379  C[4]=6f2f8239  D[4]=8d51e667
A[5]=12dd9da7  B[5]=d058e82b  C[5]=8e2f7ef4  D[5]=1c2b1429
A[6]=6007c870  B[6]=913ecf8c  C[6]=599d050e  D[6]=09a937fe
A[7]=d5c163ee  B[7]=ef3cd77c  C[7]=236a4b7a  D[7]=c707f663

Step 25: (r= 5, s=29)
A[0]=f8b72b91  B[0]=a88653f7  C[0]=df38ecaf  D[0]=e53538f1
A[1]=b9d268a5  B[1]=7628f604  C[1]=f3a167c6  D[1]=6f36b073
A[2]=6d853855  B[2]=1cd7ab91  C[2]=79ad8e83  D[2]=21fcd291
A[3]=acd17ca5  B[3]=1e2cae0c  C[3]=5ec1ab9c  D[3]=45c427ab
A[4]=5da5455f  B[4]=3c54dfb9  C[4]=9f6f6379  D[4]=6f2f8239
A[5]=42a0757c  B[5]=5bb3b4e2  C[5]=d058e82b  D[5]=8e2f7ef4
A[6]=a5dc886e  B[6]=00f90e0c  C[6]=913ecf8c  D[6]=599d050e
A[7]=30910448  B[7]=b82c7dda  C[7]=ef3cd77c  D[7]=236a4b7a

Step 26: (r=29, s= 9)
A[0]=ffb135a3  B[0]=3f16e572  C[0]=a88653f7  D[0]=df38ecaf
A[1]=ca2be164  B[1]=b73a4d14  C[1]=7628f604  D[1]=f3a167c6
A[2]=03a84274  B[2]=adb0a70a  C[2]=1cd7ab91  D[2]=79ad8e83
A[3]=b680802c  B[3]=b59a2f94  C[3]=1e2cae0c  D[3]=5ec1ab9c
```

```
A[4]=94420f4a  B[4]=ebb4a8ab  C[4]=3c54dfb9  D[4]=9f6f6379
A[5]=73683418  B[5]=88540eaf  C[5]=5bb3b4e2  D[5]=d058e82b
A[6]=266fac23  B[6]=d4bb910d  C[6]=00f90e0c  D[6]=913ecf8c
A[7]=9d2babb5  B[7]=06122089  C[7]=b82c7dda  D[7]=ef3cd77c

Step 27: (r= 9, s=15)
A[0]=8f3f7158  B[0]=626b47ff  C[0]=3f16e572  D[0]=a88653f7
A[1]=0004d102  B[1]=57c2c994  C[1]=b73a4d14  D[1]=7628f604
A[2]=7ffe9794  B[2]=5084e807  C[2]=adb0a70a  D[2]=1cd7ab91
A[3]=22066ad5  B[3]=0100596d  C[3]=b59a2f94  D[3]=1e2cae0c
A[4]=69c47e6a  B[4]=841e9528  C[4]=ebb4a8ab  D[4]=3c54dfb9
A[5]=5a6c67c5  B[5]=d06830e6  C[5]=88540eaf  D[5]=5bb3b4e2
A[6]=bf11906e  B[6]=df58464c  C[6]=d4bb910d  D[6]=00f90e0c
A[7]=b4caf7fd  B[7]=57576b3a  C[7]=06122089  D[7]=b82c7dda

Step 28: (r=15, s= 5)
A[0]=8d995169  B[0]=b8ac479f  C[0]=626b47ff  D[0]=3f16e572
A[1]=c7e4bc54  B[1]=68810002  C[1]=57c2c994  D[1]=b73a4d14
A[2]=d53e726b  B[2]=4bca3fff  C[2]=5084e807  D[2]=adb0a70a
A[3]=92577f1f  B[3]=356a9103  C[3]=0100596d  D[3]=b59a2f94
A[4]=a9187033  B[4]=3f3534e2  C[4]=841e9528  D[4]=ebb4a8ab
A[5]=2851b42f  B[5]=33e2ad36  C[5]=d06830e6  D[5]=88540eaf
A[6]=bbd26b38  B[6]=c8375f88  C[6]=df58464c  D[6]=d4bb910d
A[7]=377d2069  B[7]=7bfeda65  C[7]=57576b3a  D[7]=06122089

Step 29: (r= 5, s=29)
A[0]=c417b139  B[0]=b32a2d31  C[0]=b8ac479f  D[0]=626b47ff
A[1]=3fa90a4e  B[1]=fc978a98  C[1]=68810002  D[1]=57c2c994
A[2]=d86af991  B[2]=a7ce4d7a  C[2]=4bca3fff  D[2]=5084e807
A[3]=07e94e97  B[3]=4aefe3f2  C[3]=356a9103  D[3]=0100596d
A[4]=1211b03a  B[4]=230e0675  C[4]=3f3534e2  D[4]=841e9528
A[5]=491e4a9f  B[5]=0a3685e5  C[5]=33e2ad36  D[5]=d06830e6
A[6]=770385c4  B[6]=7a4d6717  C[6]=c8375f88  D[6]=df58464c
A[7]=98a875ab  B[7]=efa40d26  C[7]=7bfeda65  D[7]=57576b3a

Step 30: (r=29, s= 9)
A[0]=1d3eecdf  B[0]=3882f627  C[0]=b32a2d31  D[0]=b8ac479f
A[1]=80f6b83d  B[1]=c7f52149  C[1]=fc978a98  D[1]=68810002
A[2]=23e6b409  B[2]=3b0d5f32  C[2]=a7ce4d7a  D[2]=4bca3fff
A[3]=489cfa17  B[3]=e0fd29d2  C[3]=4aefe3f2  D[3]=356a9103
A[4]=6cbfb3b8  B[4]=42423607  C[4]=230e0675  D[4]=3f3534e2
A[5]=4cad2f8d  B[5]=e923c953  C[5]=0a3685e5  D[5]=33e2ad36
A[6]=85318559  B[6]=8ee070b8  C[6]=7a4d6717  D[6]=c8375f88
A[7]=3ee16b14  B[7]=73150eb5  C[7]=efa40d26  D[7]=7bfeda65

Step 31: (r= 9, s=15)
A[0]=c6d49417  B[0]=7dd9be3a  C[0]=3882f627  D[0]=b32a2d31
A[1]=2d0f3155  B[1]=ed707b01  C[1]=c7f52149  D[1]=fc978a98
A[2]=bfc2b43a  B[2]=cd681247  C[2]=3b0d5f32  D[2]=a7ce4d7a
```

```
A[3]=8b43afb7  B[3]=39f42e91  C[3]=e0fd29d2  D[3]=4aefe3f2
A[4]=8c428df3  B[4]=7f6770d9  C[4]=42423607  D[4]=230e0675
A[5]=a5c7c0c2  B[5]=5a5f1a99  C[5]=e923c953  D[5]=0a3685e5
A[6]=42612245  B[6]=630ab30a  C[6]=8ee070b8  D[6]=7a4d6717
A[7]=8a58cb55  B[7]=c2d6287d  C[7]=73150eb5  D[7]=efa40d26

Feistel Step 0: (r=15, s= 5)
A[0]=3aea448e  B[0]=4a0be36a  C[0]=7dd9be3a  D[0]=3882f627
A[1]=935e523a  B[1]=98aa9687  C[1]=ed707b01  D[1]=c7f52149
A[2]=a6c1213c  B[2]=5a1d5fe1  C[2]=cd681247  D[2]=3b0d5f32
A[3]=85e5386e  B[3]=d7dbc5a1  C[3]=39f42e91  D[3]=e0fd29d2
A[4]=a22c8d8d  B[4]=46f9c621  C[4]=7f6770d9  D[4]=42423607
A[5]=f414c34d  B[5]=e06152e3  C[5]=5a5f1a99  D[5]=e923c953
A[6]=6e4ccb62  B[6]=9122a130  C[6]=630ab30a  D[6]=8ee070b8
A[7]=c5138917  B[7]=65aac52c  C[7]=c2d6287d  D[7]=73150eb5

Feistel Step 1: (r= 5, s=29)
A[0]=888ce8c8  B[0]=5d4891c7  C[0]=4a0be36a  D[0]=7dd9be3a
A[1]=42ee60ed  B[1]=6bca4752  C[1]=98aa9687  D[1]=ed707b01
A[2]=7db0c369  B[2]=d8242794  C[2]=5a1d5fe1  D[2]=cd681247
A[3]=1644e84a  B[3]=bca70dd0  C[3]=d7dbc5a1  D[3]=39f42e91
A[4]=365226f9  B[4]=4591b1b4  C[4]=46f9c621  D[4]=7f6770d9
A[5]=ba45a5c0  B[5]=829869be  C[5]=e06152e3  D[5]=5a5f1a99
A[6]=aee5087b  B[6]=c9996c4d  C[6]=9122a130  D[6]=630ab30a
A[7]=74319211  B[7]=a27122f8  C[7]=65aac52c  D[7]=c2d6287d

Feistel Step 2: (r=29, s= 9)
A[0]=b2e57b9e  B[0]=11119d19  C[0]=5d4891c7  D[0]=4a0be36a
A[1]=b95f4c00  B[1]=a85dcc1d  C[1]=6bca4752  D[1]=98aa9687
A[2]=08d41029  B[2]=2fb6186d  C[2]=d8242794  D[2]=5a1d5fe1
A[3]=59cac594  B[3]=42c89d09  C[3]=bca70dd0  D[3]=d7dbc5a1
A[4]=03139130  B[4]=26ca44df  C[4]=4591b1b4  D[4]=46f9c621
A[5]=7e7809d2  B[5]=1748b4b8  C[5]=829869be  D[5]=e06152e3
A[6]=f1b8e9ed  B[6]=75dca10f  C[6]=c9996c4d  D[6]=9122a130
A[7]=8178d617  B[7]=2e863242  C[7]=a27122f8  D[7]=65aac52c

Feistel Step 3: (r= 9, s=15)
A[0]=7e3f2fcc  B[0]=caf73d65  C[0]=11119d19  D[0]=5d4891c7
A[1]=b73f0ce2  B[1]=be980172  C[1]=a85dcc1d  D[1]=6bca4752
A[2]=40a7d6df  B[2]=a8205211  C[2]=2fb6186d  D[2]=d8242794
A[3]=516f00b3  B[3]=958b28b3  C[3]=42c89d09  D[3]=bca70dd0
A[4]=e861b8ca  B[4]=27226006  C[4]=26ca44df  D[4]=4591b1b4
A[5]=8027c425  B[5]=f013a4fc  C[5]=1748b4b8  D[5]=829869be
A[6]=24025984  B[6]=71d3dbe3  C[6]=75dca10f  D[6]=c9996c4d
A[7]=175a2586  B[7]=f1ac2f02  C[7]=2e863242  D[7]=a27122f8
```

Compression Function Output

```
A[0]=7e3f2fcc  B[0]=caf73d65  C[0]=11119d19  D[0]=5d4891c7
```

```
A[1]=b73f0ce2  B[1]=be980172  C[1]=a85dcc1d  D[1]=6bca4752
A[2]=40a7d6df  B[2]=a8205211  C[2]=2fb6186d  D[2]=d8242794
A[3]=516f00b3  B[3]=958b28b3  C[3]=42c89d09  D[3]=bca70dd0
A[4]=e861b8ca  B[4]=27226006  C[4]=26ca44df  D[4]=4591b1b4
A[5]=8027c425  B[5]=f013a4fc  C[5]=1748b4b8  D[5]=829869be
A[6]=24025984  B[6]=71d3dbe3  C[6]=75dca10f  D[6]=c9996c4d
A[7]=175a2586  B[7]=f1ac2f02  C[7]=2e863242  D[7]=a27122f8
```

Final block

```
M[  0..  7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
```

```
y[168..175] =  249  239  118   96   69  105  140  102
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
Z[11] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
Z[17] = a06f5f91  bad4452c  c4d73b29  f5140aec
```

```
        f2590da7  ff1700e9  74808b80  0748f8b8
Z[18] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
Z[19] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
Z[20] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
Z[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
Z[22] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
Z[23] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
Z[24] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
Z[25] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
Z[26] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
Z[27] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
Z[28] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
Z[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
Z[30] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
Z[31] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
```

```
         e8e01f13  b92ee6b5  44a749b6  e827f5e2
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
         cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
         582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
         410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
         b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
         3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
         f2fefa38  45605546  4be131dd  49b6ab73
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
         121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a06f5f91  bad4452c  c4d73b29  f5140aec
         f2590da7  ff1700e9  74808b80  0748f8b8
W[17] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
         f8b80748  6b66949a  3ecdc133  95836a7d
W[18] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
         2723d8dd  e0251fdb  5cd6a32a  f3420cbe
W[19] = c5c03a40  e2e01d20  065ff9a1  4188be78
         fe2e01d2  fc5c03a4  ab5b54a5  c792386e
W[20] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
         65f09a10  e0251fdb  02bbfd45  e3c91c37
W[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
         f0870f79  f9a1065f  5dbfa241  d70b28f5
W[22] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
         e684197c  5677a989  a4fc5b04  4aa2b55e
W[23] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
         cfc3303d  4aa2b55e  5849a7b7  29ded622
W[24] = afe85018  949a6b66  6a7d9583  4443bbbd
         16c1e93f  4d5db2a3  3785c87b  fd4502bb
W[25] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
         51eaae16  e85617aa  6e2191df  f42b0bd5
W[26] = e59b1a65  5beda413  32f8cd08  32f8cd08
         a6ce5932  b81947e7  00e9ff17  c87b3785
W[27] = d8dd2723  e3c91c37  d62229de  b81947e7
         e2e01d20  a6ce5932  5677a989  e1f71e09
W[28] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
         c21c3de4  f0870f79  b73048d0  2551daaf
W[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
         4e46b1ba  ceda3126  6c4f93b1  6ff3900d
W[30] = 68ab9755  dc81237f  1893e76d  0f79f087
         6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
W[31] = b0d14f2f  3ecdc133  14efeb11  f1700e90
         ef9e1062  5760a8a0  5f91a06f  5cd6a32a
```

Feistel Steps

```
IV :
A[0]=7e3f2fcc  B[0]=caf73d65  C[0]=11119d19  D[0]=5d4891c7
A[1]=b73f0ce2  B[1]=be980172  C[1]=a85dcc1d  D[1]=6bca4752
A[2]=40a7d6df  B[2]=a8205211  C[2]=2fb6186d  D[2]=d8242794
A[3]=516f00b3  B[3]=958b28b3  C[3]=42c89d09  D[3]=bca70dd0
A[4]=e861b8ca  B[4]=27226006  C[4]=26ca44df  D[4]=4591b1b4
A[5]=8027c425  B[5]=f013a4fc  C[5]=1748b4b8  D[5]=829869be
A[6]=24025984  B[6]=71d3dbe3  C[6]=75dca10f  D[6]=c9996c4d
A[7]=175a2586  B[7]=f1ac2f02  C[7]=2e863242  D[7]=a27122f8

IV XOR M :
A[0]=7e3f2bcc  B[0]=caf73d65  C[0]=11119d19  D[0]=5d4891c7
A[1]=b73f0ce2  B[1]=be980172  C[1]=a85dcc1d  D[1]=6bca4752
A[2]=40a7d6df  B[2]=a8205211  C[2]=2fb6186d  D[2]=d8242794
A[3]=516f00b3  B[3]=958b28b3  C[3]=42c89d09  D[3]=bca70dd0
A[4]=e861b8ca  B[4]=27226006  C[4]=26ca44df  D[4]=4591b1b4
A[5]=8027c425  B[5]=f013a4fc  C[5]=1748b4b8  D[5]=829869be
A[6]=24025984  B[6]=71d3dbe3  C[6]=75dca10f  D[6]=c9996c4d
A[7]=175a2586  B[7]=f1ac2f02  C[7]=2e863242  D[7]=a27122f8

Step  0: (r= 3, s=20)
A[0]=8fbdbd6c  B[0]=f1f95e63  C[0]=caf73d65  D[0]=11119d19
A[1]=e10dc384  B[1]=b9f86715  C[1]=be980172  D[1]=a85dcc1d
A[2]=56e742c1  B[2]=053eb6fa  C[2]=a8205211  D[2]=2fb6186d
A[3]=7d7af5a1  B[3]=8b78059a  C[3]=958b28b3  D[3]=42c89d09
A[4]=750f624d  B[4]=430dc657  C[4]=27226006  D[4]=26ca44df
A[5]=58f1bdd9  B[5]=013e212c  C[5]=f013a4fc  D[5]=1748b4b8
A[6]=4bb1015a  B[6]=2012cc21  C[6]=71d3dbe3  D[6]=75dca10f
A[7]=90938719  B[7]=bad12c30  C[7]=f1ac2f02  D[7]=2e863242

Step  1: (r=20, s=14)
A[0]=8dfcb31d  B[0]=d6c8fbdb  C[0]=f1f95e63  D[0]=caf73d65
A[1]=74c046fe  B[1]=384e10dc  C[1]=b9f86715  D[1]=be980172
A[2]=cfb59dae  B[2]=2c156e74  C[2]=053eb6fa  D[2]=a8205211
A[3]=e3adf67f  B[3]=5a17d7af  C[3]=8b78059a  D[3]=958b28b3
A[4]=e3325109  B[4]=24d750f6  C[4]=430dc657  D[4]=27226006
A[5]=ed64e7bb  B[5]=dd958f1b  C[5]=013e212c  D[5]=f013a4fc
A[6]=0338af7c  B[6]=15a4bb10  C[6]=2012cc21  D[6]=71d3dbe3
A[7]=7ac457b6  B[7]=71990938  C[7]=bad12c30  D[7]=f1ac2f02

Step  2: (r=14, s=27)
A[0]=c66798ba  B[0]=2cc7637f  C[0]=d6c8fbdb  D[0]=f1f95e63
A[1]=8ef21893  B[1]=11bf9d30  C[1]=384e10dc  D[1]=b9f86715
A[2]=90a67861  B[2]=676bb3ed  C[2]=2c156e74  D[2]=053eb6fa
A[3]=611c506c  B[3]=7d9ff8eb  C[3]=5a17d7af  D[3]=8b78059a
A[4]=3dd1bb3f  B[4]=944278cc  C[4]=24d750f6  D[4]=430dc657
A[5]=0deb9b28  B[5]=39eefb59  C[5]=dd958f1b  D[5]=013e212c
A[6]=d39bcda9  B[6]=2bdf00ce  C[6]=15a4bb10  D[6]=2012cc21
A[7]=b4247c66  B[7]=15ed9eb1  C[7]=71990938  D[7]=bad12c30
```

```
Step  3: (r=27, s= 3)
A[0]=2733702b  B[0]=d6333cc5  C[0]=2cc7637f  D[0]=d6c8fbdb
A[1]=073d5aee  B[1]=9c7790c4  C[1]=11bf9d30  D[1]=384e10dc
A[2]=553b686e  B[2]=0c8533c3  C[2]=676bb3ed  D[2]=2c156e74
A[3]=c6e745b3  B[3]=6308e283  C[3]=7d9ff8eb  D[3]=5a17d7af
A[4]=f8e56420  B[4]=f9ee8dd9  C[4]=944278cc  D[4]=24d750f6
A[5]=4b62e8d0  B[5]=406f5cd9  C[5]=39eefb59  D[5]=dd958f1b
A[6]=ec139aa9  B[6]=4e9cde6d  C[6]=2bdf00ce  D[6]=15a4bb10
A[7]=99cdd231  B[7]=35a123e3  C[7]=15ed9eb1  D[7]=71990938

Step  4: (r= 3, s=20)
A[0]=73cc9876  B[0]=399b8159  C[0]=d6333cc5  D[0]=2cc7637f
A[1]=e641c0a7  B[1]=39ead770  C[1]=9c7790c4  D[1]=11bf9d30
A[2]=8873558a  B[2]=a9db4372  C[2]=0c8533c3  D[2]=676bb3ed
A[3]=414aef60  B[3]=373a2d9e  C[3]=6308e283  D[3]=7d9ff8eb
A[4]=45ca946b  B[4]=c72b2107  C[4]=f9ee8dd9  D[4]=944278cc
A[5]=db21fe71  B[5]=5b174682  C[5]=406f5cd9  D[5]=39eefb59
A[6]=92e28b6c  B[6]=609cd54f  C[6]=4e9cde6d  D[6]=2bdf00ce
A[7]=c116cb49  B[7]=ce6e918c  C[7]=35a123e3  D[7]=15ed9eb1

Step  5: (r=20, s=14)
A[0]=2da81f67  B[0]=87673cc9  C[0]=399b8159  D[0]=d6333cc5
A[1]=405f9283  B[1]=0a7e641c  C[1]=39ead770  D[1]=9c7790c4
A[2]=4f778e86  B[2]=58a88735  C[2]=a9db4372  D[2]=0c8533c3
A[3]=caec9962  B[3]=f60414ae  C[3]=373a2d9e  D[3]=6308e283
A[4]=79613529  B[4]=46b45ca9  C[4]=c72b2107  D[4]=f9ee8dd9
A[5]=cc6a8073  B[5]=e71db21f  C[5]=5b174682  D[5]=406f5cd9
A[6]=ac2762c8  B[6]=b6c92e28  C[6]=609cd54f  D[6]=4e9cde6d
A[7]=37dd92ab  B[7]=b49c116c  C[7]=ce6e918c  D[7]=35a123e3

Step  6: (r=14, s=27)
A[0]=db3adbab  B[0]=07d9cb6a  C[0]=87673cc9  D[0]=399b8159
A[1]=ee7bc634  B[1]=e4a0d017  C[1]=0a7e641c  D[1]=39ead770
A[2]=8285d2ff  B[2]=e3a193dd  C[2]=58a88735  D[2]=a9db4372
A[3]=aeca8039  B[3]=2658b2bb  C[3]=f60414ae  D[3]=373a2d9e
A[4]=a1ea5205  B[4]=4d4a5e58  C[4]=46b45ca9  D[4]=c72b2107
A[5]=348058fa  B[5]=a01cf31a  C[5]=e71db21f  D[5]=5b174682
A[6]=c608a80b  B[6]=d8b22b09  C[6]=b6c92e28  D[6]=609cd54f
A[7]=9650b80c  B[7]=64aacdf7  C[7]=b49c116c  D[7]=ce6e918c

Step  7: (r=27, s= 3)
A[0]=dd749bbe  B[0]=5ed9d6dd  C[0]=07d9cb6a  D[0]=87673cc9
A[1]=ccea964d  B[1]=a773de31  C[1]=e4a0d017  D[1]=0a7e641c
A[2]=7e587882  B[2]=fc142e97  C[2]=e3a193dd  D[2]=58a88735
A[3]=0d08bded  B[3]=cd765401  C[3]=2658b2bb  D[3]=f60414ae
A[4]=fe162617  B[4]=2d0f5290  C[4]=4d4a5e58  D[4]=46b45ca9
A[5]=69cda8da  B[5]=d1a402c7  C[5]=a01cf31a  D[5]=e71db21f
A[6]=af794558  B[6]=5e304540  C[6]=d8b22b09  D[6]=b6c92e28
```

```
A[7]=465f7d86  B[7]=64b285c0  C[7]=64aacdf7  D[7]=b49c116c

Step  8: (r=26, s= 4)
A[0]=aa152f75  B[0]=fb75d26e  C[0]=5ed9d6dd  D[0]=07d9cb6a
A[1]=832564c7  B[1]=3733aa59  C[1]=a773de31  D[1]=e4a0d017
A[2]=0605293a  B[2]=09f961e2  C[2]=fc142e97  D[2]=e3a193dd
A[3]=cdd8fbc0  B[3]=b43422f7  C[3]=cd765401  D[3]=2658b2bb
A[4]=37d497e8  B[4]=5ff85898  C[4]=2d0f5290  D[4]=4d4a5e58
A[5]=7e0721fe  B[5]=69a736a3  C[5]=d1a402c7  D[5]=a01cf31a
A[6]=bb47efeb  B[6]=62bde515  C[6]=5e304540  D[6]=d8b22b09
A[7]=7a26b905  B[7]=19197df6  C[7]=64b285c0  D[7]=64aacdf7

Step  9: (r= 4, s=23)
A[0]=4b6ede40  B[0]=a152f75a  C[0]=fb75d26e  D[0]=5ed9d6dd
A[1]=db0ba851  B[1]=32564c78  C[1]=3733aa59  D[1]=a773de31
A[2]=82458396  B[2]=605293a0  C[2]=09f961e2  D[2]=fc142e97
A[3]=f3402cc6  B[3]=dd8fbc0c  C[3]=b43422f7  D[3]=cd765401
A[4]=061cffff  B[4]=7d497e83  C[4]=5ff85898  D[4]=2d0f5290
A[5]=222a4dff  B[5]=e0721fe7  C[5]=69a736a3  D[5]=d1a402c7
A[6]=8ecc0aae  B[6]=b47efebb  C[6]=62bde515  D[6]=5e304540
A[7]=5d418dfd  B[7]=a26b9057  C[7]=19197df6  D[7]=64b285c0

Step 10: (r=23, s=11)
A[0]=4aa6fbe0  B[0]=2025b76f  C[0]=a152f75a  D[0]=fb75d26e
A[1]=15d2b410  B[1]=28ed85d4  C[1]=32564c78  D[1]=3733aa59
A[2]=804d45f2  B[2]=cb4122c1  C[2]=605293a0  D[2]=09f961e2
A[3]=9d3503f6  B[3]=6379a016  C[3]=dd8fbc0c  D[3]=b43422f7
A[4]=79f6af2f  B[4]=ff830e7f  C[4]=7d497e83  D[4]=5ff85898
A[5]=8d3f736e  B[5]=ff911526  C[5]=e0721fe7  D[5]=69a736a3
A[6]=d07bb9da  B[6]=57476605  C[6]=b47efebb  D[6]=62bde515
A[7]=fa700119  B[7]=feaea0c6  C[7]=a26b9057  D[7]=19197df6

Step 11: (r=11, s=26)
A[0]=feaf31e5  B[0]=37df0255  C[0]=2025b76f  D[0]=a152f75a
A[1]=cd5a0eee  B[1]=95a080ae  C[1]=28ed85d4  D[1]=32564c78
A[2]=54ed4dd3  B[2]=6a2f9402  C[2]=cb4122c1  D[2]=605293a0
A[3]=f8f32b80  B[3]=a81fb4e9  C[3]=6379a016  D[3]=dd8fbc0c
A[4]=64593ce1  B[4]=b5797bcf  C[4]=ff830e7f  D[4]=7d497e83
A[5]=5ab13b11  B[5]=fb9b7469  C[5]=ff911526  D[5]=e0721fe7
A[6]=32e9700d  B[6]=ddced683  C[6]=57476605  D[6]=b47efebb
A[7]=a047360e  B[7]=8008cfd3  C[7]=feaea0c6  D[7]=a26b9057

Step 12: (r=26, s= 4)
A[0]=ec135627  B[0]=97fabcc7  C[0]=37df0255  D[0]=2025b76f
A[1]=2bc46467  B[1]=bb35683b  C[1]=95a080ae  D[1]=28ed85d4
A[2]=376a635b  B[2]=4d53b537  C[2]=6a2f9402  D[2]=cb4122c1
A[3]=3598f345  B[3]=03e3ccae  C[3]=a81fb4e9  D[3]=6379a016
A[4]=0285ee9e  B[4]=859164f3  C[4]=b5797bcf  D[4]=ff830e7f
A[5]=b466a9ed  B[5]=456ac4ec  C[5]=fb9b7469  D[5]=ff911526
```

```
A[6]=0afe30d8  B[6]=34cba5c0  C[6]=ddced683  D[6]=57476605
A[7]=9b1f7411  B[7]=3a811cd8  C[7]=8008cfd3  D[7]=feaea0c6

Step 13: (r= 4, s=23)
A[0]=3cb2026d  B[0]=c135627e  C[0]=97fabcc7  D[0]=37df0255
A[1]=aeece4e8  B[1]=bc464672  C[1]=bb35683b  D[1]=95a080ae
A[2]=62a75d5d  B[2]=76a635b3  C[2]=4d53b537  D[2]=6a2f9402
A[3]=988e99af  B[3]=598f3453  C[3]=03e3ccae  D[3]=a81fb4e9
A[4]=3ac4ab38  B[4]=285ee9e0  C[4]=859164f3  D[4]=b5797bcf
A[5]=345e3c93  B[5]=466a9edb  C[5]=456ac4ec  D[5]=fb9b7469
A[6]=c2c3f492  B[6]=afe30d80  C[6]=34cba5c0  D[6]=ddced683
A[7]=cfe36cc9  B[7]=b1f74119  C[7]=3a811cd8  D[7]=8008cfd3

Step 14: (r=23, s=11)
A[0]=f73ab62b  B[0]=369e5901  C[0]=c135627e  D[0]=97fabcc7
A[1]=5e881e29  B[1]=74577672  C[1]=bc464672  D[1]=bb35683b
A[2]=f8c57629  B[2]=aeb153ae  C[2]=76a635b3  D[2]=4d53b537
A[3]=97748005  B[3]=d7cc474c  C[3]=598f3453  D[3]=03e3ccae
A[4]=42cc05d6  B[4]=9c1d6255  C[4]=285ee9e0  D[4]=859164f3
A[5]=e1e5a7d9  B[5]=499a2f1e  C[5]=466a9edb  D[5]=456ac4ec
A[6]=11c67cf5  B[6]=496161fa  C[6]=afe30d80  D[6]=34cba5c0
A[7]=4cdf552e  B[7]=64e7f1b6  C[7]=b1f74119  D[7]=3a811cd8

Step 15: (r=11, s=26)
A[0]=9d6d3799  B[0]=d5b15fb9  C[0]=369e5901  D[0]=c135627e
A[1]=acc7a89d  B[1]=40f14af4  C[1]=74577672  D[1]=bc464672
A[2]=ea69c25f  B[2]=2bb14fc6  C[2]=aeb153ae  D[2]=76a635b3
A[3]=36f1019e  B[3]=a4002cbb  C[3]=d7cc474c  D[3]=598f3453
A[4]=b4315c17  B[4]=602eb216  C[4]=9c1d6255  D[4]=285ee9e0
A[5]=34045861  B[5]=2d3ecf0f  C[5]=499a2f1e  D[5]=466a9edb
A[6]=995c601d  B[6]=33e7a88e  C[6]=496161fa  D[6]=afe30d80
A[7]=62756619  B[7]=faa97266  C[7]=64e7f1b6  D[7]=b1f74119

Step 16: (r=19, s=28)
A[0]=c682e857  B[0]=bccceb69  C[0]=d5b15fb9  D[0]=369e5901
A[1]=094baa12  B[1]=44ed663d  C[1]=40f14af4  D[1]=74577672
A[2]=3394a3d4  B[2]=12ff534e  C[2]=2bb14fc6  D[2]=aeb153ae
A[3]=a63a4baf  B[3]=0cf1b788  C[3]=a4002cbb  D[3]=d7cc474c
A[4]=9737e2bf  B[4]=e0bda18a  C[4]=602eb216  D[4]=9c1d6255
A[5]=1befa278  B[5]=c309a022  C[5]=2d3ecf0f  D[5]=499a2f1e
A[6]=18279f59  B[6]=00eccae3  C[6]=33e7a88e  D[6]=496161fa
A[7]=72eb0dba  B[7]=30cb13ab  C[7]=faa97266  D[7]=64e7f1b6

Step 17: (r=28, s= 7)
A[0]=15ce15ba  B[0]=7c682e85  C[0]=bccceb69  D[0]=d5b15fb9
A[1]=2278d86c  B[1]=2094baa1  C[1]=44ed663d  D[1]=40f14af4
A[2]=efa7e97b  B[2]=43394a3d  C[2]=12ff534e  D[2]=2bb14fc6
A[3]=0cbc3f9e  B[3]=fa63a4ba  C[3]=0cf1b788  D[3]=a4002cbb
A[4]=1b0f8daf  B[4]=f9737e2b  C[4]=e0bda18a  D[4]=602eb216
```

```
A[5]=b48720c9  B[5]=81befa27  C[5]=c309a022  D[5]=2d3ecf0f
A[6]=035a7881  B[6]=918279f5  C[6]=00eccae3  D[6]=33e7a88e
A[7]=1d270b00  B[7]=a72eb0db  C[7]=30cb13ab  D[7]=faa97266

Step 18: (r= 7, s=22)
A[0]=772cb9de  B[0]=e70add0a  C[0]=7c682e85  D[0]=bccceb69
A[1]=711127d7  B[1]=3c6c3611  C[1]=2094baa1  D[1]=44ed663d
A[2]=b065438f  B[2]=d3f4bdf7  C[2]=43394a3d  D[2]=12ff534e
A[3]=56227710  B[3]=5e1fcf06  C[3]=fa63a4ba  D[3]=0cf1b788
A[4]=25c01073  B[4]=87c6d78d  C[4]=f9737e2b  D[4]=e0bda18a
A[5]=9768fa9a  B[5]=439064da  C[5]=81befa27  D[5]=c309a022
A[6]=e350cf62  B[6]=ad3c4081  C[6]=918279f5  D[6]=00eccae3
A[7]=dacfd36d  B[7]=9385800e  C[7]=a72eb0db  D[7]=30cb13ab

Step 19: (r=22, s=19)
A[0]=4270feb2  B[0]=779dcb2e  C[0]=e70add0a  D[0]=7c682e85
A[1]=b3189cd0  B[1]=f5dc4449  C[1]=3c6c3611  D[1]=2094baa1
A[2]=8df03b0d  B[2]=e3ec1950  C[2]=d3f4bdf7  D[2]=43394a3d
A[3]=c8c919e5  B[3]=c415889d  C[3]=5e1fcf06  D[3]=fa63a4ba
A[4]=82cbb227  B[4]=1cc97004  C[4]=87c6d78d  D[4]=f9737e2b
A[5]=1a0a5c29  B[5]=a6a5da3e  C[5]=439064da  D[5]=81befa27
A[6]=64d70824  B[6]=d8b8d433  C[6]=ad3c4081  D[6]=918279f5
A[7]=29d308b4  B[7]=db76b3f4  C[7]=9385800e  D[7]=a72eb0db

Step 20: (r=19, s=28)
A[0]=08aa85b2  B[0]=f5921387  C[0]=779dcb2e  D[0]=e70add0a
A[1]=fbc647a1  B[1]=e68598c4  C[1]=f5dc4449  D[1]=3c6c3611
A[2]=4542d8df  B[2]=d86c6f81  C[2]=e3ec1950  D[2]=d3f4bdf7
A[3]=149a429f  B[3]=cf2e4648  C[3]=c415889d  D[3]=5e1fcf06
A[4]=efabd0f6  B[4]=913c165d  C[4]=1cc97004  D[4]=87c6d78d
A[5]=57825dc0  B[5]=e148d052  C[5]=a6a5da3e  D[5]=439064da
A[6]=fdb0fa0d  B[6]=412326b8  C[6]=d8b8d433  D[6]=ad3c4081
A[7]=a3901b94  B[7]=45a14e98  C[7]=db76b3f4  D[7]=9385800e

Step 21: (r=28, s= 7)
A[0]=c23c0b03  B[0]=208aa85b  C[0]=f5921387  D[0]=779dcb2e
A[1]=455bd1ee  B[1]=1fbc647a  C[1]=e68598c4  D[1]=f5dc4449
A[2]=58260596  B[2]=f4542d8d  C[2]=d86c6f81  D[2]=e3ec1950
A[3]=5155237b  B[3]=f149a429  C[3]=cf2e4648  D[3]=c415889d
A[4]=db76bcaa  B[4]=6efabd0f  C[4]=913c165d  D[4]=1cc97004
A[5]=a35ac74b  B[5]=057825dc  C[5]=e148d052  D[5]=a6a5da3e
A[6]=c5673b01  B[6]=dfdb0fa0  C[6]=412326b8  D[6]=d8b8d433
A[7]=25da7173  B[7]=4a3901b9  C[7]=45a14e98  D[7]=db76b3f4

Step 22: (r= 7, s=22)
A[0]=d70d6a08  B[0]=1e0581e1  C[0]=208aa85b  D[0]=f5921387
A[1]=94ba4c59  B[1]=ade8f722  C[1]=1fbc647a  D[1]=e68598c4
A[2]=a0087cac  B[2]=1302cb2c  C[2]=f4542d8d  D[2]=d86c6f81
A[3]=9ec78c94  B[3]=aa91bda8  C[3]=f149a429  D[3]=cf2e4648
```

```
A[4]=0e8970b9  B[4]=bb5e556d  C[4]=6efabd0f  D[4]=913c165d
A[5]=5b6a68be  B[5]=ad63a5d1  C[5]=057825dc  D[5]=e148d052
A[6]=63b9bd39  B[6]=b39d80e2  C[6]=dfdb0fa0  D[6]=412326b8
A[7]=e0e0768b  B[7]=ed38b992  C[7]=4a3901b9  D[7]=45a14e98

Step 23: (r=22, s=19)
A[0]=b0c85b5d  B[0]=8235c35a  C[0]=1e0581e1  D[0]=208aa85b
A[1]=0afb0b21  B[1]=16652e93  C[1]=ade8f722  D[1]=1fbc647a
A[2]=ce5a9b40  B[2]=2b28021f  C[2]=1302cb2c  D[2]=f4542d8d
A[3]=96d22b46  B[3]=2527b1e3  C[3]=aa91bda8  D[3]=f149a429
A[4]=60724227  B[4]=2e43a25c  C[4]=bb5e556d  D[4]=6efabd0f
A[5]=72c6f940  B[5]=2f96da9a  C[5]=ad63a5d1  D[5]=057825dc
A[6]=0ba46a51  B[6]=4e58ee6f  C[6]=b39d80e2  D[6]=dfdb0fa0
A[7]=d7d26fa5  B[7]=a2f8381d  C[7]=ed38b992  D[7]=4a3901b9

Step 24: (r=15, s= 5)
A[0]=54a812e8  B[0]=2daed864  C[0]=8235c35a  D[0]=1e0581e1
A[1]=a4c894cf  B[1]=8590857d  C[1]=16652e93  D[1]=ade8f722
A[2]=50e3f2f8  B[2]=4da0672d  C[2]=2b28021f  D[2]=1302cb2c
A[3]=7fc32139  B[3]=15a34b69  C[3]=2527b1e3  D[3]=aa91bda8
A[4]=9df7ecab  B[4]=2113b039  C[4]=2e43a25c  D[4]=bb5e556d
A[5]=70ca5239  B[5]=7ca03963  C[5]=2f96da9a  D[5]=ad63a5d1
A[6]=672b4bc3  B[6]=352885d2  C[6]=4e58ee6f  D[6]=b39d80e2
A[7]=84001750  B[7]=37d2ebe9  C[7]=a2f8381d  D[7]=ed38b992

Step 25: (r= 5, s=29)
A[0]=449315f8  B[0]=95025d0a  C[0]=2daed864  D[0]=8235c35a
A[1]=245fd875  B[1]=991299f4  C[1]=8590857d  D[1]=16652e93
A[2]=ff61c82b  B[2]=1c7e5f0a  C[2]=4da0672d  D[2]=2b28021f
A[3]=1be8b917  B[3]=f864272f  C[3]=15a34b69  D[3]=2527b1e3
A[4]=eb750d2c  B[4]=befd9573  C[4]=2113b039  D[4]=2e43a25c
A[5]=42acb4d3  B[5]=194a472e  C[5]=7ca03963  D[5]=2f96da9a
A[6]=a8e48c88  B[6]=e569786c  C[6]=352885d2  D[6]=4e58ee6f
A[7]=9a55c544  B[7]=8002ea10  C[7]=37d2ebe9  D[7]=a2f8381d

Step 26: (r=29, s= 9)
A[0]=92c04fd1  B[0]=089262bf  C[0]=95025d0a  D[0]=2daed864
A[1]=dffcd778  B[1]=a48bfb0e  C[1]=991299f4  D[1]=8590857d
A[2]=6ad20190  B[2]=7fec3905  C[2]=1c7e5f0a  D[2]=4da0672d
A[3]=a533568e  B[3]=e37d1722  C[3]=f864272f  D[3]=15a34b69
A[4]=f6de9621  B[4]=9d6ea1a5  C[4]=befd9573  D[4]=2113b039
A[5]=f04b7f4c  B[5]=6855969a  C[5]=194a472e  D[5]=7ca03963
A[6]=fa79bb17  B[6]=151c9191  C[6]=e569786c  D[6]=352885d2
A[7]=f546f8e0  B[7]=934ab8a8  C[7]=8002ea10  D[7]=37d2ebe9

Step 27: (r= 9, s=15)
A[0]=e63d49f4  B[0]=809fa325  C[0]=089262bf  D[0]=95025d0a
A[1]=d59f10d2  B[1]=f9aef1bf  C[1]=a48bfb0e  D[1]=991299f4
A[2]=6b81014b  B[2]=a40320d5  C[2]=7fec3905  D[2]=1c7e5f0a
```

```
A[3]=732ba582  B[3]=66ad1d4a  C[3]=e37d1722  D[3]=f864272f
A[4]=2805f356  B[4]=bd2c43ed  C[4]=9d6ea1a5  D[4]=befd9573
A[5]=ce0eb816  B[5]=96fe99e0  C[5]=6855969a  D[5]=194a472e
A[6]=246d7131  B[6]=f3762ff4  C[6]=151c9191  D[6]=e569786c
A[7]=c8fe72d0  B[7]=8df1c1ea  C[7]=934ab8a8  D[7]=8002ea10

Step 28: (r=15, s= 5)
A[0]=1659a919  B[0]=a4fa731e  C[0]=809fa325  D[0]=089262bf
A[1]=49cf14ec  B[1]=88696acf  C[1]=f9aef1bf  D[1]=a48bfb0e
A[2]=cd6fc8e7  B[2]=80a5b5c0  C[2]=a40320d5  D[2]=7fec3905
A[3]=6f06bfd1  B[3]=d2c13995  C[3]=66ad1d4a  D[3]=e37d1722
A[4]=24e24e8e  B[4]=f9ab1402  C[4]=bd2c43ed  D[4]=9d6ea1a5
A[5]=ffa8fb3d  B[5]=5c0b6707  C[5]=96fe99e0  D[5]=6855969a
A[6]=7c26c239  B[6]=b8989236  C[6]=f3762ff4  D[6]=151c9191
A[7]=a28f471b  B[7]=3968647f  C[7]=8df1c1ea  D[7]=934ab8a8

Step 29: (r= 5, s=29)
A[0]=49a9f3b1  B[0]=cb352322  C[0]=a4fa731e  D[0]=809fa325
A[1]=a82b4e28  B[1]=39e29d89  C[1]=88696acf  D[1]=f9aef1bf
A[2]=1e10ac02  B[2]=adf91cf9  C[2]=80a5b5c0  D[2]=a40320d5
A[3]=a4f50655  B[3]=e0d7fa2d  C[3]=d2c13995  D[3]=66ad1d4a
A[4]=3a043a6c  B[4]=9c49d1c4  C[4]=f9ab1402  D[4]=bd2c43ed
A[5]=f4a43bd0  B[5]=f51f67bf  C[5]=5c0b6707  D[5]=96fe99e0
A[6]=6b7e26b2  B[6]=84d8472f  C[6]=b8989236  D[6]=f3762ff4
A[7]=0ac45985  B[7]=51e8e374  C[7]=3968647f  D[7]=8df1c1ea

Step 30: (r=29, s= 9)
A[0]=aab3e496  B[0]=29353e76  C[0]=cb352322  D[0]=a4fa731e
A[1]=843753d3  B[1]=150569c5  C[1]=39e29d89  D[1]=88696acf
A[2]=b01e8c0c  B[2]=43c21580  C[2]=adf91cf9  D[2]=80a5b5c0
A[3]=7fd053fa  B[3]=b49ea0ca  C[3]=e0d7fa2d  D[3]=d2c13995
A[4]=3468f092  B[4]=8740874d  C[4]=9c49d1c4  D[4]=f9ab1402
A[5]=b823ac37  B[5]=1e94877a  C[5]=f51f67bf  D[5]=5c0b6707
A[6]=3ed5339a  B[6]=4d6fc4d6  C[6]=84d8472f  D[6]=b8989236
A[7]=b9f4214d  B[7]=a1588b30  C[7]=51e8e374  D[7]=3968647f

Step 31: (r= 9, s=15)
A[0]=4622a4e8  B[0]=67c92d55  C[0]=29353e76  D[0]=cb352322
A[1]=8a3a5d9f  B[1]=6ea7a708  C[1]=150569c5  D[1]=39e29d89
A[2]=8913d034  B[2]=3d181960  C[2]=43c21580  D[2]=adf91cf9
A[3]=05ca77f7  B[3]=a0a7f4ff  C[3]=b49ea0ca  D[3]=e0d7fa2d
A[4]=62dd6c1d  B[4]=d1e12468  C[4]=8740874d  D[4]=9c49d1c4
A[5]=4a1adec9  B[5]=47586f70  C[5]=1e94877a  D[5]=f51f67bf
A[6]=fa39abe3  B[6]=aa67347d  C[6]=4d6fc4d6  D[6]=84d8472f
A[7]=7636991a  B[7]=e8429b73  C[7]=a1588b30  D[7]=51e8e374

Feistel Step 0: (r=15, s= 5)
A[0]=4001edb4  B[0]=52742311  C[0]=67c92d55  D[0]=29353e76
A[1]=5b8e1973  B[1]=2ecfc51d  C[1]=6ea7a708  D[1]=150569c5
```

```
A[2]=8a1cb1ec  B[2]=e81a4489  C[2]=3d181960  D[2]=43c21580
A[3]=43d84085  B[3]=3bfb82e5  C[3]=a0a7f4ff  D[3]=b49ea0ca
A[4]=bd0adfd6  B[4]=b60eb16e  C[4]=d1e12468  D[4]=8740874d
A[5]=327e1c47  B[5]=6f64a50d  C[5]=47586f70  D[5]=1e94877a
A[6]=54cde026  B[6]=d5f1fd1c  C[6]=aa67347d  D[6]=4d6fc4d6
A[7]=27a682a5  B[7]=4c8d3b1b  C[7]=e8429b73  D[7]=a1588b30

Feistel Step 1: (r= 5, s=29)
A[0]=cf14d136  B[0]=003db688  C[0]=52742311  D[0]=67c92d55
A[1]=7b51b2f2  B[1]=71c32e6b  C[1]=2ecfc51d  D[1]=6ea7a708
A[2]=355d048b  B[2]=43963d91  C[2]=e81a4489  D[2]=3d181960
A[3]=0f885e3a  B[3]=7b0810a8  C[3]=3bfb82e5  D[3]=a0a7f4ff
A[4]=ce25d7e2  B[4]=a15bfad7  C[4]=b60eb16e  D[4]=d1e12468
A[5]=6391e719  B[5]=4fc388e6  C[5]=6f64a50d  D[5]=47586f70
A[6]=7920ed79  B[6]=99bc04ca  C[6]=d5f1fd1c  D[6]=aa67347d
A[7]=fbbca396  B[7]=f4d054a4  C[7]=4c8d3b1b  D[7]=e8429b73

Feistel Step 2: (r=29, s= 9)
A[0]=7e707384  B[0]=d9e29a26  C[0]=003db688  D[0]=52742311
A[1]=d8d946c8  B[1]=4f6a365e  C[1]=71c32e6b  D[1]=2ecfc51d
A[2]=f55ed94e  B[2]=66aba091  C[2]=43963d91  D[2]=e81a4489
A[3]=320aa539  B[3]=41f10bc7  C[3]=7b0810a8  D[3]=3bfb82e5
A[4]=b0a93718  B[4]=59c4bafc  C[4]=a15bfad7  D[4]=b60eb16e
A[5]=73f3f9ee  B[5]=2c723ce3  C[5]=4fc388e6  D[5]=6f64a50d
A[6]=b93de7da  B[6]=2f241daf  C[6]=99bc04ca  D[6]=d5f1fd1c
A[7]=8daf1e3c  B[7]=df779472  C[7]=f4d054a4  D[7]=4c8d3b1b

Feistel Step 3: (r= 9, s=15)
A[0]=77e03576  B[0]=e0e708fc  C[0]=d9e29a26  D[0]=003db688
A[1]=0560ded9  B[1]=b28d91b1  C[1]=4f6a365e  D[1]=71c32e6b
A[2]=0426c8d6  B[2]=bdb29dea  C[2]=66aba091  D[2]=43963d91
A[3]=af5799ec  B[3]=154a7264  C[3]=41f10bc7  D[3]=7b0810a8
A[4]=8fe78fb5  B[4]=526e3161  C[4]=59c4bafc  D[4]=a15bfad7
A[5]=566420e8  B[5]=e7f3dce7  C[5]=2c723ce3  D[5]=4fc388e6
A[6]=752c8281  B[6]=7bcfb572  C[6]=2f241daf  D[6]=99bc04ca
A[7]=eeac689e  B[7]=5e3c791b  C[7]=df779472  D[7]=f4d054a4
```

Compression Function Output

```
A[0]=77e03576  B[0]=e0e708fc  C[0]=d9e29a26  D[0]=003db688
A[1]=0560ded9  B[1]=b28d91b1  C[1]=4f6a365e  D[1]=71c32e6b
A[2]=0426c8d6  B[2]=bdb29dea  C[2]=66aba091  D[2]=43963d91
A[3]=af5799ec  B[3]=154a7264  C[3]=41f10bc7  D[3]=7b0810a8
A[4]=8fe78fb5  B[4]=526e3161  C[4]=59c4bafc  D[4]=a15bfad7
A[5]=566420e8  B[5]=e7f3dce7  C[5]=2c723ce3  D[5]=4fc388e6
A[6]=752c8281  B[6]=7bcfb572  C[6]=2f241daf  D[6]=99bc04ca
A[7]=eeac689e  B[7]=5e3c791b  C[7]=df779472  D[7]=f4d054a4
```

Hash Function Output

