Cross Block Chaining (XBC)

Submission To NIST For A General Block Cipher Mode Of Operation

May 26, 2014

Inventor / Owner / Developer / Submitter :

Andre Watson
andre.watson@gmail.com

14027 Eastern St
Poway, CA 92064
+1 858 349 1023

1 Mode of Operation

Cross Block Chaining (XBC) is designed to be similar to the classic standard modes of operation, specifically CBC, except that it operates using two IVs that "collect" data through the course of the encryption process in a way that resembles CFB and OFB operation. This has two main net effects. Firstly, for very short messages, the keys can be split to prevent decryption by a single person, effectively creating a two-man rule [1]. Secondly, because the mode crosses itself, the entire previous message is necessary to decrypt the remaining blocks, which insures extra security in that the entire message must be decrypted from the beginning with no errors. This does, however, mean that any error will propagate through the entire message.

Two versions of this algorithm are presented with what is a minute difference in operations. Each version has different implications and will be discussed inline. An interesting feature for both versions is that technically only one vector can be necessary to decrypt the majority of a longer message. While this would break any sort of two-man rule for longer messages, it still creates another layer of security through obfuscation by creating another mode of operation which would need to be tested against in an attack. Further, with two positions that a compromised vector could occupy, this increases the challenge of any attack. It is also possible that the same vector can be used for both IVs, which is another option to consider.

1.1 Algorithm XBC-1

The first version of XBC is quite similar to CBC, but with an additional IV that is XORed with the entry data into the block cipher, and this in turn is fed into the output of the block cipher of the next round. As can be seen in Figure 1, this creates the crossing between rounds of the block cipher that the algorithm is named after.

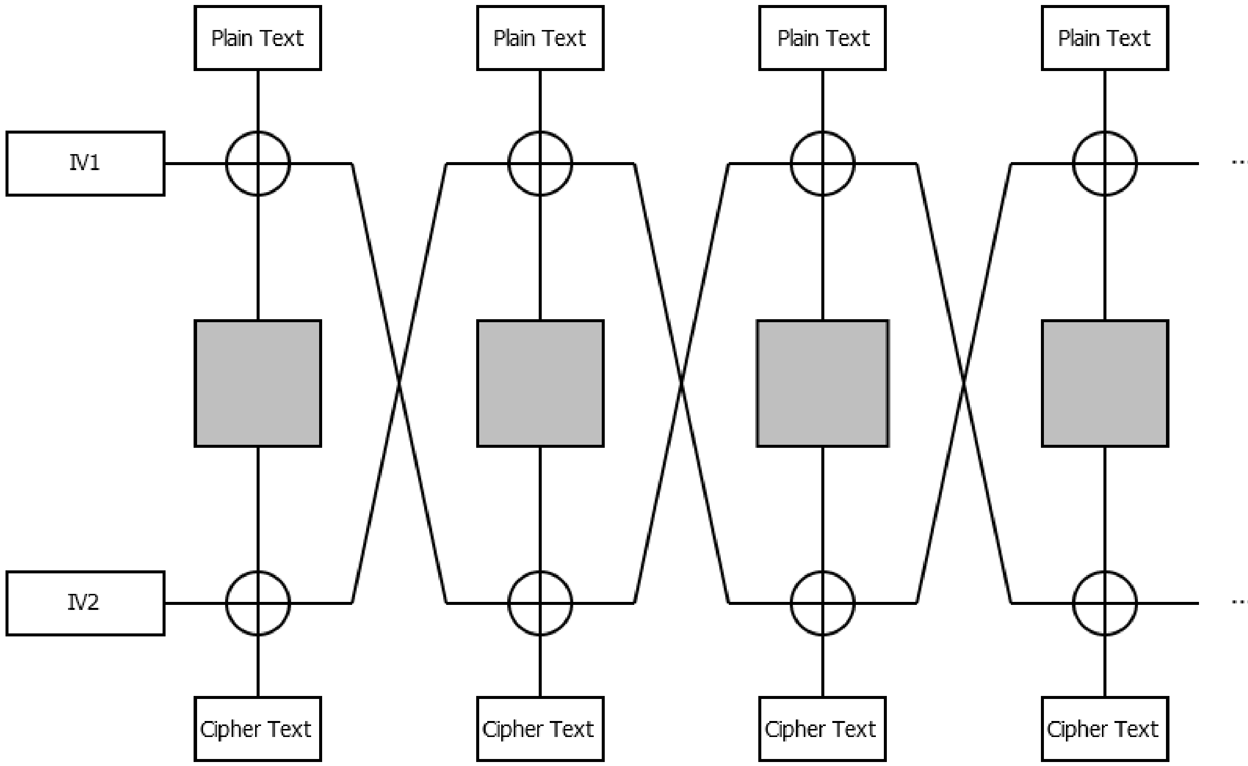

Figure 1: The block diagram of XBC-1 operation. The grey blocks are the underlying block cipher used which is not covered in this paper, as any block cipher may be used.

The pseudo code description for XBC-1 is as follows:

Variables:

$\boldsymbol{K}$:	The key for the underlying block cipher.
$\boldsymbol{IV_0^1}$:	The first provided initialization vector, must have length of the underlying block cipher.
$\boldsymbol{IV_0^2}$:	The second provided initialization vector, must have length of the underlying block cipher.
$\boldsymbol{PT}$:	The plain text, of arbitrary length, padded out to a multiple of the block length of the underlying block cipher, described as blocks $\mathbf{0}$ to $\boldsymbol{n}$.
$\boldsymbol{CT}$:	The cipher text blocks, described as blocks $\mathbf{0}$ to $\boldsymbol{n}$.
$\boldsymbol{IV_n^1}$:	The first initialization vector sent into round $\boldsymbol{n}$.
$\boldsymbol{IV_n^2}$:	The second initialization vector sent into round $\boldsymbol{n}$.