```
7635e077d9de6005d6c82604ec9957afb58fe78fe8206456
81822c759e68aceefc08e7e0b1918db2ea9db2bd64724a15
```

6.3.3 Two-block Message

We use the message made of 1079 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
y[ 16.. 23] =  129   99   49  124  176  112   29   25
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
```

```
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
```

```
Z[17] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
Z[18] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
Z[19] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
        c21c3de4  1062ef9e  e0251fdb  aeff5101
Z[20] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
Z[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
Z[22] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
Z[23] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
Z[24] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
Z[25] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
Z[26] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
Z[27] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
Z[28] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
Z[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
Z[30] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
Z[31] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
```

```
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
W[11] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
W[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
W[15] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
W[17] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
W[18] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
W[19] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
W[20] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
W[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
W[22] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
W[23] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
        c21c3de4  1062ef9e  e0251fdb  aeff5101
W[24] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
W[25] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
W[26] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
W[27] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
W[28] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
W[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
W[30] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
W[31] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
```

Feistel Steps

```
IV :
A[0]=0d14da0d  B[0]=fba71944  C[0]=e65ced88  D[0]=f8773176
A[1]=95c2d7d5  B[1]=6e1b3ca0  C[1]=b0667012  D[1]=4c45a87d
A[2]=a95b8260  B[2]=7d0b1a7c  C[2]=916393e6  D[2]=c3280609
A[3]=b4722c01  B[3]=b506d742  C[3]=4b0643ce  D[3]=e6996ca4
A[4]=e4be208b  B[4]=c417ab0b  C[4]=4fbed3f1  D[4]=694e541f
A[5]=12cb4873  B[5]=eb34f21c  C[5]=9627d2bc  D[5]=0e3dcf80
A[6]=67773662  B[6]=bab7945b  C[6]=eb96513b  D[6]=042ab187
A[7]=56a66d24  B[7]=d1ed927e  C[7]=9aa6c3e3  D[7]=71fb0b87

IV XOR M :
A[0]=f2eb25f2  B[0]=0458e6bb  C[0]=19a31277  D[0]=0788ce89
A[1]=6a3d282a  B[1]=91e4c35f  C[1]=4f998fed  D[1]=b3ba5782
A[2]=56a47d9f  B[2]=82f4e583  C[2]=6e9c6c19  D[2]=3cd7f9f6
A[3]=4b8dd3fe  B[3]=4af928bd  C[3]=b4f9bc31  D[3]=1966935b
A[4]=1b41df74  B[4]=3be854f4  C[4]=b0412c0e  D[4]=96b1abe0
A[5]=ed34b78c  B[5]=14cb0de3  C[5]=69d82d43  D[5]=f1c2307f
A[6]=9888c99d  B[6]=45486ba4  C[6]=1469aec4  D[6]=fbd54e78
A[7]=a95992db  B[7]=2e126d81  C[7]=65593c1c  D[7]=8e04f478

Step  0: (r= 3, s=20)
A[0]=eceb63f2  B[0]=97592f97  C[0]=0458e6bb  D[0]=19a31277
A[1]=5fd2a623  B[1]=51e94153  C[1]=91e4c35f  D[1]=4f998fed
A[2]=5261b608  B[2]=b523ecfa  C[2]=82f4e583  D[2]=6e9c6c19
A[3]=3aeb0cba  B[3]=5c6e9ff2  C[3]=4af928bd  D[3]=b4f9bc31
A[4]=f8aef7ba  B[4]=da0efba0  C[4]=3be854f4  D[4]=b0412c0e
A[5]=56214853  B[5]=69a5bc67  C[5]=14cb0de3  D[5]=69d82d43
A[6]=2b2bcab3  B[6]=c4464cec  C[6]=45486ba4  D[6]=1469aec4
A[7]=08d70f5a  B[7]=4acc96dd  C[7]=2e126d81  D[7]=65593c1c

Step  1: (r=20, s=14)
A[0]=0e50cc56  B[0]=3f2eceb6  C[0]=97592f97  D[0]=0458e6bb
A[1]=d6013a50  B[1]=6235fd2a  C[1]=51e94153  D[1]=91e4c35f
A[2]=7d5f4d75  B[2]=6085261b  C[2]=b523ecfa  D[2]=82f4e583
A[3]=a0f46f5d  B[3]=cba3aeb0  C[3]=5c6e9ff2  D[3]=4af928bd
A[4]=1d815178  B[4]=7baf8aef  C[4]=da0efba0  D[4]=3be854f4
A[5]=4f9db9ef  B[5]=85356214  C[5]=69a5bc67  D[5]=14cb0de3
A[6]=712a9bdc  B[6]=ab32b2bc  C[6]=c4464cec  D[6]=45486ba4
A[7]=6a278e83  B[7]=f5a08d70  C[7]=4acc96dd  D[7]=2e126d81

Step  2: (r=14, s=27)
A[0]=0aad2147  B[0]=33158394  C[0]=3f2eceb6  D[0]=97592f97
A[1]=4cf82063  B[1]=4e943580  C[1]=6235fd2a  D[1]=51e94153
A[2]=9b51d25d  B[2]=d35d5f57  C[2]=6085261b  D[2]=b523ecfa
A[3]=230817ea  B[3]=1bd7683d  C[3]=cba3aeb0  D[3]=5c6e9ff2
A[4]=6e8fe8e9  B[4]=545e0760  C[4]=7baf8aef  D[4]=da0efba0
A[5]=53703b73  B[5]=6e7bd3e7  C[5]=85356214  D[5]=69a5bc67
A[6]=48260817  B[6]=a6f71c4a  C[6]=ab32b2bc  D[6]=c4464cec
```

```
A[7]=07d88a8d  B[7]=e3a0da89  C[7]=f5a08d70  D[7]=4acc96dd

Step  3: (r=27, s= 3)
A[0]=03e307a5  B[0]=3855690a  C[0]=33158394  D[0]=3f2eceb6
A[1]=19a31b78  B[1]=1a67c103  C[1]=4e943580  D[1]=6235fd2a
A[2]=bb0e478e  B[2]=ecda8e92  C[2]=d35d5f57  D[2]=6085261b
A[3]=6fee7298  B[3]=511840bf  C[3]=1bd7683d  D[3]=cba3aeb0
A[4]=0a9a9db2  B[4]=4b747f47  C[4]=545e0760  D[4]=7baf8aef
A[5]=462f6f53  B[5]=9a9b81db  C[5]=6e7bd3e7  D[5]=85356214
A[6]=d7d45ff4  B[6]=ba413040  C[6]=a6f71c4a  D[6]=ab32b2bc
A[7]=e327aebb  B[7]=683ec454  C[7]=e3a0da89  D[7]=f5a08d70

Step  4: (r= 3, s=20)
A[0]=d99abb3d  B[0]=1f183d28  C[0]=3855690a  D[0]=33158394
A[1]=c312d7db  B[1]=cd18dbc0  C[1]=1a67c103  D[1]=4e943580
A[2]=e135aa6d  B[2]=d8723c75  C[2]=ecda8e92  D[2]=d35d5f57
A[3]=9203d8f0  B[3]=7f7394c3  C[3]=511840bf  D[3]=1bd7683d
A[4]=20d58241  B[4]=54d4ed90  C[4]=4b747f47  D[4]=545e0760
A[5]=19bc73c3  B[5]=317b7a9a  C[5]=9a9b81db  D[5]=6e7bd3e7
A[6]=f526ee09  B[6]=bea2ffa6  C[6]=ba413040  D[6]=a6f71c4a
A[7]=d3a2f0f1  B[7]=193d75df  C[7]=683ec454  D[7]=e3a0da89

Step  5: (r=20, s=14)
A[0]=549b34d9  B[0]=b3dd99ab  C[0]=1f183d28  D[0]=3855690a
A[1]=cf00d7a8  B[1]=7dbc312d  C[1]=cd18dbc0  D[1]=1a67c103
A[2]=b94d942f  B[2]=a6de135a  C[2]=d8723c75  D[2]=ecda8e92
A[3]=d510d028  B[3]=8f09203d  C[3]=7f7394c3  D[3]=511840bf
A[4]=a159e662  B[4]=24120d58  C[4]=54d4ed90  D[4]=4b747f47
A[5]=b774ed66  B[5]=3c319bc7  C[5]=317b7a9a  D[5]=9a9b81db
A[6]=b7d4f8af  B[6]=e09f526e  C[6]=bea2ffa6  D[6]=ba413040
A[7]=2872d8bf  B[7]=0f1d3a2f  C[7]=193d75df  D[7]=683ec454

Step  6: (r=14, s=27)
A[0]=55f98698  B[0]=cd365526  C[0]=b3dd99ab  D[0]=1f183d28
A[1]=fd67f96d  B[1]=35ea33c0  C[1]=7dbc312d  D[1]=cd18dbc0
A[2]=2894cbf3  B[2]=650bee53  C[2]=a6de135a  D[2]=d8723c75
A[3]=38643d93  B[3]=340a3544  C[3]=8f09203d  D[3]=7f7394c3
A[4]=10e90a31  B[4]=7998a856  C[4]=24120d58  D[4]=54d4ed90
A[5]=5e6a99d7  B[5]=3b59addd  C[5]=3c319bc7  D[5]=317b7a9a
A[6]=ff402de1  B[6]=3e2bedf5  C[6]=e09f526e  D[6]=bea2ffa6
A[7]=edde3911  B[7]=b62fca1c  C[7]=0f1d3a2f  D[7]=193d75df

Step  7: (r=27, s= 3)
A[0]=6d92fae2  B[0]=c2afcc34  C[0]=cd365526  D[0]=b3dd99ab
A[1]=e00cd983  B[1]=6feb3fcb  C[1]=35ea33c0  D[1]=7dbc312d
A[2]=80086b69  B[2]=9944a65f  C[2]=650bee53  D[2]=a6de135a
A[3]=fbd5e836  B[3]=99c321ec  C[3]=340a3544  D[3]=8f09203d
A[4]=9fafd1f1  B[4]=88874851  C[4]=7998a856  D[4]=24120d58
A[5]=ec5a4318  B[5]=baf354ce  C[5]=3b59addd  D[5]=3c319bc7
```

```
A[6]=59856e52  B[6]=0ffa016f  C[6]=3e2bedf5  D[6]=e09f526e
A[7]=499ade27  B[7]=8f6ef1c8  C[7]=b62fca1c  D[7]=0f1d3a2f

Step  8: (r=26, s= 4)
A[0]=d046b77a  B[0]=89b64beb  C[0]=c2afcc34  D[0]=cd365526
A[1]=8c2a59a0  B[1]=0f803366  C[1]=6feb3fcb  D[1]=35ea33c0
A[2]=ee77ec4e  B[2]=a60021ad  C[2]=9944a65f  D[2]=650bee53
A[3]=402ab902  B[3]=dbef57a0  C[3]=99c321ec  D[3]=340a3544
A[4]=4c1b79bf  B[4]=c67ebf47  C[4]=88874851  D[4]=7998a856
A[5]=73d5e219  B[5]=63b1690c  C[5]=baf354ce  D[5]=3b59addd
A[6]=a535c4ae  B[6]=496615b9  C[6]=0ffa016f  D[6]=3e2bedf5
A[7]=546165cb  B[7]=9d266b78  C[7]=8f6ef1c8  D[7]=b62fca1c

Step  9: (r= 4, s=23)
A[0]=c19e0bc9  B[0]=046b77ad  C[0]=89b64beb  D[0]=c2afcc34
A[1]=625c6eec  B[1]=c2a59a08  C[1]=0f803366  D[1]=6feb3fcb
A[2]=5684b1a5  B[2]=e77ec4ee  C[2]=a60021ad  D[2]=9944a65f
A[3]=f34cbd40  B[3]=02ab9024  C[3]=dbef57a0  D[3]=99c321ec
A[4]=8fe89cc2  B[4]=c1b79bf4  C[4]=c67ebf47  D[4]=88874851
A[5]=1d0901cc  B[5]=3d5e2197  C[5]=63b1690c  D[5]=baf354ce
A[6]=0b891ae1  B[6]=535c4aea  C[6]=496615b9  D[6]=0ffa016f
A[7]=c7244754  B[7]=46165cb5  C[7]=9d266b78  D[7]=8f6ef1c8

Step 10: (r=23, s=11)
A[0]=1b3f10ed  B[0]=e4e0cf05  C[0]=046b77ad  D[0]=89b64beb
A[1]=13f2c2d3  B[1]=76312e37  C[1]=c2a59a08  D[1]=0f803366
A[2]=6ec7b12d  B[2]=d2ab4258  C[2]=e77ec4ee  D[2]=a60021ad
A[3]=7eaa3c10  B[3]=a079a65e  C[3]=02ab9024  D[3]=dbef57a0
A[4]=77d5c726  B[4]=6147f44e  C[4]=c1b79bf4  D[4]=c67ebf47
A[5]=60d1e1c8  B[5]=e60e8480  C[5]=3d5e2197  D[5]=63b1690c
A[6]=f93e232b  B[6]=7085c48d  C[6]=535c4aea  D[6]=496615b9
A[7]=49b690f2  B[7]=aa639223  C[7]=46165cb5  D[7]=9d266b78

Step 11: (r=11, s=26)
A[0]=8c660286  B[0]=f88768d9  C[0]=e4e0cf05  D[0]=046b77ad
A[1]=4ba4d320  B[1]=9616989f  C[1]=76312e37  D[1]=c2a59a08
A[2]=32699850  B[2]=3d896b76  C[2]=d2ab4258  D[2]=e77ec4ee
A[3]=5d793d94  B[3]=51e083f5  C[3]=a079a65e  D[3]=02ab9024
A[4]=b87c1ef2  B[4]=ae3933be  C[4]=6147f44e  D[4]=c1b79bf4
A[5]=81f61afe  B[5]=8f0e4306  C[5]=e60e8480  D[5]=3d5e2197
A[6]=cc0478ad  B[6]=f1195fc9  C[6]=7085c48d  D[6]=535c4aea
A[7]=5b5e25be  B[7]=b487924d  C[7]=aa639223  D[7]=46165cb5

Step 12: (r=26, s= 4)
A[0]=f9507e77  B[0]=1a31980a  C[0]=f88768d9  D[0]=e4e0cf05
A[1]=d112a577  B[1]=812e934c  C[1]=9616989f  D[1]=76312e37
A[2]=cc3a8173  B[2]=40c9a661  C[2]=3d896b76  D[2]=d2ab4258
A[3]=8b4bd691  B[3]=5175e4f6  C[3]=51e083f5  D[3]=a079a65e
A[4]=17845a1e  B[4]=cae1f07b  C[4]=ae3933be  D[4]=6147f44e
```

```
A[5]=23b772d3  B[5]=fa07d86b  C[5]=8f0e4306  D[5]=e60e8480
A[6]=f78d38df  B[6]=b73011e2  C[6]=f1195fc9  D[6]=7085c48d
A[7]=148a877e  B[7]=f96d7896  C[7]=b487924d  D[7]=aa639223

Step 13: (r= 4, s=23)
A[0]=57e85062  B[0]=9507e77f  C[0]=1a31980a  D[0]=f88768d9
A[1]=32a36bfc  B[1]=112a577d  C[1]=812e934c  D[1]=9616989f
A[2]=813d166d  B[2]=c3a8173c  C[2]=40c9a661  D[2]=3d896b76
A[3]=aa0207a1  B[3]=b4bd6918  C[3]=5175e4f6  D[3]=51e083f5
A[4]=9a72892c  B[4]=7845a1e1  C[4]=cae1f07b  D[4]=ae3933be
A[5]=dc738a9f  B[5]=3b772d32  C[5]=fa07d86b  D[5]=8f0e4306
A[6]=43e819b5  B[6]=78d38dff  C[6]=b73011e2  D[6]=f1195fc9
A[7]=a92534d3  B[7]=48a877e1  C[7]=f96d7896  D[7]=b487924d

Step 14: (r=23, s=11)
A[0]=1d10ad02  B[0]=312bf428  C[0]=9507e77f  D[0]=1a31980a
A[1]=fc5c1070  B[1]=fe1951b5  C[1]=112a577d  D[1]=812e934c
A[2]=c2009457  B[2]=36c09e8b  C[2]=c3a8173c  D[2]=40c9a661
A[3]=582d73e7  B[3]=d0d50103  C[3]=b4bd6918  D[3]=5175e4f6
A[4]=e239c76d  B[4]=964d3944  C[4]=7845a1e1  D[4]=cae1f07b
A[5]=fdeac832  B[5]=4fee39c5  C[5]=3b772d32  D[5]=fa07d86b
A[6]=2052a2ec  B[6]=daa1f40c  C[6]=78d38dff  D[6]=b73011e2
A[7]=7b2daf5e  B[7]=69d4929a  C[7]=48a877e1  D[7]=f96d7896

Step 15: (r=11, s=26)
A[0]=2e422911  B[0]=856810e8  C[0]=312bf428  D[0]=9507e77f
A[1]=b38c2a21  B[1]=e08387e2  C[1]=fe1951b5  D[1]=112a577d
A[2]=211bdf57  B[2]=04a2be10  C[2]=36c09e8b  D[2]=c3a8173c
A[3]=0f07eca8  B[3]=6b9f3ac1  C[3]=d0d50103  D[3]=b4bd6918
A[4]=e57de08a  B[4]=ce3b6f11  C[4]=964d3944  D[4]=7845a1e1
A[5]=1dfd8b35  B[5]=564197ef  C[5]=4fee39c5  D[5]=3b772d32
A[6]=2d2ec5f5  B[6]=95176102  C[6]=daa1f40c  D[6]=78d38dff
A[7]=e06713bf  B[7]=6d7af3d9  C[7]=69d4929a  D[7]=48a877e1

Step 16: (r=19, s=28)
A[0]=c2fcc0d3  B[0]=48897211  C[0]=856810e8  D[0]=312bf428
A[1]=f59b9f8d  B[1]=510d9c61  C[1]=e08387e2  D[1]=fe1951b5
A[2]=1782bf00  B[2]=fab908de  C[2]=04a2be10  D[2]=36c09e8b
A[3]=021c03ae  B[3]=6540783f  C[3]=6b9f3ac1  D[3]=d0d50103
A[4]=1db67278  B[4]=04572bef  C[4]=ce3b6f11  D[4]=964d3944
A[5]=018b65e7  B[5]=59a8efec  C[5]=564197ef  D[5]=4fee39c5
A[6]=49ac8c80  B[6]=2fa96976  C[6]=95176102  D[6]=daa1f40c
A[7]=85316fcf  B[7]=9dff0338  C[7]=6d7af3d9  D[7]=69d4929a

Step 17: (r=28, s= 7)
A[0]=7bfd3cc8  B[0]=3c2fcc0d  C[0]=48897211  D[0]=856810e8
A[1]=c5e97890  B[1]=df59b9f8  C[1]=510d9c61  D[1]=e08387e2
A[2]=e0ab2609  B[2]=01782bf0  C[2]=fab908de  D[2]=04a2be10
A[3]=ecc29249  B[3]=e021c03a  C[3]=6540783f  D[3]=6b9f3ac1
```

```
A[4]=4b980f2d  B[4]=81db6727  C[4]=04572bef  D[4]=ce3b6f11
A[5]=365b8de0  B[5]=7018b65e  C[5]=59a8efec  D[5]=564197ef
A[6]=d5a9c943  B[6]=049ac8c8  C[6]=2fa96976  D[6]=95176102
A[7]=0c079c2d  B[7]=f85316fc  C[7]=9dff0338  D[7]=6d7af3d9

Step 18: (r= 7, s=22)
A[0]=4fbdf09d  B[0]=fe9e643d  C[0]=3c2fcc0d  D[0]=48897211
A[1]=eb043509  B[1]=f4bc4862  C[1]=df59b9f8  D[1]=510d9c61
A[2]=a63f6824  B[2]=559304f0  C[2]=01782bf0  D[2]=fab908de
A[3]=26f523d3  B[3]=614924f6  C[3]=e021c03a  D[3]=6540783f
A[4]=784bd2ce  B[4]=cc0796a5  C[4]=81db6727  D[4]=04572bef
A[5]=f23ff5d6  B[5]=2dc6f01b  C[5]=7018b65e  D[5]=59a8efec
A[6]=daf7a829  B[6]=d4e4a1ea  C[6]=049ac8c8  D[6]=2fa96976
A[7]=9d85685a  B[7]=03ce1686  C[7]=f85316fc  D[7]=9dff0338

Step 19: (r=22, s=19)
A[0]=3094c0ba  B[0]=2753ef7c  C[0]=fe9e643d  D[0]=3c2fcc0d
A[1]=e2f778ad  B[1]=427ac10d  C[1]=f4bc4862  D[1]=df59b9f8
A[2]=111e1e1b  B[2]=09298fda  C[2]=559304f0  D[2]=01782bf0
A[3]=b896b54f  B[3]=f4c9bd48  C[3]=614924f6  D[3]=e021c03a
A[4]=3b896744  B[4]=b39e12f4  C[4]=cc0796a5  D[4]=81db6727
A[5]=1126d01b  B[5]=75bc8ffd  C[5]=2dc6f01b  D[5]=7018b65e
A[6]=33e4dcc9  B[6]=0a76bdea  C[6]=d4e4a1ea  D[6]=049ac8c8
A[7]=601c1f96  B[7]=16a7615a  C[7]=03ce1686  D[7]=f85316fc

Step 20: (r=19, s=28)
A[0]=1cd5d285  B[0]=05d184a6  C[0]=2753ef7c  D[0]=fe9e643d
A[1]=fb066bb8  B[1]=c56f17bb  C[1]=427ac10d  D[1]=f4bc4862
A[2]=22a63162  B[2]=f0d888f0  C[2]=09298fda  D[2]=559304f0
A[3]=8c7b31b4  B[3]=aa7dc4b5  C[3]=f4c9bd48  D[3]=614924f6
A[4]=bb82ba43  B[4]=3a21dc4b  C[4]=b39e12f4  D[4]=cc0796a5
A[5]=b0f6f839  B[5]=80d88936  C[5]=75bc8ffd  D[5]=2dc6f01b
A[6]=6366c40f  B[6]=e6499f26  C[6]=0a76bdea  D[6]=d4e4a1ea
A[7]=372990dd  B[7]=fcb300e0  C[7]=16a7615a  D[7]=03ce1686

Step 21: (r=28, s= 7)
A[0]=febc2f9b  B[0]=51cd5d28  C[0]=05d184a6  D[0]=2753ef7c
A[1]=4907d67d  B[1]=8fb066bb  C[1]=c56f17bb  D[1]=427ac10d
A[2]=6e19cfde  B[2]=222a6316  C[2]=f0d888f0  D[2]=09298fda
A[3]=b0347d2b  B[3]=48c7b31b  C[3]=aa7dc4b5  D[3]=f4c9bd48
A[4]=fed69cfc  B[4]=3bb82ba4  C[4]=3a21dc4b  D[4]=b39e12f4
A[5]=c767b343  B[5]=9b0f6f83  C[5]=80d88936  D[5]=75bc8ffd
A[6]=a8f8f09e  B[6]=f6366c40  C[6]=e6499f26  D[6]=0a76bdea
A[7]=f10801b3  B[7]=d372990d  C[7]=fcb300e0  D[7]=16a7615a

Step 22: (r= 7, s=22)
A[0]=421febf7  B[0]=5e17cdff  C[0]=51cd5d28  D[0]=05d184a6
A[1]=bb25eb70  B[1]=83eb3ea4  C[1]=8fb066bb  D[1]=c56f17bb
A[2]=3d9ed4cf  B[2]=0ce7ef37  C[2]=222a6316  D[2]=f0d888f0
```

```
A[3]=3ea89bf8  B[3]=1a3e95d8  C[3]=48c7b31b  D[3]=aa7dc4b5
A[4]=e5f3560a  B[4]=6b4e7e7f  C[4]=3bb82ba4  D[4]=3a21dc4b
A[5]=834c7c1f  B[5]=b3d9a1e3  C[5]=9b0f6f83  D[5]=80d88936
A[6]=3be23ed7  B[6]=7c784f54  C[6]=f6366c40  D[6]=e6499f26
A[7]=b027314a  B[7]=8400d9f8  C[7]=d372990d  D[7]=fcb300e0

Step 23: (r=22, s=19)
A[0]=2ee52566  B[0]=fdd087fa  C[0]=5e17cdff  D[0]=51cd5d28
A[1]=c09cd649  B[1]=dc2ec97a  C[1]=83eb3ea4  D[1]=8fb066bb
A[2]=766ea46b  B[2]=33cf67b5  C[2]=0ce7ef37  D[2]=222a6316
A[3]=7813d23d  B[3]=fe0faa26  C[3]=1a3e95d8  D[3]=48c7b31b
A[4]=c0bbc9be  B[4]=82b97cd5  C[4]=6b4e7e7f  D[4]=3bb82ba4
A[5]=0ee7edc1  B[5]=07e0d31f  C[5]=b3d9a1e3  D[5]=9b0f6f83
A[6]=9e798ebe  B[6]=b5cef88f  C[6]=7c784f54  D[6]=f6366c40
A[7]=575988cd  B[7]=52ac09cc  C[7]=8400d9f8  D[7]=d372990d

Step 24: (r=15, s= 5)
A[0]=146978e0  B[0]=92b31772  C[0]=fdd087fa  D[0]=5e17cdff
A[1]=405f1895  B[1]=6b24e04e  C[1]=dc2ec97a  D[1]=83eb3ea4
A[2]=311856b4  B[2]=5235bb37  C[2]=33cf67b5  D[2]=0ce7ef37
A[3]=ee724c39  B[3]=e91ebc09  C[3]=fe0faa26  D[3]=1a3e95d8
A[4]=4e3338bb  B[4]=e4df605d  C[4]=82b97cd5  D[4]=6b4e7e7f
A[5]=f3269863  B[5]=f6e08773  C[5]=07e0d31f  D[5]=b3d9a1e3
A[6]=082a20e7  B[6]=c75f4f3c  C[6]=b5cef88f  D[6]=7c784f54
A[7]=ba425a88  B[7]=c466abac  C[7]=52ac09cc  D[7]=8400d9f8

Step 25: (r= 5, s=29)
A[0]=0d8f8cfd  B[0]=8d2f1c02  C[0]=92b31772  D[0]=fdd087fa
A[1]=64fd63d5  B[1]=0be312a8  C[1]=6b24e04e  D[1]=dc2ec97a
A[2]=adbd4912  B[2]=230ad686  C[2]=5235bb37  D[2]=33cf67b5
A[3]=b84f0e2c  B[3]=ce49873d  C[3]=e91ebc09  D[3]=fe0faa26
A[4]=98ae233f  B[4]=c6671769  C[4]=e4df605d  D[4]=82b97cd5
A[5]=0146b500  B[5]=64d30c7e  C[5]=f6e08773  D[5]=07e0d31f
A[6]=2823079c  B[6]=05441ce1  C[6]=c75f4f3c  D[6]=b5cef88f
A[7]=a17ecab1  B[7]=484b5117  C[7]=c466abac  D[7]=52ac09cc

Step 26: (r=29, s= 9)
A[0]=b43207fe  B[0]=a1b1f19f  C[0]=8d2f1c02  D[0]=92b31772
A[1]=ec7e2228  B[1]=ac9fac7a  C[1]=0be312a8  D[1]=6b24e04e
A[2]=39a86f46  B[2]=55b7a922  C[2]=230ad686  D[2]=5235bb37
A[3]=8a03ed2d  B[3]=9709e1c5  C[3]=ce49873d  D[3]=e91ebc09
A[4]=fd12e405  B[4]=f315c467  C[4]=c6671769  D[4]=e4df605d
A[5]=7e0afe81  B[5]=0028d6a0  C[5]=64d30c7e  D[5]=f6e08773
A[6]=047d1e5d  B[6]=850460f3  C[6]=05441ce1  D[6]=c75f4f3c
A[7]=1db84039  B[7]=342fd956  C[7]=484b5117  D[7]=c466abac

Step 27: (r= 9, s=15)
A[0]=89119076  B[0]=640ffd68  C[0]=a1b1f19f  D[0]=8d2f1c02
A[1]=3aaf4a9e  B[1]=fc4451d8  C[1]=ac9fac7a  D[1]=0be312a8
```

```
A[2]=8fbd22a7  B[2]=50de8c73  C[2]=55b7a922  D[2]=230ad686
A[3]=376a6626  B[3]=07da5b14  C[3]=9709e1c5  D[3]=ce49873d
A[4]=e84b08f9  B[4]=25c80bfa  C[4]=f315c467  D[4]=c6671769
A[5]=f225ee04  B[5]=15fd02fc  C[5]=0028d6a0  D[5]=64d30c7e
A[6]=9aa22528  B[6]=fa3cba08  C[6]=850460f3  D[6]=05441ce1
A[7]=1e5a1b5e  B[7]=7080723b  C[7]=342fd956  D[7]=484b5117

Step 28: (r=15, s= 5)
A[0]=b283265a  B[0]=c83b4488  C[0]=640ffd68  D[0]=a1b1f19f
A[1]=24c6b4d6  B[1]=a54f1d57  C[1]=fc4451d8  D[1]=ac9fac7a
A[2]=d3434847  B[2]=9153c7de  C[2]=50de8c73  D[2]=55b7a922
A[3]=64036904  B[3]=33131bb5  C[3]=07da5b14  D[3]=9709e1c5
A[4]=028d7641  B[4]=847cf425  C[4]=25c80bfa  D[4]=f315c467
A[5]=ca45cb49  B[5]=f7027912  C[5]=15fd02fc  D[5]=0028d6a0
A[6]=f92ba72e  B[6]=12944d51  C[6]=fa3cba08  D[6]=850460f3
A[7]=42db4c09  B[7]=0daf0f2d  C[7]=7080723b  D[7]=342fd956

Step 29: (r= 5, s=29)
A[0]=4a10bcd0  B[0]=5064cb56  C[0]=c83b4488  D[0]=640ffd68
A[1]=2135af64  B[1]=98d69ac4  C[1]=a54f1d57  D[1]=fc4451d8
A[2]=811b414d  B[2]=686908fa  C[2]=9153c7de  D[2]=50de8c73
A[3]=0622c46b  B[3]=806d208c  C[3]=33131bb5  D[3]=07da5b14
A[4]=30bac24c  B[4]=51aec820  C[4]=847cf425  D[4]=25c80bfa
A[5]=57233035  B[5]=48b96939  C[5]=f7027912  D[5]=15fd02fc
A[6]=3c20f57f  B[6]=2574e5df  C[6]=12944d51  D[6]=fa3cba08
A[7]=96dc62ab  B[7]=5b698128  C[7]=0daf0f2d  D[7]=7080723b

Step 30: (r=29, s= 9)
A[0]=5c9badd1  B[0]=0942179a  C[0]=5064cb56  D[0]=c83b4488
A[1]=cb10ca01  B[1]=8426b5ec  C[1]=98d69ac4  D[1]=a54f1d57
A[2]=8df883e2  B[2]=b0236829  C[2]=686908fa  D[2]=9153c7de
A[3]=a9b09330  B[3]=60c4588d  C[3]=806d208c  D[3]=33131bb5
A[4]=a7023c7e  B[4]=86175849  C[4]=51aec820  D[4]=847cf425
A[5]=fd904242  B[5]=aae46606  C[5]=48b96939  D[5]=f7027912
A[6]=b944c106  B[6]=e7841eaf  C[6]=2574e5df  D[6]=12944d51
A[7]=f25a6384  B[7]=72db8c55  C[7]=5b698128  D[7]=0daf0f2d

Step 31: (r= 9, s=15)
A[0]=741c343b  B[0]=375ba2b9  C[0]=0942179a  D[0]=5064cb56
A[1]=f21a8bd7  B[1]=21940396  C[1]=8426b5ec  D[1]=98d69ac4
A[2]=80765ea5  B[2]=f107c51b  C[2]=b0236829  D[2]=686908fa
A[3]=82e127c0  B[3]=61266153  C[3]=60c4588d  D[3]=806d208c
A[4]=d06fd3b6  B[4]=0478fd4e  C[4]=86175849  D[4]=51aec820
A[5]=7444be31  B[5]=208485fb  C[5]=aae46606  D[5]=48b96939
A[6]=f418f9e5  B[6]=89820d72  C[6]=e7841eaf  D[6]=2574e5df
A[7]=de08fec2  B[7]=b4c709e4  C[7]=72db8c55  D[7]=5b698128

Feistel Step 0: (r=15, s= 5)
A[0]=a0651ca0  B[0]=1a1dba0e  C[0]=375ba2b9  D[0]=0942179a
```

```
A[1]=73d304f8  B[1]=45ebf90d  C[1]=21940396  D[1]=8426b5ec
A[2]=cd5e2de8  B[2]=2f52c03b  C[2]=f107c51b  D[2]=b0236829
A[3]=cfcb7b8d  B[3]=93e04170  C[3]=61266153  D[3]=60c4588d
A[4]=fbd0f969  B[4]=e9db6837  C[4]=0478fd4e  D[4]=86175849
A[5]=af0a2497  B[5]=5f18ba22  C[5]=208485fb  D[5]=aae46606
A[6]=8d66e466  B[6]=7cf2fa0c  C[6]=89820d72  D[6]=e7841eaf
A[7]=5951de38  B[7]=7f616f04  C[7]=b4c709e4  D[7]=72db8c55

Feistel Step 1: (r= 5, s=29)
A[0]=8f46da77  B[0]=0ca39414  C[0]=1a1dba0e  D[0]=375ba2b9
A[1]=3ff0906c  B[1]=7a609f0e  C[1]=45ebf90d  D[1]=21940396
A[2]=19f3dc70  B[2]=abc5bd19  C[2]=2f52c03b  D[2]=f107c51b
A[3]=b1968d32  B[3]=f96f71b9  C[3]=93e04170  D[3]=61266153
A[4]=13e17ac0  B[4]=7a1f2d3f  C[4]=e9db6837  D[4]=0478fd4e
A[5]=bef0863c  B[5]=e14492f5  C[5]=5f18ba22  D[5]=208485fb
A[6]=500300c2  B[6]=acdc8cd1  C[6]=7cf2fa0c  D[6]=89820d72
A[7]=c996a0c7  B[7]=2a3bc70b  C[7]=7f616f04  D[7]=b4c709e4

Feistel Step 2: (r=29, s= 9)
A[0]=a1b38e8b  B[0]=f1e8db4e  C[0]=0ca39414  D[0]=1a1dba0e
A[1]=16d9cab0  B[1]=87fe120d  C[1]=7a609f0e  D[1]=45ebf90d
A[2]=f1c84a2b  B[2]=033e7b8e  C[2]=abc5bd19  D[2]=2f52c03b
A[3]=28495217  B[3]=5632d1a6  C[3]=f96f71b9  D[3]=93e04170
A[4]=fc25be42  B[4]=027c2f58  C[4]=7a1f2d3f  D[4]=e9db6837
A[5]=ed6456bd  B[5]=97de10c7  C[5]=e14492f5  D[5]=5f18ba22
A[6]=9ab10551  B[6]=4a006018  C[6]=acdc8cd1  D[6]=7cf2fa0c
A[7]=b5227069  B[7]=f932d418  C[7]=2a3bc70b  D[7]=7f616f04

Feistel Step 3: (r= 9, s=15)
A[0]=0e4de612  B[0]=671d1743  C[0]=f1e8db4e  D[0]=0ca39414
A[1]=a4f97c6e  B[1]=b395602d  C[1]=87fe120d  D[1]=7a609f0e
A[2]=c4ba21f9  B[2]=909457e3  C[2]=033e7b8e  D[2]=abc5bd19
A[3]=54c1f93a  B[3]=92a42e50  C[3]=5632d1a6  D[3]=f96f71b9
A[4]=5d06c1f6  B[4]=4b7c85f8  C[4]=027c2f58  D[4]=7a1f2d3f
A[5]=40c9597a  B[5]=c8ad7bda  C[5]=97de10c7  D[5]=e14492f5
A[6]=aaa62f98  B[6]=620aa335  C[6]=4a006018  D[6]=acdc8cd1
A[7]=bb6f049c  B[7]=44e0d36a  C[7]=f932d418  D[7]=2a3bc70b
```

Compression Function Output

```
A[0]=0e4de612  B[0]=671d1743  C[0]=f1e8db4e  D[0]=0ca39414
A[1]=a4f97c6e  B[1]=b395602d  C[1]=87fe120d  D[1]=7a609f0e
A[2]=c4ba21f9  B[2]=909457e3  C[2]=033e7b8e  D[2]=abc5bd19
A[3]=54c1f93a  B[3]=92a42e50  C[3]=5632d1a6  D[3]=f96f71b9
A[4]=5d06c1f6  B[4]=4b7c85f8  C[4]=027c2f58  D[4]=7a1f2d3f
A[5]=40c9597a  B[5]=c8ad7bda  C[5]=97de10c7  D[5]=e14492f5
A[6]=aaa62f98  B[6]=620aa335  C[6]=4a006018  D[6]=acdc8cd1
A[7]=bb6f049c  B[7]=44e0d36a  C[7]=f932d418  D[7]=2a3bc70b
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
y[ 24.. 31] =   88   14   70  255  173  206  169   46
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
```

```
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
Z[17] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
Z[18] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
Z[19] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
Z[20] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
Z[21] = ebfa5849  ab5b2551  fb73949a  739754a5
```

```
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
Z[22] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
Z[23] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
Z[24] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
Z[25] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
Z[26] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
Z[27] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
Z[28] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
Z[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
Z[30] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
Z[31] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
```

```
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
W[17] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
W[18] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
W[19] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
W[20] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
W[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
W[22] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
W[23] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
W[24] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
W[25] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
W[26] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
W[27] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
W[28] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
W[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
W[30] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
W[31] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
```

Feistel Steps

```
IV :
A[0]=0e4de612  B[0]=671d1743  C[0]=f1e8db4e  D[0]=0ca39414
A[1]=a4f97c6e  B[1]=b395602d  C[1]=87fe120d  D[1]=7a609f0e
A[2]=c4ba21f9  B[2]=909457e3  C[2]=033e7b8e  D[2]=abc5bd19
A[3]=54c1f93a  B[3]=92a42e50  C[3]=5632d1a6  D[3]=f96f71b9
A[4]=5d06c1f6  B[4]=4b7c85f8  C[4]=027c2f58  D[4]=7a1f2d3f
A[5]=40c9597a  B[5]=c8ad7bda  C[5]=97de10c7  D[5]=e14492f5
```

```
A[6]=aaa62f98  B[6]=620aa335  C[6]=4a006018  D[6]=acdc8cd1
A[7]=bb6f049c  B[7]=44e0d36a  C[7]=f932d418  D[7]=2a3bc70b

IV XOR M :
A[0]=f1b219ed  B[0]=671d1743  C[0]=f1e8db4e  D[0]=0ca39414
A[1]=a4078391  B[1]=b395602d  C[1]=87fe120d  D[1]=7a609f0e
A[2]=c4ba21f9  B[2]=909457e3  C[2]=033e7b8e  D[2]=abc5bd19
A[3]=54c1f93a  B[3]=92a42e50  C[3]=5632d1a6  D[3]=f96f71b9
A[4]=5d06c1f6  B[4]=4b7c85f8  C[4]=027c2f58  D[4]=7a1f2d3f
A[5]=40c9597a  B[5]=c8ad7bda  C[5]=97de10c7  D[5]=e14492f5
A[6]=aaa62f98  B[6]=620aa335  C[6]=4a006018  D[6]=acdc8cd1
A[7]=bb6f049c  B[7]=44e0d36a  C[7]=f932d418  D[7]=2a3bc70b

Step  0: (r= 3, s=20)
A[0]=76417ed1  B[0]=8d90cf6f  C[0]=671d1743  D[0]=f1e8db4e
A[1]=038449fe  B[1]=203c1c8d  C[1]=b395602d  D[1]=87fe120d
A[2]=e8911f38  B[2]=25d10fce  C[2]=909457e3  D[2]=033e7b8e
A[3]=c400c804  B[3]=a60fc9d2  C[3]=92a42e50  D[3]=5632d1a6
A[4]=6962b87d  B[4]=e8360fb2  C[4]=4b7c85f8  D[4]=027c2f58
A[5]=fe5332a6  B[5]=064acbd2  C[5]=c8ad7bda  D[5]=97de10c7
A[6]=8f1e89ef  B[6]=55317cc5  C[6]=620aa335  D[6]=4a006018
A[7]=1412bc10  B[7]=db7824e5  C[7]=44e0d36a  D[7]=f932d418

Step  1: (r=20, s=14)
A[0]=7923da55  B[0]=ed176417  C[0]=8d90cf6f  D[0]=671d1743
A[1]=0050a2a9  B[1]=9fe03844  C[1]=203c1c8d  D[1]=b395602d
A[2]=0c98eb44  B[2]=f38e8911  C[2]=25d10fce  D[2]=909457e3
A[3]=5f95aa9f  B[3]=804c400c  C[3]=a60fc9d2  D[3]=92a42e50
A[4]=b8b59be7  B[4]=87d6962b  C[4]=e8360fb2  D[4]=4b7c85f8
A[5]=021f2bc2  B[5]=2a6fe533  C[5]=064acbd2  D[5]=c8ad7bda
A[6]=eba77971  B[6]=9ef8f1e8  C[6]=55317cc5  D[6]=620aa335
A[7]=766c674b  B[7]=c101412b  C[7]=db7824e5  D[7]=44e0d36a

Step  2: (r=14, s=27)
A[0]=3da5082e  B[0]=f6955e48  C[0]=ed176417  D[0]=8d90cf6f
A[1]=9add1d65  B[1]=28aa4014  C[1]=9fe03844  D[1]=203c1c8d
A[2]=5de4d744  B[2]=3ad10326  C[2]=f38e8911  D[2]=25d10fce
A[3]=00a6a7d5  B[3]=6aa7d7e5  C[3]=804c400c  D[3]=a60fc9d2
A[4]=a1117f09  B[4]=66f9ee2d  C[4]=87d6962b  D[4]=e8360fb2
A[5]=a1ead0f1  B[5]=caf08087  C[5]=2a6fe533  D[5]=064acbd2
A[6]=118039ac  B[6]=de5c7ae9  C[6]=9ef8f1e8  D[6]=55317cc5
A[7]=9fe09cae  B[7]=19d2dd9b  C[7]=c101412b  D[7]=db7824e5

Step  3: (r=27, s= 3)
A[0]=843c3c82  B[0]=71ed2841  C[0]=f6955e48  D[0]=ed176417
A[1]=f80e8b17  B[1]=2cd6e8eb  C[1]=28aa4014  D[1]=9fe03844
A[2]=8a9d63a6  B[2]=22ef26ba  C[2]=3ad10326  D[2]=f38e8911
A[3]=0c02fb90  B[3]=a805353e  C[3]=6aa7d7e5  D[3]=804c400c
A[4]=d0baf7bf  B[4]=4d088bf8  C[4]=66f9ee2d  D[4]=87d6962b
```

```
A[5]=4e51fff7  B[5]=8d0f5687  C[5]=caf08087  D[5]=2a6fe533
A[6]=6db56732  B[6]=608c01cd  C[6]=de5c7ae9  D[6]=9ef8f1e8
A[7]=c23790aa  B[7]=74ff04e5  C[7]=19d2dd9b  D[7]=c101412b

Step  4: (r= 3, s=20)
A[0]=caffcbdd  B[0]=21e1e414  C[0]=71ed2841  D[0]=f6955e48
A[1]=99702dfe  B[1]=c07458bf  C[1]=2cd6e8eb  D[1]=28aa4014
A[2]=9d8845ac  B[2]=54eb1d34  C[2]=22ef26ba  D[2]=3ad10326
A[3]=3aa04296  B[3]=6017dc80  C[3]=a805353e  D[3]=6aa7d7e5
A[4]=39287e42  B[4]=85d7bdfe  C[4]=4d088bf8  D[4]=66f9ee2d
A[5]=d1569cae  B[5]=728fffba  C[5]=8d0f5687  D[5]=caf08087
A[6]=d1cedef7  B[6]=6dab3993  C[6]=608c01cd  D[6]=de5c7ae9
A[7]=50f95273  B[7]=11bc8556  C[7]=74ff04e5  D[7]=19d2dd9b

Step  5: (r=20, s=14)
A[0]=3df77dd1  B[0]=bddcaffc  C[0]=21e1e414  D[0]=71ed2841
A[1]=db10db5a  B[1]=dfe99702  C[1]=c07458bf  D[1]=2cd6e8eb
A[2]=aac3b264  B[2]=5ac9d884  C[2]=54eb1d34  D[2]=22ef26ba
A[3]=bbd5b132  B[3]=2963aa04  C[3]=6017dc80  D[3]=a805353e
A[4]=57982780  B[4]=e4239287  C[4]=85d7bdfe  D[4]=4d088bf8
A[5]=fb090565  B[5]=caed1569  C[5]=728fffba  D[5]=8d0f5687
A[6]=c1eb9070  B[6]=ef7d1ced  C[6]=6dab3993  D[6]=608c01cd
A[7]=0f8c8315  B[7]=27350f95  C[7]=11bc8556  D[7]=74ff04e5

Step  6: (r=14, s=27)
A[0]=78e2fee1  B[0]=df744f7d  C[0]=bddcaffc  D[0]=21e1e414
A[1]=2e60fdf8  B[1]=36d6b6c4  C[1]=dfe99702  D[1]=c07458bf
A[2]=3c0f2ac1  B[2]=ec992ab0  C[2]=5ac9d884  D[2]=54eb1d34
A[3]=88768e99  B[3]=6c4caef5  C[3]=2963aa04  D[3]=6017dc80
A[4]=cbbabea6  B[4]=09e015e6  C[4]=e4239287  D[4]=85d7bdfe
A[5]=f25f3388  B[5]=41597ec2  C[5]=caed1569  D[5]=728fffba
A[6]=a3757597  B[6]=e41c307a  C[6]=ef7d1ced  D[6]=6dab3993
A[7]=31cb4439  B[7]=20c543e3  C[7]=27350f95  D[7]=11bc8556

Step  7: (r=27, s= 3)
A[0]=19cdffa4  B[0]=0bc717f7  C[0]=df744f7d  D[0]=bddcaffc
A[1]=3fb4bb91  B[1]=c17307ef  C[1]=36d6b6c4  D[1]=dfe99702
A[2]=50288db9  B[2]=09e07956  C[2]=ec992ab0  D[2]=5ac9d884
A[3]=a65caf8f  B[3]=cc43b474  C[3]=6c4caef5  D[3]=2963aa04
A[4]=d88bb9d9  B[4]=365dd5f5  C[4]=09e015e6  D[4]=e4239287
A[5]=5d4e58b0  B[5]=4792f99c  C[5]=41597ec2  D[5]=caed1569
A[6]=8c520847  B[6]=bd1babac  C[6]=e41c307a  D[6]=ef7d1ced
A[7]=72481fee  B[7]=c98e5a21  C[7]=20c543e3  D[7]=27350f95

Step  8: (r=26, s= 4)
A[0]=d7eb0d29  B[0]=906737fe  C[0]=0bc717f7  D[0]=df744f7d
A[1]=5060c7ee  B[1]=44fed2ee  C[1]=c17307ef  D[1]=36d6b6c4
A[2]=ca2d82d0  B[2]=e540a236  C[2]=09e07956  D[2]=ec992ab0
A[3]=2359bd11  B[3]=3e9972be  C[3]=cc43b474  D[3]=6c4caef5
```

```
A[4]=55c418c0  B[4]=67622ee7  C[4]=365dd5f5  D[4]=09e015e6
A[5]=1d3ad0ba  B[5]=c1753962  C[5]=4792f99c  D[5]=41597ec2
A[6]=8e13ea21  B[6]=1e314821  C[6]=bd1babac  D[6]=e41c307a
A[7]=4b0a3136  B[7]=b9c9207f  C[7]=c98e5a21  D[7]=20c543e3

Step  9: (r= 4, s=23)
A[0]=e43b7da8  B[0]=7eb0d29d  C[0]=906737fe  D[0]=0bc717f7
A[1]=c80c09fa  B[1]=060c7ee5  C[1]=44fed2ee  D[1]=c17307ef
A[2]=4a834da1  B[2]=a2d82d0c  C[2]=e540a236  D[2]=09e07956
A[3]=84bd4fe7  B[3]=359bd112  C[3]=3e9972be  D[3]=cc43b474
A[4]=030e02ea  B[4]=5c418c05  C[4]=67622ee7  D[4]=365dd5f5
A[5]=6d6a4b1a  B[5]=d3ad0ba1  C[5]=c1753962  D[5]=4792f99c
A[6]=71eef94f  B[6]=e13ea218  C[6]=1e314821  D[6]=bd1babac
A[7]=99620c23  B[7]=b0a31364  C[7]=b9c9207f  D[7]=c98e5a21

Step 10: (r=23, s=11)
A[0]=1e3ea415  B[0]=d4721dbe  C[0]=7eb0d29d  D[0]=906737fe
A[1]=edba1519  B[1]=fd640604  C[1]=060c7ee5  D[1]=44fed2ee
A[2]=482020a9  B[2]=d0a541a6  C[2]=a2d82d0c  D[2]=e540a236
A[3]=fc08bf97  B[3]=f3c25ea7  C[3]=359bd112  D[3]=3e9972be
A[4]=b5da83b6  B[4]=75018701  C[4]=5c418c05  D[4]=67622ee7
A[5]=a8a151c9  B[5]=8d36b525  C[5]=d3ad0ba1  D[5]=c1753962
A[6]=bcea3d24  B[6]=a7b8f77c  C[6]=e13ea218  D[6]=1e314821
A[7]=95edc6fc  B[7]=11ccb106  C[7]=b0a31364  D[7]=b9c9207f

Step 11: (r=11, s=26)
A[0]=af1c9fdc  B[0]=f520a8f1  C[0]=d4721dbe  D[0]=7eb0d29d
A[1]=947d0733  B[1]=d0a8cf6d  C[1]=fd640604  D[1]=060c7ee5
A[2]=892cb97f  B[2]=01054a41  C[2]=d0a541a6  D[2]=a2d82d0c
A[3]=7b77c879  B[3]=45fcbfe0  C[3]=f3c25ea7  D[3]=359bd112
A[4]=7c7867eb  B[4]=d41db5ae  C[4]=75018701  D[4]=5c418c05
A[5]=935dd442  B[5]=0a8e4d45  C[5]=8d36b525  D[5]=d3ad0ba1
A[6]=19edcf85  B[6]=51e925e7  C[6]=a7b8f77c  D[6]=e13ea218
A[7]=eee06d8d  B[7]=6e37e4af  C[7]=11ccb106  D[7]=b0a31364

Step 12: (r=26, s= 4)
A[0]=8527ff57  B[0]=72bc727f  C[0]=f520a8f1  D[0]=d4721dbe
A[1]=16d5aed7  B[1]=ce51f41c  C[1]=d0a8cf6d  D[1]=fd640604
A[2]=b7453ac6  B[2]=fe24b2e5  C[2]=01054a41  D[2]=d0a541a6
A[3]=60efbdb4  B[3]=e5eddf21  C[3]=45fcbfe0  D[3]=f3c25ea7
A[4]=2c3baee2  B[4]=adf1e19f  C[4]=d41db5ae  D[4]=75018701
A[5]=a2d0f9ef  B[5]=0a4d7751  C[5]=0a8e4d45  D[5]=8d36b525
A[6]=11395ec9  B[6]=1467b73e  C[6]=51e925e7  D[6]=a7b8f77c
A[7]=c4241d1a  B[7]=37bb81b6  C[7]=6e37e4af  D[7]=11ccb106

Step 13: (r= 4, s=23)
A[0]=9c0d78ef  B[0]=527ff578  C[0]=72bc727f  D[0]=f520a8f1
A[1]=a566af9e  B[1]=6d5aed71  C[1]=ce51f41c  D[1]=d0a8cf6d
A[2]=b9e790b4  B[2]=7453ac6b  C[2]=fe24b2e5  D[2]=01054a41
```

```
A[3]=748ea32e  B[3]=0efbdb46  C[3]=e5eddf21  D[3]=45fcbfe0
A[4]=6d43ceb4  B[4]=c3baee22  C[4]=adf1e19f  D[4]=d41db5ae
A[5]=47e55b54  B[5]=2d0f9efa  C[5]=0a4d7751  D[5]=0a8e4d45
A[6]=480b92bb  B[6]=1395ec91  C[6]=1467b73e  D[6]=51e925e7
A[7]=68387aad  B[7]=4241d1ac  C[7]=37bb81b6  D[7]=6e37e4af

Step 14: (r=23, s=11)
A[0]=26645573  B[0]=77ce06bc  C[0]=527ff578  D[0]=72bc727f
A[1]=32f201de  B[1]=cf52b357  C[1]=6d5aed71  D[1]=ce51f41c
A[2]=48dc1833  B[2]=5a5cf3c8  C[2]=7453ac6b  D[2]=fe24b2e5
A[3]=89340f44  B[3]=973a4751  C[3]=0efbdb46  D[3]=e5eddf21
A[4]=ebccdf5e  B[4]=5a36a1e7  C[4]=c3baee22  D[4]=adf1e19f
A[5]=ddd6350a  B[5]=aa23f2ad  C[5]=2d0f9efa  D[5]=0a4d7751
A[6]=906e57d2  B[6]=5da405c9  C[6]=1395ec91  D[6]=1467b73e
A[7]=8726ee55  B[7]=56b41c3d  C[7]=4241d1ac  D[7]=37bb81b6

Step 15: (r=11, s=26)
A[0]=b4004e72  B[0]=22ab9933  C[0]=77ce06bc  D[0]=527ff578
A[1]=7a6dc870  B[1]=900ef197  C[1]=cf52b357  D[1]=6d5aed71
A[2]=64189ce0  B[2]=e0c19a46  C[2]=5a5cf3c8  D[2]=7453ac6b
A[3]=100c393a  B[3]=a07a2449  C[3]=973a4751  D[3]=0efbdb46
A[4]=edb9356c  B[4]=66faf75e  C[4]=5a36a1e7  D[4]=c3baee22
A[5]=69a2bf3e  B[5]=b1a856ee  C[5]=aa23f2ad  D[5]=2d0f9efa
A[6]=ba0fe74c  B[6]=72be9483  C[6]=5da405c9  D[6]=1395ec91
A[7]=1e88c69c  B[7]=3772ac39  C[7]=56b41c3d  D[7]=4241d1ac

Step 16: (r=19, s=28)
A[0]=eda8572f  B[0]=7395a002  C[0]=22ab9933  D[0]=77ce06bc
A[1]=e4d1f12b  B[1]=4383d36e  C[1]=900ef197  D[1]=cf52b357
A[2]=d8ab8184  B[2]=e70320c4  C[2]=e0c19a46  D[2]=5a5cf3c8
A[3]=607519de  B[3]=c9d08061  C[3]=a07a2449  D[3]=973a4751
A[4]=974a7c55  B[4]=ab676dc9  C[4]=66faf75e  D[4]=5a36a1e7
A[5]=a9c1711e  B[5]=f9f34d15  C[5]=b1a856ee  D[5]=aa23f2ad
A[6]=242e868f  B[6]=3a65d07f  C[6]=72be9483  D[6]=5da405c9
A[7]=0ff1e25b  B[7]=34e0f446  C[7]=3772ac39  D[7]=56b41c3d

Step 17: (r=28, s= 7)
A[0]=a9f6fbef  B[0]=feda8572  C[0]=7395a002  D[0]=22ab9933
A[1]=0293b4a1  B[1]=be4d1f12  C[1]=4383d36e  D[1]=900ef197
A[2]=8decb878  B[2]=4d8ab818  C[2]=e70320c4  D[2]=e0c19a46
A[3]=c4771369  B[3]=e607519d  C[3]=c9d08061  D[3]=a07a2449
A[4]=a6e0ba7b  B[4]=5974a7c5  C[4]=ab676dc9  D[4]=66faf75e
A[5]=099354b0  B[5]=ea9c1711  C[5]=f9f34d15  D[5]=b1a856ee
A[6]=1ef374d9  B[6]=f242e868  C[6]=3a65d07f  D[6]=72be9483
A[7]=eece5d78  B[7]=b0ff1e25  C[7]=34e0f446  D[7]=3772ac39

Step 18: (r= 7, s=22)
A[0]=4cb4bed1  B[0]=fb7df7d4  C[0]=feda8572  D[0]=7395a002
A[1]=b66d5ec5  B[1]=49da5081  C[1]=be4d1f12  D[1]=4383d36e
```

```
A[2]=ca51c2a0  B[2]=f65c3c46  C[2]=4d8ab818  D[2]=e70320c4
A[3]=cfcde7bd  B[3]=3b89b4e2  C[3]=e607519d  D[3]=c9d08061
A[4]=0f935f5b  B[4]=705d3dd3  C[4]=5974a7c5  D[4]=ab676dc9
A[5]=f283b2f9  B[5]=c9aa5804  C[5]=ea9c1711  D[5]=f9f34d15
A[6]=521f1a4c  B[6]=79ba6c8f  C[6]=f242e868  D[6]=3a65d07f
A[7]=d2c3aaff  B[7]=672ebc77  C[7]=b0ff1e25  D[7]=34e0f446

Step 19: (r=22, s=19)
A[0]=4030ba48  B[0]=b4532d2f  C[0]=fb7df7d4  D[0]=feda8572
A[1]=bea5a1d0  B[1]=b16d9b57  C[1]=49da5081  D[1]=be4d1f12
A[2]=4f3c123b  B[2]=a8329470  C[2]=f65c3c46  D[2]=4d8ab818
A[3]=8029a819  B[3]=ef73f379  C[3]=3b89b4e2  D[3]=e607519d
A[4]=88259b6e  B[4]=d6c3e4d7  C[4]=705d3dd3  D[4]=5974a7c5
A[5]=16019515  B[5]=be7ca0ec  C[5]=c9aa5804  D[5]=ea9c1711
A[6]=b9d8550b  B[6]=931487c6  C[6]=79ba6c8f  D[6]=f242e868
A[7]=e8b5b737  B[7]=bff4b0ea  C[7]=672ebc77  D[7]=b0ff1e25

Step 20: (r=19, s=28)
A[0]=3d4087e1  B[0]=d2420185  C[0]=b4532d2f  D[0]=fb7df7d4
A[1]=759ea7f7  B[1]=0e85f52d  C[1]=b16d9b57  D[1]=49da5081
A[2]=bdef37ff  B[2]=91da79e0  C[2]=a8329470  D[2]=f65c3c46
A[3]=ec599ef4  B[3]=40cc014d  C[3]=ef73f379  D[3]=3b89b4e2
A[4]=101a29b2  B[4]=db74412c  C[4]=d6c3e4d7  D[4]=705d3dd3
A[5]=98b944ac  B[5]=a8a8b00c  C[5]=be7ca0ec  D[5]=c9aa5804
A[6]=89e468e3  B[6]=a85dcec2  C[6]=931487c6  D[6]=79ba6c8f
A[7]=76bbdb02  B[7]=b9bf45ad  C[7]=bff4b0ea  D[7]=672ebc77

Step 21: (r=28, s= 7)
A[0]=d909d4cc  B[0]=13d4087e  C[0]=d2420185  D[0]=b4532d2f
A[1]=b05c3e84  B[1]=7759ea7f  C[1]=0e85f52d  D[1]=b16d9b57
A[2]=f8d770d3  B[2]=fbdef37f  C[2]=91da79e0  D[2]=a8329470
A[3]=34a86ccc  B[3]=4ec599ef  C[3]=40cc014d  D[3]=ef73f379
A[4]=f2e565bf  B[4]=2101a29b  C[4]=db74412c  D[4]=d6c3e4d7
A[5]=01de1303  B[5]=c98b944a  C[5]=a8a8b00c  D[5]=be7ca0ec
A[6]=ef8ca29e  B[6]=389e468e  C[6]=a85dcec2  D[6]=931487c6
A[7]=49f1227b  B[7]=276bbdb0  C[7]=b9bf45ad  D[7]=bff4b0ea

Step 22: (r= 7, s=22)
A[0]=47f239ac  B[0]=84ea666c  C[0]=13d4087e  D[0]=d2420185
A[1]=08dd7685  B[1]=2e1f4258  C[1]=7759ea7f  D[1]=0e85f52d
A[2]=354316bd  B[2]=6bb869fc  C[2]=fbdef37f  D[2]=91da79e0
A[3]=560a67a5  B[3]=5436661a  C[3]=4ec599ef  D[3]=40cc014d
A[4]=74a92ada  B[4]=72b2dff9  C[4]=2101a29b  D[4]=db74412c
A[5]=c940a325  B[5]=ef098180  C[5]=c98b944a  D[5]=a8a8b00c
A[6]=f447e4f3  B[6]=c6514f77  C[6]=389e468e  D[6]=a85dcec2
A[7]=6cced04a  B[7]=f8913da4  C[7]=276bbdb0  D[7]=b9bf45ad

Step 23: (r=22, s=19)
A[0]=ecda22a6  B[0]=6b11fc8e  C[0]=84ea666c  D[0]=13d4087e
```

```
A[1]=b9e7a851  B[1]=a142375d  C[1]=2e1f4258  D[1]=7759ea7f
A[2]=327463ad  B[2]=af4d50c5  C[2]=6bb869fc  D[2]=fbdef37f
A[3]=f98964e8  B[3]=e9558299  C[3]=5436661a  D[3]=4ec599ef
A[4]=c039dc82  B[4]=b69d2a4a  C[4]=72b2dff9  D[4]=2101a29b
A[5]=fa22d6fb  B[5]=c9725028  C[5]=ef098180  D[5]=c98b944a
A[6]=d5133c93  B[6]=3cfd11f9  C[6]=c6514f77  D[6]=389e468e
A[7]=784227f9  B[7]=129b33b4  C[7]=f8913da4  D[7]=276bbdb0

Step 24: (r=15, s= 5)
A[0]=3602d010  B[0]=1153766d  C[0]=6b11fc8e  D[0]=84ea666c
A[1]=f8ca09ae  B[1]=d428dcf3  C[1]=a142375d  D[1]=2e1f4258
A[2]=a7f86350  B[2]=31d6993a  C[2]=af4d50c5  D[2]=6bb869fc
A[3]=4ae49755  B[3]=b2747cc4  C[3]=e9558299  D[3]=5436661a
A[4]=79dd1417  B[4]=ee41601c  C[4]=b69d2a4a  D[4]=72b2dff9
A[5]=ccdfe061  B[5]=6b7dfd11  C[5]=c9725028  D[5]=ef098180
A[6]=1ceab3b2  B[6]=9e49ea89  C[6]=3cfd11f9  D[6]=c6514f77
A[7]=873ebcc0  B[7]=13fcbc21  C[7]=129b33b4  D[7]=f8913da4

Step 25: (r= 5, s=29)
A[0]=cfe02c5d  B[0]=c05a0206  C[0]=1153766d  D[0]=6b11fc8e
A[1]=07bb5020  B[1]=194135df  C[1]=d428dcf3  D[1]=a142375d
A[2]=74694445  B[2]=ff0c6a14  C[2]=31d6993a  D[2]=af4d50c5
A[3]=5d3825b0  B[3]=5c92eaa9  C[3]=b2747cc4  D[3]=e9558299
A[4]=672e8da7  B[4]=3ba282ef  C[4]=ee41601c  D[4]=b69d2a4a
A[5]=91866970  B[5]=9bfc0c39  C[5]=6b7dfd11  D[5]=c9725028
A[6]=c480c54f  B[6]=9d567643  C[6]=9e49ea89  D[6]=3cfd11f9
A[7]=69b25026  B[7]=e7d79810  C[7]=13fcbc21  D[7]=129b33b4

Step 26: (r=29, s= 9)
A[0]=cf7a7d2f  B[0]=b9fc058b  C[0]=c05a0206  D[0]=1153766d
A[1]=739676c3  B[1]=00f76a04  C[1]=194135df  D[1]=d428dcf3
A[2]=ba368e07  B[2]=ae8d2888  C[2]=ff0c6a14  D[2]=31d6993a
A[3]=35ae2244  B[3]=0ba704b6  C[3]=5c92eaa9  D[3]=b2747cc4
A[4]=b3d6941f  B[4]=ece5d1b4  C[4]=3ba282ef  D[4]=ee41601c
A[5]=5462374a  B[5]=1230cd2e  C[5]=9bfc0c39  D[5]=6b7dfd11
A[6]=0d9c0c76  B[6]=f89018a9  C[6]=9d567643  D[6]=9e49ea89
A[7]=b42f2bc2  B[7]=cd364a04  C[7]=e7d79810  D[7]=13fcbc21

Step 27: (r= 9, s=15)
A[0]=d10b281b  B[0]=f4fa5f9e  C[0]=b9fc058b  D[0]=c05a0206
A[1]=76359e01  B[1]=2ced86e7  C[1]=00f76a04  D[1]=194135df
A[2]=29b9917b  B[2]=6d1c0f74  C[2]=ae8d2888  D[2]=ff0c6a14
A[3]=cae8da14  B[3]=5c44886b  C[3]=0ba704b6  D[3]=5c92eaa9
A[4]=c3472374  B[4]=ad283f67  C[4]=ece5d1b4  D[4]=3ba282ef
A[5]=ab4025d2  B[5]=c46e94a8  C[5]=1230cd2e  D[5]=9bfc0c39
A[6]=2fd35e6e  B[6]=3818ec1b  C[6]=f89018a9  D[6]=9d567643
A[7]=e8dfe932  B[7]=5e578568  C[7]=cd364a04  D[7]=e7d79810

Step 28: (r=15, s= 5)
```

```
A[0]=802fe1bc  B[0]=940de885  C[0]=f4fa5f9e  D[0]=b9fc058b
A[1]=99d08529  B[1]=cf00bb1a  C[1]=2ced86e7  D[1]=00f76a04
A[2]=87b2b238  B[2]=c8bd94dc  C[2]=6d1c0f74  D[2]=ae8d2888
A[3]=daec2b12  B[3]=6d0a6574  C[3]=5c44886b  D[3]=0ba704b6
A[4]=5eda54ac  B[4]=91ba61a3  C[4]=ad283f67  D[4]=ece5d1b4
A[5]=d7f45a88  B[5]=12e955a0  C[5]=c46e94a8  D[5]=1230cd2e
A[6]=741eae32  B[6]=af3717e9  C[6]=3818ec1b  D[6]=f89018a9
A[7]=151b6455  B[7]=f499746f  C[7]=5e578568  D[7]=cd364a04

Step 29: (r= 5, s=29)
A[0]=7291ee83  B[0]=05fc3790  C[0]=940de885  D[0]=f4fa5f9e
A[1]=cf96a3b0  B[1]=3a10a533  C[1]=cf00bb1a  D[1]=2ced86e7
A[2]=80c8e467  B[2]=f6564710  C[2]=c8bd94dc  D[2]=6d1c0f74
A[3]=0938845e  B[3]=5d85625b  C[3]=6d0a6574  D[3]=5c44886b
A[4]=3e61039e  B[4]=db4a958b  C[4]=91ba61a3  D[4]=ad283f67
A[5]=b3d23831  B[5]=fe8b511a  C[5]=12e955a0  D[5]=c46e94a8
A[6]=de1f6307  B[6]=83d5c64e  C[6]=af3717e9  D[6]=3818ec1b
A[7]=5cadf2da  B[7]=a36c8aa2  C[7]=f499746f  D[7]=5e578568

Step 30: (r=29, s= 9)
A[0]=09f5ec21  B[0]=6e523dd0  C[0]=05fc3790  D[0]=940de885
A[1]=a457d628  B[1]=19f2d476  C[1]=3a10a533  D[1]=cf00bb1a
A[2]=55e050be  B[2]=f0191c8c  C[2]=f6564710  D[2]=c8bd94dc
A[3]=697bd5d9  B[3]=c127108b  C[3]=5d85625b  D[3]=6d0a6574
A[4]=1af6912e  B[4]=c7cc2073  C[4]=db4a958b  D[4]=91ba61a3
A[5]=7824836f  B[5]=367a4706  C[5]=fe8b511a  D[5]=12e955a0
A[6]=7335eb4e  B[6]=fbc3ec60  C[6]=83d5c64e  D[6]=af3717e9
A[7]=f66873a6  B[7]=4b95be5b  C[7]=a36c8aa2  D[7]=f499746f

Step 31: (r= 9, s=15)
A[0]=dadc18bb  B[0]=ebd84213  C[0]=6e523dd0  D[0]=05fc3790
A[1]=7c32bd49  B[1]=afac5148  C[1]=19f2d476  D[1]=3a10a533
A[2]=8bce4b30  B[2]=c0a17cab  C[2]=f0191c8c  D[2]=f6564710
A[3]=5bd7a979  B[3]=f7abb2d2  C[3]=c127108b  D[3]=5d85625b
A[4]=baed20e3  B[4]=ed225c35  C[4]=c7cc2073  D[4]=db4a958b
A[5]=f3d2a2ec  B[5]=4906def0  C[5]=367a4706  D[5]=fe8b511a
A[6]=d1646add  B[6]=6bd69ce6  C[6]=fbc3ec60  D[6]=83d5c64e
A[7]=405a34ad  B[7]=d0e74dec  C[7]=4b95be5b  D[7]=a36c8aa2

Feistel Step 0: (r=15, s= 5)
A[0]=c32d1cb9  B[0]=0c5ded6e  C[0]=ebd84213  D[0]=6e523dd0
A[1]=a9ac514f  B[1]=5ea4be19  C[1]=afac5148  D[1]=19f2d476
A[2]=48f564a0  B[2]=259845e7  C[2]=c0a17cab  D[2]=f0191c8c
A[3]=e2f9d2d7  B[3]=d4bcadeb  C[3]=f7abb2d2  D[3]=c127108b
A[4]=ffa1702d  B[4]=9071dd76  C[4]=ed225c35  D[4]=c7cc2073
A[5]=20602c46  B[5]=517679e9  C[5]=4906def0  D[5]=367a4706
A[6]=62c6f980  B[6]=356ee8b2  C[6]=6bd69ce6  D[6]=fbc3ec60
A[7]=89d2b047  B[7]=1a56a02d  C[7]=d0e74dec  D[7]=4b95be5b
```

```
Feistel Step 1: (r= 5, s=29)
A[0]=de762870  B[0]=65a39738  C[0]=0c5ded6e  D[0]=ebd84213
A[1]=fabfe391  B[1]=358a29f5  C[1]=5ea4be19  D[1]=afac5148
A[2]=a5cb515b  B[2]=1eac9409  C[2]=259845e7  D[2]=c0a17cab
A[3]=fabae5e8  B[3]=5f3a5afc  C[3]=d4bcadeb  D[3]=f7abb2d2
A[4]=4d4cb05f  B[4]=f42e05bf  C[4]=9071dd76  D[4]=ed225c35
A[5]=4367e0ab  B[5]=0c0588c4  C[5]=517679e9  D[5]=4906def0
A[6]=6512b54e  B[6]=58df300c  C[6]=356ee8b2  D[6]=6bd69ce6
A[7]=692358b2  B[7]=3a5608f1  C[7]=1a56a02d  D[7]=d0e74dec

Feistel Step 2: (r=29, s= 9)
A[0]=26e9a959  B[0]=1bcec50e  C[0]=65a39738  D[0]=0c5ded6e
A[1]=35e43381  B[1]=3f57fc72  C[1]=358a29f5  D[1]=5ea4be19
A[2]=5886c9a5  B[2]=74b96a2b  C[2]=1eac9409  D[2]=259845e7
A[3]=23445d63  B[3]=1f575cbd  C[3]=5f3a5afc  D[3]=d4bcadeb
A[4]=d708f644  B[4]=e9a9960b  C[4]=f42e05bf  D[4]=9071dd76
A[5]=69cc5a0c  B[5]=686cfc15  C[5]=0c0588c4  D[5]=517679e9
A[6]=ea43707e  B[6]=cca256a9  C[6]=58df300c  D[6]=356ee8b2
A[7]=fd644716  B[7]=4d246b16  C[7]=3a5608f1  D[7]=1a56a02d

Feistel Step 3: (r= 9, s=15)
A[0]=1e41b814  B[0]=d352b24d  C[0]=1bcec50e  D[0]=65a39738
A[1]=63819ffc  B[1]=c867026b  C[1]=3f57fc72  D[1]=358a29f5
A[2]=b67591d7  B[2]=0d934ab1  C[2]=74b96a2b  D[2]=1eac9409
A[3]=07bec4cf  B[3]=88bac646  C[3]=1f575cbd  D[3]=5f3a5afc
A[4]=a48b282c  B[4]=11ec89ae  C[4]=e9a9960b  D[4]=f42e05bf
A[5]=3b3851ef  B[5]=98b418d3  C[5]=686cfc15  D[5]=0c0588c4
A[6]=f0692825  B[6]=86e0fdd4  C[6]=cca256a9  D[6]=58df300c
A[7]=e252902a  B[7]=c88e2dfa  C[7]=4d246b16  D[7]=3a5608f1
```

Compression Function Output

```
A[0]=1e41b814  B[0]=d352b24d  C[0]=1bcec50e  D[0]=65a39738
A[1]=63819ffc  B[1]=c867026b  C[1]=3f57fc72  D[1]=358a29f5
A[2]=b67591d7  B[2]=0d934ab1  C[2]=74b96a2b  D[2]=1eac9409
A[3]=07bec4cf  B[3]=88bac646  C[3]=1f575cbd  D[3]=5f3a5afc
A[4]=a48b282c  B[4]=11ec89ae  C[4]=e9a9960b  D[4]=f42e05bf
A[5]=3b3851ef  B[5]=98b418d3  C[5]=686cfc15  D[5]=0c0588c4
A[6]=f0692825  B[6]=86e0fdd4  C[6]=cca256a9  D[6]=58df300c
A[7]=e252902a  B[7]=c88e2dfa  C[7]=4d246b16  D[7]=3a5608f1
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
```

```
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   61  165  253   25  100  103   38  217
y[  8.. 15] =   83  222  217   81  155  191  230   68
y[ 16.. 23] =  160   84  131  211  120  256   67  256
y[ 24.. 31] =   70  153   56  134  184   54   47  116
y[ 32.. 39] =    3  142  144  243   16   32   20   71
y[ 40.. 47] =   63   73  194  216  243  207  172  210
y[ 48.. 55] =  183  243   53   83  146   42  138  255
y[ 56.. 63] =  108  123  230   72  215  135    9   14
y[ 64.. 71] =  119  197   87   94   48   28  240   38
y[ 72.. 79] =   57  190   59  107  148  226  117  121
y[ 80.. 87] =  177  224  217  112   89  175   90   39
y[ 88.. 95] =   72  226   62  109  209  193  100  189
y[ 96..103] =  243  143  181  173  213  195   59  237
y[104..111] =  200   30   90  227   52  251   86   58
y[112..119] =   43   98  145   86  103  101  123  134
y[120..127] =   12   87   90  153  210  217   69   88
y[128..135] =   49  202  114   85   10    7   72  150
y[136..143] =   27  145  150   29  212  176  137   42
y[144..151] =  207   26  236  156  247  111   43  111
y[152..159] =   40  214   54  233  183   56   63  251
y[160..167] =  107  225  223  124   94   78   90   39
y[168..175] =   47   37  173  151  124  160  195  157
y[176..183] =  184  124   57   27  221   68  229  112
y[184..191] =    2  244  137   38  152  232  101   96
y[192..199] =  248  170   23   16   62   82  127   72
y[200..207] =   53  177   51    3  219  141  250  246
y[208..215] =  190  143  150  255   21  192   20   71
y[216..223] =   38  141   48    1  158  174   10  178
y[224..231] =  124  224  186  194  154  172   51  130
y[232..239] =  167   80   20  140   58  116   24   52
y[240..247] =   67   12  222   24    7    9  244  233
y[248..255] =   98   23   20  214  157  150   41   22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
```

```
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
Z[17] = d27ea7b7  ece38d52  f6e66d38  27233cfb
        24683fb6  312632f8  bca6bd8f  39572ac7
Z[18] = 616302bb  e10e9927  558e0e90  51ea1234
        2ac73957  b38cc6a9  70dcf342  c792b2a3
Z[19] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
Z[20] = f7cf6c4f  14ef4f2f  386e2bb0  7397f087
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
Z[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
Z[22] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
Z[23] = 3cfb2723  e0259a10  065f5dbf  f42b6ff3
        59320aec  123451ea  a4fcd539  25513ecd
Z[24] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
Z[25] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
```

```
Z[26] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
Z[27] = 70dcf342  18934b8b  3de4263a  65f0fe2e
        f42b6ff3  22964188  e93f90f6  57600cbe
Z[28] = b0d1c964  0e90558e  4aa2197c  41882296
        b730c305  02bb6163  966ce3c9  f5fd6e21
Z[29] = 983ee1f7  fe2e65f0  c4d7b55e  409f237f
        966ce3c9  00e96335  b475c5c0  b819c21c
Z[30] = e1f7983e  c6a9b38c  b2a3c792  8c69edcc
        48d01b4e  9583e4b2  6994fa8a  2f5434ca
Z[31] = 0aec5932  15d84e46  08315bed  ea28900d
        14ef4f2f  d8dda158  9e9ddb98  14065018
```

Expanded Message

```
W[ 0] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
W[ 1] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
W[ 4] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
W[10] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
W[12] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
W[15] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
W[16] = d27ea7b7  ece38d52  f6e66d38  27233cfb
        24683fb6  312632f8  bca6bd8f  39572ac7
```

```
W[17] = 616302bb  e10e9927  558e0e90  51ea1234
        2ac73957  b38cc6a9  70dcf342  c792b2a3
W[18] = 3cfb2723  e0259a10  065f5dbf  f42b6ff3
        59320aec  123451ea  a4fcd539  25513ecd
W[19] = f7cf6c4f  14ef4f2f  386e2bb0  7397f087
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
W[20] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
W[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
W[22] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
W[23] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
W[24] = e1f7983e  c6a9b38c  b2a3c792  8c69edcc
        48d01b4e  9583e4b2  6994fa8a  2f5434ca
W[25] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
W[26] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
W[27] = 0aec5932  15d84e46  08315bed  ea28900d
        14ef4f2f  d8dda158  9e9ddb98  14065018
W[28] = 70dcf342  18934b8b  3de4263a  65f0fe2e
        f42b6ff3  22964188  e93f90f6  57600cbe
W[29] = 983ee1f7  fe2e65f0  c4d7b55e  409f237f
        966ce3c9  00e96335  b475c5c0  b819c21c
W[30] = b0d1c964  0e90558e  4aa2197c  41882296
        b730c305  02bb6163  966ce3c9  f5fd6e21
W[31] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
```

Feistel Steps

```
IV :
A[0]=1e41b814  B[0]=d352b24d  C[0]=1bcec50e  D[0]=65a39738
A[1]=63819ffc  B[1]=c867026b  C[1]=3f57fc72  D[1]=358a29f5
A[2]=b67591d7  B[2]=0d934ab1  C[2]=74b96a2b  D[2]=1eac9409
A[3]=07bec4cf  B[3]=88bac646  C[3]=1f575cbd  D[3]=5f3a5afc
A[4]=a48b282c  B[4]=11ec89ae  C[4]=e9a9960b  D[4]=f42e05bf
A[5]=3b3851ef  B[5]=98b418d3  C[5]=686cfc15  D[5]=0c0588c4
A[6]=f0692825  B[6]=86e0fdd4  C[6]=cca256a9  D[6]=58df300c
A[7]=e252902a  B[7]=c88e2dfa  C[7]=4d246b16  D[7]=3a5608f1

IV XOR M :
A[0]=1e41bc23  B[0]=d352b24d  C[0]=1bcec50e  D[0]=65a39738
A[1]=63819ffc  B[1]=c867026b  C[1]=3f57fc72  D[1]=358a29f5
A[2]=b67591d7  B[2]=0d934ab1  C[2]=74b96a2b  D[2]=1eac9409
A[3]=07bec4cf  B[3]=88bac646  C[3]=1f575cbd  D[3]=5f3a5afc
A[4]=a48b282c  B[4]=11ec89ae  C[4]=e9a9960b  D[4]=f42e05bf
```

```
A[5]=3b3851ef  B[5]=98b418d3  C[5]=686cfc15  D[5]=0c0588c4
A[6]=f0692825  B[6]=86e0fdd4  C[6]=cca256a9  D[6]=58df300c
A[7]=e252902a  B[7]=c88e2dfa  C[7]=4d246b16  D[7]=3a5608f1

Step  0: (r= 3, s=20)
A[0]=0051e150  B[0]=f20de118  C[0]=d352b24d  D[0]=1bcec50e
A[1]=a5fb3e14  B[1]=1c0cffe3  C[1]=c867026b  D[1]=3f57fc72
A[2]=551d9e9a  B[2]=b3ac8ebd  C[2]=0d934ab1  D[2]=74b96a2b
A[3]=6645c98f  B[3]=3df62678  C[3]=88bac646  D[3]=1f575cbd
A[4]=abb36635  B[4]=24594165  C[4]=11ec89ae  D[4]=e9a9960b
A[5]=28045e3c  B[5]=d9c28f79  C[5]=98b418d3  D[5]=686cfc15
A[6]=0fd1770c  B[6]=8349412f  C[6]=86e0fdd4  D[6]=cca256a9
A[7]=0f0f300b  B[7]=12948157  C[7]=c88e2dfa  D[7]=4d246b16

Step  1: (r=20, s=14)
A[0]=5528b8f5  B[0]=1500051e  C[0]=f20de118  D[0]=d352b24d
A[1]=d9f2b808  B[1]=e14a5fb3  C[1]=1c0cffe3  D[1]=c867026b
A[2]=db461d7c  B[2]=e9a551d9  C[2]=b3ac8ebd  D[2]=0d934ab1
A[3]=44b48f2b  B[3]=98f6645c  C[3]=3df62678  D[3]=88bac646
A[4]=fe634904  B[4]=635abb36  C[4]=24594165  D[4]=11ec89ae
A[5]=d3b7abce  B[5]=e3c28045  C[5]=d9c28f79  D[5]=98b418d3
A[6]=f4e10e21  B[6]=70c0fd17  C[6]=8349412f  D[6]=86e0fdd4
A[7]=918e4ea9  B[7]=00b0f0f3  C[7]=12948157  D[7]=c88e2dfa

Step  2: (r=14, s=27)
A[0]=85e9455e  B[0]=2e3d554a  C[0]=1500051e  D[0]=f20de118
A[1]=9886b833  B[1]=ae02367c  C[1]=e14a5fb3  D[1]=1c0cffe3
A[2]=5d012e23  B[2]=875f36d1  C[2]=e9a551d9  D[2]=b3ac8ebd
A[3]=776f87c8  B[3]=23cad12d  C[3]=98f6645c  D[3]=3df62678
A[4]=96a2afa5  B[4]=d2413f98  C[4]=635abb36  D[4]=24594165
A[5]=8c573ad4  B[5]=eaf3b4ed  C[5]=e3c28045  D[5]=d9c28f79
A[6]=1c59f685  B[6]=43887d38  C[6]=70c0fd17  D[6]=8349412f
A[7]=a61f742d  B[7]=93aa6463  C[7]=00b0f0f3  D[7]=12948157

Step  3: (r=27, s= 3)
A[0]=c59659ea  B[0]=f42f4a2a  C[0]=2e3d554a  D[0]=1500051e
A[1]=7e33e92d  B[1]=9cc435c1  C[1]=ae02367c  D[1]=e14a5fb3
A[2]=ac7360e7  B[2]=1ae80971  C[2]=875f36d1  D[2]=e9a551d9
A[3]=5631abe1  B[3]=43bb7c3e  C[3]=23cad12d  D[3]=98f6645c
A[4]=57c4be1c  B[4]=2cb5157d  C[4]=d2413f98  D[4]=635abb36
A[5]=dc74cb7e  B[5]=a462b9d6  C[5]=eaf3b4ed  D[5]=e3c28045
A[6]=186daa8e  B[6]=28e2cfb4  C[6]=43887d38  D[6]=70c0fd17
A[7]=de04c329  B[7]=6d30fba1  C[7]=93aa6463  D[7]=00b0f0f3

Step  4: (r= 3, s=20)
A[0]=cb534a82  B[0]=2cb2cf56  C[0]=f42f4a2a  D[0]=2e3d554a
A[1]=6fc0a68a  B[1]=f19f496b  C[1]=9cc435c1  D[1]=ae02367c
A[2]=852970e5  B[2]=639b073d  C[2]=1ae80971  D[2]=875f36d1
A[3]=ca634438  B[3]=b18d5f0a  C[3]=43bb7c3e  D[3]=23cad12d
```

```
A[4]=1395ebe6  B[4]=be25f0e2  C[4]=2cb5157d  D[4]=d2413f98
A[5]=72fe41b9  B[5]=e3a65bf6  C[5]=a462b9d6  D[5]=eaf3b4ed
A[6]=9debe57a  B[6]=c36d5470  C[6]=28e2cfb4  D[6]=43887d38
A[7]=227f4b10  B[7]=f026194e  C[7]=6d30fba1  D[7]=93aa6463

Step  5: (r=20, s=14)
A[0]=27b7533d  B[0]=a82cb534  C[0]=2cb2cf56  D[0]=f42f4a2a
A[1]=1364a561  B[1]=68a6fc0a  C[1]=f19f496b  D[1]=9cc435c1
A[2]=46528925  B[2]=0e585297  C[2]=639b073d  D[2]=1ae80971
A[3]=c4433cf3  B[3]=438ca634  C[3]=b18d5f0a  D[3]=43bb7c3e
A[4]=710b9d62  B[4]=be61395e  C[4]=be25f0e2  D[4]=2cb5157d
A[5]=7fee6f1b  B[5]=1b972fe4  C[5]=e3a65bf6  D[5]=a462b9d6
A[6]=065f612b  B[6]=57a9debe  C[6]=c36d5470  D[6]=28e2cfb4
A[7]=5d812093  B[7]=b10227f4  C[7]=f026194e  D[7]=6d30fba1

Step  6: (r=14, s=27)
A[0]=68db1ebf  B[0]=d4cf49ed  C[0]=a82cb534  D[0]=2cb2cf56
A[1]=a29df3e2  B[1]=295844d9  C[1]=68a6fc0a  D[1]=f19f496b
A[2]=17c3c5de  B[2]=a2495194  C[2]=0e585297  D[2]=639b073d
A[3]=6f775765  B[3]=cf3cf110  C[3]=438ca634  D[3]=b18d5f0a
A[4]=295ac1f7  B[4]=e7589c42  C[4]=be61395e  D[4]=be25f0e2
A[5]=ece9e246  B[5]=9bc6dffb  C[5]=1b972fe4  D[5]=e3a65bf6
A[6]=ca197d05  B[6]=d84ac197  C[6]=57a9debe  D[6]=c36d5470
A[7]=9811d30c  B[7]=4824d760  C[7]=b10227f4  D[7]=f026194e

Step  7: (r=27, s= 3)
A[0]=4b000de1  B[0]=fb46d8f5  C[0]=d4cf49ed  D[0]=a82cb534
A[1]=ff5e6851  B[1]=1514ef9f  C[1]=295844d9  D[1]=68a6fc0a
A[2]=77ae4843  B[2]=f0be1e2e  C[2]=a2495194  D[2]=0e585297
A[3]=654cc3e0  B[3]=2b7bbabb  C[3]=cf3cf110  D[3]=438ca634
A[4]=0dfcbf66  B[4]=b94ad60f  C[4]=e7589c42  D[4]=be61395e
A[5]=49709240  B[5]=37674f12  C[5]=9bc6dffb  D[5]=1b972fe4
A[6]=14ae0864  B[6]=2e50cbe8  C[6]=d84ac197  D[6]=57a9debe
A[7]=0b545009  B[7]=64c08e98  C[7]=4824d760  D[7]=b10227f4

Step  8: (r=26, s= 4)
A[0]=5280626a  B[0]=852c0037  C[0]=fb46d8f5  D[0]=d4cf49ed
A[1]=7670f5bf  B[1]=47fd79a1  C[1]=1514ef9f  D[1]=295844d9
A[2]=de1c46cf  B[2]=0ddeb921  C[2]=f0be1e2e  D[2]=a2495194
A[3]=e8c3b11e  B[3]=8195330f  C[3]=2b7bbabb  D[3]=cf3cf110
A[4]=a5b725b4  B[4]=9837f2fd  C[4]=b94ad60f  D[4]=e7589c42
A[5]=9ee0d436  B[5]=0125c249  C[5]=37674f12  D[5]=9bc6dffb
A[6]=8db3581d  B[6]=9052b821  C[6]=2e50cbe8  D[6]=d84ac197
A[7]=a4df87f1  B[7]=242d5140  C[7]=64c08e98  D[7]=4824d760

Step  9: (r= 4, s=23)
A[0]=d3b04653  B[0]=280626a5  C[0]=852c0037  D[0]=fb46d8f5
A[1]=61fd39e2  B[1]=670f5bf7  C[1]=47fd79a1  D[1]=1514ef9f
A[2]=00863ccc  B[2]=e1c46cfd  C[2]=0ddeb921  D[2]=f0be1e2e
```

```
A[3]=a8e14f83  B[3]=8c3b11ee  C[3]=8195330f  D[3]=2b7bbabb
A[4]=14f0bba0  B[4]=5b725b4a  C[4]=9837f2fd  D[4]=b94ad60f
A[5]=6fe4b1c4  B[5]=ee0d4369  C[5]=0125c249  D[5]=37674f12
A[6]=2726a1d2  B[6]=db3581d8  C[6]=9052b821  D[6]=2e50cbe8
A[7]=c1060c7d  B[7]=4df87f1a  C[7]=242d5140  D[7]=64c08e98

Step 10: (r=23, s=11)
A[0]=e5a55109  B[0]=29e9d823  C[0]=280626a5  D[0]=852c0037
A[1]=7be49f8d  B[1]=f130fe9c  C[1]=670f5bf7  D[1]=47fd79a1
A[2]=c9ff3c26  B[2]=6600431e  C[2]=e1c46cfd  D[2]=0ddeb921
A[3]=9a4affa2  B[3]=c1d470a7  C[3]=8c3b11ee  D[3]=8195330f
A[4]=54923966  B[4]=d00a785d  C[4]=5b725b4a  D[4]=9837f2fd
A[5]=23b9f85a  B[5]=e237f258  C[5]=ee0d4369  D[5]=0125c249
A[6]=83841a0b  B[6]=e9139350  C[6]=db3581d8  D[6]=9052b821
A[7]=e91ee632  B[7]=3ee08306  C[7]=4df87f1a  D[7]=242d5140

Step 11: (r=11, s=26)
A[0]=a7e7750d  B[0]=2a884f2d  C[0]=29e9d823  D[0]=280626a5
A[1]=d7ad2bc9  B[1]=24fc6bdf  C[1]=f130fe9c  D[1]=670f5bf7
A[2]=0a9c1420  B[2]=f9e1364f  C[2]=6600431e  D[2]=e1c46cfd
A[3]=0e1466a8  B[3]=57fd14d2  C[3]=c1d470a7  D[3]=8c3b11ee
A[4]=5d12f930  B[4]=91cb32a4  C[4]=d00a785d  D[4]=5b725b4a
A[5]=e10db180  B[5]=cfc2d11d  C[5]=e237f258  D[5]=ee0d4369
A[6]=aa9d26fc  B[6]=20d05c1c  C[6]=e9139350  D[6]=db3581d8
A[7]=a1bab728  B[7]=f7319748  C[7]=3ee08306  D[7]=4df87f1a

Step 12: (r=26, s= 4)
A[0]=9304afb5  B[0]=369f9dd4  C[0]=2a884f2d  D[0]=29e9d823
A[1]=739b2845  B[1]=275eb4af  C[1]=24fc6bdf  D[1]=f130fe9c
A[2]=68000eb3  B[2]=802a7050  C[2]=f9e1364f  D[2]=6600431e
A[3]=c494ca82  B[3]=a038519a  C[3]=57fd14d2  D[3]=c1d470a7
A[4]=da233d26  B[4]=c1744be4  C[4]=91cb32a4  D[4]=d00a785d
A[5]=bd4a045f  B[5]=038436c6  C[5]=cfc2d11d  D[5]=e237f258
A[6]=667d1686  B[6]=f2aa749b  C[6]=20d05c1c  D[6]=e9139350
A[7]=07deaf2b  B[7]=a286eadc  C[7]=f7319748  D[7]=3ee08306

Step 13: (r= 4, s=23)
A[0]=3685f5d1  B[0]=304afb59  C[0]=369f9dd4  D[0]=2a884f2d
A[1]=55587719  B[1]=39b28457  C[1]=275eb4af  D[1]=24fc6bdf
A[2]=7f5a8f1d  B[2]=8000eb36  C[2]=802a7050  D[2]=f9e1364f
A[3]=108f743e  B[3]=494ca82c  C[3]=a038519a  D[3]=57fd14d2
A[4]=2378354d  B[4]=a233d26d  C[4]=c1744be4  D[4]=91cb32a4
A[5]=31a44c44  B[5]=d4a045fb  C[5]=038436c6  D[5]=cfc2d11d
A[6]=d3bbdb3d  B[6]=67d16866  C[6]=f2aa749b  D[6]=20d05c1c
A[7]=98f6f617  B[7]=7deaf2b0  C[7]=a286eadc  D[7]=f7319748

Step 14: (r=23, s=11)
A[0]=d09f05ca  B[0]=e89b42fa  C[0]=304afb59  D[0]=369f9dd4
A[1]=3f25438c  B[1]=8caaac3b  C[1]=39b28457  D[1]=275eb4af
```

```
A[2]=75435fb8  B[2]=8ebfad47  C[2]=8000eb36  D[2]=802a7050
A[3]=6cc28fbb  B[3]=1f0847ba  C[3]=494ca82c  D[3]=a038519a
A[4]=e4488a39  B[4]=a691bc1a  C[4]=a233d26d  D[4]=c1744be4
A[5]=fd8929ed  B[5]=2218d226  C[5]=d4a045fb  D[5]=038436c6
A[6]=261a6aae  B[6]=9ee9dded  C[6]=67d16866  D[6]=f2aa749b
A[7]=9383b638  B[7]=0bcc7b7b  C[7]=7deaf2b0  D[7]=a286eadc

Step 15: (r=11, s=26)
A[0]=6c8f580f  B[0]=f82e5684  C[0]=e89b42fa  D[0]=304afb59
A[1]=462d5c01  B[1]=2a1c61f9  C[1]=8caaac3b  D[1]=39b28457
A[2]=32707984  B[2]=1afdc3aa  C[2]=8ebfad47  D[2]=8000eb36
A[3]=dbf8acb4  B[3]=147ddb66  C[3]=1f0847ba  D[3]=494ca82c
A[4]=46b3b118  B[4]=4451cf22  C[4]=a691bc1a  D[4]=a233d26d
A[5]=d0aa6015  B[5]=494f6fec  C[5]=2218d226  D[5]=d4a045fb
A[6]=e8b323c7  B[6]=d3557130  C[6]=9ee9dded  D[6]=67d16866
A[7]=c80d731f  B[7]=1db1c49c  C[7]=0bcc7b7b  D[7]=7deaf2b0

Step 16: (r=19, s=28)
A[0]=2eb8b0ca  B[0]=c07b647a  C[0]=f82e5684  D[0]=e89b42fa
A[1]=0b8db398  B[1]=e00a316a  C[1]=2a1c61f9  D[1]=8caaac3b
A[2]=770551a8  B[2]=cc219383  C[2]=1afdc3aa  D[2]=8ebfad47
A[3]=24701e88  B[3]=65a6dfc5  C[3]=147ddb66  D[3]=1f0847ba
A[4]=5b595f45  B[4]=88c2359d  C[4]=4451cf22  D[4]=a691bc1a
A[5]=1f404c4e  B[5]=00ae8553  C[5]=494f6fec  D[5]=2218d226
A[6]=78ab629c  B[6]=1e3f4599  C[6]=d3557130  D[6]=9ee9dded
A[7]=5a6f7bf8  B[7]=98fe406b  C[7]=1db1c49c  D[7]=0bcc7b7b

Step 17: (r=28, s= 7)
A[0]=a5c656a7  B[0]=a2eb8b0c  C[0]=c07b647a  D[0]=f82e5684
A[1]=6b2267ae  B[1]=80b8db39  C[1]=e00a316a  D[1]=2a1c61f9
A[2]=469337a4  B[2]=8770551a  C[2]=cc219383  D[2]=1afdc3aa
A[3]=10d5c58b  B[3]=824701e8  C[3]=65a6dfc5  D[3]=147ddb66
A[4]=94500297  B[4]=55b595f4  C[4]=88c2359d  D[4]=4451cf22
A[5]=60075049  B[5]=e1f404c4  C[5]=00ae8553  D[5]=494f6fec
A[6]=f8c709c9  B[6]=c78ab629  C[6]=1e3f4599  D[6]=d3557130
A[7]=90ed4a3c  B[7]=85a6f7bf  C[7]=98fe406b  D[7]=1db1c49c

Step 18: (r= 7, s=22)
A[0]=776aa770  B[0]=e32b53d2  C[0]=a2eb8b0c  D[0]=c07b647a
A[1]=3fe77f8f  B[1]=9133d735  C[1]=80b8db39  D[1]=e00a316a
A[2]=9ed4081d  B[2]=499bd223  C[2]=8770551a  D[2]=cc219383
A[3]=f15ccfe3  B[3]=6ae2c588  C[3]=824701e8  D[3]=65a6dfc5
A[4]=55914b0b  B[4]=28014bca  C[4]=55b595f4  D[4]=88c2359d
A[5]=13cade34  B[5]=03a824b0  C[5]=e1f404c4  D[5]=00ae8553
A[6]=31c39a57  B[6]=6384e4fc  C[6]=c78ab629  D[6]=1e3f4599
A[7]=5d5e4223  B[7]=76a51e48  C[7]=85a6f7bf  D[7]=98fe406b

Step 19: (r=22, s=19)
A[0]=a4024400  B[0]=dc1ddaa9  C[0]=e32b53d2  D[0]=a2eb8b0c
```

```
A[1]=4b792461  B[1]=e3cff9df  C[1]=9133d735  D[1]=80b8db39
A[2]=377ce2e6  B[2]=0767b502  C[2]=499bd223  D[2]=8770551a
A[3]=377933a4  B[3]=f8fc5733  C[3]=6ae2c588  D[3]=824701e8
A[4]=2803a3d3  B[4]=c2d56452  C[4]=28014bca  D[4]=55b595f4
A[5]=e380908c  B[5]=8d04f2b7  C[5]=03a824b0  D[5]=e1f404c4
A[6]=3e6ece96  B[6]=95cc70e6  C[6]=6384e4fc  D[6]=c78ab629
A[7]=0d1f9156  B[7]=88d75790  C[7]=76a51e48  D[7]=85a6f7bf

Step 20: (r=19, s=28)
A[0]=128798d5  B[0]=20052012  C[0]=dc1ddaa9  D[0]=e32b53d2
A[1]=403e88ca  B[1]=230a5bc9  C[1]=e3cff9df  D[1]=9133d735
A[2]=a034ddbc  B[2]=1731bbe7  C[2]=0767b502  D[2]=499bd223
A[3]=c9ec64da  B[3]=9d21bbc9  C[3]=f8fc5733  D[3]=6ae2c588
A[4]=d723f862  B[4]=1e99401d  C[4]=c2d56452  D[4]=28014bca
A[5]=4613d093  B[5]=84671c04  C[5]=8d04f2b7  D[5]=03a824b0
A[6]=bdf285a3  B[6]=74b1f376  C[6]=95cc70e6  D[6]=6384e4fc
A[7]=cf33594b  B[7]=8ab068fc  C[7]=88d75790  D[7]=76a51e48

Step 21: (r=28, s= 7)
A[0]=e55517b6  B[0]=5128798d  C[0]=20052012  D[0]=dc1ddaa9
A[1]=1ce51296  B[1]=a403e88c  C[1]=230a5bc9  D[1]=e3cff9df
A[2]=4898debe  B[2]=ca034ddb  C[2]=1731bbe7  D[2]=0767b502
A[3]=25cb8f37  B[3]=ac9ec64d  C[3]=9d21bbc9  D[3]=f8fc5733
A[4]=d055fa6a  B[4]=2d723f86  C[4]=1e99401d  D[4]=c2d56452
A[5]=6d0a106d  B[5]=34613d09  C[5]=84671c04  D[5]=8d04f2b7
A[6]=db47d8e5  B[6]=3bdf285a  C[6]=74b1f376  D[6]=95cc70e6
A[7]=6dcacf0e  B[7]=bcf33594  C[7]=8ab068fc  D[7]=88d75790

Step 22: (r= 7, s=22)
A[0]=d681f646  B[0]=aa8bdb72  C[0]=5128798d  D[0]=20052012
A[1]=d5c85881  B[1]=72894b0e  C[1]=a403e88c  D[1]=230a5bc9
A[2]=865edbb2  B[2]=4c6f5f24  C[2]=ca034ddb  D[2]=1731bbe7
A[3]=70b7396a  B[3]=e5c79b92  C[3]=ac9ec64d  D[3]=9d21bbc9
A[4]=60c58a1c  B[4]=2afd3568  C[4]=2d723f86  D[4]=1e99401d
A[5]=e383609e  B[5]=850836b6  C[5]=34613d09  D[5]=84671c04
A[6]=94437711  B[6]=a3ec72ed  C[6]=3bdf285a  D[6]=74b1f376
A[7]=d0fe001d  B[7]=e5678736  C[7]=bcf33594  D[7]=8ab068fc

Step 23: (r=22, s=19)
A[0]=470db258  B[0]=91b5a07d  C[0]=aa8bdb72  D[0]=5128798d
A[1]=cc4b3c7e  B[1]=20757216  C[1]=72894b0e  D[1]=a403e88c
A[2]=78fb36ca  B[2]=eca197b6  C[2]=4c6f5f24  D[2]=ca034ddb
A[3]=5d97816f  B[3]=5a9c2dce  C[3]=e5c79b92  D[3]=ac9ec64d
A[4]=9d5feb84  B[4]=87183162  C[4]=2afd3568  D[4]=2d723f86
A[5]=e0f3539f  B[5]=27b8e0d8  C[5]=850836b6  D[5]=34613d09
A[6]=e94fdf3f  B[6]=c46510dd  C[6]=a3ec72ed  D[6]=3bdf285a
A[7]=0cab0a71  B[7]=07743f80  C[7]=e5678736  D[7]=bcf33594

Step 24: (r=15, s= 5)
```

```
A[0]=333ecee0  B[0]=d92c2386  C[0]=91b5a07d  D[0]=aa8bdb72
A[1]=870e0959  B[1]=9e3f6625  C[1]=20757216  D[1]=72894b0e
A[2]=ea465148  B[2]=9b653c7d  C[2]=eca197b6  D[2]=4c6f5f24
A[3]=d6ff3b63  B[3]=c0b7aecb  C[3]=5a9c2dce  D[3]=e5c79b92
A[4]=6921f7fc  B[4]=f5c24eaf  C[4]=87183162  D[4]=2afd3568
A[5]=e9731d2c  B[5]=a9cff079  C[5]=27b8e0d8  D[5]=850836b6
A[6]=9062fe82  B[6]=ef9ff4a7  C[6]=c46510dd  D[6]=a3ec72ed
A[7]=251f2141  B[7]=85388655  C[7]=07743f80  D[7]=e5678736

Step 25: (r= 5, s=29)
A[0]=aa0f7e67  B[0]=67d9dc06  C[0]=d92c2386  D[0]=91b5a07d
A[1]=acb426f4  B[1]=e1c12b30  C[1]=9e3f6625  D[1]=20757216
A[2]=a4106682  B[2]=48ca291d  C[2]=9b653c7d  D[2]=eca197b6
A[3]=0b64bfef  B[3]=dfe76c7a  C[3]=c0b7aecb  D[3]=5a9c2dce
A[4]=81e49bd9  B[4]=243eff8d  C[4]=f5c24eaf  D[4]=87183162
A[5]=8dcb5650  B[5]=2e63a59d  C[5]=a9cff079  D[5]=27b8e0d8
A[6]=68068504  B[6]=0c5fd052  C[6]=ef9ff4a7  D[6]=c46510dd
A[7]=90c6e218  B[7]=a3e42824  C[7]=85388655  D[7]=07743f80

Step 26: (r=29, s= 9)
A[0]=24adca7c  B[0]=f541efcc  C[0]=67d9dc06  D[0]=d92c2386
A[1]=b655a38e  B[1]=959684de  C[1]=e1c12b30  D[1]=9e3f6625
A[2]=2f57ffa4  B[2]=54820cd0  C[2]=48ca291d  D[2]=9b653c7d
A[3]=66ef3292  B[3]=e16c97fd  C[3]=dfe76c7a  D[3]=c0b7aecb
A[4]=1ad16ba5  B[4]=303c937b  C[4]=243eff8d  D[4]=f5c24eaf
A[5]=a6ac494c  B[5]=11b96aca  C[5]=2e63a59d  D[5]=a9cff079
A[6]=8ffbd1eb  B[6]=8d00d0a0  C[6]=0c5fd052  D[6]=ef9ff4a7
A[7]=eadca2db  B[7]=1218dc43  C[7]=a3e42824  D[7]=85388655

Step 27: (r= 9, s=15)
A[0]=d05a6fea  B[0]=5b94f849  C[0]=f541efcc  D[0]=67d9dc06
A[1]=77275e23  B[1]=ab471d6c  C[1]=959684de  D[1]=e1c12b30
A[2]=4a25cb2f  B[2]=afff485e  C[2]=54820cd0  D[2]=48ca291d
A[3]=082e09fb  B[3]=de6524cd  C[3]=e16c97fd  D[3]=dfe76c7a
A[4]=761897c1  B[4]=a2d74a35  C[4]=303c937b  D[4]=243eff8d
A[5]=6a9c6338  B[5]=5892994d  C[5]=11b96aca  D[5]=2e63a59d
A[6]=0076d5ff  B[6]=f7a3d71f  C[6]=8d00d0a0  D[6]=0c5fd052
A[7]=8dcf7308  B[7]=b945b7d5  C[7]=1218dc43  D[7]=a3e42824

Step 28: (r=15, s= 5)
A[0]=f0099da8  B[0]=37f5682d  C[0]=5b94f849  D[0]=f541efcc
A[1]=6367cd63  B[1]=af11bb93  C[1]=ab471d6c  D[1]=959684de
A[2]=afb07ad1  B[2]=e597a512  C[2]=afff485e  D[2]=54820cd0
A[3]=ae25b9b3  B[3]=04fd8417  C[3]=de6524cd  D[3]=e16c97fd
A[4]=827c9377  B[4]=4be0bb0c  C[4]=a2d74a35  D[4]=303c937b
A[5]=7e2b08c1  B[5]=319c354e  C[5]=5892994d  D[5]=11b96aca
A[6]=11cb27d6  B[6]=6aff803b  C[6]=f7a3d71f  D[6]=8d00d0a0
A[7]=fd4504ad  B[7]=b98446e7  C[7]=b945b7d5  D[7]=1218dc43
```

```
Step 29: (r= 5, s=29)
A[0]=76323372  B[0]=0133b51e  C[0]=37f5682d  D[0]=5b94f849
A[1]=ec98c77b  B[1]=6cf9ac6c  C[1]=af11bb93  D[1]=ab471d6c
A[2]=1a55da6e  B[2]=f60f5a35  C[2]=e597a512  D[2]=afff485e
A[3]=e307d86e  B[3]=c4b73675  C[3]=04fd8417  D[3]=de6524cd
A[4]=6298bd11  B[4]=4f926ef0  C[4]=4be0bb0c  D[4]=a2d74a35
A[5]=3a0832a8  B[5]=c561182f  C[5]=319c354e  D[5]=5892994d
A[6]=463eb29f  B[6]=3964fac2  C[6]=6aff803b  D[6]=f7a3d71f
A[7]=55d00cd7  B[7]=a8a095bf  C[7]=b98446e7  D[7]=b945b7d5

Step 30: (r=29, s= 9)
A[0]=1e9fd821  B[0]=4ec6466e  C[0]=0133b51e  D[0]=37f5682d
A[1]=cb0cc19f  B[1]=7d9318ef  C[1]=6cf9ac6c  D[1]=af11bb93
A[2]=79b92836  B[2]=c34abb4d  C[2]=f60f5a35  D[2]=e597a512
A[3]=760acd6b  B[3]=dc60fb0d  C[3]=c4b73675  D[3]=04fd8417
A[4]=0df99058  B[4]=2c5317a2  C[4]=4f926ef0  D[4]=4be0bb0c
A[5]=6fa07865  B[5]=07410655  C[5]=c561182f  D[5]=319c354e
A[6]=9c6e20e0  B[6]=e8c7d653  C[6]=3964fac2  D[6]=6aff803b
A[7]=d51c213f  B[7]=eaba019a  C[7]=a8a095bf  D[7]=b98446e7

Step 31: (r= 9, s=15)
A[0]=dcf8c4d1  B[0]=3fb0423d  C[0]=4ec6466e  D[0]=0133b51e
A[1]=5cd311a3  B[1]=19833f96  C[1]=7d9318ef  D[1]=6cf9ac6c
A[2]=5a755108  B[2]=72506cf3  C[2]=c34abb4d  D[2]=f60f5a35
A[3]=1a547df9  B[3]=159ad6ec  C[3]=dc60fb0d  D[3]=c4b73675
A[4]=c9e6ffed  B[4]=f320b01b  C[4]=2c5317a2  D[4]=4f926ef0
A[5]=2db44bd8  B[5]=40f0cadf  C[5]=07410655  D[5]=c561182f
A[6]=950e5282  B[6]=dc41c138  C[6]=e8c7d653  D[6]=3964fac2
A[7]=a48a7a88  B[7]=38427faa  C[7]=eaba019a  D[7]=a8a095bf

Feistel Step 0: (r=15, s= 5)
A[0]=4e479c90  B[0]=6268ee7c  C[0]=3fb0423d  D[0]=4ec6466e
A[1]=a235b53d  B[1]=88d1ae69  C[1]=19833f96  D[1]=7d9318ef
A[2]=3af75759  B[2]=a8842d3a  C[2]=72506cf3  D[2]=c34abb4d
A[3]=bd5e734e  B[3]=3efc8d2a  C[3]=159ad6ec  D[3]=dc60fb0d
A[4]=4fd4fbd5  B[4]=7ff6e4f3  C[4]=f320b01b  D[4]=2c5317a2
A[5]=f14e0453  B[5]=25ec16da  C[5]=40f0cadf  D[5]=07410655
A[6]=0f413949  B[6]=29414a87  C[6]=dc41c138  D[6]=e8c7d653
A[7]=cdf57b05  B[7]=3d445245  C[7]=38427faa  D[7]=eaba019a

Feistel Step 1: (r= 5, s=29)
A[0]=71ac2406  B[0]=c8f39209  C[0]=6268ee7c  D[0]=3fb0423d
A[1]=67c02317  B[1]=46b6a7b4  C[1]=88d1ae69  D[1]=19833f96
A[2]=d01fd880  B[2]=5eeaeb27  C[2]=a8842d3a  D[2]=72506cf3
A[3]=faf5b093  B[3]=abce69d7  C[3]=3efc8d2a  D[3]=159ad6ec
A[4]=4fedb966  B[4]=fa9f7aa9  C[4]=7ff6e4f3  D[4]=f320b01b
A[5]=96ed9e79  B[5]=29c08a7e  C[5]=25ec16da  D[5]=40f0cadf
A[6]=03bcce34  B[6]=e8272921  C[6]=29414a87  D[6]=dc41c138
A[7]=a7d25b46  B[7]=beaf60b9  C[7]=3d445245  D[7]=38427faa
```

```
Feistel Step 2: (r=29, s= 9)
A[0]=949dd2a4  B[0]=ce358480  C[0]=c8f39209  D[0]=6268ee7c
A[1]=5a4ea214  B[1]=ecf80462  C[1]=46b6a7b4  D[1]=88d1ae69
A[2]=5c66648e  B[2]=1a03fb10  C[2]=5eeaeb27  D[2]=a8842d3a
A[3]=46c080f3  B[3]=7f5eb612  C[3]=abce69d7  D[3]=3efc8d2a
A[4]=52e464c0  B[4]=c9fdb72c  C[4]=fa9f7aa9  D[4]=7ff6e4f3
A[5]=56a7d8a6  B[5]=32ddb3cf  C[5]=29c08a7e  D[5]=25ec16da
A[6]=7f390e04  B[6]=807799c6  C[6]=e8272921  D[6]=29414a87
A[7]=a88b0707  B[7]=d4fa4b68  C[7]=beaf60b9  D[7]=3d445245

Feistel Step 3: (r= 9, s=15)
A[0]=cbe84ae7  B[0]=3ba54929  C[0]=ce358480  D[0]=c8f39209
A[1]=3eb05256  B[1]=9d4428b4  C[1]=ecf80462  D[1]=46b6a7b4
A[2]=484e79db  B[2]=ccc91cb8  C[2]=1a03fb10  D[2]=5eeaeb27
A[3]=feac5613  B[3]=8101e68d  C[3]=7f5eb612  D[3]=abce69d7
A[4]=5012f7bb  B[4]=c8c980a5  C[4]=c9fdb72c  D[4]=fa9f7aa9
A[5]=36825f8f  B[5]=4fb14cad  C[5]=32ddb3cf  D[5]=29c08a7e
A[6]=9ea51de3  B[6]=721c08fe  C[6]=807799c6  D[6]=e8272921
A[7]=e078edb1  B[7]=160e0f51  C[7]=d4fa4b68  D[7]=beaf60b9
```