Algorithm:

FOR blocks $\boldsymbol{i} = \boldsymbol{0}$ to $\boldsymbol{n}$ DO

$$\boldsymbol{IV_{i+1}^{2} = PT_{i} \oplus IV_{i}^{1}}$$
$$\boldsymbol{i = BLOCK\ CIPHER\left(K, IV_{i+1}^{2}\right)}$$
$$\boldsymbol{CT_{i} = IV_{i+1}^{1} = i \oplus IV_{i}^{2}}$$

It should be carefully noted what happens in the event that one of the two IVs is compromised. In the case where the cipher key is unknown, the message cannot be effectively decrypted or discerned by a compromise of either vector. But in the case where the cipher key is known, and one IV is comprised, we end up in the following situation as seen in Figure 2.

Say IV2 is compromised as represented by the dotted line. This allows the decryption process to occur back to the input of the first block cipher round. However, this value is also IV2 for the second round of the block cipher. Because we already had the second round IV1 in the form of the first block of cipher text, every needed part of the algorithm is now present to decrypt the cipher text from the second round onwards.

On the other hand, if IV2 is secure, but IV1 is compromised, this situation does not occur and the algorithm remains secure, assuming that the plain text of the first block is something that can't easily be guessed.

As such, IV2 is significantly important, and if this algorithm were used for some sort of two-man rule, it is recommended that only one or two blocks worth of data be stored so that no large plain text comprise can occur due to any compromise of IV2.

It should also be mentioned, that since the plain text plays a significant role in this algorithm due to its feedback nature, large portions of zeroes or ones in the plain text, or easily guessable plaintext, could potentially compromise the security benefits of this method in an attack.

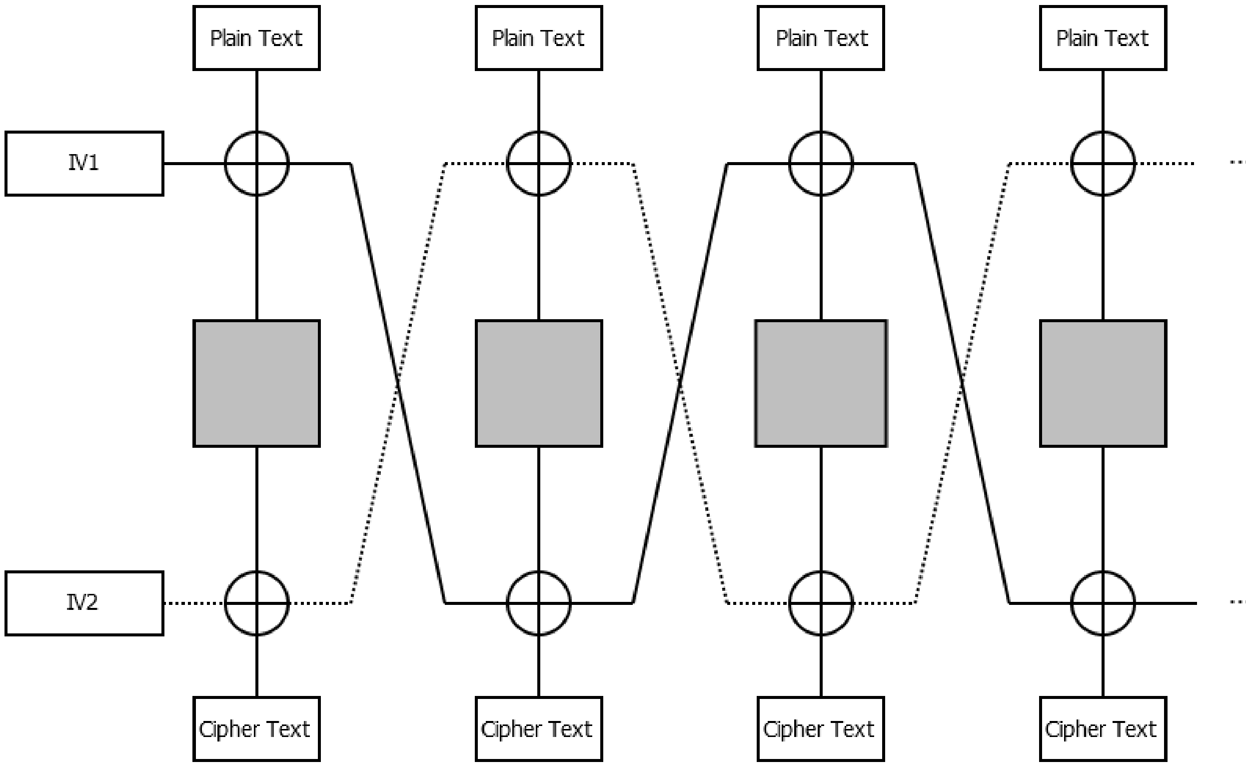

Figure 2: A compromised algorithm where IV2 and the block cipher key are known allows for decryption from the second block onwards.

The error propagation for both encryption and decryption will proceed through the rest of the message from the point of error because the IVs will become corrupted. This will make every block operation return erroneous values, even if further blocks do not contain errors.

Reuse of IVs should use the normal considerations used for CBC IV reuse. Another consideration for IV selection is that it is possible to use the same IV for both IV1 and IV2 in this algorithm.