Compression Function Output

```
A[0]=cbe84ae7  B[0]=3ba54929  C[0]=ce358480  D[0]=c8f39209
A[1]=3eb05256  B[1]=9d4428b4  C[1]=ecf80462  D[1]=46b6a7b4
A[2]=484e79db  B[2]=ccc91cb8  C[2]=1a03fb10  D[2]=5eeaeb27
A[3]=feac5613  B[3]=8101e68d  C[3]=7f5eb612  D[3]=abce69d7
A[4]=5012f7bb  B[4]=c8c980a5  C[4]=c9fdb72c  D[4]=fa9f7aa9
A[5]=36825f8f  B[5]=4fb14cad  C[5]=32ddb3cf  D[5]=29c08a7e
A[6]=9ea51de3  B[6]=721c08fe  C[6]=807799c6  D[6]=e8272921
A[7]=e078edb1  B[7]=160e0f51  C[7]=d4fa4b68  D[7]=beaf60b9
```

Hash Function Output

```
e74ae8cb5652b03edb794e481356acfebbf712508f5f8236
e31da59eb1ed78e02949a53bb428449db81cc9cc8de60181
```

6.4 SIMD-512

6.4.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
```

```
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  203  156   47  118  214  107  106
y[  8.. 15] =   45   93  212   20  111   73  162  251
y[ 16.. 23] =   97  215  249   53  211   19    3   89
y[ 24.. 31] =   49  207  101   67  151  130  223   23
y[ 32.. 39] =  189  202  178  239  253  127  204   49
y[ 40.. 47] =   76  236   82  137  232  157   65   79
y[ 48.. 55] =   96  161  176  130  161   30   47    9
y[ 56.. 63] =  189  247   61  226  248   90  107   64
y[ 64.. 71] =    0   88  131  243  133   59  113  115
y[ 72.. 79] =   17  236   33  213   12  191  111   19
y[ 80.. 87] =  251   61  103  208   57   35  148  248
y[ 88.. 95] =   47  116   65  119  249  178  143   40
y[ 96..103] =  189  129    8  163  204  227  230  196
y[104..111] =  205  122  151   45  187   19  227   72
y[112..119] =  247  125  111  121  140  220    6  107
y[120..127] =   77   69   10  101   21   65  149  171
y[128..135] =  255   54  101  210  139   43  150  151
y[136..143] =  212  164   45  237  146  184   95    6
y[144..151] =  160   42    8  204   46  238  254  168
y[152..159] =  208   50  156  190  106  127   34  234
y[160..167] =   68   55   79   18    4  130   53  208
y[168..175] =  181   21  175  120   25  100  192  178
y[176..183] =  161   96   81  127   96  227  210  248
y[184..191] =   68   10  196   31    9  167  150  193
y[192..199] =    0  169  126   14  124  198  144  142
y[200..207] =  240   21  224   44  245   66  146  238
y[208..215] =    6  196  154   49  200  222  109    9
y[216..223] =  210  141  192  138    8   79  114  217
y[224..231] =   68  128  249   94   53   30   27   61
y[232..239] =   52  135  106  212   70  238   30  185
y[240..247] =   10  132  146  136  117   37  251  150
y[248..255] =  180  188  247  156  236  192  108   86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
Z[17] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
Z[18] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
Z[19] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
Z[20] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
Z[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
Z[22] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
Z[23] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
Z[24] = 3126ceda  d5392ac7  2723d8dd  9f86607a
```

```
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
Z[25] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
Z[26] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
Z[27] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
Z[28] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
Z[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
        966c6994  93b16c4f  47e7b819  db982468
Z[30] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
Z[31] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
```

Expanded Message

```
W[ 0] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
W[ 3] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
W[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
W[ 8] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
```

```
        a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
W[17] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
W[18] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
W[19] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
W[20] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
W[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
W[22] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
W[23] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
W[24] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
W[25] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
W[26] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
W[27] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
W[28] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
W[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
        966c6994  93b16c4f  47e7b819  db982468
W[30] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
W[31] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
```

Feistel Steps

```
IV :
A[0]=c2956828  B[0]=39369835  C[0]=d9ca7181  D[0]=4d6185f6
A[1]=3da33320  B[1]=b7b6f593  C[1]=cf8e8183  D[1]=bbdcbc6e
A[2]=4149c566  B[2]=956d5c2e  C[2]=e2f28feb  D[2]=753b2bf6
A[3]=c49d9244  B[3]=2e4e80c8  C[3]=e9aa51c5  D[3]=7aac68ac
A[4]=04a3f1aa  B[4]=1e9fc449  C[4]=c5c2d649  D[4]=eb672a56
A[5]=0220c98b  B[5]=84ca34e9  C[5]=37c0b473  D[5]=ed8a5dcd
A[6]=7246bebf  B[6]=17d45ec5  C[6]=07eef0a5  D[6]=b072020d
A[7]=e51d9d96  B[7]=27db1b31  C[7]=dd23d692  D[7]=b07cf71f

IV XOR M :
A[0]=c2956828  B[0]=39369835  C[0]=d9ca7181  D[0]=4d6185f6
A[1]=3da33320  B[1]=b7b6f593  C[1]=cf8e8183  D[1]=bbdcbc6e
```

```
A[2]=4149c566  B[2]=956d5c2e  C[2]=e2f28feb  D[2]=753b2bf6
A[3]=c49d9244  B[3]=2e4e80c8  C[3]=e9aa51c5  D[3]=7aac68ac
A[4]=04a3f1aa  B[4]=1e9fc449  C[4]=c5c2d649  D[4]=eb672a56
A[5]=0220c98b  B[5]=84ca34e9  C[5]=37c0b473  D[5]=ed8a5dcd
A[6]=7246bebf  B[6]=17d45ec5  C[6]=07eef0a5  D[6]=b072020d
A[7]=e51d9d96  B[7]=27db1b31  C[7]=dd23d692  D[7]=b07cf71f

Step  0: (r= 3, s=20)
A[0]=e693fe7a  B[0]=14ab4146  C[0]=39369835  D[0]=d9ca7181
A[1]=42e5d827  B[1]=ed199901  C[1]=b7b6f593  D[1]=cf8e8183
A[2]=3580cfc8  B[2]=0a4e2b32  C[2]=956d5c2e  D[2]=e2f28feb
A[3]=cbbdda99  B[3]=24ec9226  C[3]=2e4e80c8  D[3]=e9aa51c5
A[4]=df906c37  B[4]=251f8d50  C[4]=1e9fc449  D[4]=c5c2d649
A[5]=cf0fc53a  B[5]=11064c58  C[5]=84ca34e9  D[5]=37c0b473
A[6]=bcd6777d  B[6]=9235f5fb  C[6]=17d45ec5  D[6]=07eef0a5
A[7]=b8a5ad35  B[7]=28ececb7  C[7]=27db1b31  D[7]=dd23d692

Step  1: (r=20, s=14)
A[0]=9cac7ec8  B[0]=e7ae693f  C[0]=14ab4146  D[0]=39369835
A[1]=bad3dc0a  B[1]=82742e5d  C[1]=ed199901  D[1]=b7b6f593
A[2]=88df7cab  B[2]=fc83580c  C[2]=0a4e2b32  D[2]=956d5c2e
A[3]=b694e6fe  B[3]=a99cbbdd  C[3]=24ec9226  D[3]=2e4e80c8
A[4]=c71f162a  B[4]=c37df906  C[4]=251f8d50  D[4]=1e9fc449
A[5]=0a8820dd  B[5]=53acf0fc  C[5]=11064c58  D[5]=84ca34e9
A[6]=92802335  B[6]=77dbcd67  C[6]=9235f5fb  D[6]=17d45ec5
A[7]=33734146  B[7]=d35b8a5a  C[7]=28ececb7  D[7]=27db1b31

Step  2: (r=14, s=27)
A[0]=7d088cf1  B[0]=1fb2272b  C[0]=e7ae693f  D[0]=14ab4146
A[1]=05d59a6c  B[1]=f702aeb4  C[1]=82742e5d  D[1]=ed199901
A[2]=683e3306  B[2]=df2ae237  C[2]=fc83580c  D[2]=0a4e2b32
A[3]=7e69ddce  B[3]=39bfada5  C[3]=a99cbbdd  D[3]=24ec9226
A[4]=3be74196  B[4]=c58ab1c7  C[4]=c37df906  D[4]=251f8d50
A[5]=e4614e41  B[5]=083742a2  C[5]=53acf0fc  D[5]=11064c58
A[6]=51fd0adb  B[6]=08cd64a0  C[6]=77dbcd67  D[6]=9235f5fb
A[7]=09ad5346  B[7]=d0518cdc  C[7]=d35b8a5a  D[7]=28ececb7

Step  3: (r=27, s= 3)
A[0]=167ae498  B[0]=8be84467  C[0]=1fb2272b  D[0]=e7ae693f
A[1]=48eb7b6d  B[1]=602eacd3  C[1]=f702aeb4  D[1]=82742e5d
A[2]=f09c7b38  B[2]=3341f198  C[2]=df2ae237  D[2]=fc83580c
A[3]=40ee460a  B[3]=73f34eee  C[3]=39bfada5  D[3]=a99cbbdd
A[4]=4854327d  B[4]=b1df3a0c  C[4]=c58ab1c7  D[4]=c37df906
A[5]=d0127f89  B[5]=0f230a72  C[5]=083742a2  D[5]=53acf0fc
A[6]=b9573e0b  B[6]=da8fe856  C[6]=08cd64a0  D[6]=77dbcd67
A[7]=16b06f4f  B[7]=304d6a9a  C[7]=d0518cdc  D[7]=d35b8a5a

Step  4: (r= 3, s=20)
A[0]=aa61fb56  B[0]=b3d724c0  C[0]=8be84467  D[0]=1fb2272b
```

```
A[1]=8c6ac5c2  B[1]=475bdb6a  C[1]=602eacd3  D[1]=f702aeb4
A[2]=72ef7d51  B[2]=84e3d9c7  C[2]=3341f198  D[2]=df2ae237
A[3]=72fa68b7  B[3]=07723052  C[3]=73f34eee  D[3]=39bfada5
A[4]=b01f6fe4  B[4]=42a193ea  C[4]=b1df3a0c  D[4]=c58ab1c7
A[5]=702be1be  B[5]=8093fc4e  C[5]=0f230a72  D[5]=083742a2
A[6]=3ee774bc  B[6]=cab9f05d  C[6]=da8fe856  D[6]=08cd64a0
A[7]=7d8448d7  B[7]=b5837a78  C[7]=304d6a9a  D[7]=d0518cdc

Step  5: (r=20, s=14)
A[0]=36de2ce1  B[0]=b56aa61f  C[0]=b3d724c0  D[0]=8be84467
A[1]=bd3075a7  B[1]=5c28c6ac  C[1]=475bdb6a  D[1]=602eacd3
A[2]=36b8f0f5  B[2]=d5172ef7  C[2]=84e3d9c7  D[2]=3341f198
A[3]=ce1e7078  B[3]=8b772fa6  C[3]=07723052  D[3]=73f34eee
A[4]=cfaea0f6  B[4]=fe4b01f6  C[4]=42a193ea  D[4]=b1df3a0c
A[5]=23fe2fda  B[5]=1be702be  C[5]=8093fc4e  D[5]=0f230a72
A[6]=d2182c8f  B[6]=4bc3ee77  C[6]=cab9f05d  D[6]=da8fe856
A[7]=053c0b6d  B[7]=8d77d844  C[7]=b5837a78  D[7]=304d6a9a

Step  6: (r=14, s=27)
A[0]=4ace76c3  B[0]=8b384db7  C[0]=b56aa61f  D[0]=b3d724c0
A[1]=ce30fed5  B[1]=1d69ef4c  C[1]=5c28c6ac  D[1]=475bdb6a
A[2]=0ae3ae28  B[2]=3c3d4dae  C[2]=d5172ef7  D[2]=84e3d9c7
A[3]=608d08f5  B[3]=9c1e3387  C[3]=8b772fa6  D[3]=07723052
A[4]=8fe8bfdd  B[4]=a83db3eb  C[4]=fe4b01f6  D[4]=42a193ea
A[5]=6c22e8d9  B[5]=8bf688ff  C[5]=1be702be  D[5]=8093fc4e
A[6]=c49b95bd  B[6]=0b23f486  C[6]=4bc3ee77  D[6]=cab9f05d
A[7]=5a567649  B[7]=02db414f  C[7]=8d77d844  D[7]=b5837a78

Step  7: (r=27, s= 3)
A[0]=f3bdd17f  B[0]=1a5673b6  C[0]=8b384db7  D[0]=b56aa61f
A[1]=19f73abc  B[1]=ae7187f6  C[1]=1d69ef4c  D[1]=5c28c6ac
A[2]=64dc166a  B[2]=40571d71  C[2]=3c3d4dae  D[2]=d5172ef7
A[3]=c9e5a4d8  B[3]=ab046847  C[3]=9c1e3387  D[3]=8b772fa6
A[4]=81a1ce4c  B[4]=ec7f45fe  C[4]=a83db3eb  D[4]=fe4b01f6
A[5]=959ffa4b  B[5]=cb611746  C[5]=8bf688ff  D[5]=1be702be
A[6]=1413e146  B[6]=ee24dcad  C[6]=0b23f486  D[6]=4bc3ee77
A[7]=2ed9f9e5  B[7]=4ad2b3b2  C[7]=02db414f  D[7]=8d77d844

Step  8: (r=26, s= 4)
A[0]=43088de1  B[0]=ffcef745  C[0]=1a5673b6  D[0]=8b384db7
A[1]=12f2ddd6  B[1]=f067dcea  C[1]=ae7187f6  D[1]=1d69ef4c
A[2]=e7c5ad17  B[2]=a9937059  C[2]=40571d71  D[2]=3c3d4dae
A[3]=5dc959d6  B[3]=63279693  C[3]=ab046847  D[3]=9c1e3387
A[4]=791a83f0  B[4]=32068739  C[4]=ec7f45fe  D[4]=a83db3eb
A[5]=16c76ede  B[5]=2e567fe9  C[5]=cb611746  D[5]=8bf688ff
A[6]=5386a4c9  B[6]=18504f85  C[6]=ee24dcad  D[6]=0b23f486
A[7]=7f5dcf32  B[7]=94bb67e7  C[7]=4ad2b3b2  D[7]=02db414f

Step  9: (r= 4, s=23)
```

```
A[0]=5370cd7d  B[0]=3088de14  C[0]=ffcef745  D[0]=1a5673b6
A[1]=383067e9  B[1]=2f2ddd61  C[1]=f067dcea  D[1]=ae7187f6
A[2]=f06cef75  B[2]=7c5ad17e  C[2]=a9937059  D[2]=40571d71
A[3]=40ea2f02  B[3]=dc959d65  C[3]=63279693  D[3]=ab046847
A[4]=5f1c3c6b  B[4]=91a83f07  C[4]=32068739  D[4]=ec7f45fe
A[5]=4f15d595  B[5]=6c76ede1  C[5]=2e567fe9  D[5]=cb611746
A[6]=67eb5c32  B[6]=386a4c95  C[6]=18504f85  D[6]=ee24dcad
A[7]=3beb8996  B[7]=f5dcf327  C[7]=94bb67e7  D[7]=4ad2b3b2

Step 10: (r=23, s=11)
A[0]=36ac4a7e  B[0]=bea9b866  C[0]=3088de14  D[0]=ffcef745
A[1]=d73732b5  B[1]=f49c1833  C[1]=2f2ddd61  D[1]=f067dcea
A[2]=4cebd766  B[2]=baf83677  C[2]=7c5ad17e  D[2]=a9937059
A[3]=b3510bf9  B[3]=81207517  C[3]=dc959d65  D[3]=63279693
A[4]=40e6b67c  B[4]=35af8e1e  C[4]=91a83f07  D[4]=32068739
A[5]=e272e933  B[5]=caa78aea  C[5]=6c76ede1  D[5]=2e567fe9
A[6]=85b8cae5  B[6]=1933f5ae  C[6]=386a4c95  D[6]=18504f85
A[7]=4900cffd  B[7]=cb1df5c4  C[7]=f5dcf327  D[7]=94bb67e7

Step 11: (r=11, s=26)
A[0]=1b29dc4f  B[0]=6253f1b5  C[0]=bea9b866  D[0]=3088de14
A[1]=fa73d720  B[1]=b995aeb9  C[1]=f49c1833  D[1]=2f2ddd61
A[2]=0a5da8f3  B[2]=5ebb3267  C[2]=baf83677  D[2]=7c5ad17e
A[3]=5e1035c1  B[3]=885fcd9a  C[3]=81207517  D[3]=dc959d65
A[4]=b055f58c  B[4]=35b3e207  C[4]=35af8e1e  D[4]=91a83f07
A[5]=fd4dd36e  B[5]=97499f13  C[5]=caa78aea  D[5]=6c76ede1
A[6]=672f3d77  B[6]=c6572c2d  C[6]=1933f5ae  D[6]=386a4c95
A[7]=dabb8823  B[7]=067fea48  C[7]=cb1df5c4  D[7]=f5dcf327

Step 12: (r=26, s= 4)
A[0]=14c2d584  B[0]=3c6ca771  C[0]=6253f1b5  D[0]=bea9b866
A[1]=53d4bd11  B[1]=83e9cf5c  C[1]=b995aeb9  D[1]=f49c1833
A[2]=9f0a940f  B[2]=cc2976a3  C[2]=5ebb3267  D[2]=baf83677
A[3]=118a8375  B[3]=057840d7  C[3]=885fcd9a  D[3]=81207517
A[4]=7425521b  B[4]=32c157d6  C[4]=35b3e207  D[4]=35af8e1e
A[5]=e8655cb7  B[5]=bbf5374d  C[5]=97499f13  D[5]=caa78aea
A[6]=45f8540d  B[6]=dd9cbcf5  C[6]=c6572c2d  D[6]=1933f5ae
A[7]=d57bfc8f  B[7]=8f6aee20  C[7]=067fea48  D[7]=cb1df5c4

Step 13: (r= 4, s=23)
A[0]=298cacd2  B[0]=4c2d5841  C[0]=3c6ca771  D[0]=6253f1b5
A[1]=877e250f  B[1]=3d4bd115  C[1]=83e9cf5c  D[1]=b995aeb9
A[2]=02ed44e2  B[2]=f0a940f9  C[2]=cc2976a3  D[2]=5ebb3267
A[3]=17104f57  B[3]=18a83751  C[3]=057840d7  D[3]=885fcd9a
A[4]=7e907fb3  B[4]=425521b7  C[4]=32c157d6  D[4]=35b3e207
A[5]=dbd7d03a  B[5]=8655cb7e  C[5]=bbf5374d  D[5]=97499f13
A[6]=13e13552  B[6]=5f8540d4  C[6]=dd9cbcf5  D[6]=c6572c2d
A[7]=9d70a499  B[7]=57bfc8fd  C[7]=8f6aee20  D[7]=067fea48
```

```
Step 14: (r=23, s=11)
A[0]=4b480e03  B[0]=6914c656  C[0]=4c2d5841  D[0]=3c6ca771
A[1]=c6715b0a  B[1]=87c3bf12  C[1]=3d4bd115  D[1]=83e9cf5c
A[2]=093f6204  B[2]=710176a2  C[2]=f0a940f9  D[2]=cc2976a3
A[3]=53993c10  B[3]=ab8b8827  C[3]=18a83751  D[3]=057840d7
A[4]=44a21de4  B[4]=d9bf483f  C[4]=425521b7  D[4]=32c157d6
A[5]=32bbf2f0  B[5]=1d6debe8  C[5]=8655cb7e  D[5]=bbf5374d
A[6]=8b5c5283  B[6]=a909f09a  C[6]=5f8540d4  D[6]=dd9cbcf5
A[7]=8e5509bd  B[7]=4cceb852  C[7]=57bfc8fd  D[7]=8f6aee20

Step 15: (r=11, s=26)
A[0]=747706c0  B[0]=40701a5a  C[0]=6914c656  D[0]=4c2d5841
A[1]=78d3f427  B[1]=8ad85633  C[1]=87c3bf12  D[1]=3d4bd115
A[2]=23e02058  B[2]=fb102049  C[2]=710176a2  D[2]=f0a940f9
A[3]=558246b3  B[3]=c9e0829c  C[3]=ab8b8827  D[3]=18a83751
A[4]=c4dd5476  B[4]=10ef2225  C[4]=d9bf483f  D[4]=425521b7
A[5]=09a00ff2  B[5]=df978195  C[5]=1d6debe8  D[5]=8655cb7e
A[6]=707bdd49  B[6]=e2941c5a  C[6]=a909f09a  D[6]=5f8540d4
A[7]=f8898ccf  B[7]=a84dec72  C[7]=4cceb852  D[7]=57bfc8fd

Step 16: (r=19, s=28)
A[0]=a5111dcd  B[0]=3603a3b8  C[0]=40701a5a  D[0]=6914c656
A[1]=4349f648  B[1]=a13bc69f  C[1]=8ad85633  D[1]=87c3bf12
A[2]=8e7344f2  B[2]=02c11f01  C[2]=fb102049  D[2]=710176a2
A[3]=02d88b4b  B[3]=359aac12  C[3]=c9e0829c  D[3]=ab8b8827
A[4]=528b0267  B[4]=a3b626ea  C[4]=10ef2225  D[4]=d9bf483f
A[5]=d839977a  B[5]=7f904d00  C[5]=df978195  D[5]=1d6debe8
A[6]=b110c61f  B[6]=ea4b83de  C[6]=e2941c5a  D[6]=a909f09a
A[7]=bc7baa43  B[7]=667fc44c  C[7]=a84dec72  D[7]=4cceb852

Step 17: (r=28, s= 7)
A[0]=d62d3a54  B[0]=da5111dc  C[0]=3603a3b8  D[0]=40701a5a
A[1]=52cc3be0  B[1]=84349f64  C[1]=a13bc69f  D[1]=8ad85633
A[2]=ce1c95cf  B[2]=28e7344f  C[2]=02c11f01  D[2]=fb102049
A[3]=4524dfb6  B[3]=b02d88b4  C[3]=359aac12  D[3]=c9e0829c
A[4]=b7e8f32c  B[4]=7528b026  C[4]=a3b626ea  D[4]=10ef2225
A[5]=6ce5c23d  B[5]=ad839977  C[5]=7f904d00  D[5]=df978195
A[6]=9d62cbf7  B[6]=fb110c61  C[6]=ea4b83de  D[6]=e2941c5a
A[7]=c05f8f12  B[7]=3bc7baa4  C[7]=667fc44c  D[7]=a84dec72

Step 18: (r= 7, s=22)
A[0]=fed66d08  B[0]=169d2a6b  C[0]=da5111dc  D[0]=3603a3b8
A[1]=5fd7be34  B[1]=661df029  C[1]=84349f64  D[1]=a13bc69f
A[2]=79bcb36b  B[2]=0e4ae7e7  C[2]=28e7344f  D[2]=02c11f01
A[3]=2636e0a7  B[3]=926fdb22  C[3]=b02d88b4  D[3]=359aac12
A[4]=da6fe169  B[4]=f479965b  C[4]=7528b026  D[4]=a3b626ea
A[5]=07506bac  B[5]=72e11eb6  C[5]=ad839977  D[5]=7f904d00
A[6]=5e509036  B[6]=b165fbce  C[6]=fb110c61  D[6]=ea4b83de
A[7]=33296b00  B[7]=2fc78960  C[7]=3bc7baa4  D[7]=667fc44c
```

```
Step 19: (r=22, s=19)
A[0]=3f1900be  B[0]=423fb59b  C[0]=169d2a6b  D[0]=da5111dc
A[1]=1590a51a  B[1]=8d17f5ef  C[1]=661df029  D[1]=84349f64
A[2]=b9fb736e  B[2]=dade6f2c  C[2]=0e4ae7e7  D[2]=28e7344f
A[3]=98f7d1e8  B[3]=29c98db8  C[3]=926fdb22  D[3]=b02d88b4
A[4]=77d402d1  B[4]=5a769bf8  C[4]=f479965b  D[4]=7528b026
A[5]=bd185847  B[5]=eb01d41a  C[5]=72e11eb6  D[5]=ad839977
A[6]=336af435  B[6]=0d979424  C[6]=b165fbce  D[6]=fb110c61
A[7]=4182f7be  B[7]=c00cca5a  C[7]=2fc78960  D[7]=3bc7baa4

Step 20: (r=19, s=28)
A[0]=5bb5dbd0  B[0]=05f1f8c8  C[0]=423fb59b  D[0]=169d2a6b
A[1]=7e122285  B[1]=28d0ac85  C[1]=8d17f5ef  D[1]=661df029
A[2]=9e84be76  B[2]=9b75cfdb  C[2]=dade6f2c  D[2]=0e4ae7e7
A[3]=3190e477  B[3]=8f44c7be  C[3]=29c98db8  D[3]=926fdb22
A[4]=73ed09fc  B[4]=168bbea0  C[4]=5a769bf8  D[4]=f479965b
A[5]=471bb7f1  B[5]=c23de8c2  C[5]=eb01d41a  D[5]=72e11eb6
A[6]=b4b50823  B[6]=a1a99b57  C[6]=0d979424  D[6]=b165fbce
A[7]=ab337204  B[7]=bdf20c17  C[7]=c00cca5a  D[7]=2fc78960

Step 21: (r=28, s= 7)
A[0]=4ef7b296  B[0]=05bb5dbd  C[0]=05f1f8c8  D[0]=423fb59b
A[1]=ac1244e1  B[1]=57e12228  C[1]=28d0ac85  D[1]=8d17f5ef
A[2]=a54100f7  B[2]=69e84be7  C[2]=9b75cfdb  D[2]=dade6f2c
A[3]=0afff7b7  B[3]=73190e47  C[3]=8f44c7be  D[3]=29c98db8
A[4]=8c79dd90  B[4]=c73ed09f  C[4]=168bbea0  D[4]=5a769bf8
A[5]=b3da901d  B[5]=1471bb7f  C[5]=c23de8c2  D[5]=eb01d41a
A[6]=f985274e  B[6]=3b4b5082  C[6]=a1a99b57  D[6]=0d979424
A[7]=72a7959f  B[7]=4ab33720  C[7]=bdf20c17  D[7]=c00cca5a

Step 22: (r= 7, s=22)
A[0]=561c6825  B[0]=7bd94b27  C[0]=05bb5dbd  D[0]=05f1f8c8
A[1]=6b591ceb  B[1]=092270d6  C[1]=57e12228  D[1]=28d0ac85
A[2]=8f8e4562  B[2]=a0807bd2  C[2]=69e84be7  D[2]=9b75cfdb
A[3]=f1a3b973  B[3]=7ffbdb85  C[3]=73190e47  D[3]=8f44c7be
A[4]=df69caed  B[4]=3ceec846  C[4]=c73ed09f  D[4]=168bbea0
A[5]=81aa182a  B[5]=ed480ed9  C[5]=1471bb7f  D[5]=c23de8c2
A[6]=257af759  B[6]=c293a77c  C[6]=3b4b5082  D[6]=a1a99b57
A[7]=ba7d9909  B[7]=53cacfb9  C[7]=4ab33720  D[7]=bdf20c17

Step 23: (r=22, s=19)
A[0]=85e00bce  B[0]=0955871a  C[0]=7bd94b27  D[0]=05bb5dbd
A[1]=a85659e2  B[1]=3adad647  C[1]=092270d6  D[1]=57e12228
A[2]=f93641b3  B[2]=58a3e391  C[2]=a0807bd2  D[2]=69e84be7
A[3]=b0d56132  B[3]=5cfc68ee  C[3]=7ffbdb85  D[3]=73190e47
A[4]=55af2614  B[4]=bb77da72  C[4]=3ceec846  D[4]=c73ed09f
A[5]=10eb5750  B[5]=0aa06a86  C[5]=ed480ed9  D[5]=1471bb7f
A[6]=ac9a4d4d  B[6]=d6495ebd  C[6]=c293a77c  D[6]=3b4b5082
```

```
A[7]=c21a2546  B[7]=426e9f66  C[7]=53cacfb9  D[7]=4ab33720

Step 24: (r=15, s= 5)
A[0]=df96e149  B[0]=05e742f0  C[0]=0955871a  D[0]=7bd94b27
A[1]=e22ee10a  B[1]=2cf1542b  C[1]=3adad647  D[1]=092270d6
A[2]=6bcee5c5  B[2]=20d9fc9b  C[2]=58a3e391  D[2]=a0807bd2
A[3]=749429bc  B[3]=b099586a  C[3]=5cfc68ee  D[3]=7ffbdb85
A[4]=df4947e7  B[4]=930a2ad7  C[4]=bb77da72  D[4]=3ceec846
A[5]=b6b00a92  B[5]=aba80875  C[5]=0aa06a86  D[5]=ed480ed9
A[6]=13ed626b  B[6]=26a6d64d  C[6]=d6495ebd  D[6]=c293a77c
A[7]=c56feb38  B[7]=12a3610d  C[7]=426e9f66  D[7]=53cacfb9

Step 25: (r= 5, s=29)
A[0]=f035a4b7  B[0]=f2dc293b  C[0]=05e742f0  D[0]=0955871a
A[1]=156eb5cb  B[1]=45dc215c  C[1]=2cf1542b  D[1]=3adad647
A[2]=11edf0a3  B[2]=79dcb8ad  C[2]=20d9fc9b  D[2]=58a3e391
A[3]=70eb71e9  B[3]=9285378e  C[3]=b099586a  D[3]=5cfc68ee
A[4]=d11d645a  B[4]=e928fcfb  C[4]=930a2ad7  D[4]=bb77da72
A[5]=deb3f83c  B[5]=d6015256  C[5]=aba80875  D[5]=0aa06a86
A[6]=3201e614  B[6]=7dac4d62  C[6]=26a6d64d  D[6]=d6495ebd
A[7]=016dfa48  B[7]=adfd6718  C[7]=12a3610d  D[7]=426e9f66

Step 26: (r=29, s= 9)
A[0]=cdb46593  B[0]=fe06b496  C[0]=f2dc293b  D[0]=05e742f0
A[1]=7d101532  B[1]=62add6b9  C[1]=45dc215c  D[1]=2cf1542b
A[2]=0739a9f9  B[2]=623dbe14  C[2]=79dcb8ad  D[2]=20d9fc9b
A[3]=740a9fc4  B[3]=2e1d6e3d  C[3]=9285378e  D[3]=b099586a
A[4]=38550d95  B[4]=5a23ac8b  C[4]=e928fcfb  D[4]=930a2ad7
A[5]=c02d6b9d  B[5]=9bd67f07  C[5]=d6015256  D[5]=aba80875
A[6]=712cb5b6  B[6]=86403cc2  C[6]=7dac4d62  D[6]=26a6d64d
A[7]=dc357918  B[7]=002dbf49  C[7]=adfd6718  D[7]=12a3610d

Step 27: (r= 9, s=15)
A[0]=1ad2f3a7  B[0]=68cb279b  C[0]=fe06b496  D[0]=f2dc293b
A[1]=d63b4b4e  B[1]=202a64fa  C[1]=62add6b9  D[1]=45dc215c
A[2]=22eccba4  B[2]=7353f20e  C[2]=623dbe14  D[2]=79dcb8ad
A[3]=5ee02c99  B[3]=153f88e8  C[3]=2e1d6e3d  D[3]=9285378e
A[4]=1c12be4e  B[4]=aa1b2a70  C[4]=5a23ac8b  D[4]=e928fcfb
A[5]=0fff57d9  B[5]=5ad73b80  C[5]=9bd67f07  D[5]=d6015256
A[6]=ba706e0d  B[6]=596b6ce2  C[6]=86403cc2  D[6]=7dac4d62
A[7]=be274a53  B[7]=6af231b8  C[7]=002dbf49  D[7]=adfd6718

Step 28: (r=15, s= 5)
A[0]=45989975  B[0]=79d38d69  C[0]=68cb279b  D[0]=fe06b496
A[1]=edb2254c  B[1]=a5a76b1d  C[1]=202a64fa  D[1]=62add6b9
A[2]=37e66f68  B[2]=65d21176  C[2]=7353f20e  D[2]=623dbe14
A[3]=77ffa08b  B[3]=164caf70  C[3]=153f88e8  D[3]=2e1d6e3d
A[4]=36e0cd60  B[4]=5f270e09  C[4]=aa1b2a70  D[4]=5a23ac8b
A[5]=213dc20a  B[5]=abec87ff  C[5]=5ad73b80  D[5]=9bd67f07
```

```
A[6]=698b60eb  B[6]=3706dd38  C[6]=596b6ce2  D[6]=86403cc2
A[7]=f3a2736b  B[7]=a529df13  C[7]=6af231b8  D[7]=002dbf49

Step 29: (r= 5, s=29)
A[0]=82d99c38  B[0]=b3132ea8  C[0]=79d38d69  D[0]=68cb279b
A[1]=8691535d  B[1]=b644a99d  C[1]=a5a76b1d  D[1]=202a64fa
A[2]=6a59d8d3  B[2]=fccded06  C[2]=65d21176  D[2]=7353f20e
A[3]=3ffe8b7b  B[3]=fff4116e  C[3]=164caf70  D[3]=153f88e8
A[4]=174281fc  B[4]=dc19ac06  C[4]=5f270e09  D[4]=aa1b2a70
A[5]=7fbf1b5a  B[5]=27b84144  C[5]=abec87ff  D[5]=5ad73b80
A[6]=8500183e  B[6]=316c1d6d  C[6]=3706dd38  D[6]=596b6ce2
A[7]=bfa54c21  B[7]=744e6d7e  C[7]=a529df13  D[7]=6af231b8

Step 30: (r=29, s= 9)
A[0]=45fc611d  B[0]=105b3387  C[0]=b3132ea8  D[0]=79d38d69
A[1]=ae26b6ad  B[1]=b0d22a6b  C[1]=b644a99d  D[1]=a5a76b1d
A[2]=45fa12bf  B[2]=6d4b3b1a  C[2]=fccded06  D[2]=65d21176
A[3]=a5e26c18  B[3]=67ffd16f  C[3]=fff4116e  D[3]=164caf70
A[4]=e1468fa7  B[4]=82e8503f  C[4]=dc19ac06  D[4]=5f270e09
A[5]=ad78e07f  B[5]=4ff7e36b  C[5]=27b84144  D[5]=abec87ff
A[6]=b56e4400  B[6]=d0a00307  C[6]=316c1d6d  D[6]=3706dd38
A[7]=b97b9fa4  B[7]=37f4a984  C[7]=744e6d7e  D[7]=a529df13

Step 31: (r= 9, s=15)
A[0]=cc932e61  B[0]=f8c23a8b  C[0]=105b3387  D[0]=b3132ea8
A[1]=74753582  B[1]=4d6d5b5c  C[1]=b0d22a6b  D[1]=b644a99d
A[2]=3c9db16d  B[2]=f4257e8b  C[2]=6d4b3b1a  D[2]=fccded06
A[3]=0dfb3247  B[3]=c4d8314b  C[3]=67ffd16f  D[3]=fff4116e
A[4]=bc4bd3d1  B[4]=8d1f4fc2  C[4]=82e8503f  D[4]=dc19ac06
A[5]=4b887fea  B[5]=f1c0ff5a  C[5]=4ff7e36b  D[5]=27b84144
A[6]=b7c22046  B[6]=dc88016a  C[6]=d0a00307  D[6]=316c1d6d
A[7]=af277aab  B[7]=f73f4972  C[7]=37f4a984  D[7]=744e6d7e

Feistel Step 0: (r=15, s= 5)
A[0]=691b8523  B[0]=9730e649  C[0]=f8c23a8b  D[0]=105b3387
A[1]=b10feb20  B[1]=9ac13a3a  C[1]=4d6d5b5c  D[1]=b0d22a6b
A[2]=050117f3  B[2]=d8b69e4e  C[2]=f4257e8b  D[2]=6d4b3b1a
A[3]=468941f3  B[3]=992386fd  C[3]=c4d8314b  D[3]=67ffd16f
A[4]=2d115991  B[4]=e9e8de25  C[4]=8d1f4fc2  D[4]=82e8503f
A[5]=e40a2172  B[5]=3ff525c4  C[5]=f1c0ff5a  D[5]=4ff7e36b
A[6]=c7b1c582  B[6]=10235be1  C[6]=dc88016a  D[6]=d0a00307
A[7]=3c9de323  B[7]=bd55d793  C[7]=f73f4972  D[7]=37f4a984

Feistel Step 1: (r= 5, s=29)
A[0]=5b8f4fa8  B[0]=2370a46d  C[0]=9730e649  D[0]=f8c23a8b
A[1]=19c589b7  B[1]=21fd6416  C[1]=9ac13a3a  D[1]=4d6d5b5c
A[2]=81cc471f  B[2]=a022fe60  C[2]=d8b69e4e  D[2]=f4257e8b
A[3]=24d1547c  B[3]=d1283e68  C[3]=992386fd  D[3]=c4d8314b
A[4]=5f8b7eb1  B[4]=a22b3225  C[4]=e9e8de25  D[4]=8d1f4fc2
```

```
A[5]=150cc75a  B[5]=81442e5c  C[5]=3ff525c4  D[5]=f1c0ff5a
A[6]=223ee69b  B[6]=f638b058  C[6]=10235be1  D[6]=dc88016a
A[7]=8d25205d  B[7]=93bc6467  C[7]=bd55d793  D[7]=f73f4972

Feistel Step 2: (r=29, s= 9)
A[0]=2c458ebe  B[0]=0b71e9f5  C[0]=2370a46d  D[0]=9730e649
A[1]=e665d814  B[1]=e338b136  C[1]=21fd6416  D[1]=9ac13a3a
A[2]=d87b0649  B[2]=f03988e3  C[2]=a022fe60  D[2]=d8b69e4e
A[3]=76256265  B[3]=849a2a8f  C[3]=d1283e68  D[3]=992386fd
A[4]=204a8c79  B[4]=2bf16fd6  C[4]=a22b3225  D[4]=e9e8de25
A[5]=ddeedb8d  B[5]=42a198eb  C[5]=81442e5c  D[5]=3ff525c4
A[6]=448fbf63  B[6]=6447dcd3  C[6]=f638b058  D[6]=10235be1
A[7]=bba18100  B[7]=b1a4a40b  C[7]=93bc6467  D[7]=bd55d793

Feistel Step 3: (r= 9, s=15)
A[0]=9fb36a42  B[0]=8b1d7c58  C[0]=0b71e9f5  D[0]=2370a46d
A[1]=331638e6  B[1]=cbb029cc  C[1]=e338b136  D[1]=21fd6416
A[2]=00d1659e  B[2]=f60c93b0  C[2]=f03988e3  D[2]=a022fe60
A[3]=59dd4de3  B[3]=4ac4caec  C[3]=849a2a8f  D[3]=d1283e68
A[4]=2e853830  B[4]=9518f240  C[4]=2bf16fd6  D[4]=a22b3225
A[5]=ebe560dc  B[5]=ddb71bbb  C[5]=42a198eb  D[5]=81442e5c
A[6]=73316f16  B[6]=1f7ec689  C[6]=6447dcd3  D[6]=f638b058
A[7]=24515ab3  B[7]=43020177  C[7]=b1a4a40b  D[7]=93bc6467
```

Compression Function Output

```
A[0]=9fb36a42  B[0]=8b1d7c58  C[0]=0b71e9f5  D[0]=2370a46d
A[1]=331638e6  B[1]=cbb029cc  C[1]=e338b136  D[1]=21fd6416
A[2]=00d1659e  B[2]=f60c93b0  C[2]=f03988e3  D[2]=a022fe60
A[3]=59dd4de3  B[3]=4ac4caec  C[3]=849a2a8f  D[3]=d1283e68
A[4]=2e853830  B[4]=9518f240  C[4]=2bf16fd6  D[4]=a22b3225
A[5]=ebe560dc  B[5]=ddb71bbb  C[5]=42a198eb  D[5]=81442e5c
A[6]=73316f16  B[6]=1f7ec689  C[6]=6447dcd3  D[6]=f638b058
A[7]=24515ab3  B[7]=43020177  C[7]=b1a4a40b  D[7]=93bc6467
```

Hash Function Output

```
426ab39fe63816339e65d100e34ddd593038852edc60e5eb166f3173b35a5124
587c1d8bcc29b0cbb0930cf6eccac44a40f21895bb1bb7dd89c67e1f77010243
```

6.4.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
```

```
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
y[104..111] =  129  171   92   61  218   92  254   87
y[112..119] =   84  189  205  152  233    8  203  182
y[120..127] =  168  207  190  143  124  129   57   30
y[128..135] =  192  141   92  168  121  110  169   28
y[136..143] =  128  161  211  146  197   45   44  249
y[144..151] =  171  249   62   82  157  156   70   32
y[152..159] =  122  202  163   42  174   32   21  256
y[160..167] =  244   93  107    0   28  137   44  134
y[168..175] =  129  255  154   17   97  197  180   68
y[176..183] =  132  107  244   30   65  163  147  190
y[184..191] =  115  193   79   65   69  180   30   67
y[192..199] =  205    3  191  238   12   69   15  256
y[200..207] =  106   66  122   90  108  168    4   39
y[208..215] =   82  251  217  159   43   47   16  138
y[216..223] =   62   41  152   21   23  239  124  246
y[224..231] =  176   51  194   43   74   68  188  100
y[232..239] =   19  207   16  134  197   67  195   38
y[240..247] =    3  145  211  141   79   12    7  226
y[248..255] =   91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
Z[10] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
Z[14] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
Z[16] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
Z[17] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
Z[18] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
Z[19] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
Z[20] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
Z[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
Z[22] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
Z[23] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
Z[24] = 966c4d5d  aeffa6ce  641edd6a  197c1406
```

```
        a8a0b1ba  9af9be78  28f5409f  f8b83957
Z[25] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
Z[26] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
Z[27] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
Z[28] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
Z[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
Z[30] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
Z[31] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
```

```
         dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
         6f0af514  aa725bed  b4753785  131dafe8
W[17] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
         8b80bf61  a2411893  58499a10  b9eb5dbf
W[18] = 02bb4c74  d622d0ac  47e7ea28  065fceda
         52d3aeff  5cd6c305  c79270dc  f17033e1
W[19] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
         607aedcc  6f0a1b4e  624cad2d  03a4641e
W[20] = b647cdf1  c6a98d52  435ad195  c1333957
         114b8b80  0e9053bc  c964dc81  c792fd45
W[21] = 4aa2131d  db980da7  2723e76d  0e903785
         386e93b1  a06f3c12  14ef4e46  70dc4c74
W[22] = c4d7a989  53bc71c5  6e214443  afe83126
         74807480  d622558e  c9640576  280c320f
W[23] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
         68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
W[24] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
         d27eb1ba  900d3785  3cfb53bc  22964f2f
W[25] = 966c4d5d  aeffa6ce  641edd6a  197c1406
         a8a0b1ba  9af9be78  28f5409f  f8b83957
W[26] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
         cdf16a7d  263aa06f  1d204615  ff17e76d
W[27] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
         2551d27e  6335983e  bad48b80  29de1b4e
W[28] = 6163091a  1b4e048d  aa724c74  c3055018
         c5c01234  3b290831  b9ebfe2e  3cfb4c74
W[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
         25516c4f  131d28f5  ef9e1a65  f5fdf342
W[30] = 02bba7b7  eeb53785  3ecdfb73  ff171062
         3c1217aa  51ea114b  aeff1062  237f66d9
W[31] = 54a55b04  0000fd45  92c81c37  900d1406
         fe2eb1ba  0f7935b3  c9642551  3de4b730
```

Feistel Steps

```
IV :
A[0]=c2956828  B[0]=39369835  C[0]=d9ca7181  D[0]=4d6185f6
A[1]=3da33320  B[1]=b7b6f593  C[1]=cf8e8183  D[1]=bbdcbc6e
A[2]=4149c566  B[2]=956d5c2e  C[2]=e2f28feb  D[2]=753b2bf6
A[3]=c49d9244  B[3]=2e4e80c8  C[3]=e9aa51c5  D[3]=7aac68ac
A[4]=04a3f1aa  B[4]=1e9fc449  C[4]=c5c2d649  D[4]=eb672a56
A[5]=0220c98b  B[5]=84ca34e9  C[5]=37c0b473  D[5]=ed8a5dcd
A[6]=7246bebf  B[6]=17d45ec5  C[6]=07eef0a5  D[6]=b072020d
A[7]=e51d9d96  B[7]=27db1b31  C[7]=dd23d692  D[7]=b07cf71f

IV XOR M :
A[0]=c1976928  B[0]=1a14b915  C[0]=9a8830c1  D[0]=2e03e496
A[1]=3aa53624  B[1]=9090d0b7  C[1]=88c8c4c7  D[1]=dcbad90a
```

```
A[2]=4a43cc6e  B[2]=be477506  C[2]=a9b8c6a3  D[2]=1e51429e
A[3]=cb939f48  B[3]=0160ade4  C[3]=a6e41c89  D[3]=15c205c0
A[4]=17b1e0ba  B[4]=2dadf579  C[4]=96908719  D[4]=98155b26
A[5]=1536dc9f  B[5]=b3fc01dd  C[5]=6096e127  D[5]=9afc28b9
A[6]=695ca7a7  B[6]=2cee67fd  C[6]=5cb4a9fd  D[6]=cb087b75
A[7]=fa03808a  B[7]=18e5260d  C[7]=827d8bce  D[7]=cf028a63

Step  0: (r= 3, s=20)
A[0]=4bd9d19f  B[0]=0cbb4946  C[0]=1a14b915  D[0]=9a8830c1
A[1]=f2d4e2df  B[1]=d529b121  C[1]=9090d0b7  D[1]=88c8c4c7
A[2]=0e696540  B[2]=521e6372  C[2]=be477506  D[2]=a9b8c6a3
A[3]=8522e607  B[3]=5c9cfa46  C[3]=0160ade4  D[3]=a6e41c89
A[4]=e869ed1b  B[4]=bd8f05d0  C[4]=2dadf579  D[4]=96908719
A[5]=bfd0ac86  B[5]=a9b6e4f8  C[5]=b3fc01dd  D[5]=6096e127
A[6]=6b0d53cd  B[6]=4ae53d3b  C[6]=2cee67fd  D[6]=5cb4a9fd
A[7]=9db8cfc9  B[7]=d01c0457  C[7]=18e5260d  D[7]=827d8bce

Step  1: (r=20, s=14)
A[0]=30831955  B[0]=19f4bd9d  C[0]=0cbb4946  D[0]=1a14b915
A[1]=26eefe3c  B[1]=2dff2d4e  C[1]=d529b121  D[1]=9090d0b7
A[2]=1eb84846  B[2]=5400e696  C[2]=521e6372  D[2]=be477506
A[3]=fb7cdcc9  B[3]=6078522e  C[3]=5c9cfa46  D[3]=0160ade4
A[4]=4cd8f253  B[4]=d1be869e  C[4]=bd8f05d0  D[4]=2dadf579
A[5]=2ef8e926  B[5]=c86bfd0a  C[5]=a9b6e4f8  D[5]=b3fc01dd
A[6]=02808224  B[6]=3cd6b0d5  C[6]=4ae53d3b  D[6]=2cee67fd
A[7]=73e61178  B[7]=fc99db8c  C[7]=d01c0457  D[7]=18e5260d

Step  2: (r=14, s=27)
A[0]=affff365  B[0]=c6554c20  C[0]=19f4bd9d  D[0]=0cbb4946
A[1]=ea867360  B[1]=bf8f09bb  C[1]=2dff2d4e  D[1]=d529b121
A[2]=ba004c31  B[2]=121187ae  C[2]=5400e696  D[2]=521e6372
A[3]=0046cd6d  B[3]=37327edf  C[3]=6078522e  D[3]=5c9cfa46
A[4]=963bbdab  B[4]=3c94d336  C[4]=d1be869e  D[4]=bd8f05d0
A[5]=3a5ca14b  B[5]=3a498bbe  C[5]=c86bfd0a  D[5]=a9b6e4f8
A[6]=54d82306  B[6]=208900a0  C[6]=3cd6b0d5  D[6]=4ae53d3b
A[7]=a00d6f36  B[7]=845e1cf9  C[7]=fc99db8c  D[7]=d01c0457

Step  3: (r=27, s= 3)
A[0]=b75c234c  B[0]=2d7fff9b  C[0]=c6554c20  D[0]=19f4bd9d
A[1]=71c78dfe  B[1]=0754339b  C[1]=bf8f09bb  D[1]=2dff2d4e
A[2]=26d9cd65  B[2]=8dd00261  C[2]=121187ae  D[2]=5400e696
A[3]=1af31907  B[3]=6802366b  C[3]=37327edf  D[3]=6078522e
A[4]=d5732d59  B[4]=5cb1dded  C[4]=3c94d336  D[4]=d1be869e
A[5]=7d82dfc9  B[5]=59d2e50a  C[5]=3a498bbe  D[5]=c86bfd0a
A[6]=167beb45  B[6]=32a6c118  C[6]=208900a0  D[6]=3cd6b0d5
A[7]=ff49925e  B[7]=b5006b79  C[7]=845e1cf9  D[7]=fc99db8c

Step  4: (r= 3, s=20)
A[0]=23d572d9  B[0]=bae11a65  C[0]=2d7fff9b  D[0]=c6554c20
```

```
A[1]=d232b8c6  B[1]=8e3c6ff3  C[1]=0754339b  D[1]=bf8f09bb
A[2]=a1ced1ed  B[2]=36ce6b29  C[2]=8dd00261  D[2]=121187ae
A[3]=ce44b2af  B[3]=d798c838  C[3]=6802366b  D[3]=37327edf
A[4]=28b7a33d  B[4]=ab996ace  C[4]=5cb1dded  D[4]=3c94d336
A[5]=6e3867a7  B[5]=ec16fe4b  C[5]=59d2e50a  D[5]=3a498bbe
A[6]=b15dc323  B[6]=b3df5a28  C[6]=32a6c118  D[6]=208900a0
A[7]=a74bd329  B[7]=fa4c92f7  C[7]=b5006b79  D[7]=845e1cf9

Step  5: (r=20, s=14)
A[0]=9463d66d  B[0]=2d923d57  C[0]=bae11a65  D[0]=2d7fff9b
A[1]=bf164857  B[1]=8c6d232b  C[1]=8e3c6ff3  D[1]=0754339b
A[2]=5b777851  B[2]=1eda1ced  C[2]=36ce6b29  D[2]=8dd00261
A[3]=a3b50fb1  B[3]=2afce44b  C[3]=d798c838  D[3]=6802366b
A[4]=cc8444ad  B[4]=33d28b7a  C[4]=ab996ace  D[4]=5cb1dded
A[5]=9b396675  B[5]=7a76e386  C[5]=ec16fe4b  D[5]=59d2e50a
A[6]=b44e45d1  B[6]=323b15dc  C[6]=b3df5a28  D[6]=32a6c118
A[7]=c5c06fe8  B[7]=329a74bd  C[7]=fa4c92f7  D[7]=b5006b79

Step  6: (r=14, s=27)
A[0]=1b871ae4  B[0]=f59b6518  C[0]=2d923d57  D[0]=bae11a65
A[1]=e63ddfc9  B[1]=9215efc5  C[1]=8c6d232b  D[1]=8e3c6ff3
A[2]=68e880d0  B[2]=de1456dd  C[2]=1eda1ced  D[2]=36ce6b29
A[3]=2b863249  B[3]=43ec68ed  C[3]=2afce44b  D[3]=d798c838
A[4]=a4a21b7d  B[4]=112b7321  C[4]=33d28b7a  D[4]=ab996ace
A[5]=48e8b520  B[5]=599d66ce  C[5]=7a76e386  D[5]=ec16fe4b
A[6]=e132959e  B[6]=91746d13  C[6]=323b15dc  D[6]=b3df5a28
A[7]=14bf4d5e  B[7]=1bfa3170  C[7]=329a74bd  D[7]=fa4c92f7

Step  7: (r=27, s= 3)
A[0]=7897cea9  B[0]=20dc38d7  C[0]=f59b6518  D[0]=2d923d57
A[1]=47125aaf  B[1]=4f31eefe  C[1]=9215efc5  D[1]=8c6d232b
A[2]=a86c4b59  B[2]=83474406  C[2]=de1456dd  D[2]=1eda1ced
A[3]=3ff10cf7  B[3]=495c3192  C[3]=43ec68ed  D[3]=2afce44b
A[4]=af2825b0  B[4]=ed2510db  C[4]=112b7321  D[4]=33d28b7a
A[5]=18cb6575  B[5]=024745a9  C[5]=599d66ce  D[5]=7a76e386
A[6]=68fc22e2  B[6]=f70994ac  C[6]=91746d13  D[6]=323b15dc
A[7]=15827871  B[7]=f0a5fa6a  C[7]=1bfa3170  D[7]=329a74bd

Step  8: (r=26, s= 4)
A[0]=e102daa2  B[0]=a5e25f3a  C[0]=20dc38d7  D[0]=f59b6518
A[1]=a0e17cea  B[1]=bd1c496a  C[1]=4f31eefe  D[1]=9215efc5
A[2]=baaa6cc2  B[2]=66a1b12d  C[2]=83474406  D[2]=de1456dd
A[3]=45c65072  B[3]=dcffc433  C[3]=495c3192  D[3]=43ec68ed
A[4]=bdd52a75  B[4]=c2bca096  C[4]=ed2510db  D[4]=112b7321
A[5]=6bf3ef06  B[5]=d4632d95  C[5]=024745a9  D[5]=599d66ce
A[6]=89d975df  B[6]=89a3f08b  C[6]=f70994ac  D[6]=91746d13
A[7]=76c21961  B[7]=c45609e1  C[7]=f0a5fa6a  D[7]=1bfa3170

Step  9: (r= 4, s=23)
```

```
A[0]=481932ed  B[0]=102daa2e  C[0]=a5e25f3a  D[0]=20dc38d7
A[1]=cbb071fc  B[1]=0e17ceaa  C[1]=bd1c496a  D[1]=4f31eefe
A[2]=fd8cb000  B[2]=aaa6cc2b  C[2]=66a1b12d  D[2]=83474406
A[3]=9ec7fee7  B[3]=5c650724  C[3]=dcffc433  D[3]=495c3192
A[4]=0ae92df3  B[4]=dd52a75b  C[4]=c2bca096  D[4]=ed2510db
A[5]=358614fd  B[5]=bf3ef066  C[5]=d4632d95  D[5]=024745a9
A[6]=aaff5022  B[6]=9d975df8  C[6]=89a3f08b  D[6]=f70994ac
A[7]=03c756ff  B[7]=6c219617  C[7]=c45609e1  D[7]=f0a5fa6a

Step 10: (r=23, s=11)
A[0]=1b95f1f2  B[0]=76a40c99  C[0]=102daa2e  D[0]=a5e25f3a
A[1]=b19533a4  B[1]=fe65d838  C[1]=0e17ceaa  D[1]=bd1c496a
A[2]=cd09be08  B[2]=007ec658  C[2]=aaa6cc2b  D[2]=66a1b12d
A[3]=fb9a61bf  B[3]=73cf63ff  C[3]=5c650724  D[3]=dcffc433
A[4]=d3e5cb28  B[4]=f9857496  C[4]=dd52a75b  D[4]=c2bca096
A[5]=c738801d  B[5]=7e9ac30a  C[5]=bf3ef066  D[5]=d4632d95
A[6]=8500e23a  B[6]=11557fa8  C[6]=9d975df8  D[6]=89a3f08b
A[7]=a7873b20  B[7]=7f81e3ab  C[7]=6c219617  D[7]=c45609e1

Step 11: (r=11, s=26)
A[0]=a3ec338a  B[0]=af8f90dc  C[0]=76a40c99  D[0]=102daa2e
A[1]=04ec3bd9  B[1]=a99d258c  C[1]=fe65d838  D[1]=0e17ceaa
A[2]=2e750f63  B[2]=4df04668  C[2]=007ec658  D[2]=aaa6cc2b
A[3]=a37db4ed  B[3]=d30dffdc  C[3]=73cf63ff  D[3]=5c650724
A[4]=54fb6261  B[4]=2e59469f  C[4]=f9857496  D[4]=dd52a75b
A[5]=ada6557f  B[5]=c400ee39  C[5]=7e9ac30a  D[5]=bf3ef066
A[6]=acff4b7c  B[6]=0711d428  C[6]=11557fa8  D[6]=9d975df8
A[7]=63c6bf1f  B[7]=39d9053c  C[7]=7f81e3ab  D[7]=6c219617

Step 12: (r=26, s= 4)
A[0]=853b7afa  B[0]=2a8fb0ce  C[0]=af8f90dc  D[0]=76a40c99
A[1]=8f0301dd  B[1]=6413b0ef  C[1]=a99d258c  D[1]=fe65d838
A[2]=987a9bc9  B[2]=8cb9d43d  C[2]=4df04668  D[2]=007ec658
A[3]=f9ecefb3  B[3]=b68df6d3  C[3]=d30dffdc  D[3]=73cf63ff
A[4]=258cfb18  B[4]=8553ed89  C[4]=2e59469f  D[4]=f9857496
A[5]=271b28c5  B[5]=feb69955  C[5]=c400ee39  D[5]=7e9ac30a
A[6]=1e672d57  B[6]=f2b3fd2d  C[6]=0711d428  D[6]=11557fa8
A[7]=6558c56b  B[7]=7d8f1afc  C[7]=39d9053c  D[7]=7f81e3ab

Step 13: (r= 4, s=23)
A[0]=e43aab95  B[0]=53b7afa8  C[0]=2a8fb0ce  D[0]=af8f90dc
A[1]=2d814f2d  B[1]=f0301dd8  C[1]=6413b0ef  D[1]=a99d258c
A[2]=3e0f6705  B[2]=87a9bc99  C[2]=8cb9d43d  D[2]=4df04668
A[3]=a138cd0f  B[3]=9ecefb3f  C[3]=b68df6d3  D[3]=d30dffdc
A[4]=651115b9  B[4]=58cfb182  C[4]=8553ed89  D[4]=2e59469f
A[5]=14c64445  B[5]=71b28c52  C[5]=feb69955  D[5]=c400ee39
A[6]=12dcf548  B[6]=e672d571  C[6]=f2b3fd2d  D[6]=0711d428
A[7]=d3ad4073  B[7]=558c56b6  C[7]=7d8f1afc  D[7]=39d9053c
```

```
Step 14: (r=23, s=11)
A[0]=6381f14c  B[0]=caf21d55  C[0]=53b7afa8  D[0]=2a8fb0ce
A[1]=188fcee7  B[1]=9696c0a7  C[1]=f0301dd8  D[1]=6413b0ef
A[2]=35006f51  B[2]=829f07b3  C[2]=87a9bc99  D[2]=8cb9d43d
A[3]=9da8c20f  B[3]=87d09c66  C[3]=9ecefb3f  D[3]=b68df6d3
A[4]=64cddff7  B[4]=dcb2888a  C[4]=58cfb182  D[4]=8553ed89
A[5]=8c2001db  B[5]=228a6322  C[5]=71b28c52  D[5]=feb69955
A[6]=df14171c  B[6]=a4096e7a  C[6]=e672d571  D[6]=f2b3fd2d
A[7]=23f68b59  B[7]=39e9d6a0  C[7]=558c56b6  D[7]=7d8f1afc

Step 15: (r=11, s=26)
A[0]=b54c37f4  B[0]=0f8a631c  C[0]=caf21d55  D[0]=53b7afa8
A[1]=3c5dd5a2  B[1]=7e7738c4  C[1]=9696c0a7  D[1]=f0301dd8
A[2]=c1ce83dd  B[2]=037a89a8  C[2]=829f07b3  D[2]=87a9bc99
A[3]=4ad5379b  B[3]=46107ced  C[3]=87d09c66  D[3]=9ecefb3f
A[4]=2a82696f  B[4]=6effbb26  C[4]=dcb2888a  D[4]=58cfb182
A[5]=5d910f5c  B[5]=000edc61  C[5]=228a6322  D[5]=71b28c52
A[6]=279f4a4d  B[6]=a0b8e6f8  C[6]=a4096e7a  D[6]=e672d571
A[7]=c13c4800  B[7]=b45ac91f  C[7]=39e9d6a0  D[7]=558c56b6

Step 16: (r=19, s=28)
A[0]=8264a099  B[0]=bfa5aa61  C[0]=0f8a631c  D[0]=caf21d55
A[1]=de1cfd81  B[1]=ad11e2ee  C[1]=7e7738c4  D[1]=9696c0a7
A[2]=dfda778f  B[2]=1eee0e74  C[2]=037a89a8  D[2]=829f07b3
A[3]=e9476e83  B[3]=bcda56a9  C[3]=46107ced  D[3]=87d09c66
A[4]=474bc18b  B[4]=4b795413  C[4]=6effbb26  D[4]=dcb2888a
A[5]=5f5c495d  B[5]=7ae2ec88  C[5]=000edc61  D[5]=228a6322
A[6]=43be1119  B[6]=52693cfa  C[6]=a0b8e6f8  D[6]=a4096e7a
A[7]=34817b4d  B[7]=400609e2  C[7]=b45ac91f  D[7]=39e9d6a0

Step 17: (r=28, s= 7)
A[0]=644d231f  B[0]=98264a09  C[0]=bfa5aa61  D[0]=0f8a631c
A[1]=75cb3c3a  B[1]=1de1cfd8  C[1]=ad11e2ee  D[1]=7e7738c4
A[2]=1b284666  B[2]=fdfda778  C[2]=1eee0e74  D[2]=037a89a8
A[3]=35d9a787  B[3]=3e9476e8  C[3]=bcda56a9  D[3]=46107ced
A[4]=ac9cea7b  B[4]=b474bc18  C[4]=4b795413  D[4]=6effbb26
A[5]=5a740643  B[5]=d5f5c495  C[5]=7ae2ec88  D[5]=000edc61
A[6]=f2747d87  B[6]=943be111  C[6]=52693cfa  D[6]=a0b8e6f8
A[7]=edd49d4f  B[7]=d34817b4  C[7]=400609e2  D[7]=b45ac91f

Step 18: (r= 7, s=22)
A[0]=68ba2284  B[0]=26918fb2  C[0]=98264a09  D[0]=bfa5aa61
A[1]=4d7b5eef  B[1]=e59e1d3a  C[1]=1de1cfd8  D[1]=ad11e2ee
A[2]=ca1d75cd  B[2]=9423330d  C[2]=fdfda778  D[2]=1eee0e74
A[3]=ea377e86  B[3]=ecd3c39a  C[3]=3e9476e8  D[3]=bcda56a9
A[4]=7c3e15e3  B[4]=4e753dd6  C[4]=b474bc18  D[4]=4b795413
A[5]=9016aa2f  B[5]=3a0321ad  C[5]=d5f5c495  D[5]=7ae2ec88
A[6]=391c3e68  B[6]=3a3ec3f9  C[6]=943be111  D[6]=52693cfa
A[7]=cfab52f6  B[7]=ea4ea7f6  C[7]=d34817b4  D[7]=400609e2
```

```
Step 19: (r=22, s=19)
A[0]=f6d116ba  B[0]=a11a2e88  C[0]=26918fb2  D[0]=98264a09
A[1]=18aa3a85  B[1]=bbd35ed7  C[1]=e59e1d3a  D[1]=1de1cfd8
A[2]=fdd544ee  B[2]=7372875d  C[2]=9423330d  D[2]=fdfda778
A[3]=024a237e  B[3]=a1ba8ddf  C[3]=ecd3c39a  D[3]=3e9476e8
A[4]=9ee5f1cf  B[4]=78df0f85  C[4]=4e753dd6  D[4]=b474bc18
A[5]=206d5d5a  B[5]=8be405aa  C[5]=3a0321ad  D[5]=d5f5c495
A[6]=e0760f0a  B[6]=9a0e470f  C[6]=3a3ec3f9  D[6]=943be111
A[7]=516b7d82  B[7]=bdb3ead4  C[7]=ea4ea7f6  D[7]=d34817b4

Step 20: (r=19, s=28)
A[0]=2378b7bc  B[0]=b5d7b688  C[0]=a11a2e88  D[0]=26918fb2
A[1]=cfba0e44  B[1]=d428c551  C[1]=bbd35ed7  D[1]=e59e1d3a
A[2]=bf5cca56  B[2]=2777eeaa  C[2]=7372875d  D[2]=9423330d
A[3]=018211eb  B[3]=1bf01251  C[3]=a1ba8ddf  D[3]=ecd3c39a
A[4]=dd1c5bbf  B[4]=8e7cf72f  C[4]=78df0f85  D[4]=4e753dd6
A[5]=3f6ba90e  B[5]=ead1036a  C[5]=8be405aa  D[5]=3a0321ad
A[6]=bd907ba4  B[6]=785703b0  C[6]=9a0e470f  D[6]=3a3ec3f9
A[7]=719b73fc  B[7]=ec128b5b  C[7]=bdb3ead4  D[7]=ea4ea7f6

Step 21: (r=28, s= 7)
A[0]=b322782e  B[0]=c2378b7b  C[0]=b5d7b688  D[0]=a11a2e88
A[1]=2854bc6e  B[1]=4cfba0e4  C[1]=d428c551  D[1]=bbd35ed7
A[2]=212bf7f4  B[2]=6bf5cca5  C[2]=2777eeaa  D[2]=7372875d
A[3]=d8021e62  B[3]=b018211e  C[3]=1bf01251  D[3]=a1ba8ddf
A[4]=ebf1a2eb  B[4]=fdd1c5bb  C[4]=8e7cf72f  D[4]=78df0f85
A[5]=f0c92c02  B[5]=e3f6ba90  C[5]=ead1036a  D[5]=8be405aa
A[6]=9ffcb73e  B[6]=4bd907ba  C[6]=785703b0  D[6]=9a0e470f
A[7]=4366ddbc  B[7]=c719b73f  C[7]=ec128b5b  D[7]=bdb3ead4

Step 22: (r= 7, s=22)
A[0]=42352885  B[0]=913c1759  C[0]=c2378b7b  D[0]=b5d7b688
A[1]=3e72a16c  B[1]=2a5e3714  C[1]=4cfba0e4  D[1]=d428c551
A[2]=f5974466  B[2]=95fbfa10  C[2]=6bf5cca5  D[2]=2777eeaa
A[3]=4ecbe2a9  B[3]=010f316c  C[3]=b018211e  D[3]=1bf01251
A[4]=ed4685c6  B[4]=f8d175f5  C[4]=fdd1c5bb  D[4]=8e7cf72f
A[5]=e48d2ff1  B[5]=64960178  C[5]=e3f6ba90  D[5]=ead1036a
A[6]=3a4e0ae9  B[6]=fe5b9f4f  C[6]=4bd907ba  D[6]=785703b0
A[7]=99e74c08  B[7]=b36ede21  C[7]=c719b73f  D[7]=ec128b5b

Step 23: (r=22, s=19)
A[0]=283b83df  B[0]=21508d4a  C[0]=913c1759  D[0]=c2378b7b
A[1]=5a08d9c3  B[1]=5b0f9ca8  C[1]=2a5e3714  D[1]=4cfba0e4
A[2]=42f9584d  B[2]=19bd65d1  C[2]=95fbfa10  D[2]=6bf5cca5
A[3]=738c38c3  B[3]=aa53b2f8  C[3]=010f316c  D[3]=b018211e
A[4]=a9903519  B[4]=71bb51a1  C[4]=f8d175f5  D[4]=fdd1c5bb
A[5]=b8c05721  B[5]=fc79234b  C[5]=64960178  D[5]=e3f6ba90
A[6]=19def1ce  B[6]=ba4e9382  C[6]=fe5b9f4f  D[6]=4bd907ba
```

```
A[7]=7860897c  B[7]=022679d3  C[7]=b36ede21  D[7]=c719b73f

Step 24: (r=15, s= 5)
A[0]=a3c986d8  B[0]=c1ef941d  C[0]=21508d4a  D[0]=913c1759
A[1]=91a9475a  B[1]=6ce1ad04  C[1]=5b0f9ca8  D[1]=2a5e3714
A[2]=0f2fdc0d  B[2]=ac26a17c  C[2]=19bd65d1  D[2]=95fbfa10
A[3]=5013f801  B[3]=1c61b9c6  C[3]=aa53b2f8  D[3]=010f316c
A[4]=6fca07a8  B[4]=1a8cd4c8  C[4]=71bb51a1  D[4]=f8d175f5
A[5]=25cb8296  B[5]=2b90dc60  C[5]=fc79234b  D[5]=64960178
A[6]=293d9b60  B[6]=78e70cef  C[6]=ba4e9382  D[6]=fe5b9f4f
A[7]=14b3c4dc  B[7]=44be3c30  C[7]=022679d3  D[7]=b36ede21

Step 25: (r= 5, s=29)
A[0]=fb2bbfdb  B[0]=7930db14  C[0]=c1ef941d  D[0]=21508d4a
A[1]=46ffaf9a  B[1]=3528eb52  C[1]=6ce1ad04  D[1]=5b0f9ca8
A[2]=3c0b0a3e  B[2]=e5fb81a1  C[2]=ac26a17c  D[2]=19bd65d1
A[3]=8fc28b5f  B[3]=027f002a  C[3]=1c61b9c6  D[3]=aa53b2f8
A[4]=3f38db8c  B[4]=f940f50d  C[4]=1a8cd4c8  D[4]=71bb51a1
A[5]=d5a0a7a9  B[5]=b97052c4  C[5]=2b90dc60  D[5]=fc79234b
A[6]=1577f227  B[6]=27b36c05  C[6]=78e70cef  D[6]=ba4e9382
A[7]=2fcbfd55  B[7]=96789b82  C[7]=44be3c30  D[7]=022679d3

Step 26: (r=29, s= 9)
A[0]=81e7f0d1  B[0]=7f6577fb  C[0]=7930db14  D[0]=c1ef941d
A[1]=987f59e7  B[1]=48dff5f3  C[1]=3528eb52  D[1]=6ce1ad04
A[2]=3b1461b9  B[2]=c7816147  C[2]=e5fb81a1  D[2]=ac26a17c
A[3]=36cc6924  B[3]=f1f8516b  C[3]=027f002a  D[3]=1c61b9c6
A[4]=551b265d  B[4]=87e71b71  C[4]=f940f50d  D[4]=1a8cd4c8
A[5]=8fbe5702  B[5]=3ab414f5  C[5]=b97052c4  D[5]=2b90dc60
A[6]=8d6cbe7d  B[6]=e2aefe44  C[6]=27b36c05  D[6]=78e70cef
A[7]=f55a388a  B[7]=a5f97faa  C[7]=96789b82  D[7]=44be3c30

Step 27: (r= 9, s=15)
A[0]=1f542564  B[0]=cfe1a303  C[0]=7f6577fb  D[0]=7930db14
A[1]=9d611d76  B[1]=feb3cf30  C[1]=48dff5f3  D[1]=3528eb52
A[2]=1e5fba99  B[2]=28c37276  C[2]=c7816147  D[2]=e5fb81a1
A[3]=0fc7ae7d  B[3]=98d2486d  C[3]=f1f8516b  D[3]=027f002a
A[4]=0d2d9994  B[4]=364cbaaa  C[4]=87e71b71  D[4]=f940f50d
A[5]=4365340d  B[5]=7cae051f  C[5]=3ab414f5  D[5]=b97052c4
A[6]=f41d5db3  B[6]=d97cfb1a  C[6]=e2aefe44  D[6]=27b36c05
A[7]=22565377  B[7]=b47115ea  C[7]=a5f97faa  D[7]=96789b82

Step 28: (r=15, s= 5)
A[0]=cddcc0d7  B[0]=12b20faa  C[0]=cfe1a303  D[0]=7f6577fb
A[1]=c00bb9cf  B[1]=8ebb4eb0  C[1]=feb3cf30  D[1]=48dff5f3
A[2]=bd669576  B[2]=dd4c8f2f  C[2]=28c37276  D[2]=c7816147
A[3]=c81fa51a  B[3]=d73e87e3  C[3]=98d2486d  D[3]=f1f8516b
A[4]=67daffea  B[4]=ccca0696  C[4]=364cbaaa  D[4]=87e71b71
A[5]=b477e8e3  B[5]=9a06a1b2  C[5]=7cae051f  D[5]=3ab414f5
```

```
A[6]=6548b9e5  B[6]=aed9fa0e  C[6]=d97cfb1a  D[6]=e2aefe44
A[7]=ab81f61c  B[7]=29bb912b  C[7]=b47115ea  D[7]=a5f97faa

Step 29: (r= 5, s=29)
A[0]=560ecc57  B[0]=bb981af9  C[0]=12b20faa  D[0]=cfe1a303
A[1]=5bc1e7c5  B[1]=017739f8  C[1]=8ebb4eb0  D[1]=feb3cf30
A[2]=718a0241  B[2]=acd2aed7  C[2]=dd4c8f2f  D[2]=28c37276
A[3]=6d3047bd  B[3]=03f4a359  C[3]=d73e87e3  D[3]=98d2486d
A[4]=eb97a579  B[4]=fb5ffd4c  C[4]=ccca0696  D[4]=364cbaaa
A[5]=117dbf88  B[5]=8efd1c76  C[5]=9a06a1b2  D[5]=7cae051f
A[6]=f354bfc2  B[6]=a9173cac  C[6]=aed9fa0e  D[6]=d97cfb1a
A[7]=57b23d78  B[7]=703ec395  C[7]=29bb912b  D[7]=b47115ea

Step 30: (r=29, s= 9)
A[0]=79a9b379  B[0]=eac1d98a  C[0]=bb981af9  D[0]=12b20faa
A[1]=1757e3ea  B[1]=ab783cf8  C[1]=017739f8  D[1]=8ebb4eb0
A[2]=ba2818bb  B[2]=2e314048  C[2]=acd2aed7  D[2]=dd4c8f2f
A[3]=7934866d  B[3]=ada608f7  C[3]=03f4a359  D[3]=d73e87e3
A[4]=2a9569b3  B[4]=3d72f4af  C[4]=fb5ffd4c  D[4]=ccca0696
A[5]=59d9791a  B[5]=022fb7f1  C[5]=8efd1c76  D[5]=9a06a1b2
A[6]=4f0c515f  B[6]=5e6a97f8  C[6]=a9173cac  D[6]=aed9fa0e
A[7]=40ddd21d  B[7]=0af647af  C[7]=703ec395  D[7]=29bb912b

Step 31: (r= 9, s=15)
A[0]=ae2717c5  B[0]=5366f2f3  C[0]=eac1d98a  D[0]=bb981af9
A[1]=75e8fdcc  B[1]=afc7d42e  C[1]=ab783cf8  D[1]=017739f8
A[2]=72c34dc0  B[2]=50317774  C[2]=2e314048  D[2]=acd2aed7
A[3]=cad78301  B[3]=690cdaf2  C[3]=ada608f7  D[3]=03f4a359
A[4]=ae66761b  B[4]=2ad36655  C[4]=3d72f4af  D[4]=fb5ffd4c
A[5]=3a33ae6c  B[5]=b2f234b3  C[5]=022fb7f1  D[5]=8efd1c76
A[6]=6adf5b1a  B[6]=18a2be9e  C[6]=5e6a97f8  D[6]=a9173cac
A[7]=ef092f41  B[7]=bba43a81  C[7]=0af647af  D[7]=703ec395

Feistel Step 0: (r=15, s= 5)
A[0]=a171f88c  B[0]=8be2d713  C[0]=5366f2f3  D[0]=eac1d98a
A[1]=694b01b0  B[1]=7ee63af4  C[1]=afc7d42e  D[1]=ab783cf8
A[2]=0b381614  B[2]=a6e03961  C[2]=50317774  D[2]=2e314048
A[3]=5db84bc7  B[3]=c180e56b  C[3]=690cdaf2  D[3]=ada608f7
A[4]=4210d280  B[4]=3b0dd733  C[4]=2ad36655  D[4]=3d72f4af
A[5]=a6914d8b  B[5]=d7361d19  C[5]=b2f234b3  D[5]=022fb7f1
A[6]=97b4442b  B[6]=ad8d356f  C[6]=18a2be9e  D[6]=5e6a97f8
A[7]=d7e6b0af  B[7]=97a0f784  C[7]=bba43a81  D[7]=0af647af

Feistel Step 1: (r= 5, s=29)
A[0]=c5eeab07  B[0]=2e3f1194  C[0]=8be2d713  D[0]=5366f2f3
A[1]=e14839d4  B[1]=2960360d  C[1]=7ee63af4  D[1]=afc7d42e
A[2]=f0f7134e  B[2]=6702c281  C[2]=a6e03961  D[2]=50317774
A[3]=710f6173  B[3]=b70978eb  C[3]=c180e56b  D[3]=690cdaf2
A[4]=a7635b5b  B[4]=421a5008  C[4]=3b0dd733  D[4]=2ad36655
```

```
A[5]=60839b3c  B[5]=d229b174  C[5]=d7361d19  D[5]=b2f234b3
A[6]=c29306b7  B[6]=f6888572  C[6]=ad8d356f  D[6]=18a2be9e
A[7]=7077f520  B[7]=fcd615fa  C[7]=97a0f784  D[7]=bba43a81

Feistel Step 2: (r=29, s= 9)
A[0]=cd820f1a  B[0]=f8bdd560  C[0]=2e3f1194  D[0]=8be2d713
A[1]=71620c54  B[1]=9c29073a  C[1]=2960360d  D[1]=7ee63af4
A[2]=d8737499  B[2]=de1ee269  C[2]=6702c281  D[2]=a6e03961
A[3]=f70eaf73  B[3]=6e21ec2e  C[3]=b70978eb  D[3]=c180e56b
A[4]=b8437843  B[4]=74ec6b6b  C[4]=421a5008  D[4]=3b0dd733
A[5]=af1b99ec  B[5]=8c107367  C[5]=d229b174  D[5]=d7361d19
A[6]=d7f2815a  B[6]=f85260d6  C[6]=f6888572  D[6]=ad8d356f
A[7]=350f4481  B[7]=0e0efea4  C[7]=fcd615fa  D[7]=97a0f784

Feistel Step 3: (r= 9, s=15)
A[0]=40376970  B[0]=041e359b  C[0]=f8bdd560  D[0]=2e3f1194
A[1]=cdf182cf  B[1]=c418a8e2  C[1]=9c29073a  D[1]=2960360d
A[2]=08b2c346  B[2]=e6e933b0  C[2]=de1ee269  D[2]=6702c281
A[3]=c3e9d381  B[3]=1d5ee7ee  C[3]=6e21ec2e  D[3]=b70978eb
A[4]=b9088201  B[4]=86f08770  C[4]=74ec6b6b  D[4]=421a5008
A[5]=1a45f95a  B[5]=3733d95e  C[5]=8c107367  D[5]=d229b174
A[6]=84e05adc  B[6]=e502b5af  C[6]=f85260d6  D[6]=f6888572
A[7]=3fad726c  B[7]=1e89026a  C[7]=0e0efea4  D[7]=fcd615fa
```

Compression Function Output

```
A[0]=40376970  B[0]=041e359b  C[0]=f8bdd560  D[0]=2e3f1194
A[1]=cdf182cf  B[1]=c418a8e2  C[1]=9c29073a  D[1]=2960360d
A[2]=08b2c346  B[2]=e6e933b0  C[2]=de1ee269  D[2]=6702c281
A[3]=c3e9d381  B[3]=1d5ee7ee  C[3]=6e21ec2e  D[3]=b70978eb
A[4]=b9088201  B[4]=86f08770  C[4]=74ec6b6b  D[4]=421a5008
A[5]=1a45f95a  B[5]=3733d95e  C[5]=8c107367  D[5]=d229b174
A[6]=84e05adc  B[6]=e502b5af  C[6]=f85260d6  D[6]=f6888572
A[7]=3fad726c  B[7]=1e89026a  C[7]=0e0efea4  D[7]=fcd615fa
```

Final block

```
M[  0..  7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
```

```
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
y[168..175] =  249  239  118   96   69  105  140  102
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
```

```
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
Z[11] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
Z[17] = a06f5f91  bad4452c  c4d73b29  f5140aec
        f2590da7  ff1700e9  74808b80  0748f8b8
Z[18] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
Z[19] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
Z[20] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
Z[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
Z[22] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
Z[23] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
Z[24] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
Z[25] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
Z[26] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
Z[27] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
Z[28] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
```

```
Z[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
Z[30] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
Z[31] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a06f5f91  bad4452c  c4d73b29  f5140aec
        f2590da7  ff1700e9  74808b80  0748f8b8
W[17] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
W[18] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
W[19] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
```

```
W[20] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
W[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
W[22] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
W[23] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
W[24] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
W[25] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
W[26] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
W[27] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
W[28] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
W[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
W[30] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
W[31] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
```