1.2 Algorithm XBC-2

XBC-2 is nearly identical to XBC-1 except that the encryption block output is used as IV1 for the next block operation, instead of using the cipher text value. This can be seen in **Figure 3**. This is a clear departure from the CBC base style and has something in common with the OFB algorithm structure.

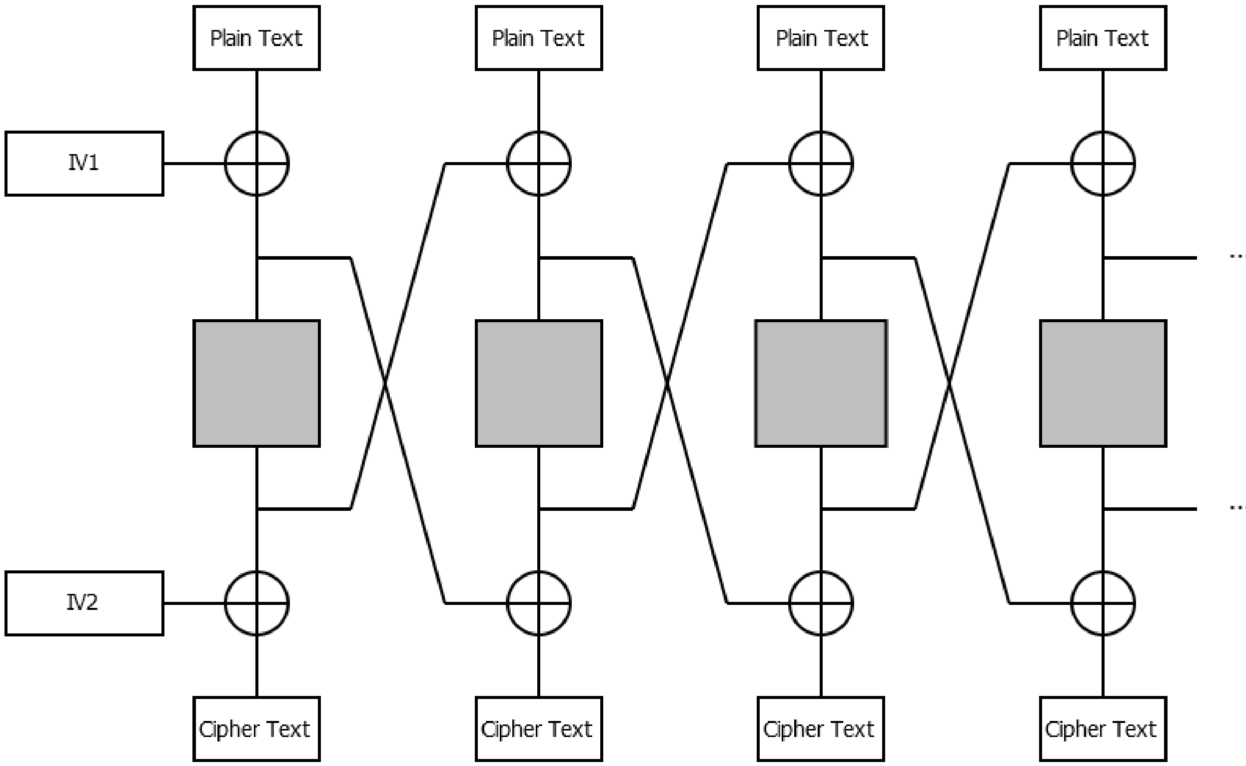

Figure 3: The block diagram of XBC-2 operation.

The pseudo code description for XBC-2 is as follows:

Variables:

$\boldsymbol{K}$:	The key for the underlying block cipher.
$\boldsymbol{IV_0^1}$:	The first provided initialization vector, must have length of the underlying block cipher.
$\boldsymbol{IV_0^2}$:	The second provided initialization vector, must have length of the underlying block cipher.
$\boldsymbol{PT}$:	The plain text, of arbitrary length, padded out to a multiple of the block length of the underlying block cipher, described as blocks $\mathbf{0}$ to $\boldsymbol{n}$.
$\boldsymbol{CT}$:	The cipher text blocks, described as blocks $\mathbf{0}$ to $\boldsymbol{n}$.
$\boldsymbol{IV_n^1}$:	The first initialization vector sent into round $\boldsymbol{n}$.
$\boldsymbol{IV_n^2}$:	The second initialization vector sent into round $\boldsymbol{n}$.

Algorithm:

FOR blocks $\boldsymbol{i} = \mathbf{0}$ to $\boldsymbol{n}$ DO

$$\boldsymbol{IV_{i+1}^2 = PT_i \oplus IV_i^1}$$

$$\boldsymbol{IV_{i+1}^1 = BLOCK\ CIPHER(K, IV_{i+1}^2)}$$

$$\boldsymbol{CT_i = IV_{i+1}^1 \oplus IV_i^2}$$

In XBC-2, IV2 has a much reduced role. As seen in **Figure 4** with the dotted line, IV2 is primarily used to hide the intermediate value that becomes IV1 in the next block operation. Looking carefully at the subsequent block operations reveals that no IV1 value in any block frame is exposed in the cipher text. This can remove the one exposed IV value that is normally the cipher text output from any potential attack. This does, however, mean that IV1 is the primary vector controlling the IVs passed into the next block operation, and should be chosen with care.

If the key and IV2 are both compromised, similarly to the situation in XBC-1, the second block round can be decrypted because both of the IVs can be determined from the first round. The first block will remain uncompromised.

Because of both of the previous statements, both IVs are significantly important, but for different situations, and if this algorithm were used for some sort of two-man rule, it is recommended that only one or two blocks worth of data be stored so that no large plain text compromise can occur due to any compromise of IV2 with the key.