Feistel Steps

```
IV :
A[0]=40376970  B[0]=041e359b  C[0]=f8bdd560  D[0]=2e3f1194
A[1]=cdf182cf  B[1]=c418a8e2  C[1]=9c29073a  D[1]=2960360d
A[2]=08b2c346  B[2]=e6e933b0  C[2]=de1ee269  D[2]=6702c281
A[3]=c3e9d381  B[3]=1d5ee7ee  C[3]=6e21ec2e  D[3]=b70978eb
A[4]=b9088201  B[4]=86f08770  C[4]=74ec6b6b  D[4]=421a5008
A[5]=1a45f95a  B[5]=3733d95e  C[5]=8c107367  D[5]=d229b174
A[6]=84e05adc  B[6]=e502b5af  C[6]=f85260d6  D[6]=f6888572
A[7]=3fad726c  B[7]=1e89026a  C[7]=0e0efea4  D[7]=fcd615fa

IV XOR M :
A[0]=40376d70  B[0]=041e359b  C[0]=f8bdd560  D[0]=2e3f1194
A[1]=cdf182cf  B[1]=c418a8e2  C[1]=9c29073a  D[1]=2960360d
A[2]=08b2c346  B[2]=e6e933b0  C[2]=de1ee269  D[2]=6702c281
A[3]=c3e9d381  B[3]=1d5ee7ee  C[3]=6e21ec2e  D[3]=b70978eb
A[4]=b9088201  B[4]=86f08770  C[4]=74ec6b6b  D[4]=421a5008
A[5]=1a45f95a  B[5]=3733d95e  C[5]=8c107367  D[5]=d229b174
A[6]=84e05adc  B[6]=e502b5af  C[6]=f85260d6  D[6]=f6888572
A[7]=3fad726c  B[7]=1e89026a  C[7]=0e0efea4  D[7]=fcd615fa

Step  0: (r= 3, s=20)
A[0]=bdd552ad  B[0]=01bb6b82  C[0]=041e359b  D[0]=f8bdd560
```

```
A[1]=33ad05ff  B[1]=6f8c167e  C[1]=c418a8e2  D[1]=9c29073a
A[2]=29013edc  B[2]=45961a30  C[2]=e6e933b0  D[2]=de1ee269
A[3]=8eb39ad3  B[3]=1f4e9c0e  C[3]=1d5ee7ee  D[3]=6e21ec2e
A[4]=a07ab823  B[4]=c844100d  C[4]=86f08770  D[4]=74ec6b6b
A[5]=c5bced05  B[5]=d22fcad0  C[5]=3733d95e  D[5]=8c107367
A[6]=90c6dab0  B[6]=2702d6e4  C[6]=e502b5af  D[6]=f85260d6
A[7]=42078821  B[7]=fd6b9361  C[7]=1e89026a  D[7]=0e0efea4

Step  1: (r=20, s=14)
A[0]=7087de8f  B[0]=2adbdd55  C[0]=01bb6b82  D[0]=041e359b
A[1]=b0eaa17c  B[1]=5ff33ad0  C[1]=6f8c167e  D[1]=c418a8e2
A[2]=d85f71b3  B[2]=edc29013  C[2]=45961a30  D[2]=e6e933b0
A[3]=db03509f  B[3]=ad38eb39  C[3]=1f4e9c0e  D[3]=1d5ee7ee
A[4]=b77c46d4  B[4]=823a07ab  C[4]=c844100d  D[4]=86f08770
A[5]=5b5730ac  B[5]=d05c5bce  C[5]=d22fcad0  D[5]=3733d95e
A[6]=d7d093fb  B[6]=ab090c6d  C[6]=2702d6e4  D[6]=e502b5af
A[7]=3639f6ff  B[7]=82142078  C[7]=fd6b9361  D[7]=1e89026a

Step  2: (r=14, s=27)
A[0]=316a8f45  B[0]=f7a3dc21  C[0]=2adbdd55  D[0]=01bb6b82
A[1]=ad718398  B[1]=a85f2c3a  C[1]=5ff33ad0  D[1]=6f8c167e
A[2]=12e5f247  B[2]=dc6cf617  C[2]=edc29013  D[2]=45961a30
A[3]=04e55b1c  B[3]=d427f6c0  C[3]=ad38eb39  D[3]=1f4e9c0e
A[4]=7ca8ec51  B[4]=11b52ddf  C[4]=823a07ab  D[4]=c844100d
A[5]=7540d193  B[5]=cc2b16d5  C[5]=d05c5bce  D[5]=d22fcad0
A[6]=a9e3ce4d  B[6]=24fef5f4  C[6]=ab090c6d  D[6]=2702d6e4
A[7]=ff3de366  B[7]=7dbfcd8e  C[7]=82142078  D[7]=fd6b9361

Step  3: (r=27, s= 3)
A[0]=6e5e575d  B[0]=298b547a  C[0]=f7a3dc21  D[0]=2adbdd55
A[1]=5fbe7fc5  B[1]=c56b8c1c  C[1]=a85f2c3a  D[1]=5ff33ad0
A[2]=00469f33  B[2]=38972f92  C[2]=dc6cf617  D[2]=edc29013
A[3]=f8e59641  B[3]=e0272ad8  C[3]=d427f6c0  D[3]=ad38eb39
A[4]=694d82fd  B[4]=8be54762  C[4]=11b52ddf  D[4]=823a07ab
A[5]=4cd00f56  B[5]=9baa068c  C[5]=cc2b16d5  D[5]=d05c5bce
A[6]=29027af1  B[6]=6d4f1e72  C[6]=24fef5f4  D[6]=ab090c6d
A[7]=67c47339  B[7]=37f9ef1b  C[7]=7dbfcd8e  D[7]=82142078

Step  4: (r= 3, s=20)
A[0]=901f95dc  B[0]=72f2baeb  C[0]=298b547a  D[0]=f7a3dc21
A[1]=f256f885  B[1]=fdf3fe2a  C[1]=c56b8c1c  D[1]=a85f2c3a
A[2]=e48f2686  B[2]=0234f998  C[2]=38972f92  D[2]=dc6cf617
A[3]=34126115  B[3]=c72cb20f  C[3]=e0272ad8  D[3]=d427f6c0
A[4]=6ffaaeb1  B[4]=4a6c17eb  C[4]=8be54762  D[4]=11b52ddf
A[5]=094a5572  B[5]=66807ab2  C[5]=9baa068c  D[5]=cc2b16d5
A[6]=589cd4df  B[6]=4813d789  C[6]=6d4f1e72  D[6]=24fef5f4
A[7]=e324f63a  B[7]=3e2399cb  C[7]=37f9ef1b  D[7]=7dbfcd8e

Step  5: (r=20, s=14)
```

```
A[0]=5abfc31b  B[0]=5dc901f9  C[0]=72f2baeb  D[0]=298b547a
A[1]=4a3b32e7  B[1]=885f256f  C[1]=fdf3fe2a  D[1]=c56b8c1c
A[2]=6d57d6e8  B[2]=686e48f2  C[2]=0234f998  D[2]=38972f92
A[3]=14e9509e  B[3]=11534126  C[3]=c72cb20f  D[3]=e0272ad8
A[4]=1e7851ab  B[4]=eb16ffaa  C[4]=4a6c17eb  D[4]=8be54762
A[5]=4053f1fd  B[5]=572094a5  C[5]=66807ab2  D[5]=9baa068c
A[6]=0baf0572  B[6]=4df589cd  C[6]=4813d789  D[6]=6d4f1e72
A[7]=126c2ba4  B[7]=63ae324f  C[7]=3e2399cb  D[7]=37f9ef1b

Step  6: (r=14, s=27)
A[0]=b57e5642  B[0]=f0c6d6af  C[0]=5dc901f9  D[0]=72f2baeb
A[1]=8e6da0f3  B[1]=ccb9d28e  C[1]=885f256f  D[1]=fdf3fe2a
A[2]=693c9a66  B[2]=f5ba1b55  C[2]=686e48f2  D[2]=0234f998
A[3]=22cdc555  B[3]=5427853a  C[3]=11534126  D[3]=c72cb20f
A[4]=2463b364  B[4]=146ac79e  C[4]=eb16ffaa  D[4]=4a6c17eb
A[5]=f529c134  B[5]=fc7f5014  C[5]=572094a5  D[5]=66807ab2
A[6]=e4408d7f  B[6]=c15c82eb  C[6]=4df589cd  D[6]=4813d789
A[7]=532b16fc  B[7]=0ae9049b  C[7]=63ae324f  D[7]=3e2399cb

Step  7: (r=27, s= 3)
A[0]=0ed60b56  B[0]=15abf2b2  C[0]=f0c6d6af  D[0]=5dc901f9
A[1]=b34ffe33  B[1]=9c736d07  C[1]=ccb9d28e  D[1]=885f256f
A[2]=16fc1ca5  B[2]=3349e4d3  C[2]=f5ba1b55  D[2]=686e48f2
A[3]=5a7d5844  B[3]=a9166e2a  C[3]=5427853a  D[3]=11534126
A[4]=c2b4c637  B[4]=21231d9b  C[4]=146ac79e  D[4]=eb16ffaa
A[5]=427dca03  B[5]=a7a94e09  C[5]=fc7f5014  D[5]=572094a5
A[6]=98ca0c93  B[6]=ff22046b  C[6]=c15c82eb  D[6]=4df589cd
A[7]=183bc53f  B[7]=e29958b7  C[7]=0ae9049b  D[7]=63ae324f

Step  8: (r=26, s= 4)
A[0]=025b55fb  B[0]=583b582d  C[0]=15abf2b2  D[0]=f0c6d6af
A[1]=47006771  B[1]=cecd3ff8  C[1]=9c736d07  D[1]=ccb9d28e
A[2]=b91cd694  B[2]=945bf072  C[2]=3349e4d3  D[2]=f5ba1b55
A[3]=d999c440  B[3]=1169f561  C[3]=a9166e2a  D[3]=5427853a
A[4]=931c3cb6  B[4]=df0ad318  C[4]=21231d9b  D[4]=146ac79e
A[5]=c6b82a14  B[5]=0d09f728  C[5]=a7a94e09  D[5]=fc7f5014
A[6]=b7968dfa  B[6]=4e632832  C[6]=ff22046b  D[6]=c15c82eb
A[7]=3959b6b6  B[7]=fc60ef14  C[7]=e29958b7  D[7]=0ae9049b

Step  9: (r= 4, s=23)
A[0]=bde99981  B[0]=25b55fb0  C[0]=583b582d  D[0]=15abf2b2
A[1]=54e7bc8e  B[1]=70067714  C[1]=cecd3ff8  D[1]=9c736d07
A[2]=187e1c94  B[2]=91cd694b  C[2]=945bf072  D[2]=3349e4d3
A[3]=44ddabaf  B[3]=999c440d  C[3]=1169f561  D[3]=a9166e2a
A[4]=aeb41904  B[4]=31c3cb69  C[4]=df0ad318  D[4]=21231d9b
A[5]=45260b5b  B[5]=6b82a14c  C[5]=0d09f728  D[5]=a7a94e09
A[6]=cdaea2d1  B[6]=7968dfab  C[6]=4e632832  D[6]=ff22046b
A[7]=629446d5  B[7]=959b6b63  C[7]=fc60ef14  D[7]=e29958b7
```

```
Step 10: (r=23, s=11)
A[0]=43a24096  B[0]=c0def4cc  C[0]=25b55fb0  D[0]=583b582d
A[1]=0551b223  B[1]=472a73de  C[1]=70067714  D[1]=cecd3ff8
A[2]=8434b9dd  B[2]=4a0c3f0e  C[2]=91cd694b  D[2]=945bf072
A[3]=620b5844  B[3]=d7a26ed5  C[3]=999c440d  D[3]=1169f561
A[4]=9edc7e2b  B[4]=82575a0c  C[4]=31c3cb69  D[4]=df0ad318
A[5]=5c10ad67  B[5]=ada29305  C[5]=6b82a14c  D[5]=0d09f728
A[6]=d9894023  B[6]=68e6d751  C[6]=7968dfab  D[6]=4e632832
A[7]=8998474a  B[7]=6ab14a23  C[7]=959b6b63  D[7]=fc60ef14

Step 11: (r=11, s=26)
A[0]=d1a6b3c3  B[0]=1204b21d  C[0]=c0def4cc  D[0]=25b55fb0
A[1]=4ad14266  B[1]=8d91182a  C[1]=472a73de  D[1]=70067714
A[2]=380f07ef  B[2]=a5ceec21  C[2]=4a0c3f0e  D[2]=91cd694b
A[3]=9f00f183  B[3]=5ac22310  C[3]=d7a26ed5  D[3]=999c440d
A[4]=a5126885  B[4]=e3f15cf6  C[4]=82575a0c  D[4]=31c3cb69
A[5]=fe38231d  B[5]=856b3ae0  C[5]=ada29305  D[5]=6b82a14c
A[6]=8209c31e  B[6]=4a011ecc  C[6]=68e6d751  D[6]=7968dfab
A[7]=3f006161  B[7]=c23a544c  C[7]=6ab14a23  D[7]=959b6b63

Step 12: (r=26, s= 4)
A[0]=ada7aed7  B[0]=0f469acf  C[0]=1204b21d  D[0]=c0def4cc
A[1]=989fc42f  B[1]=992b4509  C[1]=8d91182a  D[1]=472a73de
A[2]=33c29be4  B[2]=bce03c1f  C[2]=a5ceec21  D[2]=4a0c3f0e
A[3]=d65a2b49  B[3]=0e7c03c6  C[3]=5ac22310  D[3]=d7a26ed5
A[4]=5c5a71f4  B[4]=169449a2  C[4]=e3f15cf6  D[4]=82575a0c
A[5]=1001832f  B[5]=77f8e08c  C[5]=856b3ae0  D[5]=ada29305
A[6]=c73d3a01  B[6]=7a08270c  C[6]=4a011ecc  D[6]=68e6d751
A[7]=b5733fd9  B[7]=84fc0185  C[7]=c23a544c  D[7]=6ab14a23

Step 13: (r= 4, s=23)
A[0]=fcb17d6e  B[0]=da7aed7a  C[0]=0f469acf  D[0]=1204b21d
A[1]=bdfe7f1b  B[1]=89fc42f9  C[1]=992b4509  D[1]=8d91182a
A[2]=2b4f796b  B[2]=3c29be43  C[2]=bce03c1f  D[2]=a5ceec21
A[3]=ef1d09b5  B[3]=65a2b49d  C[3]=0e7c03c6  D[3]=5ac22310
A[4]=505f476f  B[4]=c5a71f45  C[4]=169449a2  D[4]=e3f15cf6
A[5]=a8820133  B[5]=001832f1  C[5]=77f8e08c  D[5]=856b3ae0
A[6]=abab96f4  B[6]=73d3a01c  C[6]=7a08270c  D[6]=4a011ecc
A[7]=b5bc3a90  B[7]=5733fd9b  C[7]=84fc0185  D[7]=c23a544c

Step 14: (r=23, s=11)
A[0]=0f03dba9  B[0]=b77e58be  C[0]=da7aed7a  D[0]=0f469acf
A[1]=e34d6896  B[1]=8ddeff3f  C[1]=89fc42f9  D[1]=992b4509
A[2]=53f92096  B[2]=b595a7bc  C[2]=3c29be43  D[2]=bce03c1f
A[3]=2997b596  B[3]=daf78e84  C[3]=65a2b49d  D[3]=0e7c03c6
A[4]=182c37e0  B[4]=b7a82fa3  C[4]=c5a71f45  D[4]=169449a2
A[5]=d31c6717  B[5]=99d44100  C[5]=001832f1  D[5]=77f8e08c
A[6]=fd9527ca  B[6]=7a55d5cb  C[6]=73d3a01c  D[6]=7a08270c
A[7]=2148ddcb  B[7]=485ade1d  C[7]=5733fd9b  D[7]=84fc0185
```

```
Step 15: (r=11, s=26)
A[0]=fb7ba75a  B[0]=1edd4878  C[0]=b77e58be  D[0]=da7aed7a
A[1]=ce6fc7ea  B[1]=6b44b71a  C[1]=8ddeff3f  D[1]=89fc42f9
A[2]=aa5af495  B[2]=c904b29f  C[2]=b595a7bc  D[2]=3c29be43
A[3]=21a7f7df  B[3]=bdacb14c  C[3]=daf78e84  D[3]=65a2b49d
A[4]=edd68fe1  B[4]=61bf00c1  C[4]=b7a82fa3  D[4]=c5a71f45
A[5]=b45ec3c3  B[5]=e338be98  C[5]=99d44100  D[5]=001832f1
A[6]=cd8c7ddb  B[6]=a93e57ec  C[6]=7a55d5cb  D[6]=73d3a01c
A[7]=a4bd646e  B[7]=46ee590a  C[7]=485ade1d  D[7]=5733fd9b

Step 16: (r=19, s=28)
A[0]=b8eaedde  B[0]=3ad7dbdd  C[0]=1edd4878  D[0]=b77e58be
A[1]=83e23051  B[1]=3f56737e  C[1]=6b44b71a  D[1]=8ddeff3f
A[2]=58e17811  B[2]=a4ad52d7  C[2]=c904b29f  D[2]=b595a7bc
A[3]=fa180a64  B[3]=bef90d3f  C[3]=bdacb14c  D[3]=daf78e84
A[4]=10d987d0  B[4]=7f0f6eb4  C[4]=61bf00c1  D[4]=b7a82fa3
A[5]=299bea19  B[5]=1e1da2f6  C[5]=e338be98  D[5]=99d44100
A[6]=6db04601  B[6]=eede6c63  C[6]=a93e57ec  D[6]=7a55d5cb
A[7]=d9952969  B[7]=237525eb  C[7]=46ee590a  D[7]=485ade1d

Step 17: (r=28, s= 7)
A[0]=eb07ca93  B[0]=eb8eaedd  C[0]=3ad7dbdd  D[0]=1edd4878
A[1]=62254dfa  B[1]=183e2305  C[1]=3f56737e  D[1]=6b44b71a
A[2]=493a1d0a  B[2]=158e1781  C[2]=a4ad52d7  D[2]=c904b29f
A[3]=60520de2  B[3]=4fa180a6  C[3]=bef90d3f  D[3]=bdacb14c
A[4]=de79c270  B[4]=010d987d  C[4]=7f0f6eb4  D[4]=61bf00c1
A[5]=57df67fd  B[5]=9299bea1  C[5]=1e1da2f6  D[5]=e338be98
A[6]=e2040e4f  B[6]=16db0460  C[6]=eede6c63  D[6]=a93e57ec
A[7]=4176c193  B[7]=9d995296  C[7]=237525eb  D[7]=46ee590a

Step 18: (r= 7, s=22)
A[0]=15aa31d6  B[0]=83e549f5  C[0]=eb8eaedd  D[0]=3ad7dbdd
A[1]=0414dc40  B[1]=12a6fd31  C[1]=183e2305  D[1]=3f56737e
A[2]=78c4b7b8  B[2]=9d0e8524  C[2]=158e1781  D[2]=a4ad52d7
A[3]=38b8d4ea  B[3]=2906f130  C[3]=4fa180a6  D[3]=bef90d3f
A[4]=cdb16dd1  B[4]=3ce1386f  C[4]=010d987d  D[4]=7f0f6eb4
A[5]=e2c60305  B[5]=efb3feab  C[5]=9299bea1  D[5]=1e1da2f6
A[6]=f02c3908  B[6]=020727f1  C[6]=16db0460  D[6]=eede6c63
A[7]=347c9a67  B[7]=bb60c9a0  C[7]=9d995296  D[7]=237525eb

Step 19: (r=22, s=19)
A[0]=a44ace40  B[0]=75856a8c  C[0]=83e549f5  D[0]=eb8eaedd
A[1]=3e9284ac  B[1]=10010537  C[1]=12a6fd31  D[1]=183e2305
A[2]=cf0a4bec  B[2]=ee1e312d  C[2]=9d0e8524  D[2]=158e1781
A[3]=78a89b42  B[3]=3a8e2e35  C[3]=2906f130  D[3]=4fa180a6
A[4]=bd21b9e5  B[4]=74736c5b  C[4]=3ce1386f  D[4]=010d987d
A[5]=39d96de2  B[5]=c178b180  C[5]=efb3feab  D[5]=9299bea1
A[6]=216339b4  B[6]=423c0b0e  C[6]=020727f1  D[6]=16db0460
```

```
A[7]=72db557e  B[7]=99cd1f26  C[7]=bb60c9a0  D[7]=9d995296

Step 20: (r=19, s=28)
A[0]=72641041  B[0]=72052256  C[0]=75856a8c  D[0]=83e549f5
A[1]=fd865404  B[1]=2561f494  C[1]=10010537  D[1]=12a6fd31
A[2]=fdff412d  B[2]=5f667852  C[2]=ee1e312d  D[2]=9d0e8524
A[3]=07af3c49  B[3]=da13c544  C[3]=3a8e2e35  D[3]=2906f130
A[4]=3947c57a  B[4]=cf2de90d  C[4]=74736c5b  D[4]=3ce1386f
A[5]=b4f976ce  B[5]=6f11cecb  C[5]=c178b180  D[5]=efb3feab
A[6]=3daf79af  B[6]=cda10b19  C[6]=423c0b0e  D[6]=020727f1
A[7]=0173c7d8  B[7]=abf396da  C[7]=99cd1f26  D[7]=bb60c9a0

Step 21: (r=28, s= 7)
A[0]=504d95d5  B[0]=17264104  C[0]=72052256  D[0]=75856a8c
A[1]=a0785b13  B[1]=4fd86540  C[1]=2561f494  D[1]=10010537
A[2]=e4b0e2c2  B[2]=dfdff412  C[2]=5f667852  D[2]=ee1e312d
A[3]=2d770d51  B[3]=907af3c4  C[3]=da13c544  D[3]=3a8e2e35
A[4]=5bf5996f  B[4]=a3947c57  C[4]=cf2de90d  D[4]=74736c5b
A[5]=e79526e4  B[5]=eb4f976c  C[5]=6f11cecb  D[5]=c178b180
A[6]=5d7f1d2d  B[6]=f3daf79a  C[6]=cda10b19  D[6]=423c0b0e
A[7]=1b14cefa  B[7]=80173c7d  C[7]=abf396da  D[7]=99cd1f26

Step 22: (r= 7, s=22)
A[0]=e0180229  B[0]=26caeaa8  C[0]=17264104  D[0]=72052256
A[1]=e4a961ff  B[1]=3c2d89d0  C[1]=4fd86540  D[1]=2561f494
A[2]=67bcba85  B[2]=58716172  C[2]=dfdff412  D[2]=5f667852
A[3]=fb0556a6  B[3]=bb86a896  C[3]=907af3c4  D[3]=da13c544
A[4]=851053f5  B[4]=faccb7ad  C[4]=a3947c57  D[4]=cf2de90d
A[5]=d5b322ea  B[5]=ca937273  C[5]=eb4f976c  D[5]=6f11cecb
A[6]=871ed6b1  B[6]=bf8e96ae  C[6]=f3daf79a  D[6]=cda10b19
A[7]=0666cc84  B[7]=8a677d0d  C[7]=80173c7d  D[7]=abf396da

Step 23: (r=22, s=19)
A[0]=c5526092  B[0]=8a780600  C[0]=26caeaa8  D[0]=17264104
A[1]=5f4a0bba  B[1]=7ff92a58  C[1]=3c2d89d0  D[1]=4fd86540
A[2]=861d2c42  B[2]=a159ef2e  C[2]=58716172  D[2]=dfdff412
A[3]=3babe633  B[3]=a9bec155  C[3]=bb86a896  D[3]=907af3c4
A[4]=14721a2c  B[4]=fd614414  C[4]=faccb7ad  D[4]=a3947c57
A[5]=34955495  B[5]=bab56cc8  C[5]=ca937273  D[5]=eb4f976c
A[6]=edb0db7a  B[6]=ac61c7b5  C[6]=bf8e96ae  D[6]=f3daf79a
A[7]=f2098324  B[7]=210199b3  C[7]=8a677d0d  D[7]=80173c7d

Step 24: (r=15, s= 5)
A[0]=42c09832  B[0]=304962a9  C[0]=8a780600  D[0]=26caeaa8
A[1]=ac54c275  B[1]=05dd2fa5  C[1]=7ff92a58  D[1]=3c2d89d0
A[2]=4df876b9  B[2]=9621430e  C[2]=a159ef2e  D[2]=58716172
A[3]=63d045dd  B[3]=f3199dd5  C[3]=a9bec155  D[3]=bb86a896
A[4]=d2abfdc1  B[4]=0d160a39  C[4]=fd614414  D[4]=faccb7ad
A[5]=75ac285f  B[5]=aa4a9a4a  C[5]=bab56cc8  D[5]=ca937273
```

```
A[6]=f3837241  B[6]=6dbd76d8  C[6]=ac61c7b5  D[6]=bf8e96ae
A[7]=2645030c  B[7]=c1927904  C[7]=210199b3  D[7]=8a677d0d

Step 25: (r= 5, s=29)
A[0]=887381c5  B[0]=58130648  C[0]=304962a9  D[0]=8a780600
A[1]=6ff7eec1  B[1]=8a984eb5  C[1]=05dd2fa5  D[1]=7ff92a58
A[2]=722f714e  B[2]=bf0ed729  C[2]=9621430e  D[2]=a159ef2e
A[3]=2a3fe9b3  B[3]=7a08bbac  C[3]=f3199dd5  D[3]=a9bec155
A[4]=7fad75f9  B[4]=557fb83a  C[4]=0d160a39  D[4]=fd614414
A[5]=b440bc60  B[5]=b5850bee  C[5]=aa4a9a4a  D[5]=bab56cc8
A[6]=88f1fc4a  B[6]=706e483e  C[6]=6dbd76d8  D[6]=ac61c7b5
A[7]=e5777041  B[7]=c8a06184  C[7]=c1927904  D[7]=210199b3

Step 26: (r=29, s= 9)
A[0]=99b48958  B[0]=b10e7038  C[0]=58130648  D[0]=304962a9
A[1]=4f5a6155  B[1]=2dfefdd8  C[1]=8a984eb5  D[1]=05dd2fa5
A[2]=d8a694a0  B[2]=ce45ee29  C[2]=bf0ed729  D[2]=9621430e
A[3]=b08e326e  B[3]=6547fd36  C[3]=7a08bbac  D[3]=f3199dd5
A[4]=42f6fb28  B[4]=2ff5aebf  C[4]=557fb83a  D[4]=0d160a39
A[5]=7fc4208a  B[5]=1688178c  C[5]=b5850bee  D[5]=aa4a9a4a
A[6]=9e21c9fd  B[6]=511e3f89  C[6]=706e483e  D[6]=6dbd76d8
A[7]=eb82e98c  B[7]=3caeee08  C[7]=c8a06184  D[7]=c1927904

Step 27: (r= 9, s=15)
A[0]=b5e8bd9b  B[0]=6912b133  C[0]=b10e7038  D[0]=58130648
A[1]=e62750bf  B[1]=b4c2aa9e  C[1]=2dfefdd8  D[1]=8a984eb5
A[2]=5d9ea8e4  B[2]=4d2941b1  C[2]=ce45ee29  D[2]=bf0ed729
A[3]=d5842473  B[3]=1c64dd61  C[3]=6547fd36  D[3]=7a08bbac
A[4]=51dc352c  B[4]=edf65085  C[4]=2ff5aebf  D[4]=557fb83a
A[5]=b4771e6a  B[5]=884114ff  C[5]=1688178c  D[5]=b5850bee
A[6]=e21f5bf2  B[6]=4393fb3c  C[6]=511e3f89  D[6]=706e483e
A[7]=5befc377  B[7]=05d319d7  C[7]=3caeee08  D[7]=c8a06184

Step 28: (r=15, s= 5)
A[0]=a5cf09db  B[0]=5ecddaf4  C[0]=6912b133  D[0]=b10e7038
A[1]=1f39f4d6  B[1]=a85ff313  C[1]=b4c2aa9e  D[1]=2dfefdd8
A[2]=10906964  B[2]=54722ecf  C[2]=4d2941b1  D[2]=ce45ee29
A[3]=ba62d68f  B[3]=1239eac2  C[3]=1c64dd61  D[3]=6547fd36
A[4]=413ab3ab  B[4]=1a9628ee  C[4]=edf65085  D[4]=2ff5aebf
A[5]=643c7395  B[5]=8f355a3b  C[5]=884114ff  D[5]=1688178c
A[6]=397d46c4  B[6]=adf9710f  C[6]=4393fb3c  D[6]=511e3f89
A[7]=2a3a6250  B[7]=e1bbadf7  C[7]=05d319d7  D[7]=3caeee08

Step 29: (r= 5, s=29)
A[0]=7fec03c4  B[0]=b9e13b74  C[0]=5ecddaf4  D[0]=6912b133
A[1]=432a1680  B[1]=e73e9ac3  C[1]=a85ff313  D[1]=b4c2aa9e
A[2]=9089141c  B[2]=120d2c82  C[2]=54722ecf  D[2]=4d2941b1
A[3]=1905d470  B[3]=4c5ad1f7  C[3]=1239eac2  D[3]=1c64dd61
A[4]=48a72aac  B[4]=27567568  C[4]=1a9628ee  D[4]=edf65085
```

```
A[5]=757f3d73  B[5]=878e72ac  C[5]=8f355a3b  D[5]=884114ff
A[6]=04435e30  B[6]=2fa8d887  C[6]=adf9710f  D[6]=4393fb3c
A[7]=215a27a9  B[7]=474c4a05  C[7]=e1bbadf7  D[7]=05d319d7

Step 30: (r=29, s= 9)
A[0]=7af43d98  B[0]=8ffd8078  C[0]=b9e13b74  D[0]=5ecddaf4
A[1]=0549acaf  B[1]=086542d0  C[1]=e73e9ac3  D[1]=a85ff313
A[2]=fb5b4099  B[2]=92112283  C[2]=120d2c82  D[2]=54722ecf
A[3]=7a5299dc  B[3]=0320ba8e  C[3]=4c5ad1f7  D[3]=1239eac2
A[4]=3135895d  B[4]=8914e555  C[4]=27567568  D[4]=1a9628ee
A[5]=eb8e4043  B[5]=6eafe7ae  C[5]=878e72ac  D[5]=8f355a3b
A[6]=906f3e4f  B[6]=00886bc6  C[6]=2fa8d887  D[6]=adf9710f
A[7]=c7089cce  B[7]=242b44f5  C[7]=474c4a05  D[7]=e1bbadf7

Step 31: (r= 9, s=15)
A[0]=9ce0a02c  B[0]=e87b30f5  C[0]=8ffd8078  D[0]=b9e13b74
A[1]=bc057e24  B[1]=93595e0a  C[1]=086542d0  D[1]=e73e9ac3
A[2]=7bae9cdd  B[2]=b68133f6  C[2]=92112283  D[2]=120d2c82
A[3]=5ad1c48c  B[3]=a533b8f4  C[3]=0320ba8e  D[3]=4c5ad1f7
A[4]=77d1c699  B[4]=6b12ba62  C[4]=8914e555  D[4]=27567568
A[5]=c61e491c  B[5]=1c8087d7  C[5]=6eafe7ae  D[5]=878e72ac
A[6]=7ca3bb0f  B[6]=de7c9f20  C[6]=00886bc6  D[6]=2fa8d887
A[7]=f426fbc1  B[7]=11399d8e  C[7]=242b44f5  D[7]=474c4a05

Feistel Step 0: (r=15, s= 5)
A[0]=71cb0912  B[0]=50164e70  C[0]=e87b30f5  D[0]=8ffd8078
A[1]=0245dab8  B[1]=bf125e02  C[1]=93595e0a  D[1]=086542d0
A[2]=8c6a8141  B[2]=4e6ebdd7  C[2]=b68133f6  D[2]=92112283
A[3]=7d3abd99  B[3]=e2462d68  C[3]=a533b8f4  D[3]=0320ba8e
A[4]=9301b8c8  B[4]=e34cbbe8  C[4]=6b12ba62  D[4]=8914e555
A[5]=b20f3381  B[5]=248e630f  C[5]=1c8087d7  D[5]=6eafe7ae
A[6]=9422de75  B[6]=dd87be51  C[6]=de7c9f20  D[6]=00886bc6
A[7]=c1f30303  B[7]=7de0fa13  C[7]=11399d8e  D[7]=242b44f5

Feistel Step 1: (r= 5, s=29)
A[0]=9ad9e612  B[0]=3961224e  C[0]=50164e70  D[0]=e87b30f5
A[1]=334a7c65  B[1]=48bb5700  C[1]=bf125e02  D[1]=93595e0a
A[2]=905de393  B[2]=8d502831  C[2]=4e6ebdd7  D[2]=b68133f6
A[3]=48cbb0fd  B[3]=a757b32f  C[3]=e2462d68  D[3]=a533b8f4
A[4]=83bed3a7  B[4]=60371912  C[4]=e34cbbe8  D[4]=6b12ba62
A[5]=b8aead84  B[5]=41e67036  C[5]=248e630f  D[5]=1c8087d7
A[6]=38b4512a  B[6]=845bceb2  C[6]=dd87be51  D[6]=de7c9f20
A[7]=147a0cf3  B[7]=3e606078  C[7]=7de0fa13  D[7]=11399d8e

Feistel Step 2: (r=29, s= 9)
A[0]=62f0b011  B[0]=535b3cc2  C[0]=3961224e  D[0]=50164e70
A[1]=808d179c  B[1]=a6694f8c  C[1]=48bb5700  D[1]=bf125e02
A[2]=bbbb3e76  B[2]=720bbc72  C[2]=8d502831  D[2]=4e6ebdd7
A[3]=2b3c79df  B[3]=a919761f  C[3]=a757b32f  D[3]=e2462d68
```

```
A[4]=93d7a49f  B[4]=f077da74  C[4]=60371912  D[4]=e34cbbe8
A[5]=e0c657cc  B[5]=9715d5b0  C[5]=41e67036  D[5]=248e630f
A[6]=6c4622c3  B[6]=47168a25  C[6]=845bceb2  D[6]=dd87be51
A[7]=a67881fc  B[7]=628f419e  C[7]=3e606078  D[7]=7de0fa13

Feistel Step 3: (r= 9, s=15)
A[0]=f872abfa  B[0]=e16022c5  C[0]=535b3cc2  D[0]=3961224e
A[1]=7a7d7217  B[1]=1a2f3901  C[1]=a6694f8c  D[1]=48bb5700
A[2]=eaab7cb6  B[2]=767ced77  C[2]=720bbc72  D[2]=8d502831
A[3]=bd4d1ca1  B[3]=78f3be56  C[3]=a919761f  D[3]=a757b32f
A[4]=33e22db4  B[4]=af493f27  C[4]=f077da74  D[4]=60371912
A[5]=5f49f4ef  B[5]=8caf99c1  C[5]=9715d5b0  D[5]=41e67036
A[6]=7f77398f  B[6]=8c4586d8  C[6]=47168a25  D[6]=845bceb2
A[7]=31c898b5  B[7]=f103f94c  C[7]=628f419e  D[7]=3e606078
```

Compression Function Output

```
A[0]=f872abfa  B[0]=e16022c5  C[0]=535b3cc2  D[0]=3961224e
A[1]=7a7d7217  B[1]=1a2f3901  C[1]=a6694f8c  D[1]=48bb5700
A[2]=eaab7cb6  B[2]=767ced77  C[2]=720bbc72  D[2]=8d502831
A[3]=bd4d1ca1  B[3]=78f3be56  C[3]=a919761f  D[3]=a757b32f
A[4]=33e22db4  B[4]=af493f27  C[4]=f077da74  D[4]=60371912
A[5]=5f49f4ef  B[5]=8caf99c1  C[5]=9715d5b0  D[5]=41e67036
A[6]=7f77398f  B[6]=8c4586d8  C[6]=47168a25  D[6]=845bceb2
A[7]=31c898b5  B[7]=f103f94c  C[7]=628f419e  D[7]=3e606078
```

Hash Function Output

```
faab72f817727d7ab67cabeaa11c4dbdb42de233eff4495f8f39777fb598c831
c52260e101392f1a77ed7c7656bef378273f49afc199af8cd886458c4cf903f1
```

6.4.3 Two-block Message

We use the message made of 1079 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
```

```
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
y[ 16.. 23] =  129   99   49  124  176  112   29   25
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
```

```
          41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
          baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
          ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
          da6cd4a4  a4f21667  357adec2  264d5546
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
          5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
          c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
          44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
          da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
          cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
          4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
          484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
          31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff1701d2  a6ce5932  a9895677  cb3634ca
          e4b21b4e  992766d9  eb1114ef  35b3ca4d
Z[17] = 74808b80  d3672c99  49b9b647  e59b1a65
          f2590da7  4188be78  6a7d9583  a5e55a1b
Z[18] = 3a40c5c0  5ea8a158  afe85018  67c2983e
          6e2191df  20c4df3c  c04a3fb6  47e7b819
Z[19] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
          c21c3de4  1062ef9e  e0251fdb  aeff5101
Z[20] = 0e90f170  17aae856  ebfa1406  a4fc5b04
          e10e1ef2  0831f7cf  65079af9  4c74b38c
Z[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
          f0870f79  8f2470dc  bd8f4271  263ad9c6
Z[22] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
          6d3892c8  c792386e  53bcac44  131dece3
Z[23] = 01d2fe2e  c87b3785  c3053cfb  6994966c
          369cc964  e3c91c37  29ded622  949a6b66
Z[24] = fc5c4e46  558ee4b2  e4b24615  5101983e
          6b665018  1d20b9eb  db985a1b  a06f0bd5
Z[25] = b7305a1b  b2a370dc  ac4465f0  9be216c1
          b9024443  b0d15018  7480a989  b647983e
Z[26] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
          5677e59b  9583ca4d  b1baf342  bad46994
Z[27] = ea2892c8  aa720000  1c3702bb  510192c8
          d0ac3785  ad2d7397  6ff3a7b7  452c8b80
Z[28] = 123415d8  0bd5d539  1c37bbbd  699470dc
          c21c52d3  9f863a40  5ea8ef9e  650716c1
```

```
Z[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
Z[30] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
Z[31] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
W[11] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
W[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
W[15] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
W[17] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
W[18] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
W[19] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
```

```
W[20] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
W[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
W[22] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
W[23] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
        c21c3de4  1062ef9e  e0251fdb  aeff5101
W[24] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
W[25] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
W[26] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
W[27] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
W[28] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
W[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
W[30] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
W[31] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
```

Feistel Steps

```
IV :
A[0]=c2956828  B[0]=39369835  C[0]=d9ca7181  D[0]=4d6185f6
A[1]=3da33320  B[1]=b7b6f593  C[1]=cf8e8183  D[1]=bbdcbc6e
A[2]=4149c566  B[2]=956d5c2e  C[2]=e2f28feb  D[2]=753b2bf6
A[3]=c49d9244  B[3]=2e4e80c8  C[3]=e9aa51c5  D[3]=7aac68ac
A[4]=04a3f1aa  B[4]=1e9fc449  C[4]=c5c2d649  D[4]=eb672a56
A[5]=0220c98b  B[5]=84ca34e9  C[5]=37c0b473  D[5]=ed8a5dcd
A[6]=7246bebf  B[6]=17d45ec5  C[6]=07eef0a5  D[6]=b072020d
A[7]=e51d9d96  B[7]=27db1b31  C[7]=dd23d692  D[7]=b07cf71f

IV XOR M :
A[0]=3d6a97d7  B[0]=c6c967ca  C[0]=26358e7e  D[0]=b29e7a09
A[1]=c25cccdf  B[1]=48490a6c  C[1]=30717e7c  D[1]=44234391
A[2]=beb63a99  B[2]=6a92a3d1  C[2]=1d0d7014  D[2]=8ac4d409
A[3]=3b626dbb  B[3]=d1b17f37  C[3]=1655ae3a  D[3]=85539753
A[4]=fb5c0e55  B[4]=e1603bb6  C[4]=3a3d29b6  D[4]=1498d5a9
A[5]=fddf3674  B[5]=7b35cb16  C[5]=c83f4b8c  D[5]=1275a232
A[6]=8db94140  B[6]=e82ba13a  C[6]=f8110f5a  D[6]=4f8dfdf2
A[7]=1ae26269  B[7]=d824e4ce  C[7]=22dc296d  D[7]=4f8308e0

Step  0: (r= 3, s=20)
A[0]=f9230c45  B[0]=eb54beb9  C[0]=c6c967ca  D[0]=26358e7e
```

```
A[1]=9e8de81f  B[1]=12e666fe  C[1]=48490a6c  D[1]=30717e7c
A[2]=435b70ad  B[2]=f5b1d4cd  C[2]=6a92a3d1  D[2]=1d0d7014
A[3]=e2611729  B[3]=db136dd9  C[3]=d1b17f37  D[3]=1655ae3a
A[4]=8e0d2f78  B[4]=dae072af  C[4]=e1603bb6  D[4]=3a3d29b6
A[5]=4fbc116d  B[5]=eef9b3a7  C[5]=7b35cb16  D[5]=c83f4b8c
A[6]=a466bea3  B[6]=6dca0a04  C[6]=e82ba13a  D[6]=f8110f5a
A[7]=c553a717  B[7]=d7131348  C[7]=d824e4ce  D[7]=22dc296d

Step  1: (r=20, s=14)
A[0]=099d79f2  B[0]=c45f9230  C[0]=eb54beb9  D[0]=c6c967ca
A[1]=80e74a1f  B[1]=81f9e8de  C[1]=12e666fe  D[1]=48490a6c
A[2]=3f2332c2  B[2]=0ad435b7  C[2]=f5b1d4cd  D[2]=6a92a3d1
A[3]=8d54922e  B[3]=729e2611  C[3]=db136dd9  D[3]=d1b17f37
A[4]=aba54baa  B[4]=f788e0d2  C[4]=dae072af  D[4]=e1603bb6
A[5]=4660a8c6  B[5]=16d4fbc1  C[5]=eef9b3a7  D[5]=7b35cb16
A[6]=ed8674ab  B[6]=ea3a466b  C[6]=6dca0a04  D[6]=e82ba13a
A[7]=6e57032e  B[7]=717c553a  C[7]=d7131348  D[7]=d824e4ce

Step  2: (r=14, s=27)
A[0]=70060390  B[0]=5e7c8267  C[0]=c45f9230  D[0]=eb54beb9
A[1]=8356e152  B[1]=d287e039  C[1]=81f9e8de  D[1]=12e666fe
A[2]=6597d880  B[2]=ccb08fc8  C[2]=0ad435b7  D[2]=f5b1d4cd
A[3]=e975e3b0  B[3]=248ba355  C[3]=729e2611  D[3]=db136dd9
A[4]=7d316964  B[4]=52eaaae9  C[4]=f788e0d2  D[4]=dae072af
A[5]=d443e68d  B[5]=2a319198  C[5]=16d4fbc1  D[5]=eef9b3a7
A[6]=1347e839  B[6]=9d2afb61  C[6]=ea3a466b  D[6]=6dca0a04
A[7]=0d1378c3  B[7]=c0cb9b95  C[7]=717c553a  D[7]=d7131348

Step  3: (r=27, s= 3)
A[0]=66e2a019  B[0]=8380301c  C[0]=5e7c8267  D[0]=c45f9230
A[1]=966242c8  B[1]=941ab70a  C[1]=d287e039  D[1]=81f9e8de
A[2]=a5b05023  B[2]=032cbec4  C[2]=ccb08fc8  D[2]=0ad435b7
A[3]=4c7eb009  B[3]=874baf1d  C[3]=248ba355  D[3]=729e2611
A[4]=482651a0  B[4]=23e98b4b  C[4]=52eaaae9  D[4]=f788e0d2
A[5]=cb845268  B[5]=6ea21f34  C[5]=2a319198  D[5]=16d4fbc1
A[6]=ea6616ae  B[6]=c89a3f41  C[6]=9d2afb61  D[6]=ea3a466b
A[7]=62036e71  B[7]=18689bc6  C[7]=c0cb9b95  D[7]=717c553a

Step  4: (r= 3, s=20)
A[0]=c0cd8187  B[0]=371500cb  C[0]=8380301c  D[0]=5e7c8267
A[1]=a6c94d7a  B[1]=b3121644  C[1]=941ab70a  D[1]=d287e039
A[2]=b21ae00a  B[2]=2d82811d  C[2]=032cbec4  D[2]=ccb08fc8
A[3]=83291414  B[3]=63f5804a  C[3]=874baf1d  D[3]=248ba355
A[4]=7213e14a  B[4]=41328d02  C[4]=23e98b4b  D[4]=52eaaae9
A[5]=9734f374  B[5]=5c229346  C[5]=6ea21f34  D[5]=2a319198
A[6]=5909f181  B[6]=5330b577  C[6]=c89a3f41  D[6]=9d2afb61
A[7]=b88e36cb  B[7]=101b738b  C[7]=18689bc6  D[7]=c0cb9b95

Step  5: (r=20, s=14)
```

```
A[0]=9ff6a8a2  B[0]=187c0cd8  C[0]=371500cb  D[0]=8380301c
A[1]=3ccfc5ba  B[1]=d7aa6c94  C[1]=b3121644  D[1]=941ab70a
A[2]=e66dd456  B[2]=00ab21ae  C[2]=2d82811d  D[2]=032cbec4
A[3]=aa8f59d1  B[3]=41483291  C[3]=63f5804a  D[3]=874baf1d
A[4]=a834acce  B[4]=14a7213e  C[4]=41328d02  D[4]=23e98b4b
A[5]=4c65bc21  B[5]=3749734f  C[5]=5c229346  D[5]=6ea21f34
A[6]=0dfff0df  B[6]=1815909f  C[6]=5330b577  D[6]=c89a3f41
A[7]=a38b1745  B[7]=6cbb88e3  C[7]=101b738b  D[7]=18689bc6

Step  6: (r=14, s=27)
A[0]=f83351f0  B[0]=aa28a7fd  C[0]=187c0cd8  D[0]=371500cb
A[1]=4e94f22f  B[1]=f16e8f33  C[1]=d7aa6c94  D[1]=b3121644
A[2]=e0586e16  B[2]=7515b99b  C[2]=00ab21ae  D[2]=2d82811d
A[3]=17d6b6c2  B[3]=d6746aa3  C[3]=41483291  D[3]=63f5804a
A[4]=c0f615ee  B[4]=2b33aa0d  C[4]=14a7213e  D[4]=41328d02
A[5]=3e4c17c6  B[5]=6f085319  C[5]=3749734f  D[5]=5c229346
A[6]=4e4c477e  B[6]=fc37c37f  C[6]=1815909f  D[6]=5330b577
A[7]=810cc77b  B[7]=c5d168e2  C[7]=6cbb88e3  D[7]=101b738b

Step  7: (r=27, s= 3)
A[0]=2ccd02c8  B[0]=87c19a8f  C[0]=aa28a7fd  D[0]=187c0cd8
A[1]=54db9fe5  B[1]=7a74a791  C[1]=f16e8f33  D[1]=d7aa6c94
A[2]=e6d5e3d1  B[2]=b702c370  C[2]=7515b99b  D[2]=00ab21ae
A[3]=46dea451  B[3]=10beb5b6  C[3]=d6746aa3  D[3]=41483291
A[4]=48a762ca  B[4]=7607b0af  C[4]=2b33aa0d  D[4]=14a7213e
A[5]=52923bff  B[5]=31f260be  C[5]=6f085319  D[5]=3749734f
A[6]=0c03e6bb  B[6]=f272623b  C[6]=fc37c37f  D[6]=1815909f
A[7]=2b5ad582  B[7]=dc08663b  C[7]=c5d168e2  D[7]=6cbb88e3

Step  8: (r=26, s= 4)
A[0]=03aecef6  B[0]=20b3340b  C[0]=87c19a8f  D[0]=aa28a7fd
A[1]=7aafb52d  B[1]=95536e7f  C[1]=7a74a791  D[1]=f16e8f33
A[2]=14484461  B[2]=479b578f  C[2]=b702c370  D[2]=7515b99b
A[3]=34f2a90e  B[3]=451b7a91  C[3]=10beb5b6  D[3]=d6746aa3
A[4]=97099b89  B[4]=29229d8b  C[4]=7607b0af  D[4]=2b33aa0d
A[5]=ac5e77f5  B[5]=fd4a48ef  C[5]=31f260be  D[5]=6f085319
A[6]=90dec11b  B[6]=ec300f9a  C[6]=f272623b  D[6]=fc37c37f
A[7]=a6aa0f92  B[7]=08ad6b56  C[7]=dc08663b  D[7]=c5d168e2

Step  9: (r= 4, s=23)
A[0]=d8931ffa  B[0]=3aecef60  C[0]=20b3340b  D[0]=87c19a8f
A[1]=11897ad0  B[1]=aafb52d7  C[1]=95536e7f  D[1]=7a74a791
A[2]=ab063390  B[2]=44844611  C[2]=479b578f  D[2]=b702c370
A[3]=ed08c4bf  B[3]=4f2a90e3  C[3]=451b7a91  D[3]=10beb5b6
A[4]=5a1f6552  B[4]=7099b899  C[4]=29229d8b  D[4]=7607b0af
A[5]=f01690fa  B[5]=c5e77f5a  C[5]=fd4a48ef  D[5]=31f260be
A[6]=27b55e7f  B[6]=0dec11b9  C[6]=ec300f9a  D[6]=f272623b
A[7]=ac1232a3  B[7]=6aa0f92a  C[7]=08ad6b56  D[7]=dc08663b
```

```
Step 10: (r=23, s=11)
A[0]=00820f8f  B[0]=fd6c498f  C[0]=3aecef60  D[0]=20b3340b
A[1]=e81eaaf4  B[1]=6808c4bd  C[1]=aafb52d7  D[1]=95536e7f
A[2]=bd4553d8  B[2]=c8558319  C[2]=44844611  D[2]=479b578f
A[3]=226dbd3f  B[3]=5ff68462  C[3]=4f2a90e3  D[3]=451b7a91
A[4]=527c3a12  B[4]=a92d0fb2  C[4]=7099b899  D[4]=29229d8b
A[5]=fe5278ae  B[5]=7d780b48  C[5]=c5e77f5a  D[5]=fd4a48ef
A[6]=5e2a1d16  B[6]=3f93daaf  C[6]=0dec11b9  D[6]=ec300f9a
A[7]=664f7436  B[7]=51d60919  C[7]=6aa0f92a  D[7]=08ad6b56

Step 11: (r=11, s=26)
A[0]=e7318708  B[0]=107c7804  C[0]=fd6c498f  D[0]=3aecef60
A[1]=24d627d3  B[1]=f557a740  C[1]=6808c4bd  D[1]=aafb52d7
A[2]=58d37f59  B[2]=2a9ec5ea  C[2]=c8558319  D[2]=44844611
A[3]=a2f50288  B[3]=6de9f913  C[3]=5ff68462  D[3]=4f2a90e3
A[4]=f2f8d44d  B[4]=e1d09293  C[4]=a92d0fb2  D[4]=7099b899
A[5]=6fa1275a  B[5]=93c577f2  C[5]=7d780b48  D[5]=c5e77f5a
A[6]=d65b0248  B[6]=50e8b2f1  C[6]=3f93daaf  D[6]=0dec11b9
A[7]=b200c58f  B[7]=7ba1b332  C[7]=51d60919  D[7]=6aa0f92a

Step 12: (r=26, s= 4)
A[0]=b62ca76e  B[0]=239cc61c  C[0]=107c7804  D[0]=fd6c498f
A[1]=41fa3a19  B[1]=4c93589f  C[1]=f557a740  D[1]=6808c4bd
A[2]=d090533e  B[2]=65634dfd  C[2]=2a9ec5ea  D[2]=c8558319
A[3]=5f930d03  B[3]=228bd40a  C[3]=6de9f913  D[3]=5ff68462
A[4]=0d12c9ee  B[4]=37cbe351  C[4]=e1d09293  D[4]=a92d0fb2
A[5]=a6698f11  B[5]=69be849d  C[5]=93c577f2  D[5]=7d780b48
A[6]=53479612  B[6]=23596c09  C[6]=50e8b2f1  D[6]=3f93daaf
A[7]=5cec97b3  B[7]=3ec80316  C[7]=7ba1b332  D[7]=51d60919

Step 13: (r= 4, s=23)
A[0]=baeec887  B[0]=62ca76eb  C[0]=239cc61c  D[0]=107c7804
A[1]=16ea1d39  B[1]=1fa3a194  C[1]=4c93589f  D[1]=f557a740
A[2]=f5047f4b  B[2]=090533ed  C[2]=65634dfd  D[2]=2a9ec5ea
A[3]=c16a2532  B[3]=f930d035  C[3]=228bd40a  D[3]=6de9f913
A[4]=d287e788  B[4]=d12c9ee0  C[4]=37cbe351  D[4]=e1d09293
A[5]=6d5cb5d1  B[5]=6698f11a  C[5]=69be849d  D[5]=93c577f2
A[6]=d0e4b60d  B[6]=34796125  C[6]=23596c09  D[6]=50e8b2f1
A[7]=b97fde77  B[7]=cec97b35  C[7]=3ec80316  D[7]=7ba1b332

Step 14: (r=23, s=11)
A[0]=ff435b74  B[0]=43dd7764  C[0]=62ca76eb  D[0]=239cc61c
A[1]=f748a224  B[1]=9c8b750e  C[1]=1fa3a194  D[1]=4c93589f
A[2]=e8e8ad70  B[2]=a5fa823f  C[2]=090533ed  D[2]=65634dfd
A[3]=7d6680fe  B[3]=9960b512  C[3]=f930d035  D[3]=228bd40a
A[4]=d7eedce2  B[4]=c46943f3  C[4]=d12c9ee0  D[4]=37cbe351
A[5]=5036ffa5  B[5]=e8b6ae5a  C[5]=6698f11a  D[5]=69be849d
A[6]=83aeb727  B[6]=06e8725b  C[6]=34796125  D[6]=23596c09
A[7]=3e19777f  B[7]=3bdcbfef  C[7]=cec97b35  D[7]=3ec80316
```

```
Step 15: (r=11, s=26)
A[0]=084e9bc0  B[0]=1adba7fa  C[0]=43dd7764  D[0]=62ca76eb
A[1]=9f031d06  B[1]=451127ba  C[1]=9c8b750e  D[1]=1fa3a194
A[2]=e9edc146  B[2]=456b8747  C[2]=a5fa823f  D[2]=090533ed
A[3]=892fd738  B[3]=3407f3eb  C[3]=9960b512  D[3]=f930d035
A[4]=c8319c5d  B[4]=76e716bf  C[4]=c46943f3  D[4]=d12c9ee0
A[5]=ebcd2915  B[5]=b7fd2a81  C[5]=e8b6ae5a  D[5]=6698f11a
A[6]=f5e087cd  B[6]=75b93c1d  C[6]=06e8725b  D[6]=34796125
A[7]=3d39ea32  B[7]=cbbbf9f0  C[7]=3bdcbfef  D[7]=cec97b35

Step 16: (r=19, s=28)
A[0]=da6766bc  B[0]=de004274  C[0]=1adba7fa  D[0]=43dd7764
A[1]=5d8985a7  B[1]=e834f818  C[1]=451127ba  D[1]=9c8b750e
A[2]=f347f059  B[2]=0a374f6e  C[2]=456b8747  D[2]=a5fa823f
A[3]=59288d4a  B[3]=b9c4497e  C[3]=3407f3eb  D[3]=9960b512
A[4]=a92e4ead  B[4]=e2ee418c  C[4]=76e716bf  D[4]=c46943f3
A[5]=b7b05769  B[5]=48af5e69  C[5]=b7fd2a81  D[5]=e8b6ae5a
A[6]=c2fbe07b  B[6]=3e6faf04  C[6]=75b93c1d  D[6]=06e8725b
A[7]=167a7c38  B[7]=5191e9cf  C[7]=cbbbf9f0  D[7]=3bdcbfef

Step 17: (r=28, s= 7)
A[0]=fab4cc31  B[0]=cda6766b  C[0]=de004274  D[0]=1adba7fa
A[1]=47eec7f5  B[1]=75d8985a  C[1]=e834f818  D[1]=451127ba
A[2]=d6b34919  B[2]=9f347f05  C[2]=0a374f6e  D[2]=456b8747
A[3]=8b3d35f9  B[3]=a59288d4  C[3]=b9c4497e  D[3]=3407f3eb
A[4]=7942f61b  B[4]=da92e4ea  C[4]=e2ee418c  D[4]=76e716bf
A[5]=b5ede748  B[5]=9b7b0576  C[5]=48af5e69  D[5]=b7fd2a81
A[6]=29c9efe9  B[6]=bc2fbe07  C[6]=3e6faf04  D[6]=75b93c1d
A[7]=46abeda4  B[7]=8167a7c3  C[7]=5191e9cf  D[7]=cbbbf9f0

Step 18: (r= 7, s=22)
A[0]=797126de  B[0]=5a6618fd  C[0]=cda6766b  D[0]=de004274
A[1]=caf6cdd9  B[1]=f763faa3  C[1]=75d8985a  D[1]=e834f818
A[2]=e15d4d9e  B[2]=59a48ceb  C[2]=9f347f05  D[2]=0a374f6e
A[3]=6ccee8f0  B[3]=9e9afcc5  C[3]=a59288d4  D[3]=b9c4497e
A[4]=0afd0976  B[4]=a17b0dbc  C[4]=da92e4ea  D[4]=e2ee418c
A[5]=6001d944  B[5]=f6f3a45a  C[5]=9b7b0576  D[5]=48af5e69
A[6]=089b6c93  B[6]=e4f7f494  C[6]=bc2fbe07  D[6]=3e6faf04
A[7]=22c27b7f  B[7]=55f6d223  C[7]=8167a7c3  D[7]=5191e9cf

Step 19: (r=22, s=19)
A[0]=84910afe  B[0]=b79e5c49  C[0]=5a6618fd  D[0]=cda6766b
A[1]=18a7bacb  B[1]=7672bdb3  C[1]=f763faa3  D[1]=75d8985a
A[2]=34bcd188  B[2]=67b85753  C[2]=59a48ceb  D[2]=9f347f05
A[3]=4a00137a  B[3]=3c1b33ba  C[3]=9e9afcc5  D[3]=a59288d4
A[4]=2973000b  B[4]=5d82bf42  C[4]=a17b0dbc  D[4]=da92e4ea
A[5]=4bc52099  B[5]=51180076  C[5]=f6f3a45a  D[5]=9b7b0576
A[6]=6c4318cd  B[6]=24c226db  C[6]=e4f7f494  D[6]=bc2fbe07
```

```
A[7]=dc0c332d  B[7]=dfc8b09e  C[7]=55f6d223  D[7]=8167a7c3

Step 20: (r=19, s=28)
A[0]=1cd6ddf9  B[0]=57f42488  C[0]=b79e5c49  D[0]=5a6618fd
A[1]=cfc750a8  B[1]=d658c53d  C[1]=7672bdb3  D[1]=f763faa3
A[2]=74209e4d  B[2]=8c41a5e6  C[2]=67b85753  D[2]=59a48ceb
A[3]=8710631e  B[3]=9bd25000  C[3]=3c1b33ba  D[3]=9e9afcc5
A[4]=cbde4674  B[4]=00594b98  C[4]=5d82bf42  D[4]=a17b0dbc
A[5]=ebc7317b  B[5]=04ca5e29  C[5]=51180076  D[5]=f6f3a45a
A[6]=20b9da53  B[6]=c66b6218  C[6]=24c226db  D[6]=e4f7f494
A[7]=1d908685  B[7]=996ee061  C[7]=dfc8b09e  D[7]=55f6d223

Step 21: (r=28, s= 7)
A[0]=99f94920  B[0]=91cd6ddf  C[0]=57f42488  D[0]=b79e5c49
A[1]=aed34a1d  B[1]=8cfc750a  C[1]=d658c53d  D[1]=7672bdb3
A[2]=72e488b8  B[2]=d74209e4  C[2]=8c41a5e6  D[2]=67b85753
A[3]=a2cb2592  B[3]=e8710631  C[3]=9bd25000  D[3]=3c1b33ba
A[4]=2041e092  B[4]=4cbde467  C[4]=00594b98  D[4]=5d82bf42
A[5]=42ebe14b  B[5]=bebc7317  C[5]=04ca5e29  D[5]=51180076
A[6]=060a94ca  B[6]=320b9da5  C[6]=c66b6218  D[6]=24c226db
A[7]=bbe2aa23  B[7]=51d90868  C[7]=996ee061  D[7]=dfc8b09e

Step 22: (r= 7, s=22)
A[0]=da273e8f  B[0]=fca4904c  C[0]=91cd6ddf  D[0]=57f42488
A[1]=05f56b5a  B[1]=69a50ed7  C[1]=8cfc750a  D[1]=d658c53d
A[2]=61aa862e  B[2]=72445c39  C[2]=d74209e4  D[2]=8c41a5e6
A[3]=461cd22b  B[3]=6592c951  C[3]=e8710631  D[3]=9bd25000
A[4]=2e236cff  B[4]=20f04910  C[4]=4cbde467  D[4]=00594b98
A[5]=0900a6af  B[5]=75f0a5a1  C[5]=bebc7317  D[5]=04ca5e29
A[6]=7e2a868b  B[6]=054a6503  C[6]=320b9da5  D[6]=c66b6218
A[7]=cfd06a14  B[7]=f15511dd  C[7]=51d90868  D[7]=996ee061

Step 23: (r=22, s=19)
A[0]=6185f6ad  B[0]=a3f689cf  C[0]=fca4904c  D[0]=91cd6ddf
A[1]=d5dadd41  B[1]=d6817d5a  C[1]=69a50ed7  D[1]=8cfc750a
A[2]=73d6465f  B[2]=8b986aa1  C[2]=72445c39  D[2]=d74209e4
A[3]=77b59240  B[3]=8ad18734  C[3]=6592c951  D[3]=e8710631
A[4]=53960306  B[4]=3fcb88db  C[4]=20f04910  D[4]=4cbde467
A[5]=81f41449  B[5]=abc24029  C[5]=75f0a5a1  D[5]=bebc7317
A[6]=c74f4f79  B[6]=a2df8aa1  C[6]=054a6503  D[6]=320b9da5
A[7]=58c2592d  B[7]=8533f41a  C[7]=f15511dd  D[7]=51d90868

Step 24: (r=15, s= 5)
A[0]=321df48f  B[0]=fb56b0c2  C[0]=a3f689cf  D[0]=fca4904c
A[1]=7933590c  B[1]=6ea0eaed  C[1]=d6817d5a  D[1]=69a50ed7
A[2]=cc2c0dd5  B[2]=232fb9eb  C[2]=8b986aa1  D[2]=72445c39
A[3]=c11f1352  B[3]=c9203bda  C[3]=8ad18734  D[3]=6592c951
A[4]=7ec7b255  B[4]=018329cb  C[4]=3fcb88db  D[4]=20f04910
A[5]=3e66e51d  B[5]=0a24c0fa  C[5]=abc24029  D[5]=75f0a5a1
```

```
A[6]=abcc58d5  B[6]=a7bce3a7  C[6]=a2df8aa1  D[6]=054a6503
A[7]=494cb5dd  B[7]=2c96ac61  C[7]=8533f41a  D[7]=f15511dd

Step 25: (r= 5, s=29)
A[0]=1b20adc3  B[0]=43be91e6  C[0]=fb56b0c2  D[0]=a3f689cf
A[1]=199cf654  B[1]=266b218f  C[1]=6ea0eaed  D[1]=d6817d5a
A[2]=2f14f3ab  B[2]=8581bab9  C[2]=232fb9eb  D[2]=8b986aa1
A[3]=d6b5c0af  B[3]=23e26a58  C[3]=c9203bda  D[3]=8ad18734
A[4]=eb4752f3  B[4]=d8f64aaf  C[4]=018329cb  D[4]=3fcb88db
A[5]=ad6d7fa1  B[5]=ccdca3a7  C[5]=0a24c0fa  D[5]=abc24029
A[6]=49869ae7  B[6]=798b1ab5  C[6]=a7bce3a7  D[6]=a2df8aa1
A[7]=709c23e5  B[7]=2996bba9  C[7]=2c96ac61  D[7]=8533f41a

Step 26: (r=29, s= 9)
A[0]=e8fedcf9  B[0]=636415b8  C[0]=43be91e6  D[0]=fb56b0c2
A[1]=835e9b3a  B[1]=83339eca  C[1]=266b218f  D[1]=6ea0eaed
A[2]=46c4a46e  B[2]=65e29e75  C[2]=8581bab9  D[2]=232fb9eb
A[3]=259b84c2  B[3]=fad6b815  C[3]=23e26a58  D[3]=c9203bda
A[4]=23484b98  B[4]=7d68ea5e  C[4]=d8f64aaf  D[4]=018329cb
A[5]=264b184a  B[5]=35adaff4  C[5]=ccdca3a7  D[5]=0a24c0fa
A[6]=b8933cd8  B[6]=e930d35c  C[6]=798b1ab5  D[6]=a7bce3a7
A[7]=87dc0888  B[7]=ae13847c  C[7]=2996bba9  D[7]=2c96ac61

Step 27: (r= 9, s=15)
A[0]=3e98c627  B[0]=fdb9f3d1  C[0]=636415b8  D[0]=43be91e6
A[1]=0525d976  B[1]=bd367506  C[1]=83339eca  D[1]=266b218f
A[2]=2e0d5b9d  B[2]=8948dc8d  C[2]=65e29e75  D[2]=8581bab9
A[3]=c264a350  B[3]=3709844b  C[3]=fad6b815  D[3]=23e26a58
A[4]=a01510f8  B[4]=90973046  C[4]=7d68ea5e  D[4]=d8f64aaf
A[5]=ba4f10b6  B[5]=9630944c  C[5]=35adaff4  D[5]=ccdca3a7
A[6]=a608577b  B[6]=2679b171  C[6]=e930d35c  D[6]=798b1ab5
A[7]=feed2580  B[7]=b811110f  C[7]=ae13847c  D[7]=2996bba9

Step 28: (r=15, s= 5)
A[0]=a0ba8e87  B[0]=63139f4c  C[0]=fdb9f3d1  D[0]=636415b8
A[1]=25b379f6  B[1]=ecbb0292  C[1]=bd367506  D[1]=83339eca
A[2]=31dbe36b  B[2]=adce9706  C[2]=8948dc8d  D[2]=65e29e75
A[3]=92e24532  B[3]=51a86132  C[3]=3709844b  D[3]=fad6b815
A[4]=bf51af72  B[4]=887c500a  C[4]=90973046  D[4]=7d68ea5e
A[5]=8f71d650  B[5]=885b5d27  C[5]=9630944c  D[5]=35adaff4
A[6]=89b33c27  B[6]=2bbdd304  C[6]=2679b171  D[6]=e930d35c
A[7]=c64759a9  B[7]=92c07f76  C[7]=b811110f  D[7]=ae13847c

Step 29: (r= 5, s=29)
A[0]=f5906d2f  B[0]=1751d0f4  C[0]=63139f4c  D[0]=fdb9f3d1
A[1]=19115eec  B[1]=b66f3ec4  C[1]=ecbb0292  D[1]=bd367506
A[2]=a51c86ec  B[2]=3b7c6d66  C[2]=adce9706  D[2]=8948dc8d
A[3]=edc7a079  B[3]=5c48a652  C[3]=51a86132  D[3]=3709844b
A[4]=4568dd59  B[4]=ea35ee57  C[4]=887c500a  D[4]=90973046
```

```
A[5]=c23b108d  B[5]=ee3aca11  C[5]=885b5d27  D[5]=9630944c
A[6]=a75d4a47  B[6]=366784f1  C[6]=2bbdd304  D[6]=2679b171
A[7]=b5d0fa48  B[7]=c8eb3538  C[7]=92c07f76  D[7]=b811110f

Step 30: (r=29, s= 9)
A[0]=16884a56  B[0]=feb20da5  C[0]=1751d0f4  D[0]=63139f4c
A[1]=83bdb052  B[1]=83222bdd  C[1]=b66f3ec4  D[1]=ecbb0292
A[2]=7286c2b6  B[2]=94a390dd  C[2]=3b7c6d66  D[2]=adce9706
A[3]=f5d84fa7  B[3]=3db8f40f  C[3]=5c48a652  D[3]=51a86132
A[4]=9e77dc45  B[4]=28ad1bab  C[4]=ea35ee57  D[4]=887c500a
A[5]=78f0b4dc  B[5]=b8476211  C[5]=ee3aca11  D[5]=885b5d27
A[6]=c3e8d536  B[6]=f4eba948  C[6]=366784f1  D[6]=2bbdd304
A[7]=b0009f00  B[7]=16ba1f49  C[7]=c8eb3538  D[7]=92c07f76

Step 31: (r= 9, s=15)
A[0]=694eeebc  B[0]=1094ac2d  C[0]=feb20da5  D[0]=1751d0f4
A[1]=f5a56010  B[1]=7b60a507  C[1]=83222bdd  D[1]=b66f3ec4
A[2]=0c389217  B[2]=0d856ce5  C[2]=94a390dd  D[2]=3b7c6d66
A[3]=dcd41d01  B[3]=b09f4feb  C[3]=3db8f40f  D[3]=5c48a652
A[4]=1a8af0c2  B[4]=efb88b3c  C[4]=28ad1bab  D[4]=ea35ee57
A[5]=80233030  B[5]=e169b8f1  C[5]=b8476211  D[5]=ee3aca11
A[6]=3360d717  B[6]=d1aa6d87  C[6]=f4eba948  D[6]=366784f1
A[7]=34a8bf0a  B[7]=013e0160  C[7]=16ba1f49  D[7]=c8eb3538

Feistel Step 0: (r=15, s= 5)
A[0]=c3854400  B[0]=775e34a7  C[0]=1094ac2d  D[0]=feb20da5
A[1]=5df1ead3  B[1]=b0087ad2  C[1]=7b60a507  D[1]=83222bdd
A[2]=37a7618d  B[2]=490b861c  C[2]=0d856ce5  D[2]=94a390dd
A[3]=9d703ad6  B[3]=0e80ee6a  C[3]=b09f4feb  D[3]=3db8f40f
A[4]=c905a554  B[4]=78610d45  C[4]=efb88b3c  D[4]=28ad1bab
A[5]=9081c6fa  B[5]=98184011  C[5]=e169b8f1  D[5]=b8476211
A[6]=2abb3a43  B[6]=6b8b99b0  C[6]=d1aa6d87  D[6]=f4eba948
A[7]=73e61ba6  B[7]=5f851a54  C[7]=013e0160  D[7]=16ba1f49

Feistel Step 1: (r= 5, s=29)
A[0]=e64bdbe6  B[0]=70a88018  C[0]=775e34a7  D[0]=1094ac2d
A[1]=7ba28cfb  B[1]=be3d5a6b  C[1]=b0087ad2  D[1]=7b60a507
A[2]=570aff46  B[2]=f4ec31a6  C[2]=490b861c  D[2]=0d856ce5
A[3]=115036f3  B[3]=ae075ad3  C[3]=0e80ee6a  D[3]=b09f4feb
A[4]=6e280651  B[4]=20b4aa99  C[4]=78610d45  D[4]=efb88b3c
A[5]=e292b6af  B[5]=1038df52  C[5]=98184011  D[5]=e169b8f1
A[6]=41be174b  B[6]=57674865  C[6]=6b8b99b0  D[6]=d1aa6d87
A[7]=e27f09e9  B[7]=7cc374ce  C[7]=5f851a54  D[7]=013e0160

Feistel Step 2: (r=29, s= 9)
A[0]=33d33ff3  B[0]=dcc97b7c  C[0]=70a88018  D[0]=775e34a7
A[1]=9779acf3  B[1]=6f74519f  C[1]=be3d5a6b  D[1]=b0087ad2
A[2]=feae336e  B[2]=cae15fe8  C[2]=f4ec31a6  D[2]=490b861c
A[3]=c2be181b  B[3]=622a06de  C[3]=ae075ad3  D[3]=0e80ee6a
```

```
A[4]=1b033ca9  B[4]=2dc500ca  C[4]=20b4aa99  D[4]=78610d45
A[5]=51684c4a  B[5]=fc5256d5  C[5]=1038df52  D[5]=98184011
A[6]=f1428c28  B[6]=6837c2e9  C[6]=57674865  D[6]=6b8b99b0
A[7]=269f1834  B[7]=3c4fe13d  C[7]=7cc374ce  D[7]=5f851a54

Feistel Step 3: (r= 9, s=15)
A[0]=c183dd0a  B[0]=a67fe667  C[0]=dcc97b7c  D[0]=70a88018
A[1]=9586624e  B[1]=f359e72e  C[1]=6f74519f  D[1]=be3d5a6b
A[2]=e8159675  B[2]=5c66ddfd  C[2]=cae15fe8  D[2]=f4ec31a6
A[3]=8b28e3f9  B[3]=7c303785  C[3]=622a06de  D[3]=ae075ad3
A[4]=8399ad25  B[4]=06795236  C[4]=2dc500ca  D[4]=20b4aa99
A[5]=adf15227  B[5]=d09894a2  C[5]=fc5256d5  D[5]=1038df52
A[6]=0a7c1f0f  B[6]=851851e2  C[6]=6837c2e9  D[6]=57674865
A[7]=3768fdad  B[7]=3e30684d  C[7]=3c4fe13d  D[7]=7cc374ce
```

Compression Function Output

```
A[0]=c183dd0a  B[0]=a67fe667  C[0]=dcc97b7c  D[0]=70a88018
A[1]=9586624e  B[1]=f359e72e  C[1]=6f74519f  D[1]=be3d5a6b
A[2]=e8159675  B[2]=5c66ddfd  C[2]=cae15fe8  D[2]=f4ec31a6
A[3]=8b28e3f9  B[3]=7c303785  C[3]=622a06de  D[3]=ae075ad3
A[4]=8399ad25  B[4]=06795236  C[4]=2dc500ca  D[4]=20b4aa99
A[5]=adf15227  B[5]=d09894a2  C[5]=fc5256d5  D[5]=1038df52
A[6]=0a7c1f0f  B[6]=851851e2  C[6]=6837c2e9  D[6]=57674865
A[7]=3768fdad  B[7]=3e30684d  C[7]=3c4fe13d  D[7]=7cc374ce
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
```

```
y[ 24.. 31] =   88   14   70  255  173  206  169   46
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
```

```
        f18c00b9  109fe0ed  363351a9  4d53b9e7
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
Z[17] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
Z[18] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
Z[19] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
Z[20] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
Z[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
Z[22] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
Z[23] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
Z[24] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
Z[25] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
Z[26] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
Z[27] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
Z[28] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
Z[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
Z[30] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
Z[31] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
W[17] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
W[18] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
W[19] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
W[20] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
W[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
W[22] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
W[23] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
W[24] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
```

```
        5cd64aa2  983e0e90  3957d539  0748ad2d
W[25] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
W[26] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
W[27] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
W[28] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
W[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
W[30] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
W[31] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
```

Feistel Steps

```
IV :
A[0]=c183dd0a  B[0]=a67fe667  C[0]=dcc97b7c  D[0]=70a88018
A[1]=9586624e  B[1]=f359e72e  C[1]=6f74519f  D[1]=be3d5a6b
A[2]=e8159675  B[2]=5c66ddfd  C[2]=cae15fe8  D[2]=f4ec31a6
A[3]=8b28e3f9  B[3]=7c303785  C[3]=622a06de  D[3]=ae075ad3
A[4]=8399ad25  B[4]=06795236  C[4]=2dc500ca  D[4]=20b4aa99
A[5]=adf15227  B[5]=d09894a2  C[5]=fc5256d5  D[5]=1038df52
A[6]=0a7c1f0f  B[6]=851851e2  C[6]=6837c2e9  D[6]=57674865
A[7]=3768fdad  B[7]=3e30684d  C[7]=3c4fe13d  D[7]=7cc374ce

IV XOR M :
A[0]=3e7c22f5  B[0]=a67fe667  C[0]=dcc97b7c  D[0]=70a88018
A[1]=95789db1  B[1]=f359e72e  C[1]=6f74519f  D[1]=be3d5a6b
A[2]=e8159675  B[2]=5c66ddfd  C[2]=cae15fe8  D[2]=f4ec31a6
A[3]=8b28e3f9  B[3]=7c303785  C[3]=622a06de  D[3]=ae075ad3
A[4]=8399ad25  B[4]=06795236  C[4]=2dc500ca  D[4]=20b4aa99
A[5]=adf15227  B[5]=d09894a2  C[5]=fc5256d5  D[5]=1038df52
A[6]=0a7c1f0f  B[6]=851851e2  C[6]=6837c2e9  D[6]=57674865
A[7]=3768fdad  B[7]=3e30684d  C[7]=3c4fe13d  D[7]=7cc374ce

Step  0: (r= 3, s=20)
A[0]=44a8ea69  B[0]=f3e117a9  C[0]=a67fe667  D[0]=dcc97b7c
A[1]=71be45ff  B[1]=abc4ed8c  C[1]=f359e72e  D[1]=6f74519f
A[2]=05f97ca1  B[2]=40acb3af  C[2]=5c66ddfd  D[2]=cae15fe8
A[3]=5f9d0c64  B[3]=59471fcc  C[3]=7c303785  D[3]=622a06de
A[4]=b79b1545  B[4]=1ccd692c  C[4]=06795236  D[4]=2dc500ca
A[5]=a9ed0a90  B[5]=6f8a913d  C[5]=d09894a2  D[5]=fc5256d5
A[6]=1548dcb6  B[6]=53e0f878  C[6]=851851e2  D[6]=6837c2e9
A[7]=70473ba8  B[7]=bb47ed69  C[7]=3e30684d  D[7]=3c4fe13d

Step  1: (r=20, s=14)
```

```
A[0]=256c230a  B[0]=a6944a8e  C[0]=f3e117a9  D[0]=a67fe667
A[1]=05ee9337  B[1]=5ff71be4  C[1]=abc4ed8c  D[1]=f359e72e
A[2]=d7b8cdaa  B[2]=ca105f97  C[2]=40acb3af  D[2]=5c66ddfd
A[3]=0157c9dd  B[3]=c645f9d0  C[3]=59471fcc  D[3]=7c303785
A[4]=e6dbf409  B[4]=545b79b1  C[4]=1ccd692c  D[4]=06795236
A[5]=9f3e64d1  B[5]=a90a9ed0  C[5]=6f8a913d  D[5]=d09894a2
A[6]=bc876f95  B[6]=cb61548d  C[6]=53e0f878  D[6]=851851e2
A[7]=f8d12d11  B[7]=ba870473  C[7]=bb47ed69  D[7]=3e30684d

Step  2: (r=14, s=27)
A[0]=f1594dcb  B[0]=08c2895b  C[0]=a6944a8e  D[0]=f3e117a9
A[1]=dee007f3  B[1]=a4cdc17b  C[1]=5ff71be4  D[1]=abc4ed8c
A[2]=e789aa4d  B[2]=336ab5ee  C[2]=ca105f97  D[2]=40acb3af
A[3]=63bd509c  B[3]=f2774055  C[3]=c645f9d0  D[3]=59471fcc
A[4]=a39714f2  B[4]=fd0279b6  C[4]=545b79b1  D[4]=1ccd692c
A[5]=29ddb226  B[5]=993467cf  C[5]=a90a9ed0  D[5]=6f8a913d
A[6]=4021b381  B[6]=dbe56f21  C[6]=cb61548d  D[6]=53e0f878
A[7]=196c007f  B[7]=4b447e34  C[7]=ba870473  D[7]=bb47ed69

Step  3: (r=27, s= 3)
A[0]=9037a4b4  B[0]=5f8aca6e  C[0]=08c2895b  D[0]=a6944a8e
A[1]=ba0c75b1  B[1]=9ef7003f  C[1]=a4cdc17b  D[1]=5ff71be4
A[2]=8d66e4c9  B[2]=6f3c4d52  C[2]=336ab5ee  D[2]=ca105f97
A[3]=55c312b7  B[3]=e31dea84  C[3]=f2774055  D[3]=c645f9d0
A[4]=d6a7c1fc  B[4]=951cb8a7  C[4]=fd0279b6  D[4]=545b79b1
A[5]=fbf48d3e  B[5]=314eed91  C[5]=993467cf  D[5]=a90a9ed0
A[6]=16c1dc8b  B[6]=0a010d9c  C[6]=dbe56f21  D[6]=cb61548d
A[7]=8bf7bf59  B[7]=f8cb6003  C[7]=4b447e34  D[7]=ba870473

Step  4: (r= 3, s=20)
A[0]=063cf4ce  B[0]=81bd25a4  C[0]=5f8aca6e  D[0]=08c2895b
A[1]=c580d4e4  B[1]=d063ad8d  C[1]=9ef7003f  D[1]=a4cdc17b
A[2]=7636b01f  B[2]=6b37264c  C[2]=6f3c4d52  D[2]=336ab5ee
A[3]=9b3d603f  B[3]=ae1895ba  C[3]=e31dea84  D[3]=f2774055
A[4]=7e32b5ae  B[4]=b53e0fe6  C[4]=951cb8a7  D[4]=fd0279b6
A[5]=0c038a73  B[5]=dfa469f7  C[5]=314eed91  D[5]=993467cf
A[6]=e41dfd42  B[6]=b60ee458  C[6]=0a010d9c  D[6]=dbe56f21
A[7]=64344293  B[7]=5fbdfacc  C[7]=f8cb6003  D[7]=4b447e34

Step  5: (r=20, s=14)
A[0]=ef0ff6b7  B[0]=4ce063cf  C[0]=81bd25a4  D[0]=5f8aca6e
A[1]=5cec1751  B[1]=4e4c580d  C[1]=d063ad8d  D[1]=9ef7003f
A[2]=6e21faf1  B[2]=01f7636b  C[2]=6b37264c  D[2]=6f3c4d52
A[3]=275e74f7  B[3]=03f9b3d6  C[3]=ae1895ba  D[3]=e31dea84
A[4]=de969c02  B[4]=5ae7e32b  C[4]=b53e0fe6  D[4]=951cb8a7
A[5]=b9ad7fa3  B[5]=a730c038  C[5]=dfa469f7  D[5]=314eed91
A[6]=6a9df197  B[6]=d42e41df  C[6]=b60ee458  D[6]=0a010d9c
A[7]=6b794530  B[7]=29364344  C[7]=5fbdfacc  D[7]=f8cb6003
```

```
Step  6: (r=14, s=27)
A[0]=ad547ebc  B[0]=fdadfbc3  C[0]=4ce063cf  D[0]=81bd25a4
A[1]=fe4382ef  B[1]=05d4573b  C[1]=4e4c580d  D[1]=d063ad8d
A[2]=458461f1  B[2]=7ebc5b88  C[2]=01f7636b  D[2]=6b37264c
A[3]=ff5ffdf2  B[3]=9d3dc9d7  C[3]=03f9b3d6  D[3]=ae1895ba
A[4]=4fb591aa  B[4]=a700b7a5  C[4]=5ae7e32b  D[4]=b53e0fe6
A[5]=1fcd1bba  B[5]=5fe8ee6b  C[5]=a730c038  D[5]=dfa469f7
A[6]=57ffdcb4  B[6]=7c65daa7  C[6]=d42e41df  D[6]=b60ee458
A[7]=b73f5939  B[7]=514c1ade  C[7]=29364344  D[7]=5fbdfacc

Step  7: (r=27, s= 3)
A[0]=b4444147  B[0]=e56aa3f5  C[0]=fdadfbc3  D[0]=4ce063cf
A[1]=c3b7a4bb  B[1]=7ff21c17  C[1]=05d4573b  D[1]=4e4c580d
A[2]=3186f4f9  B[2]=8a2c230f  C[2]=7ebc5b88  D[2]=01f7636b
A[3]=d348740e  B[3]=97faffef  C[3]=9d3dc9d7  D[3]=03f9b3d6
A[4]=5d7abd3d  B[4]=527dac8d  C[4]=a700b7a5  D[4]=5ae7e32b
A[5]=70cd5256  B[5]=d0fe68dd  C[5]=5fe8ee6b  D[5]=a730c038
A[6]=b75025ee  B[6]=a2bffee5  C[6]=7c65daa7  D[6]=d42e41df
A[7]=29d3b474  B[7]=cdb9fac9  C[7]=514c1ade  D[7]=29364344

Step  8: (r=26, s= 4)
A[0]=51809278  B[0]=1ed11105  C[0]=e56aa3f5  D[0]=fdadfbc3
A[1]=2cfba691  B[1]=ef0ede92  C[1]=7ff21c17  D[1]=05d4573b
A[2]=5269dfe7  B[2]=e4c61bd3  C[2]=8a2c230f  D[2]=7ebc5b88
A[3]=00156a79  B[3]=3b4d21d0  C[3]=97faffef  D[3]=9d3dc9d7
A[4]=6b48a83d  B[4]=f575eaf4  C[4]=527dac8d  D[4]=a700b7a5
A[5]=1d201467  B[5]=59c33549  C[5]=d0fe68dd  D[5]=5fe8ee6b
A[6]=d180d222  B[6]=badd4097  C[6]=a2bffee5  D[6]=7c65daa7
A[7]=98cf6f2d  B[7]=d0a74ed1  C[7]=cdb9fac9  D[7]=514c1ade

Step  9: (r= 4, s=23)
A[0]=4e1ead74  B[0]=18092785  C[0]=1ed11105  D[0]=e56aa3f5
A[1]=a28d2ab6  B[1]=cfba6912  C[1]=ef0ede92  D[1]=7ff21c17
A[2]=aa27f5c2  B[2]=269dfe75  C[2]=e4c61bd3  D[2]=8a2c230f
A[3]=70589ce4  B[3]=0156a790  C[3]=3b4d21d0  D[3]=97faffef
A[4]=78b0213f  B[4]=b48a83d6  C[4]=f575eaf4  D[4]=527dac8d
A[5]=f7988969  B[5]=d2014671  C[5]=59c33549  D[5]=d0fe68dd
A[6]=6dbde906  B[6]=180d222d  C[6]=badd4097  D[6]=a2bffee5
A[7]=5a74a019  B[7]=8cf6f2d9  C[7]=d0a74ed1  D[7]=cdb9fac9

Step 10: (r=23, s=11)
A[0]=dc90594e  B[0]=ba270f56  C[0]=18092785  D[0]=1ed11105
A[1]=22e2a8d9  B[1]=5b514695  C[1]=cfba6912  D[1]=ef0ede92
A[2]=f7acd9c3  B[2]=e15513fa  C[2]=269dfe75  D[2]=e4c61bd3
A[3]=c2c31d6a  B[3]=72382c4e  C[3]=0156a790  D[3]=3b4d21d0
A[4]=600394c9  B[4]=9fbc5810  C[4]=b48a83d6  D[4]=f575eaf4
A[5]=44933931  B[5]=b4fbcc44  C[5]=d2014671  D[5]=59c33549
A[6]=a974ae3b  B[6]=8336def4  C[6]=180d222d  D[6]=badd4097
A[7]=3f1adf78  B[7]=0cad3a50  C[7]=8cf6f2d9  D[7]=d0a74ed1
```

```
Step 11: (r=11, s=26)
A[0]=be6c37f7  B[0]=82ca76e4  C[0]=ba270f56  D[0]=18092785
A[1]=6de1538b  B[1]=1546c917  C[1]=5b514695  D[1]=cfba6912
A[2]=98abfb72  B[2]=66ce1fbd  C[2]=e15513fa  D[2]=269dfe75
A[3]=797479bf  B[3]=18eb5616  C[3]=72382c4e  D[3]=0156a790
A[4]=90b89edf  B[4]=1ca64b00  C[4]=9fbc5810  D[4]=b48a83d6
A[5]=ed4aa2a8  B[5]=99c98a24  C[5]=b4fbcc44  D[5]=d2014671
A[6]=38d7583e  B[6]=a571dd4b  C[6]=8336def4  D[6]=180d222d
A[7]=3f96f324  B[7]=d6fbc1f8  C[7]=0cad3a50  D[7]=8cf6f2d9

Step 12: (r=26, s= 4)
A[0]=cdec7e9f  B[0]=def9b0df  C[0]=82ca76e4  D[0]=ba270f56
A[1]=ab45572c  B[1]=2db7854e  C[1]=1546c917  D[1]=5b514695
A[2]=06376d4a  B[2]=ca62afed  C[2]=66ce1fbd  D[2]=e15513fa
A[3]=30f4f669  B[3]=fde5d1e6  C[3]=18eb5616  D[3]=72382c4e
A[4]=d45e0583  B[4]=7e42e27b  C[4]=1ca64b00  D[4]=9fbc5810
A[5]=8330f5bf  B[5]=a3b52a8a  C[5]=99c98a24  D[5]=b4fbcc44
A[6]=d04383bc  B[6]=f8e35d60  C[6]=a571dd4b  D[6]=8336def4
A[7]=6b8e9895  B[7]=90fe5bcc  C[7]=d6fbc1f8  D[7]=0cad3a50

Step 13: (r= 4, s=23)
A[0]=8b105d5b  B[0]=dec7e9fc  C[0]=def9b0df  D[0]=82ca76e4
A[1]=46946c77  B[1]=b45572ca  C[1]=2db7854e  D[1]=1546c917
A[2]=03ff8d9c  B[2]=6376d4a0  C[2]=ca62afed  D[2]=66ce1fbd
A[3]=f231df79  B[3]=0f4f6693  C[3]=fde5d1e6  D[3]=18eb5616
A[4]=8fd381a7  B[4]=45e0583d  C[4]=7e42e27b  D[4]=1ca64b00
A[5]=02dd6820  B[5]=330f5bf8  C[5]=a3b52a8a  D[5]=99c98a24
A[6]=428e391c  B[6]=04383bcd  C[6]=f8e35d60  D[6]=a571dd4b
A[7]=226c0b99  B[7]=b8e98956  C[7]=90fe5bcc  D[7]=d6fbc1f8

Step 14: (r=23, s=11)
A[0]=8efc080d  B[0]=adc5882e  C[0]=dec7e9fc  D[0]=def9b0df
A[1]=66f62710  B[1]=3ba34a36  C[1]=b45572ca  D[1]=2db7854e
A[2]=6c4ba9a1  B[2]=ce01ffc6  C[2]=6376d4a0  D[2]=ca62afed
A[3]=275d6a88  B[3]=bcf918ef  C[3]=0f4f6693  D[3]=fde5d1e6
A[4]=ccc28e4f  B[4]=d3c7e9c0  C[4]=45e0583d  D[4]=7e42e27b
A[5]=abbcfe24  B[5]=10016eb4  C[5]=330f5bf8  D[5]=a3b52a8a
A[6]=568e92d3  B[6]=8e21471c  C[6]=04383bcd  D[6]=f8e35d60
A[7]=6dda3582  B[7]=cc913605  C[7]=b8e98956  D[7]=90fe5bcc

Step 15: (r=11, s=26)
A[0]=b38a273e  B[0]=e0406c77  C[0]=adc5882e  D[0]=dec7e9fc
A[1]=6552c027  B[1]=b1388337  C[1]=3ba34a36  D[1]=b45572ca
A[2]=5979381a  B[2]=5d4d0b62  C[2]=ce01ffc6  D[2]=6376d4a0
A[3]=dd260ca8  B[3]=eb54413a  C[3]=bcf918ef  D[3]=0f4f6693
A[4]=b6775c17  B[4]=14727e66  C[4]=d3c7e9c0  D[4]=45e0583d
A[5]=974a06cb  B[5]=e7f1255d  C[5]=10016eb4  D[5]=330f5bf8
A[6]=edff5639  B[6]=74969ab4  C[6]=8e21471c  D[6]=04383bcd
```

```
A[7]=e562c058  B[7]=d1ac136e  C[7]=cc913605  D[7]=b8e98956

Step 16: (r=19, s=28)
A[0]=68aba7d7  B[0]=39f59c51  C[0]=e0406c77  D[0]=adc5882e
A[1]=3a0abf42  B[1]=013b2a96  C[1]=b1388337  D[1]=3ba34a36
A[2]=99646a1e  B[2]=c0d2cbc9  C[2]=5d4d0b62  D[2]=ce01ffc6
A[3]=7074283a  B[3]=6546e930  C[3]=eb54413a  D[3]=bcf918ef
A[4]=e9c984b1  B[4]=e0bdb3ba  C[4]=14727e66  D[4]=d3c7e9c0
A[5]=9db1b43c  B[5]=365cba50  C[5]=e7f1255d  D[5]=10016eb4
A[6]=e00d5b3e  B[6]=b1cf6ffa  C[6]=74969ab4  D[6]=8e21471c
A[7]=65fdc6f2  B[7]=02c72b16  C[7]=d1ac136e  D[7]=cc913605

Step 17: (r=28, s= 7)
A[0]=f0e572b6  B[0]=768aba7d  C[0]=39f59c51  D[0]=e0406c77
A[1]=410b51d5  B[1]=23a0abf4  C[1]=013b2a96  D[1]=b1388337
A[2]=db3b3daf  B[2]=e99646a1  C[2]=c0d2cbc9  D[2]=5d4d0b62
A[3]=7e55e6f3  B[3]=a7074283  C[3]=6546e930  D[3]=eb54413a
A[4]=cfc86a0b  B[4]=1e9c984b  C[4]=e0bdb3ba  D[4]=14727e66
A[5]=a166c50b  B[5]=c9db1b43  C[5]=365cba50  D[5]=e7f1255d
A[6]=1859e498  B[6]=ee00d5b3  C[6]=b1cf6ffa  D[6]=74969ab4
A[7]=adada392  B[7]=265fdc6f  C[7]=02c72b16  D[7]=d1ac136e

Step 18: (r= 7, s=22)
A[0]=d226e034  B[0]=72b95b78  C[0]=768aba7d  D[0]=39f59c51
A[1]=f39d145b  B[1]=85a8eaa0  C[1]=23a0abf4  D[1]=013b2a96
A[2]=8c3fa50b  B[2]=9d9ed7ed  C[2]=e99646a1  D[2]=c0d2cbc9
A[3]=1e4ec647  B[3]=2af379bf  C[3]=a7074283  D[3]=6546e930
A[4]=3fb1d787  B[4]=e43505e7  C[4]=1e9c984b  D[4]=e0bdb3ba
A[5]=c4fb7b5c  B[5]=b36285d0  C[5]=c9db1b43  D[5]=365cba50
A[6]=fb4bfa68  B[6]=2cf24c0c  C[6]=ee00d5b3  D[6]=b1cf6ffa
A[7]=0f42f530  B[7]=d6d1c956  C[7]=265fdc6f  D[7]=02c72b16

Step 19: (r=22, s=19)
A[0]=41eed633  B[0]=0d3489b8  C[0]=72b95b78  D[0]=768aba7d
A[1]=6123f87f  B[1]=16fce745  C[1]=85a8eaa0  D[1]=23a0abf4
A[2]=2b165a15  B[2]=42e30fe9  C[2]=9d9ed7ed  D[2]=e99646a1
A[3]=b1e9a15c  B[3]=91c793b1  C[3]=2af379bf  D[3]=a7074283
A[4]=904f40e4  B[4]=e1cfec75  C[4]=e43505e7  D[4]=1e9c984b
A[5]=4800ca6e  B[5]=d7313ede  C[5]=b36285d0  D[5]=c9db1b43
A[6]=7bd66b0c  B[6]=9a3ed2fe  C[6]=2cf24c0c  D[6]=ee00d5b3
A[7]=a8cde79a  B[7]=4c03d0bd  C[7]=d6d1c956  D[7]=265fdc6f

Step 20: (r=19, s=28)
A[0]=5f4550e2  B[0]=b19a0f76  C[0]=0d3489b8  D[0]=72b95b78
A[1]=c007a440  B[1]=c3fb091f  C[1]=16fce745  D[1]=85a8eaa0
A[2]=c39f239f  B[2]=d0a958b2  C[2]=42e30fe9  D[2]=9d9ed7ed
A[3]=c7a41ce8  B[3]=0ae58f4d  C[3]=91c793b1  D[3]=2af379bf
A[4]=f836d125  B[4]=0724827a  C[4]=e1cfec75  D[4]=e43505e7
A[5]=85acf62b  B[5]=53724006  C[5]=d7313ede  D[5]=b36285d0
```

```
A[6]=94cc28c2  B[6]=5863deb3  C[6]=9a3ed2fe  D[6]=2cf24c0c
A[7]=2be8c7aa  B[7]=3cd5466f  C[7]=4c03d0bd  D[7]=d6d1c956

Step 21: (r=28, s= 7)
A[0]=e018cbf6  B[0]=25f4550e  C[0]=b19a0f76  D[0]=0d3489b8
A[1]=8e54dd48  B[1]=0c007a44  C[1]=c3fb091f  D[1]=16fce745
A[2]=04b0763b  B[2]=fc39f239  C[2]=d0a958b2  D[2]=42e30fe9
A[3]=4437a0d5  B[3]=8c7a41ce  C[3]=0ae58f4d  D[3]=91c793b1
A[4]=39a74b7f  B[4]=5f836d12  C[4]=0724827a  D[4]=e1cfec75
A[5]=953278d1  B[5]=b85acf62  C[5]=53724006  D[5]=d7313ede
A[6]=570443f6  B[6]=294cc28c  C[6]=5863deb3  D[6]=9a3ed2fe
A[7]=8b414f81  B[7]=a2be8c7a  C[7]=3cd5466f  D[7]=4c03d0bd

Step 22: (r= 7, s=22)
A[0]=bcd28b38  B[0]=0c65fb70  C[0]=25f4550e  D[0]=b19a0f76
A[1]=881d82a3  B[1]=2a6ea447  C[1]=0c007a44  D[1]=c3fb091f
A[2]=cf9360e6  B[2]=583b1d82  C[2]=fc39f239  D[2]=d0a958b2
A[3]=c517c70e  B[3]=1bd06aa2  C[3]=8c7a41ce  D[3]=0ae58f4d
A[4]=925102de  B[4]=d3a5bf9c  C[4]=5f836d12  D[4]=0724827a
A[5]=404b7dc0  B[5]=993c68ca  C[5]=b85acf62  D[5]=53724006
A[6]=c8853b74  B[6]=8221fb2b  C[6]=294cc28c  D[6]=5863deb3
A[7]=158d9fa1  B[7]=a0a7c0c5  C[7]=a2be8c7a  D[7]=3cd5466f

Step 23: (r=22, s=19)
A[0]=f3c9af72  B[0]=ce2f34a2  C[0]=0c65fb70  D[0]=25f4550e
A[1]=ff61e42b  B[1]=a8e20760  C[1]=2a6ea447  D[1]=0c007a44
A[2]=ae5e6c81  B[2]=39b3e4d8  C[2]=583b1d82  D[2]=fc39f239
A[3]=1e2b9fc7  B[3]=c3b145f1  C[3]=1bd06aa2  D[3]=8c7a41ce
A[4]=53db8914  B[4]=b7a49440  C[4]=d3a5bf9c  D[4]=5f836d12
A[5]=e7a677d2  B[5]=701012df  C[5]=993c68ca  D[5]=b85acf62
A[6]=80a3ee4c  B[6]=dd32214e  C[6]=8221fb2b  D[6]=294cc28c
A[7]=d2b3a320  B[7]=e8456367  C[7]=a0a7c0c5  D[7]=a2be8c7a

Step 24: (r=15, s= 5)
A[0]=579b6f3c  B[0]=d7b979e4  C[0]=ce2f34a2  D[0]=0c65fb70
A[1]=76764738  B[1]=f215ffb0  C[1]=a8e20760  D[1]=2a6ea447
A[2]=5dace283  B[2]=3640d72f  C[2]=39b3e4d8  D[2]=583b1d82
A[3]=dd3039f4  B[3]=cfe38f15  C[3]=c3b145f1  D[3]=1bd06aa2
A[4]=3bb73b5c  B[4]=c48a29ed  C[4]=b7a49440  D[4]=d3a5bf9c
A[5]=daa94386  B[5]=3be973d3  C[5]=701012df  D[5]=993c68ca
A[6]=6a698ff5  B[6]=f7264051  C[6]=dd32214e  D[6]=8221fb2b
A[7]=38b9f1e2  B[7]=d1906959  C[7]=e8456367  D[7]=a0a7c0c5

Step 25: (r= 5, s=29)
A[0]=0834c4f8  B[0]=f36de78a  C[0]=d7b979e4  D[0]=ce2f34a2
A[1]=d5eb1160  B[1]=cec8e70e  C[1]=f215ffb0  D[1]=a8e20760
A[2]=265556d3  B[2]=b59c506b  C[2]=3640d72f  D[2]=39b3e4d8
A[3]=31389e79  B[3]=a6073e9b  C[3]=cfe38f15  D[3]=c3b145f1
A[4]=75f0a264  B[4]=76e76b87  C[4]=c48a29ed  D[4]=b7a49440
```

```
A[5]=545ad70b  B[5]=552870db  C[5]=3be973d3  D[5]=701012df
A[6]=ce9a5310  B[6]=4d31fead  C[6]=f7264051  D[6]=dd32214e
A[7]=6f8459af  B[7]=173e3c47  C[7]=d1906959  D[7]=e8456367

Step 26: (r=29, s= 9)
A[0]=dffbb734  B[0]=0106989f  C[0]=f36de78a  D[0]=d7b979e4
A[1]=8b1f28b7  B[1]=1abd622c  C[1]=cec8e70e  D[1]=f215ffb0
A[2]=cba9a44c  B[2]=64caaada  C[2]=b59c506b  D[2]=3640d72f
A[3]=6c598671  B[3]=262713cf  C[3]=a6073e9b  D[3]=cfe38f15
A[4]=e9c02bcd  B[4]=8ebe144c  C[4]=76e76b87  D[4]=c48a29ed
A[5]=9dce7bf1  B[5]=6a8b5ae1  C[5]=552870db  D[5]=3be973d3
A[6]=6747ab9c  B[6]=19d34a62  C[6]=4d31fead  D[6]=f7264051
A[7]=ba91d0c8  B[7]=edf08b35  C[7]=173e3c47  D[7]=d1906959

Step 27: (r= 9, s=15)
A[0]=0abf3381  B[0]=f76e69bf  C[0]=0106989f  D[0]=f36de78a
A[1]=22259e8e  B[1]=3e516f16  C[1]=1abd622c  D[1]=cec8e70e
A[2]=e420232c  B[2]=53489997  C[2]=64caaada  D[2]=b59c506b
A[3]=526a2301  B[3]=b30ce2d8  C[3]=262713cf  D[3]=a6073e9b
A[4]=8150939b  B[4]=80579bd3  C[4]=8ebe144c  D[4]=76e76b87
A[5]=9edd4cae  B[5]=9cf7e33b  C[5]=6a8b5ae1  D[5]=552870db
A[6]=b2e3cd50  B[6]=8f5738ce  C[6]=19d34a62  D[6]=4d31fead
A[7]=1f3f954d  B[7]=23a19175  C[7]=edf08b35  D[7]=173e3c47

Step 28: (r=15, s= 5)
A[0]=097868bd  B[0]=99c0855f  C[0]=f76e69bf  D[0]=0106989f
A[1]=f875491c  B[1]=cf471112  C[1]=3e516f16  D[1]=1abd622c
A[2]=d39a0596  B[2]=11967210  C[2]=53489997  D[2]=64caaada
A[3]=3b82f8ec  B[3]=1180a935  C[3]=b30ce2d8  D[3]=262713cf
A[4]=b9116e54  B[4]=49cdc0a8  C[4]=80579bd3  D[4]=8ebe144c
A[5]=456cee07  B[5]=a6574f6e  C[5]=9cf7e33b  D[5]=6a8b5ae1
A[6]=adfa5984  B[6]=e6a85971  C[6]=8f5738ce  D[6]=19d34a62
A[7]=a49a376f  B[7]=caa68f9f  C[7]=23a19175  D[7]=edf08b35

Step 29: (r= 5, s=29)
A[0]=b904bcb4  B[0]=2f0d17a1  C[0]=99c0855f  D[0]=f76e69bf
A[1]=33bbb61e  B[1]=0ea9239f  C[1]=cf471112  D[1]=3e516f16
A[2]=115d2425  B[2]=7340b2da  C[2]=11967210  D[2]=53489997
A[3]=3c079c9f  B[3]=705f1d87  C[3]=1180a935  D[3]=b30ce2d8
A[4]=8b84e0dd  B[4]=222dca97  C[4]=49cdc0a8  D[4]=80579bd3
A[5]=e469608a  B[5]=ad9dc0e8  C[5]=a6574f6e  D[5]=9cf7e33b
A[6]=77a673bb  B[6]=bf4b3095  C[6]=e6a85971  D[6]=8f5738ce
A[7]=59a89130  B[7]=9346edf4  C[7]=caa68f9f  D[7]=23a19175

Step 30: (r=29, s= 9)
A[0]=7ef7e93a  B[0]=97209796  C[0]=2f0d17a1  D[0]=99c0855f
A[1]=1478ece3  B[1]=c67776c3  C[1]=0ea9239f  D[1]=cf471112
A[2]=c3e2f236  B[2]=a22ba484  C[2]=7340b2da  D[2]=11967210
A[3]=e2479df5  B[3]=e780f393  C[3]=705f1d87  D[3]=1180a935
```

```
A[4]=e78770bd  B[4]=b1709c1b  C[4]=222dca97  D[4]=49cdc0a8
A[5]=60b3a4fb  B[5]=5c8d2c11  C[5]=ad9dc0e8  D[5]=a6574f6e
A[6]=c2a8b71a  B[6]=6ef4ce77  C[6]=bf4b3095  D[6]=e6a85971
A[7]=a4847ac5  B[7]=0b351226  C[7]=9346edf4  D[7]=caa68f9f