Also like XBC-1, a compromise of IV1 and the key will not compromise the algorithm. The plain text is somewhat less important in XBC-2 than it was in XBC-1, since the actual IVs are not exposed in the cipher text, thereby making mid-stream attacks more difficult.

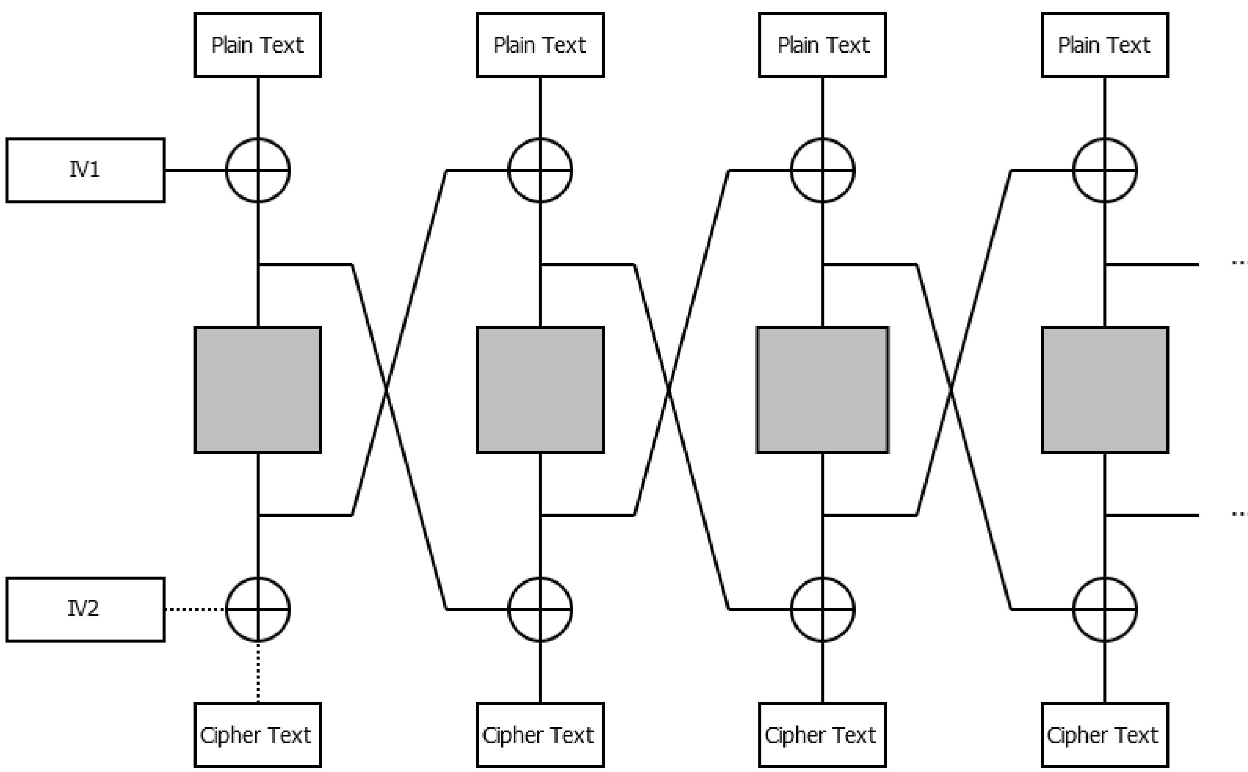

Figure 4: The main effect of IV2 on XBC-2

The error propagation for both encryption and decryption will proceed through the rest of the message from the point of error because the IVs will become corrupted. This will make every block operation return erroneous values, even if further blocks do not contain errors.

For the selection of the IVs, it is possible to use the same IV for both IV1 and IV2 in this algorithm. Reuse of IVs should use the normal considerations used for CBC IV reuse.

2 Summary of Properties

2.1 Algorithm XBC-1

Security Function	A cipher mode of operation for block cipher encryption with two completely separate IVs
Error Propagation	Infinite from the point of error onwards, resulting in total message loss from the point of error
Synchronization	The same two IVs must be used for encryption and decryption
Parallelizability	Sequential
Keying Material Requirements	One key for the underlying block cipher
Counter/IV/Nonce Requirements	Some IV reuse will be fine, but as the same first IV could be used with different second IVs, any “master key” situation will need to be wary of reuse as well
Memory Requirements	The block cipher memory requirements, plus two accumulation values for the IVs which are both block length
Pre-processing Capability	No values can be pre-processed
Message Length Requirements	Arbitrary length is acceptable, but the underlying block cipher will determine any padding scheme to make the message be a multiple of block length
Ciphertext Expansion	None

2.2 Algorithm XBC-2

Security Function	A cipher mode of operation for block cipher encryption with two completely separate IVs
Error Propagation	Infinite from the point of error onwards, resulting in total message loss from the point of error
Synchronization	The same two IVs must be used for encryption and decryption

Parallelizability	Sequential
Keying Material Requirements	One key for the underlying block cipher
Counter/IV/Nonce Requirements	Some IV reuse will be fine, but as the same first IV could be used with different second IVs, any "master key" situation will need to be wary of reuse as well
Memory Requirements	The block cipher memory requirements, plus two accumulation values for the IVs which are both block length
Pre-processing Capability	No values can be pre-processed
Message Length Requirements	Arbitrary length is acceptable, but the underlying block cipher will determine any padding scheme to make the message be a multiple of block length
Ciphertext Expansion	None
Other Characteristics	Arguably, the first IV is significantly more important than the second IV for this algorithm because the second IV mainly serves only to obscure the first ciphertext block and prevents output of the intermediate values of the mode of operation process in the ciphertext. Due to the reliance of every block on the previous blocks, this makes decryption impossible without the second IV. However, it is the first IV that is being accumulated throughout the encryption process, so care of choosing a non-obvious first IV should be noted.

3 Test Vectors

All three of the following test vector cases were output using the Crypto++ AES-128 [2][3] functionality with a new cipher mode of operation class added for both XBC-1 and XBC-2. Intermediate values are provided for the first two sets of vectors for each variant.

3.1 Algorithm XBC-1

Test Case 1:

The first vector is exactly 128 bits in length and therefore uses $\boldsymbol{n}$ (for $\boldsymbol{n}$ext) for what would be the next block's IV iteration because there will not be another cipher block in this test case.

$\boldsymbol{K}$:	**00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00**
$\boldsymbol{IV^1}$:	**FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00**
$\boldsymbol{IV^2}$:	**00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF**
$\boldsymbol{PT}$:	**00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00**
$\boldsymbol{IV_n^2 = PT \oplus IV^1}$:	**FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00**
$\boldsymbol{i = AES(K, N)}$:	**61 3A 30 90 C5 20 FE 8D A2 94 61 33 84 3B D3 32**
$\boldsymbol{CT = IV_n^1 = i \oplus IV^2}$:	**61 C5 30 6F C5 DF FE 72 A2 6B 61 CC 84 C4 D3 CD**

Test Case 2:

In the second vector, a 196 bit plain text value is used with zero padding to complete the 128 bit boundary for the block. In a real encryption scenario, a non-block aligned input value could be padded in any number of ways, as long as this padding is supported by the block algorithm; potentially by null termination for a string, a length for a non-string value, a sentinel for file end, or some other method.

$\boldsymbol{K}$:	**E5 C7 CD DE 87 2B F2 7C 43 E9 34 00 8C 38 9C 0F**
$\boldsymbol{IV_0^1}$:	**F3 09 62 49 C7 F4 6E 51 A6 9E 83 9B 1A 92 F7 84**
$\boldsymbol{IV_0^2}$:	**4E 6F 77 20 69 73 20 74 68 65 20 74 69 6D 65 20**
$\boldsymbol{PT}$:	**12 34 56 78 90 AB CD EF 12 34 56 78 90 AB CD EF**
	12 34 56 78 90 AB CD EF
$\boldsymbol{IV_1^2 = PT_0 \oplus IV_0^1}$:	**E1 3D 34 31 57 5F A3 BE B4 AA D5 E3 8A 39 3A 6B**
$\boldsymbol{i = AES(K, IV_1^2)}$:	**CB CD 7B DC BC DD D2 1B DA 2D 7D 36 14 F6 73 C4**
$\boldsymbol{CT_0 = IV_1^1 = i \oplus IV_0^2}$:	**85 A2 0C FC D5 AE F2 6F B2 48 5D 42 7D 9B 16 E4**
$\boldsymbol{IV_2^2 = PT_1 \oplus IV_1^1}$:	**97 96 5A 84 45 05 3F 80 B2 48 5D 42 7D 9B 16 E4**
$\boldsymbol{i = AES(K, IV_2^2)}$:	**40 51 4E B0 E4 8C 2C 2D 4B 02 F7 58 76 2D 34 BE**
$\boldsymbol{CT_1 = IV_2^1 = i \oplus IV_1^2}$:	**A1 6C 7A 81 B3 D3 8F 93 FF A8 22 BB FC 14 0E D5**

Test Case 3:

For the third vector, a quote from Nikola Tesla was used with ASCII characters and single spacing after punctuation. Both the string and hex values for the string are presented for clarity and verifiability. No intermediate values are presented for this case.

For completeness sake, it is worth mentioning that this string, with a null terminator, coincidentally happened to fall on a 128 bit boundary, so no padding was necessary (beyond the null terminator of the string).

K : A4 B2 FF 1C 29 21 B2 88 34 AB 71 3D 50 CC B4 7E

IV_0^1 : 4C E3 A2 B7 55 57 93 98 81 26 52 0E AC F2 E3 06

IV_0^2 : 7A 62 3E F8 4C 3D 33 C1 95 D2 3E E3 20 C4 0D E0

$PT\ (ASCII)$:

When we speak of man, we have a conception of humanity as a whole, and before applying scientific methods to the investigation of his movement we must accept this as a physical fact. But can anyone doubt to-day that all the millions of individuals and all the innumerable types and characters constitute an entity, a unit? Though free to think and act, we are held together, like the stars in the firmament, with ties inseparable. These ties cannot be seen, but we can feel them. I cut myself in the finger, and it pains me: this finger is a part of me. I see a friend hurt, and it hurts me, too: my friend and I are one. And now I see stricken down an enemy, a lump of matter which, of all the lumps of matter in the universe, I care least for, and it still grieves me. Does this not prove that each of us is only part of a whole?