Step 31: (r= 9, s=15)
A[0]=f81953c7  B[0]=efd274fd  C[0]=97209796  D[0]=2f0d17a1
A[1]=0eba3c50  B[1]=f1d9c628  C[1]=c67776c3  D[1]=0ea9239f
A[2]=0efcffc4  B[2]=c5e46d87  C[2]=a22ba484  D[2]=7340b2da
A[3]=dc2485a1  B[3]=8f3bebc4  C[3]=e780f393  D[3]=705f1d87
A[4]=12239383  B[4]=0ee17bcf  C[4]=b1709c1b  D[4]=222dca97
A[5]=e3dc58bc  B[5]=6749f6c1  C[5]=5c8d2c11  D[5]=ad9dc0e8
A[6]=db4f74fb  B[6]=516e3585  C[6]=6ef4ce77  D[6]=bf4b3095
A[7]=45a3a871  B[7]=08f58b49  C[7]=0b351226  D[7]=9346edf4

Feistel Step 0: (r=15, s= 5)
A[0]=16613778  B[0]=a9e3fc0c  C[0]=efd274fd  D[0]=97209796
A[1]=4b7d8a18  B[1]=1e28075d  C[1]=f1d9c628  D[1]=c67776c3
A[2]=4a87c872  B[2]=7fe2077e  C[2]=c5e46d87  D[2]=a22ba484
A[3]=e500a9d3  B[3]=42d0ee12  C[3]=8f3bebc4  D[3]=e780f393
A[4]=53715cd7  B[4]=c9c18911  C[4]=0ee17bcf  D[4]=b1709c1b
A[5]=24d27b2c  B[5]=2c5e71ee  C[5]=6749f6c1  D[5]=5c8d2c11
A[6]=ccfa67f8  B[6]=ba7deda7  C[6]=516e3585  D[6]=6ef4ce77
A[7]=672eaac1  B[7]=d438a2d1  C[7]=08f58b49  D[7]=0b351226

Feistel Step 1: (r= 5, s=29)
A[0]=95eb8c9a  B[0]=cc26ef02  C[0]=a9e3fc0c  D[0]=efd274fd
A[1]=cea46f01  B[1]=6fb14309  C[1]=1e28075d  D[1]=f1d9c628
A[2]=e5f58411  B[2]=50f90e49  C[2]=7fe2077e  D[2]=c5e46d87
A[3]=456ee5ae  B[3]=a0153a7c  C[3]=42d0ee12  D[3]=8f3bebc4
A[4]=e0026246  B[4]=6e2b9aea  C[4]=c9c18911  D[4]=0ee17bcf
A[5]=f8658f00  B[5]=9a4f6584  C[5]=2c5e71ee  D[5]=6749f6c1
A[6]=3fdccda9  B[6]=9f4cff19  C[6]=ba7deda7  D[6]=516e3585
A[7]=2d1b494b  B[7]=e5d5582c  C[7]=d438a2d1  D[7]=08f58b49

Feistel Step 2: (r=29, s= 9)
A[0]=e37c681a  B[0]=52bd7193  C[0]=cc26ef02  D[0]=a9e3fc0c
A[1]=14b1e334  B[1]=39d48de0  C[1]=6fb14309  D[1]=1e28075d
A[2]=90b66fb7  B[2]=3cbeb082  C[2]=50f90e49  D[2]=7fe2077e
A[3]=d03a0a2f  B[3]=c8addcb5  C[3]=a0153a7c  D[3]=42d0ee12
A[4]=9cbdb601  B[4]=dc004c48  C[4]=6e2b9aea  D[4]=c9c18911
A[5]=3445ba81  B[5]=1f0cb1e0  C[5]=9a4f6584  D[5]=2c5e71ee
A[6]=619f8892  B[6]=27fb99b5  C[6]=9f4cff19  D[6]=ba7deda7
A[7]=416bae07  B[7]=65a36929  C[7]=e5d5582c  D[7]=d438a2d1

Feistel Step 3: (r= 9, s=15)
A[0]=2d07379e  B[0]=f8d035c6  C[0]=52bd7193  D[0]=cc26ef02
A[1]=7cedae62  B[1]=63c66829  C[1]=39d48de0  D[1]=6fb14309
A[2]=ec0887a9  B[2]=6cdf6f21  C[2]=3cbeb082  D[2]=50f90e49
```

```
A[3]=98097704  B[3]=74145fa0  C[3]=c8addcb5  D[3]=a0153a7c
A[4]=191aaa02  B[4]=7b6c0339  C[4]=dc004c48  D[4]=6e2b9aea
A[5]=8728d57c  B[5]=8b750268  C[5]=1f0cb1e0  D[5]=9a4f6584
A[6]=07b25801  B[6]=3f1124c3  C[6]=27fb99b5  D[6]=9f4cff19
A[7]=3bf87af9  B[7]=d75c0e82  C[7]=65a36929  D[7]=e5d5582c
```

Compression Function Output

```
A[0]=2d07379e  B[0]=f8d035c6  C[0]=52bd7193  D[0]=cc26ef02
A[1]=7cedae62  B[1]=63c66829  C[1]=39d48de0  D[1]=6fb14309
A[2]=ec0887a9  B[2]=6cdf6f21  C[2]=3cbeb082  D[2]=50f90e49
A[3]=98097704  B[3]=74145fa0  C[3]=c8addcb5  D[3]=a0153a7c
A[4]=191aaa02  B[4]=7b6c0339  C[4]=dc004c48  D[4]=6e2b9aea
A[5]=8728d57c  B[5]=8b750268  C[5]=1f0cb1e0  D[5]=9a4f6584
A[6]=07b25801  B[6]=3f1124c3  C[6]=27fb99b5  D[6]=9f4cff19
A[7]=3bf87af9  B[7]=d75c0e82  C[7]=65a36929  D[7]=e5d5582c
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   61  165  253   25  100  103   38  217
y[  8.. 15] =   83  222  217   81  155  191  230   68
y[ 16.. 23] =  160   84  131  211  120  256   67  256
y[ 24.. 31] =   70  153   56  134  184   54   47  116
y[ 32.. 39] =    3  142  144  243   16   32   20   71
y[ 40.. 47] =   63   73  194  216  243  207  172  210
y[ 48.. 55] =  183  243   53   83  146   42  138  255
y[ 56.. 63] =  108  123  230   72  215  135    9   14
y[ 64.. 71] =  119  197   87   94   48   28  240   38
y[ 72.. 79] =   57  190   59  107  148  226  117  121
y[ 80.. 87] =  177  224  217  112   89  175   90   39
y[ 88.. 95] =   72  226   62  109  209  193  100  189
```

```
y[ 96..103] =  243  143  181  173  213  195   59  237
y[104..111] =  200   30   90  227   52  251   86   58
y[112..119] =   43   98  145   86  103  101  123  134
y[120..127] =   12   87   90  153  210  217   69   88
y[128..135] =   49  202  114   85   10    7   72  150
y[136..143] =   27  145  150   29  212  176  137   42
y[144..151] =  207   26  236  156  247  111   43  111
y[152..159] =   40  214   54  233  183   56   63  251
y[160..167] =  107  225  223  124   94   78   90   39
y[168..175] =   47   37  173  151  124  160  195  157
y[176..183] =  184  124   57   27  221   68  229  112
y[184..191] =    2  244  137   38  152  232  101   96
y[192..199] =  248  170   23   16   62   82  127   72
y[200..207] =   53  177   51    3  219  141  250  246
y[208..215] =  190  143  150  255   21  192   20   71
y[216..223] =   38  141   48    1  158  174   10  178
y[224..231] =  124  224  186  194  154  172   51  130
y[232..239] =  167   80   20  140   58  116   24   52
y[240..247] =   67   12  222   24    7    9  244  233
y[248..255] =   98   23   20  214  157  150   41   22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
```

```
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
Z[17] = d27ea7b7  ece38d52  f6e66d38  27233cfb
        24683fb6  312632f8  bca6bd8f  39572ac7
Z[18] = 616302bb  e10e9927  558e0e90  51ea1234
        2ac73957  b38cc6a9  70dcf342  c792b2a3
Z[19] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
Z[20] = f7cf6c4f  14ef4f2f  386e2bb0  7397f087
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
Z[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
Z[22] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
Z[23] = 3cfb2723  e0259a10  065f5dbf  f42b6ff3
        59320aec  123451ea  a4fcd539  25513ecd
Z[24] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
Z[25] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
Z[26] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
Z[27] = 70dcf342  18934b8b  3de4263a  65f0fe2e
        f42b6ff3  22964188  e93f90f6  57600cbe
Z[28] = b0d1c964  0e90558e  4aa2197c  41882296
        b730c305  02bb6163  966ce3c9  f5fd6e21
Z[29] = 983ee1f7  fe2e65f0  c4d7b55e  409f237f
        966ce3c9  00e96335  b475c5c0  b819c21c
Z[30] = e1f7983e  c6a9b38c  b2a3c792  8c69edcc
        48d01b4e  9583e4b2  6994fa8a  2f5434ca
Z[31] = 0aec5932  15d84e46  08315bed  ea28900d
        14ef4f2f  d8dda158  9e9ddb98  14065018
```

Expanded Message

```
W[ 0] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
W[ 1] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
```

```
W[ 4] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
W[10] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
W[12] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
W[15] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
W[16] = d27ea7b7  ece38d52  f6e66d38  27233cfb
        24683fb6  312632f8  bca6bd8f  39572ac7
W[17] = 616302bb  e10e9927  558e0e90  51ea1234
        2ac73957  b38cc6a9  70dcf342  c792b2a3
W[18] = 3cfb2723  e0259a10  065f5dbf  f42b6ff3
        59320aec  123451ea  a4fcd539  25513ecd
W[19] = f7cf6c4f  14ef4f2f  386e2bb0  7397f087
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
W[20] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
W[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
W[22] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
W[23] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
W[24] = e1f7983e  c6a9b38c  b2a3c792  8c69edcc
        48d01b4e  9583e4b2  6994fa8a  2f5434ca
W[25] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
W[26] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
W[27] = 0aec5932  15d84e46  08315bed  ea28900d
        14ef4f2f  d8dda158  9e9ddb98  14065018
W[28] = 70dcf342  18934b8b  3de4263a  65f0fe2e
```

```
        f42b6ff3  22964188  e93f90f6  57600cbe
W[29] = 983ee1f7  fe2e65f0  c4d7b55e  409f237f
        966ce3c9  00e96335  b475c5c0  b819c21c
W[30] = b0d1c964  0e90558e  4aa2197c  41882296
        b730c305  02bb6163  966ce3c9  f5fd6e21
W[31] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
```

Feistel Steps

```
IV :
A[0]=2d07379e  B[0]=f8d035c6  C[0]=52bd7193  D[0]=cc26ef02
A[1]=7cedae62  B[1]=63c66829  C[1]=39d48de0  D[1]=6fb14309
A[2]=ec0887a9  B[2]=6cdf6f21  C[2]=3cbeb082  D[2]=50f90e49
A[3]=98097704  B[3]=74145fa0  C[3]=c8addcb5  D[3]=a0153a7c
A[4]=191aaa02  B[4]=7b6c0339  C[4]=dc004c48  D[4]=6e2b9aea
A[5]=8728d57c  B[5]=8b750268  C[5]=1f0cb1e0  D[5]=9a4f6584
A[6]=07b25801  B[6]=3f1124c3  C[6]=27fb99b5  D[6]=9f4cff19
A[7]=3bf87af9  B[7]=d75c0e82  C[7]=65a36929  D[7]=e5d5582c

IV XOR M :
A[0]=2d0733a9  B[0]=f8d035c6  C[0]=52bd7193  D[0]=cc26ef02
A[1]=7cedae62  B[1]=63c66829  C[1]=39d48de0  D[1]=6fb14309
A[2]=ec0887a9  B[2]=6cdf6f21  C[2]=3cbeb082  D[2]=50f90e49
A[3]=98097704  B[3]=74145fa0  C[3]=c8addcb5  D[3]=a0153a7c
A[4]=191aaa02  B[4]=7b6c0339  C[4]=dc004c48  D[4]=6e2b9aea
A[5]=8728d57c  B[5]=8b750268  C[5]=1f0cb1e0  D[5]=9a4f6584
A[6]=07b25801  B[6]=3f1124c3  C[6]=27fb99b5  D[6]=9f4cff19
A[7]=3bf87af9  B[7]=d75c0e82  C[7]=65a36929  D[7]=e5d5582c

Step  0: (r= 3, s=20)
A[0]=509f2b4e  B[0]=68399d49  C[0]=f8d035c6  D[0]=52bd7193
A[1]=20baf483  B[1]=e76d7313  C[1]=63c66829  D[1]=39d48de0
A[2]=4219d75a  B[2]=60443d4f  C[2]=6cdf6f21  D[2]=3cbeb082
A[3]=3e85005f  B[3]=c04bb824  C[3]=74145fa0  D[3]=c8addcb5
A[4]=df785874  B[4]=c8d55010  C[4]=7b6c0339  D[4]=dc004c48
A[5]=d9cd7c7b  B[5]=3946abe4  C[5]=8b750268  D[5]=1f0cb1e0
A[6]=005edbcc  B[6]=3d92c008  C[6]=3f1124c3  D[6]=27fb99b5
A[7]=c12c0a23  B[7]=dfc3d7c9  C[7]=d75c0e82  D[7]=65a36929

Step  1: (r=20, s=14)
A[0]=d6f39bca  B[0]=b4e509f2  C[0]=68399d49  D[0]=f8d035c6
A[1]=79bbc073  B[1]=48320baf  C[1]=e76d7313  D[1]=63c66829
A[2]=a86d691f  B[2]=75a4219d  C[2]=60443d4f  D[2]=6cdf6f21
A[3]=21f14a41  B[3]=05f3e850  C[3]=c04bb824  D[3]=74145fa0
A[4]=9a4c3c6d  B[4]=874df785  C[4]=c8d55010  D[4]=7b6c0339
A[5]=698e9bf4  B[5]=c7bd9cd7  C[5]=3946abe4  D[5]=8b750268
A[6]=f0231033  B[6]=bcc005ed  C[6]=3d92c008  D[6]=3f1124c3
A[7]=3331b68e  B[7]=a23c12c0  C[7]=dfc3d7c9  D[7]=d75c0e82
```

```
Step  2: (r=14, s=27)
A[0]=613d7848  B[0]=e6f2b5bc  C[0]=b4e509f2  D[0]=68399d49
A[1]=062f70cb  B[1]=f01cde6e  C[1]=48320baf  D[1]=e76d7313
A[2]=b7b8b1c9  B[2]=5a47ea1b  C[2]=75a4219d  D[2]=60443d4f
A[3]=dfe4aa2e  B[3]=5290487c  C[3]=05f3e850  D[3]=c04bb824
A[4]=9bb83e16  B[4]=0f1b6693  C[4]=874df785  D[4]=c8d55010
A[5]=fb06470d  B[5]=a6fd1a63  C[5]=c7bd9cd7  D[5]=3946abe4
A[6]=a6846347  B[6]=c40cfc08  C[6]=bcc005ed  D[6]=3d92c008
A[7]=eeae5032  B[7]=6da38ccc  C[7]=a23c12c0  D[7]=dfc3d7c9

Step  3: (r=27, s= 3)
A[0]=05544b60  B[0]=4309ebc2  C[0]=e6f2b5bc  D[0]=b4e509f2
A[1]=9b3c18f9  B[1]=58317b86  C[1]=f01cde6e  D[1]=48320baf
A[2]=887b6b00  B[2]=4dbdc58e  C[2]=5a47ea1b  D[2]=75a4219d
A[3]=c8e5eb23  B[3]=76ff2551  C[3]=5290487c  D[3]=05f3e850
A[4]=aaad1512  B[4]=b4ddc1f0  C[4]=0f1b6693  D[4]=874df785
A[5]=6b52450c  B[5]=6fd83238  C[5]=a6fd1a63  D[5]=c7bd9cd7
A[6]=fb6e9a23  B[6]=3d34231a  C[6]=c40cfc08  D[6]=bcc005ed
A[7]=cafc0e32  B[7]=97757281  C[7]=6da38ccc  D[7]=a23c12c0

Step  4: (r= 3, s=20)
A[0]=2834f84d  B[0]=2aa25b00  C[0]=4309ebc2  D[0]=e6f2b5bc
A[1]=85784451  B[1]=d9e0c7cc  C[1]=58317b86  D[1]=f01cde6e
A[2]=b88fcb33  B[2]=43db5804  C[2]=4dbdc58e  D[2]=5a47ea1b
A[3]=ee1b586e  B[3]=472f591e  C[3]=76ff2551  D[3]=5290487c
A[4]=b6c97507  B[4]=5568a895  C[4]=b4ddc1f0  D[4]=0f1b6693
A[5]=56076f74  B[5]=5a922863  C[5]=6fd83238  D[5]=a6fd1a63
A[6]=37ea41ef  B[6]=db74d11f  C[6]=3d34231a  D[6]=c40cfc08
A[7]=0d4fedb4  B[7]=57e07196  C[7]=97757281  D[7]=6da38ccc

Step  5: (r=20, s=14)
A[0]=9106c74a  B[0]=84d2834f  C[0]=2aa25b00  D[0]=4309ebc2
A[1]=09416854  B[1]=45185784  C[1]=d9e0c7cc  D[1]=58317b86
A[2]=01af1d78  B[2]=b33b88fc  C[2]=43db5804  D[2]=4dbdc58e
A[3]=fdd18cc3  B[3]=86eee1b5  C[3]=472f591e  D[3]=76ff2551
A[4]=bdffaa03  B[4]=507b6c97  C[4]=5568a895  D[4]=b4ddc1f0
A[5]=f7a92a13  B[5]=f7456076  C[5]=5a922863  D[5]=6fd83238
A[6]=d71961e7  B[6]=1ef37ea4  C[6]=db74d11f  D[6]=3d34231a
A[7]=48ee756f  B[7]=db40d4fe  C[7]=57e07196  D[7]=97757281

Step  6: (r=14, s=27)
A[0]=33274e07  B[0]=b1d2a441  C[0]=84d2834f  D[0]=2aa25b00
A[1]=17655d12  B[1]=5a150250  C[1]=45185784  D[1]=d9e0c7cc
A[2]=e6039a58  B[2]=c75e006b  C[2]=b33b88fc  D[2]=43db5804
A[3]=346cdc46  B[3]=6330ff74  C[3]=86eee1b5  D[3]=472f591e
A[4]=fe4ae538  B[4]=ea80ef7f  C[4]=507b6c97  D[4]=5568a895
A[5]=0c3912a4  B[5]=4a84fdea  C[5]=f7456076  D[5]=5a922863
A[6]=9838e603  B[6]=5879f5c6  C[6]=1ef37ea4  D[6]=db74d11f
```

```
A[7]=b9be43b9  B[7]=9d5bd23b  C[7]=db40d4fe  D[7]=57e07196

Step  7: (r=27, s= 3)
A[0]=913f3099  B[0]=39993a70  C[0]=b1d2a441  D[0]=84d2834f
A[1]=9e27e705  B[1]=90bb2ae8  C[1]=5a150250  D[1]=45185784
A[2]=6eb380d1  B[2]=c7301cd2  C[2]=c75e006b  D[2]=b33b88fc
A[3]=34ea2a08  B[3]=31a366e2  C[3]=6330ff74  D[3]=86eee1b5
A[4]=5df77dc0  B[4]=c7f25729  C[4]=ea80ef7f  D[4]=507b6c97
A[5]=0e6138f2  B[5]=2061c895  C[5]=4a84fdea  D[5]=f7456076
A[6]=9edcb3f2  B[6]=1cc1c730  C[6]=5879f5c6  D[6]=1ef37ea4
A[7]=5a1e9924  B[7]=cdcdf21d  C[7]=9d5bd23b  D[7]=db40d4fe

Step  8: (r=26, s= 4)
A[0]=0bff2047  B[0]=6644fcc2  C[0]=39993a70  D[0]=b1d2a441
A[1]=d08b0554  B[1]=16789f9c  C[1]=90bb2ae8  D[1]=5a150250
A[2]=345c9900  B[2]=45bace03  C[2]=c7301cd2  D[2]=c75e006b
A[3]=da67ca51  B[3]=20d3a8a8  C[3]=31a366e2  D[3]=6330ff74
A[4]=59122f67  B[4]=0177ddf7  C[4]=c7f25729  D[4]=ea80ef7f
A[5]=92fba618  B[5]=c83984e3  C[5]=2061c895  D[5]=4a84fdea
A[6]=799853a6  B[6]=ca7b72cf  C[6]=1cc1c730  D[6]=5879f5c6
A[7]=51c7beba  B[7]=91687a64  C[7]=cdcdf21d  D[7]=9d5bd23b

Step  9: (r= 4, s=23)
A[0]=3ee869d7  B[0]=bff20470  C[0]=6644fcc2  D[0]=39993a70
A[1]=453b8d4a  B[1]=08b0554d  C[1]=16789f9c  D[1]=90bb2ae8
A[2]=5cd1e229  B[2]=45c99003  C[2]=45bace03  D[2]=c7301cd2
A[3]=f61b4818  B[3]=a67ca51d  C[3]=20d3a8a8  D[3]=31a366e2
A[4]=c9b9c18e  B[4]=9122f675  C[4]=0177ddf7  D[4]=c7f25729
A[5]=f7ff065e  B[5]=2fba6189  C[5]=c83984e3  D[5]=2061c895
A[6]=ceec5835  B[6]=99853a67  C[6]=ca7b72cf  D[6]=1cc1c730
A[7]=de7a63d3  B[7]=1c7beba5  C[7]=91687a64  D[7]=cdcdf21d

Step 10: (r=23, s=11)
A[0]=e83138fd  B[0]=eb9f7434  C[0]=bff20470  D[0]=6644fcc2
A[1]=f58293a1  B[1]=a5229dc6  C[1]=08b0554d  D[1]=16789f9c
A[2]=1e2919c5  B[2]=14ae68f1  C[2]=45c99003  D[2]=45bace03
A[3]=ea7fe544  B[3]=0c7b0da4  C[3]=a67ca51d  D[3]=20d3a8a8
A[4]=574a6620  B[4]=c764dce0  C[4]=9122f675  D[4]=0177ddf7
A[5]=501f3383  B[5]=2f7bff83  C[5]=2fba6189  D[5]=c83984e3
A[6]=d457e852  B[6]=1ae7762c  C[6]=99853a67  D[6]=ca7b72cf
A[7]=9ee5134e  B[7]=e9ef3d31  C[7]=1c7beba5  D[7]=91687a64

Step 11: (r=11, s=26)
A[0]=d02a680b  B[0]=89c7ef41  C[0]=eb9f7434  D[0]=bff20470
A[1]=21a07d9f  B[1]=149d0fac  C[1]=a5229dc6  D[1]=08b0554d
A[2]=c1c5601a  B[2]=48ce28f1  C[2]=14ae68f1  D[2]=45c99003
A[3]=601a647e  B[3]=ff2a2753  C[3]=0c7b0da4  D[3]=a67ca51d
A[4]=47a79258  B[4]=533102ba  C[4]=c764dce0  D[4]=9122f675
A[5]=80d0ba58  B[5]=f99c1a80  C[5]=2f7bff83  D[5]=2fba6189
```

```
A[6]=07751402  B[6]=bf4296a2  C[6]=1ae7762c  D[6]=99853a67
A[7]=340d33c8  B[7]=289a74f7  C[7]=e9ef3d31  D[7]=1c7beba5

Step 12: (r=26, s= 4)
A[0]=414b46ef  B[0]=2f40a9a0  C[0]=89c7ef41  D[0]=eb9f7434
A[1]=8486e48e  B[1]=7c8681f6  C[1]=149d0fac  D[1]=a5229dc6
A[2]=667f853e  B[2]=6b071580  C[2]=48ce28f1  D[2]=14ae68f1
A[3]=99e5afe6  B[3]=f9806991  C[3]=ff2a2753  D[3]=0c7b0da4
A[4]=f55da844  B[4]=611e9e49  C[4]=533102ba  D[4]=c764dce0
A[5]=e4d2cf45  B[5]=620342e9  C[5]=f99c1a80  D[5]=2f7bff83
A[6]=3721e5cd  B[6]=081dd450  C[6]=bf4296a2  D[6]=1ae7762c
A[7]=1372c624  B[7]=20d034cf  C[7]=289a74f7  D[7]=e9ef3d31

Step 13: (r= 4, s=23)
A[0]=3d4994ff  B[0]=14b46ef4  C[0]=2f40a9a0  D[0]=89c7ef41
A[1]=af371a54  B[1]=486e48e8  C[1]=7c8681f6  D[1]=149d0fac
A[2]=fbdc7132  B[2]=67f853e6  C[2]=6b071580  D[2]=48ce28f1
A[3]=3e0afe0d  B[3]=9e5afe69  C[3]=f9806991  D[3]=ff2a2753
A[4]=c190b414  B[4]=55da844f  C[4]=611e9e49  D[4]=533102ba
A[5]=b134c5f7  B[5]=4d2cf45e  C[5]=620342e9  D[5]=f99c1a80
A[6]=06697bd0  B[6]=721e5cd3  C[6]=081dd450  D[6]=bf4296a2
A[7]=f695c9ba  B[7]=372c6241  C[7]=20d034cf  D[7]=289a74f7

Step 14: (r=23, s=11)
A[0]=24c79063  B[0]=7f9ea4ca  C[0]=14b46ef4  D[0]=2f40a9a0
A[1]=e803ab90  B[1]=2a579b8d  C[1]=486e48e8  D[1]=7c8681f6
A[2]=41cca9ca  B[2]=997dee38  C[2]=67f853e6  D[2]=6b071580
A[3]=2d93ff25  B[3]=069f057f  C[3]=9e5afe69  D[3]=f9806991
A[4]=4c66fafb  B[4]=0a60c85a  C[4]=55da844f  D[4]=611e9e49
A[5]=d69446a9  B[5]=fbd89a62  C[5]=4d2cf45e  D[5]=620342e9
A[6]=64c00f67  B[6]=e80334bd  C[6]=721e5cd3  D[6]=081dd450
A[7]=dce64581  B[7]=dd7b4ae4  C[7]=372c6241  D[7]=20d034cf

Step 15: (r=11, s=26)
A[0]=b107d503  B[0]=3c831926  C[0]=7f9ea4ca  D[0]=14b46ef4
A[1]=61126e1c  B[1]=1d5c8740  C[1]=2a579b8d  D[1]=486e48e8
A[2]=ee399a01  B[2]=654e520e  C[2]=997dee38  D[2]=67f853e6
A[3]=98dd651e  B[3]=9ff9296c  C[3]=069f057f  D[3]=9e5afe69
A[4]=a82061bc  B[4]=37d7da63  C[4]=0a60c85a  D[4]=55da844f
A[5]=3d10d3df  B[5]=a2354eb4  C[5]=fbd89a62  D[5]=4d2cf45e
A[6]=2c3e227a  B[6]=007b3b26  C[6]=e80334bd  D[6]=721e5cd3
A[7]=4088738f  B[7]=322c0ee7  C[7]=dd7b4ae4  D[7]=372c6241

Step 16: (r=19, s=28)
A[0]=c73fed1a  B[0]=a81d883e  C[0]=3c831926  D[0]=7f9ea4ca
A[1]=5c27ff19  B[1]=70e30893  C[1]=1d5c8740  D[1]=2a579b8d
A[2]=96377a60  B[2]=d00f71cc  C[2]=654e520e  D[2]=997dee38
A[3]=e6550799  B[3]=28f4c6eb  C[3]=9ff9296c  D[3]=069f057f
A[4]=18c2214c  B[4]=0de54103  C[4]=37d7da63  D[4]=0a60c85a
```

```
A[5]=b3f7f823  B[5]=9ef9e886  C[5]=a2354eb4  D[5]=fbd89a62
A[6]=3b6a0953  B[6]=13d161f1  C[6]=007b3b26  D[6]=e80334bd
A[7]=04b14b6f  B[7]=9c7a0443  C[7]=322c0ee7  D[7]=dd7b4ae4

Step 17: (r=28, s= 7)
A[0]=d9035972  B[0]=ac73fed1  C[0]=a81d883e  D[0]=3c831926
A[1]=0f03d327  B[1]=95c27ff1  C[1]=70e30893  D[1]=1d5c8740
A[2]=da2a8a41  B[2]=096377a6  C[2]=d00f71cc  D[2]=654e520e
A[3]=d865d03a  B[3]=9e655079  C[3]=28f4c6eb  D[3]=9ff9296c
A[4]=b2a50ac7  B[4]=c18c2214  C[4]=0de54103  D[4]=37d7da63
A[5]=1bf2e557  B[5]=3b3f7f82  C[5]=9ef9e886  D[5]=a2354eb4
A[6]=da39dc4a  B[6]=33b6a095  C[6]=13d161f1  D[6]=007b3b26
A[7]=e040a4ef  B[7]=f04b14b6  C[7]=9c7a0443  D[7]=322c0ee7

Step 18: (r= 7, s=22)
A[0]=499adf76  B[0]=81acb96c  C[0]=ac73fed1  D[0]=a81d883e
A[1]=5d4afe8c  B[1]=81e99387  C[1]=95c27ff1  D[1]=70e30893
A[2]=cfcfa0d5  B[2]=154520ed  C[2]=096377a6  D[2]=d00f71cc
A[3]=6898aa55  B[3]=32e81d6c  C[3]=9e655079  D[3]=28f4c6eb
A[4]=47afd0f6  B[4]=528563d9  C[4]=c18c2214  D[4]=0de54103
A[5]=9d5a0a30  B[5]=f972ab8d  C[5]=3b3f7f82  D[5]=9ef9e886
A[6]=0617edb3  B[6]=1cee256d  C[6]=33b6a095  D[6]=13d161f1
A[7]=1841b740  B[7]=205277f0  C[7]=f04b14b6  D[7]=9c7a0443

Step 19: (r=22, s=19)
A[0]=b1241aa9  B[0]=dd9266b7  C[0]=81acb96c  D[0]=ac73fed1
A[1]=e9df9359  B[1]=a31752bf  C[1]=81e99387  D[1]=95c27ff1
A[2]=17d9f513  B[2]=3573f3e8  C[2]=154520ed  D[2]=096377a6
A[3]=4ef8ac3d  B[3]=955a262a  C[3]=32e81d6c  D[3]=9e655079
A[4]=9b326bf5  B[4]=3d91ebf4  C[4]=528563d9  D[4]=c18c2214
A[5]=90f399a3  B[5]=8c275682  C[5]=f972ab8d  D[5]=3b3f7f82
A[6]=547d2af9  B[6]=6cc185fb  C[6]=1cee256d  D[6]=33b6a095
A[7]=cb0dd957  B[7]=d006106d  C[7]=205277f0  D[7]=f04b14b6

Step 20: (r=19, s=28)
A[0]=a5bea1c8  B[0]=d54d8920  C[0]=dd9266b7  D[0]=81acb96c
A[1]=24bdc606  B[1]=9acf4efc  C[1]=a31752bf  D[1]=81e99387
A[2]=9df9ebdd  B[2]=a898becf  C[2]=3573f3e8  D[2]=154520ed
A[3]=36d549f4  B[3]=61ea77c5  C[3]=955a262a  D[3]=32e81d6c
A[4]=55cfcd3e  B[4]=5facd993  C[4]=3d91ebf4  D[4]=528563d9
A[5]=5e0b5061  B[5]=cd1c879c  C[5]=8c275682  D[5]=f972ab8d
A[6]=f71537cc  B[6]=57caa3e9  C[6]=6cc185fb  D[6]=1cee256d
A[7]=742d3f30  B[7]=cabe586e  C[7]=d006106d  D[7]=205277f0

Step 21: (r=28, s= 7)
A[0]=0268bcca  B[0]=8a5bea1c  C[0]=d54d8920  D[0]=dd9266b7
A[1]=d6c84380  B[1]=624bdc60  C[1]=9acf4efc  D[1]=a31752bf
A[2]=b892c80f  B[2]=d9df9ebd  C[2]=a898becf  D[2]=3573f3e8
A[3]=ddb7799d  B[3]=436d549f  C[3]=61ea77c5  D[3]=955a262a
```

```
A[4]=2428df65  B[4]=e55cfcd3  C[4]=5facd993  D[4]=3d91ebf4
A[5]=a06011eb  B[5]=15e0b506  C[5]=cd1c879c  D[5]=8c275682
A[6]=302dcff0  B[6]=cf71537c  C[6]=57caa3e9  D[6]=6cc185fb
A[7]=e3566582  B[7]=0742d3f3  C[7]=cabe586e  D[7]=d006106d

Step 22: (r= 7, s=22)
A[0]=3c55dec2  B[0]=345e6501  C[0]=8a5bea1c  D[0]=d54d8920
A[1]=95df617f  B[1]=6421c06b  C[1]=624bdc60  D[1]=9acf4efc
A[2]=8f06c00b  B[2]=496407dc  C[2]=d9df9ebd  D[2]=a898becf
A[3]=abb5e701  B[3]=dbbcceee  C[3]=436d549f  D[3]=61ea77c5
A[4]=306ba373  B[4]=146fb292  C[4]=e55cfcd3  D[4]=5facd993
A[5]=3390114d  B[5]=3008f5d0  C[5]=15e0b506  D[5]=cd1c879c
A[6]=ab888e26  B[6]=16e7f818  C[6]=cf71537c  D[6]=57caa3e9
A[7]=a367ee53  B[7]=ab32c171  C[7]=0742d3f3  D[7]=cabe586e

Step 23: (r=22, s=19)
A[0]=7b0294d1  B[0]=b08f1577  C[0]=345e6501  D[0]=8a5bea1c
A[1]=506e7be5  B[1]=5fe577d8  C[1]=6421c06b  D[1]=624bdc60
A[2]=8cd56b02  B[2]=02e3c1b0  C[2]=496407dc  D[2]=d9df9ebd
A[3]=25117b61  B[3]=c06aed79  C[3]=dbbcceee  D[3]=436d549f
A[4]=2623c4ee  B[4]=dccc1ae8  C[4]=146fb292  D[4]=e55cfcd3
A[5]=82520309  B[5]=534ce404  C[5]=3008f5d0  D[5]=15e0b506
A[6]=c2400292  B[6]=89aae223  C[6]=16e7f818  D[6]=cf71537c
A[7]=e1013dea  B[7]=94e8d9fb  C[7]=ab32c171  D[7]=0742d3f3

Step 24: (r=15, s= 5)
A[0]=54319dab  B[0]=4a68bd81  C[0]=b08f1577  D[0]=345e6501
A[1]=f5d93454  B[1]=3df2a837  C[1]=5fe577d8  D[1]=6421c06b
A[2]=8a461801  B[2]=b581466a  C[2]=02e3c1b0  D[2]=496407dc
A[3]=060751bf  B[3]=bdb09288  C[3]=c06aed79  D[3]=dbbcceee
A[4]=50ae2451  B[4]=e2771311  C[4]=dccc1ae8  D[4]=146fb292
A[5]=9828e42c  B[5]=0184c129  C[5]=534ce404  D[5]=3008f5d0
A[6]=54be7299  B[6]=01496120  C[6]=89aae223  D[6]=16e7f818
A[7]=1a85b838  B[7]=9ef57080  C[7]=94e8d9fb  D[7]=ab32c171

Step 25: (r= 5, s=29)
A[0]=a522d614  B[0]=8633b56a  C[0]=4a68bd81  D[0]=b08f1577
A[1]=df189f39  B[1]=bb268a9e  C[1]=3df2a837  D[1]=5fe577d8
A[2]=00405a53  B[2]=48c30031  C[2]=b581466a  D[2]=02e3c1b0
A[3]=82fef787  B[3]=c0ea37e0  C[3]=bdb09288  D[3]=c06aed79
A[4]=a72b28d8  B[4]=15c48a2a  C[4]=e2771311  D[4]=dccc1ae8
A[5]=826d66f9  B[5]=051c8593  C[5]=0184c129  D[5]=534ce404
A[6]=208b9daf  B[6]=97ce532a  C[6]=01496120  D[6]=89aae223
A[7]=1327d3b6  B[7]=50b70703  C[7]=9ef57080  D[7]=94e8d9fb

Step 26: (r=29, s= 9)
A[0]=0aa3d3a3  B[0]=94a45ac2  C[0]=8633b56a  D[0]=4a68bd81
A[1]=9c01a534  B[1]=3be313e7  C[1]=bb268a9e  D[1]=3df2a837
A[2]=89d7ad1a  B[2]=60080b4a  C[2]=48c30031  D[2]=b581466a
```

```
A[3]=cf2d96e1  B[3]=f05fdef0  C[3]=c0ea37e0  D[3]=bdb09288
A[4]=ec0e72e5  B[4]=14e5651b  C[4]=15c48a2a  D[4]=e2771311
A[5]=63fb4fc8  B[5]=304dacdf  C[5]=051c8593  D[5]=0184c129
A[6]=16ebfb63  B[6]=e41173b5  C[6]=97ce532a  D[6]=01496120
A[7]=69717d1a  B[7]=c264fa76  C[7]=50b70703  D[7]=9ef57080

Step 27: (r= 9, s=15)
A[0]=e3a4b8da  B[0]=47a74615  C[0]=94a45ac2  D[0]=8633b56a
A[1]=f7b55840  B[1]=034a6938  C[1]=3be313e7  D[1]=bb268a9e
A[2]=2db84506  B[2]=af5a3513  C[2]=60080b4a  D[2]=48c30031
A[3]=5034e926  B[3]=5b2dc39e  C[3]=f05fdef0  D[3]=c0ea37e0
A[4]=ecccccaa  B[4]=1ce5cbd8  C[4]=14e5651b  D[4]=15c48a2a
A[5]=faf8e88f  B[5]=f69f90c7  C[5]=304dacdf  D[5]=051c8593
A[6]=074ac789  B[6]=d7f6c62d  C[6]=e41173b5  D[6]=97ce532a
A[7]=7883458f  B[7]=e2fa34d2  C[7]=c264fa76  D[7]=50b70703

Step 28: (r=15, s= 5)
A[0]=82c0ebb1  B[0]=5c6d71d2  C[0]=47a74615  D[0]=94a45ac2
A[1]=501362f2  B[1]=ac207bda  C[1]=034a6938  D[1]=3be313e7
A[2]=ec7895d0  B[2]=228316dc  C[2]=af5a3513  D[2]=60080b4a
A[3]=05a34f6a  B[3]=7493281a  C[3]=5b2dc39e  D[3]=f05fdef0
A[4]=4f00f460  B[4]=66557666  C[4]=1ce5cbd8  D[4]=14e5651b
A[5]=b86373a9  B[5]=7447fd7c  C[5]=f69f90c7  D[5]=304dacdf
A[6]=aedd35ea  B[6]=63c483a5  C[6]=d7f6c62d  D[6]=e41173b5
A[7]=c2f59696  B[7]=a2c7bc41  C[7]=e2fa34d2  D[7]=c264fa76

Step 29: (r= 5, s=29)
A[0]=dd8bce26  B[0]=581d7630  C[0]=5c6d71d2  D[0]=47a74615
A[1]=dbac69fa  B[1]=026c5e4a  C[1]=ac207bda  D[1]=034a6938
A[2]=7284b0ff  B[2]=8f12ba1d  C[2]=228316dc  D[2]=af5a3513
A[3]=3340a7fb  B[3]=b469ed40  C[3]=7493281a  D[3]=5b2dc39e
A[4]=7ad9c53d  B[4]=e01e8c09  C[4]=66557666  D[4]=1ce5cbd8
A[5]=8362b318  B[5]=0c6e7537  C[5]=7447fd7c  D[5]=f69f90c7
A[6]=302a042d  B[6]=dba6bd55  C[6]=63c483a5  D[6]=d7f6c62d
A[7]=981d4363  B[7]=5eb2d2d8  C[7]=a2c7bc41  D[7]=e2fa34d2

Step 30: (r=29, s= 9)
A[0]=800eff15  B[0]=dbb179c4  C[0]=581d7630  D[0]=5c6d71d2
A[1]=b47a81bd  B[1]=5b758d3f  C[1]=026c5e4a  D[1]=ac207bda
A[2]=0e6f2e9b  B[2]=ee50961f  C[2]=8f12ba1d  D[2]=228316dc
A[3]=9e825648  B[3]=666814ff  C[3]=b469ed40  D[3]=7493281a
A[4]=4f0e296b  B[4]=af5b38a7  C[4]=e01e8c09  D[4]=66557666
A[5]=721f641a  B[5]=106c5663  C[5]=0c6e7537  D[5]=7447fd7c
A[6]=6fd3c503  B[6]=a6054085  C[6]=dba6bd55  D[6]=63c483a5
A[7]=fa9be2ab  B[7]=7303a86c  C[7]=5eb2d2d8  D[7]=a2c7bc41

Step 31: (r= 9, s=15)
A[0]=e0706253  B[0]=1dfe2b00  C[0]=dbb179c4  D[0]=581d7630
A[1]=3cf5cca0  B[1]=f5037b68  C[1]=5b758d3f  D[1]=026c5e4a
```

```
A[2]=a09802c8  B[2]=de5d361c  C[2]=ee50961f  D[2]=8f12ba1d
A[3]=9645ff32  B[3]=04ac913d  C[3]=666814ff  D[3]=b469ed40
A[4]=8e7f6690  B[4]=1c52d69e  C[4]=af5b38a7  D[4]=e01e8c09
A[5]=9b328d86  B[5]=3ec834e4  C[5]=106c5663  D[5]=0c6e7537
A[6]=ebf1b39e  B[6]=a78a06df  C[6]=a6054085  D[6]=dba6bd55
A[7]=3eddf269  B[7]=37c557f5  C[7]=7303a86c  D[7]=5eb2d2d8

Feistel Step 0: (r=15, s= 5)
A[0]=090d48ce  B[0]=3129f038  C[0]=1dfe2b00  D[0]=dbb179c4
A[1]=fc94adb6  B[1]=e6501e7a  C[1]=f5037b68  D[1]=5b758d3f
A[2]=2e1447cb  B[2]=0164504c  C[2]=de5d361c  D[2]=ee50961f
A[3]=15631882  B[3]=ff994b22  C[3]=04ac913d  D[3]=666814ff
A[4]=1835e5dd  B[4]=b348473f  C[4]=1c52d69e  D[4]=af5b38a7
A[5]=6fbc7a54  B[5]=46c34d99  C[5]=3ec834e4  D[5]=106c5663
A[6]=54df9e1f  B[6]=d9cf75f8  C[6]=a78a06df  D[6]=a6054085
A[7]=28247cba  B[7]=f9349f6e  C[7]=37c557f5  D[7]=7303a86c

Feistel Step 1: (r= 5, s=29)
A[0]=1fd89bb7  B[0]=21a919c1  C[0]=3129f038  D[0]=1dfe2b00
A[1]=00ecfabe  B[1]=9295b6df  C[1]=e6501e7a  D[1]=f5037b68
A[2]=a718c874  B[2]=c288f965  C[2]=0164504c  D[2]=de5d361c
A[3]=7096f69a  B[3]=ac631042  C[3]=ff994b22  D[3]=04ac913d
A[4]=83d4f649  B[4]=06bcbba3  C[4]=b348473f  D[4]=1c52d69e
A[5]=82e3cbf4  B[5]=f78f4a8d  C[5]=46c34d99  D[5]=3ec834e4
A[6]=21d96ae7  B[6]=9bf3c3ea  C[6]=d9cf75f8  D[6]=a78a06df
A[7]=a8d7e558  B[7]=048f9745  C[7]=f9349f6e  D[7]=37c557f5

Feistel Step 2: (r=29, s= 9)
A[0]=df4735cf  B[0]=e3fb1376  C[0]=21a919c1  D[0]=3129f038
A[1]=bdbb7986  B[1]=c01d9f57  C[1]=9295b6df  D[1]=e6501e7a
A[2]=a1da8eb9  B[2]=94e3190e  C[2]=c288f965  D[2]=0164504c
A[3]=fb88c7c1  B[3]=4e12ded3  C[3]=ac631042  D[3]=ff994b22
A[4]=2dbf1928  B[4]=307a9ec9  C[4]=06bcbba3  D[4]=b348473f
A[5]=454dbb56  B[5]=905c797e  C[5]=f78f4a8d  D[5]=46c34d99
A[6]=7a0ebca9  B[6]=e43b2d5c  C[6]=9bf3c3ea  D[6]=d9cf75f8
A[7]=04bc1d54  B[7]=151afcab  C[7]=048f9745  D[7]=f9349f6e

Feistel Step 3: (r= 9, s=15)
A[0]=7a72c0f8  B[0]=8e6b9fbe  C[0]=e3fb1376  D[0]=21a919c1
A[1]=1be81899  B[1]=76f30d7b  C[1]=c01d9f57  D[1]=9295b6df
A[2]=0969dd83  B[2]=b51d7343  C[2]=94e3190e  D[2]=c288f965
A[3]=a66b9f12  B[3]=118f83f7  C[3]=4e12ded3  D[3]=ac631042
A[4]=dcc5c195  B[4]=7e32505b  C[4]=307a9ec9  D[4]=06bcbba3
A[5]=0d71576b  B[5]=9b76ac8a  C[5]=905c797e  D[5]=f78f4a8d
A[6]=a74b20ce  B[6]=1d7952f4  C[6]=e43b2d5c  D[6]=9bf3c3ea
A[7]=dc5d7589  B[7]=783aa809  C[7]=151afcab  D[7]=048f9745
```

Compression Function Output

```
A[0]=7a72c0f8  B[0]=8e6b9fbe  C[0]=e3fb1376  D[0]=21a919c1
```

```
A[1]=1be81899  B[1]=76f30d7b  C[1]=c01d9f57  D[1]=9295b6df
A[2]=0969dd83  B[2]=b51d7343  C[2]=94e3190e  D[2]=c288f965
A[3]=a66b9f12  B[3]=118f83f7  C[3]=4e12ded3  D[3]=ac631042
A[4]=dcc5c195  B[4]=7e32505b  C[4]=307a9ec9  D[4]=06bcbba3
A[5]=0d71576b  B[5]=9b76ac8a  C[5]=905c797e  D[5]=f78f4a8d
A[6]=a74b20ce  B[6]=1d7952f4  C[6]=e43b2d5c  D[6]=9bf3c3ea
A[7]=dc5d7589  B[7]=783aa809  C[7]=151afcab  D[7]=048f9745
```

Hash Function Output

```
f8c0727a9918e81b83dd6909129f6ba695c1c5dc6b57710dce204ba789755ddc
be9f6b8e7b0df37643731db5f7838f115b50327e8aac769bf452791d09a83a78
```

Bibliography

[1] Bellare, M.: New Proofs for NMAC and HMAC: Security without Collision-Resistance. In Dwork, C., ed.: CRYPTO. Volume 4117 of Lecture Notes in Computer Science., Springer (2006) 602–619

[2] Bellare, M., Canetti, R., Krawczyk, H.: Pseudorandom Functions Revisited: The Cascade Construction and Its Concrete Security. In: FOCS. (1996) 514–523

[3] Biham, E., Youssef, A.M., eds.: Selected Areas in Cryptography, 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers. In Biham, E., Youssef, A.M., eds.: Selected Areas in Cryptography. Volume 4356 of Lecture Notes in Computer Science., Springer (2007)

[4] Black, J., Rogaway, P., Shrimpton, T.: Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Yung, M., ed.: CRYPTO. Volume 2442 of Lecture Notes in Computer Science., Springer (2002) 320–335

[5] Chang, D., Nandi, M.: Improved Indifferentiability Security Analysis of chopMD Hash Function. [20] 429–443

[6] Coron, J.S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-Damgård Revisited: How to Construct a Hash Function. In: CRYPTO'05. (2005) 430–448

[7] Cramer, R., ed.: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. In Cramer, R., ed.: EUROCRYPT'05. Volume 3494 of Lecture Notes in Computer Science., Springer (2005)

[8] Dean, R.D.: Formal Aspects of Mobile Code Security. PhD thesis, Princeton University (January 1999)

[9] den Boer, B., Bosselaers, A.: Collisions for the Compression Function of MD5. In: EUROCRYPT. (1993) 293–304

[10] Dodis, Y., Gennaro, R., Håstad, J., Krawczyk, H., Rabin, T.: Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. [12] 494–510

[11] Fouque, P.A., Pointcheval, D., Zimmer, S.: HMAC is a randomness extractor and applications to TLS. In Abe, M., Gligor, V.D., eds.: ASIACCS, ACM (2008) 21–32

[12] Franklin, M.K., ed.: Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. In Franklin, M.K., ed.: CRYPTO'04. Volume 3152 of Lecture Notes in Computer Science., Springer (2004)

[13] Joux, A.: Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. [12] 306–316

[14] Jutla, C.S., Patthak, A.C.: Provably Good Codes for Hash Function Design. [3] 376–393

[15] Kelsey, J., Schneier, B.: Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. [7] 474–490

[16] Lucks, S.: A Failure-Friendly Design Principle for Hash Functions. In Roy, B.K., ed.: ASIACRYPT'05. Volume 3788 of Lecture Notes in Computer Science., Springer (2005) 474–494

[17] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: A Modest Proposal for FFT Hashing. [20] 54–72

[18] Maurer, U.M., Tessaro, S.: Domain Extension of Public Random Functions: Beyond the Birthday Barrier. In Menezes, A., ed.: CRYPTO. Volume 4622 of Lecture Notes in Computer Science., Springer (2007) 187–204

[19] Nussbaumer, H.: Fast Fourier Transform and Convolution Algorithms. Springer-Verlag (1982)

[20] Nyberg, K., ed.: Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers. In Nyberg, K., ed.: FSE. Volume 5086 of Lecture Notes in Computer Science., Springer (2008)

[21] Preneel, B., Govaerts, R., Vandewalle, J.: Differential Cryptanalysis of Hash Functions Based on Block Ciphers. In: ACM Conference on Computer and Communications Security. (1993) 183–188

[22] Projet RNRT SAPHIR: sphlib 1.0. `http://www.crypto-hash.fr/modules/wfdownloads/singlefile.php?cid=9&lid=5`

[23] Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In Shoup, V., ed.: CRYPTO. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 17–36

[24] Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. [7] 19–35