$PT\ (hex)$:

```
57 68 65 6E 20 77 65 20 73 70 65 61 6B 20 6F 66
20 6D 61 6E 2C 20 77 65 20 68 61 76 65 20 61 20
63 6F 6E 63 65 70 74 69 6F 6E 20 6F 66 20 68 75
6D 61 6E 69 74 79 20 61 73 20 61 20 77 68 6F 6C
65 2C 20 61 6E 64 20 62 65 66 6F 72 65 20 61 70
70 6C 79 69 6E 67 20 73 63 69 65 6E 74 69 66 69
63 20 6D 65 74 68 6F 64 73 20 74 6F 20 74 68 65
20 69 6E 76 65 73 74 69 67 61 74 69 6F 6E 20 6F
66 20 68 69 73 20 6D 6F 76 65 6D 65 6E 74 20 77
65 20 6D 75 73 74 20 61 63 63 65 70 74 20 74 68
69 73 20 61 73 20 61 20 70 68 79 73 69 63 61 6C
20 66 61 63 74 2E 20 42 75 74 20 63 61 6E 20 61
6E 79 6F 6E 65 20 64 6F 75 62 74 20 74 6F 2D 64
61 79 20 74 68 61 74 20 61 6C 6C 20 74 68 65 20
6D 69 6C 6C 69 6F 6E 73 20 6F 66 20 69 6E 64 69
76 69 64 75 61 6C 73 20 61 6E 64 20 61 6C 6C 20
74 68 65 20 69 6E 6E 75 6D 65 72 61 62 6C 65 20
74 79 70 65 73 20 61 6E 64 20 63 68 61 72 61 63
74 65 72 73 20 63 6F 6E 73 74 69 74 75 74 65 20
61 6E 20 65 6E 74 69 74 79 2C 20 61 20 75 6E 69
74 3F 20 54 68 6F 75 67 68 20 66 72 65 65 20 74
6F 20 74 68 69 6E 6B 20 61 6E 64 20 61 63 74 2C
20 77 65 20 61 72 65 20 68 65 6C 64 20 74 6F 67
65 74 68 65 72 2C 20 6C 69 6B 65 20 74 68 65 20
73 74 61 72 73 20 69 6E 20 74 68 65 20 66 69 72
```

```
6D 61 6D 65 6E 74 2C 20 77 69 74 68 20 74 69 65
73 20 69 6E 73 65 70 61 72 61 62 6C 65 2E 20 54
68 65 73 65 20 74 69 65 73 20 63 61 6E 6E 6F 74
20 62 65 20 73 65 65 6E 2C 20 62 75 74 20 77 65
20 63 61 6E 20 66 65 65 6C 20 74 68 65 6D 2E 20
49 20 63 75 74 20 6D 79 73 65 6C 66 20 69 6E 20
74 68 65 20 66 69 6E 67 65 72 2C 20 61 6E 64 20
69 74 20 70 61 69 6E 73 20 6D 65 3A 20 74 68 69
73 20 66 69 6E 67 65 72 20 69 73 20 61 20 70 61
72 74 20 6F 66 20 6D 65 2E 20 49 20 73 65 65 20
61 20 66 72 69 65 6E 64 20 68 75 72 74 2C 20 61
6E 64 20 69 74 20 68 75 72 74 73 20 6D 65 2C 20
74 6F 6F 3A 20 6D 79 20 66 72 69 65 6E 64 20 61
6E 64 20 49 20 61 72 65 20 6F 6E 65 2E 20 41 6E
64 20 6E 6F 77 20 49 20 73 65 65 20 73 74 72 69
63 6B 65 6E 20 64 6F 77 6E 20 61 6E 20 65 6E 65
6D 79 2C 20 61 20 6C 75 6D 70 20 6F 66 20 6D 61
74 74 65 72 20 77 68 69 63 68 2C 20 6F 66 20 61
6C 6C 20 74 68 65 20 6C 75 6D 70 73 20 6F 66 20
6D 61 74 74 65 72 20 69 6E 20 74 68 65 20 75 6E
69 76 65 72 73 65 2C 20 49 20 63 61 72 65 20 6C
65 61 73 74 20 66 6F 72 2C 20 61 6E 64 20 69 74
20 73 74 69 6C 6C 20 67 72 69 65 76 65 73 20 6D
65 2E 20 44 6F 65 73 20 74 68 69 73 20 6E 6F 74
20 70 72 6F 76 65 20 74 68 61 74 20 65 61 63 68
20 6F 66 20 75 73 20 69 73 20 6F 6E 6C 79 20 70
61 72 74 20 6F 66 20 61 20 77 68 6F 6C 65 3F 00
```

CT :

```
08 C8 B0 8B 68 5A 19 93 F0 7A C1 29 E2 69 E4 53
CB E9 B5 8A C3 0E 73 DD 3A F6 8F 16 0D B9 44 55
36 87 E4 86 04 B6 2C 8F EA AA 70 40 92 A7 50 1F
6D 62 FC C2 23 21 B3 A0 CD B8 44 3F 55 96 11 BE
5D B5 D5 84 22 91 72 C3 50 13 FE B3 F0 01 25 85
B2 01 BD 01 A4 5B 37 40 4E 68 CE ED DA 05 C5 37
D9 04 82 0B 77 3F AD 13 6C 53 00 C1 99 0A D9 A2
9C 00 48 A6 D1 DC 7B CC D4 94 CB 20 F8 77 2E EF
3D 6B 28 2B 3A 81 69 81 DD 1D A0 45 DD FD 3D 28
E9 6A CC 26 7A 81 5E 25 28 A0 0C FD AF 56 CB 72
5B B8 A1 9F C9 B5 7C BD 98 5E FC 4B D1 DE C7 30
26 DE 01 47 6D 5E E7 12 2F 98 5D 95 6A 72 94 A3
5F 69 92 12 21 AF 26 F9 E6 F5 F5 13 21 65 42 82
55 7C 7C F7 AB 52 89 5E A6 18 AA 82 8B 99 45 A7
71 97 F5 A7 F5 43 E8 3E 99 78 46 6B CA 4C 2E 11
F7 B8 00 21 89 29 C6 7F 7E BB 2D 7F C8 57 46 5B
78 2A 2F C4 BD BE 85 15 2C A1 45 1B 81 1E 82 00
A4 D5 4B 38 C5 55 67 25 72 BF 89 D3 E6 60 D3 33
E0 33 74 90 F6 5C 2C 00 89 18 32 B9 B6 84 17 9E
F8 BB 8B A2 C2 EA D2 48 E3 5F 13 DE 97 66 60 93
7E EE 07 9E 78 D8 A9 A2 31 D6 3A 45 6F C7 42 4A
82 18 EF 85 29 82 17 CA F4 52 29 38 05 96 19 7E
C1 90 21 84 63 A9 17 29 6D 9B A7 B0 26 95 B6 87
```

```
98 59 A3 B1 38 E9 7F 39 06 FB EA A0 A4 26 0A 19
F5 62 CD F4 60 24 4E 14 07 32 89 9E D1 BF 51 BB
33 DF C2 12 AE C0 86 5D B8 03 F0 D1 6E F1 F3 5E
24 D4 61 6C 6D 8D D6 E6 82 AC E4 80 7C 1D D5 72
4C 3B DF D9 EC F9 6C 19 CB 3F 61 5C 16 6F 65 D4
D6 F9 AE 83 AA 62 12 90 54 CA 83 68 66 EC 2B AC
87 B8 CA C9 F9 5C A5 12 A8 7E 17 BE B8 EB 73 EA
CE DE 7E B5 AF 98 51 0D D6 DD FB 9C FF 0E 0D 68
54 94 E7 A9 FF 6F 9E C2 C8 EB D6 87 9D A2 D3 7B
6A 1F 47 95 E7 09 4F 98 6A 56 49 A9 6A C3 35 E3
02 6A BA A6 CC 1B 9A 15 4E 8B 0A 6B 70 92 07 BB
EB 46 C5 6C 71 C9 6A 01 BE 1D EC 74 2B C0 3A 61
C4 4E A6 36 2F AD 6B 2F 82 AF 1B BC 05 AB 81 26
18 98 B4 DB DD 0F 17 11 3B 29 34 8D B8 48 30 0C
D9 42 15 B4 66 1E 5C 5E 4F FB A0 A0 D6 60 C2 8F
89 0E 6B 1E 86 E0 BD 5B B2 F8 AC 2D 23 26 7A 26
46 00 BD 77 BB EF B3 EF 54 A5 EC 7C 45 DF A1 A9
81 03 46 91 CA E9 B6 23 DA A5 7E 23 BC B9 AC 53
03 F8 FE 74 F7 56 05 00 F6 E7 7F A7 59 A8 B3 99
0F FA 24 74 51 B7 D0 FA 27 3E 21 D8 AB BA CF 58
02 0D 91 C3 54 64 14 DE F7 E8 B6 90 53 4E C7 F6
2B B1 28 41 ED E0 03 95 56 50 4B C2 1C AE B0 CB
A4 2F 95 F6 1A FC EE CF 34 AC 45 32 CC 40 C9 AF
7B 2C C5 3C 3F 21 65 10 71 1D 09 BC 67 E0 44 0A
4A D9 6C 9C 29 4E 8B 00 73 93 C3 22 4E 3A 6C 7D
0F 5D 47 D9 0C AD 21 54 82 DB 3A 6B 36 CE AF E3
7B 2D 84 F6 C7 A5 58 76 25 60 97 0D E5 DC 86 AD
90 A9 9C 20 28 39 FB DE FB FB EC DF 1F EF F9 E2
41 C4 35 9C 34 A1 8C 56 48 DB 81 E2 CC 4F CE FA
```

3.2 Algorithm XBC-2

The same three test cases are used for XBC-2. Note that the first test case produces the same output since the vectors do not carry forward for that case.

Test Case 1:

$\boldsymbol{K}$:	`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
$\boldsymbol{IV^1}$:	`FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00`
$\boldsymbol{IV^2}$:	`00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF`
$\boldsymbol{PT}$:	`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
$\boldsymbol{IV_n^2 = PT \oplus IV^1}$:	`FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00 FF 00`
$\boldsymbol{IV_n^1 = AES(K, N)}$:	`61 3A 30 90 C5 20 FE 8D A2 94 61 33 84 3B D3 32`
$\boldsymbol{CT = IV_n^1 \oplus IV^2}$:	`61 C5 30 6F C5 DF FE 72 A2 6B 61 CC 84 C4 D3 CD`

Test Case 2:

K :	E5 C7 CD DE 87 2B F2 7C 43 E9 34 00 8C 38 9C 0F
IV_0^1 :	F3 09 62 49 C7 F4 6E 51 A6 9E 83 9B 1A 92 F7 84
IV_0^2 :	4E 6F 77 20 69 73 20 74 68 65 20 74 69 6D 65 20
PT :	12 34 56 78 90 AB CD EF 12 34 56 78 90 AB CD EF 12 34 56 78 90 AB CD EF

$IV_1^2 = PT_0 \oplus IV_0^1$:	E1 3D 34 31 57 5F A3 BE B4 AA D5 E3 8A 39 3A 6B
$IV_1^1 = AES(K, IV_1^2)$:	CB CD 7B DC BC DD D2 1B DA 2D 7D 36 14 F6 73 C4
$CT_0 = IV_1^1 \oplus IV_0^2$:	85 A2 0C FC D5 AE F2 6F B2 48 5D 42 7D 9B 16 E4

$IV_2^2 = PT_1 \oplus IV_1^1$:	D9 F9 2D A4 2C 76 1F F4 DA 2D 7D 36 14 F6 73 C4
$IV_2^1 = AES(K, IV_2^2)$:	25 67 3B 1E DB 07 EF 62 10 BB DE EA 12 77 DA 9D
$CT_1 = IV_2^1 \oplus IV_1^2$:	C4 5A 0F 2F 8C 58 4C DC A4 11 0B 09 98 4E E0 F6

Test Case 3:

K :	A4 B2 FF 1C 29 21 B2 88 34 AB 71 3D 50 CC B4 7E
IV_0^1 :	4C E3 A2 B7 55 57 93 98 81 26 52 0E AC F2 E3 06
IV_0^2 :	7A 62 3E F8 4C 3D 33 C1 95 D2 3E E3 20 C4 0D E0

PT $(ASCII)$:

When we speak of man, we have a conception of humanity as a whole, and before applying scientific methods to the investigation of his movement we must accept this as a physical fact. But can anyone doubt to-day that all the millions of individuals and all the innumerable types and characters constitute an entity, a unit? Though free to think and act, we are held together, like the stars in the firmament, with ties inseparable. These ties cannot be seen, but we can feel them. I cut myself in the finger, and it pains me: this finger is a part of me. I see a friend hurt, and it hurts me, too: my friend and I are one. And now I see stricken down an enemy, a lump of matter which, of all the lumps of matter in the universe, I care least for, and it still grieves me. Does this not prove that each of us is only part of a whole?

PT (hex):

57 68 65 6E 20 77 65 20 73 70 65 61 6B 20 6F 66
20 6D 61 6E 2C 20 77 65 20 68 61 76 65 20 61 20
63 6F 6E 63 65 70 74 69 6F 6E 20 6F 66 20 68 75
6D 61 6E 69 74 79 20 61 73 20 61 20 77 68 6F 6C
65 2C 20 61 6E 64 20 62 65 66 6F 72 65 20 61 70

```
70 6C 79 69 6E 67 20 73 63 69 65 6E 74 69 66 69
63 20 6D 65 74 68 6F 64 73 20 74 6F 20 74 68 65
20 69 6E 76 65 73 74 69 67 61 74 69 6F 6E 20 6F
66 20 68 69 73 20 6D 6F 76 65 6D 65 6E 74 20 77
65 20 6D 75 73 74 20 61 63 63 65 70 74 20 74 68
69 73 20 61 73 20 61 20 70 68 79 73 69 63 61 6C
20 66 61 63 74 2E 20 42 75 74 20 63 61 6E 20 61
6E 79 6F 6E 65 20 64 6F 75 62 74 20 74 6F 2D 64
61 79 20 74 68 61 74 20 61 6C 6C 20 74 68 65 20
6D 69 6C 6C 69 6F 6E 73 20 6F 66 20 69 6E 64 69
76 69 64 75 61 6C 73 20 61 6E 64 20 61 6C 6C 20
74 68 65 20 69 6E 6E 75 6D 65 72 61 62 6C 65 20
74 79 70 65 73 20 61 6E 64 20 63 68 61 72 61 63
74 65 72 73 20 63 6F 6E 73 74 69 74 75 74 65 20
61 6E 20 65 6E 74 69 74 79 2C 20 61 20 75 6E 69
74 3F 20 54 68 6F 75 67 68 20 66 72 65 65 20 74
6F 20 74 68 69 6E 6B 20 61 6E 64 20 61 63 74 2C
20 77 65 20 61 72 65 20 68 65 6C 64 20 74 6F 67
65 74 68 65 72 2C 20 6C 69 6B 65 20 74 68 65 20
73 74 61 72 73 20 69 6E 20 74 68 65 20 66 69 72
6D 61 6D 65 6E 74 2C 20 77 69 74 68 20 74 69 65
73 20 69 6E 73 65 70 61 72 61 62 6C 65 2E 20 54
68 65 73 65 20 74 69 65 73 20 63 61 6E 6E 6F 74
20 62 65 20 73 65 65 6E 2C 20 62 75 74 20 77 65
20 63 61 6E 20 66 65 65 6C 20 74 68 65 6D 2E 20
49 20 63 75 74 20 6D 79 73 65 6C 66 20 69 6E 20
74 68 65 20 66 69 6E 67 65 72 2C 20 61 6E 64 20
69 74 20 70 61 69 6E 73 20 6D 65 3A 20 74 68 69
73 20 66 69 6E 67 65 72 20 69 73 20 61 20 70 61
72 74 20 6F 66 20 6D 65 2E 20 49 20 73 65 65 20
61 20 66 72 69 65 6E 64 20 68 75 72 74 2C 20 61
6E 64 20 69 74 20 68 75 72 74 73 20 6D 65 2C 20
74 6F 6F 3A 20 6D 79 20 66 72 69 65 6E 64 20 61
6E 64 20 49 20 61 72 65 20 6F 6E 65 2E 20 41 6E
64 20 6E 6F 77 20 49 20 73 65 65 20 73 74 72 69
63 6B 65 6E 20 64 6F 77 6E 20 61 6E 20 65 6E 65
6D 79 2C 20 61 20 6C 75 6D 70 20 6F 66 20 6D 61
74 74 65 72 20 77 68 69 63 68 2C 20 6F 66 20 61
6C 6C 20 74 68 65 20 6C 75 6D 70 73 20 6F 66 20
6D 61 74 74 65 72 20 69 6E 20 74 68 65 20 75 6E
69 76 65 72 73 65 2C 20 49 20 63 61 72 65 20 6C
65 61 73 74 20 66 6F 72 2C 20 61 6E 64 20 69 74
20 73 74 69 6C 6C 20 67 72 69 65 76 65 73 20 6D
65 2E 20 44 6F 65 73 20 74 68 69 73 20 6E 6F 74
20 70 72 6F 76 65 20 74 68 61 74 20 65 61 63 68
20 6F 66 20 75 73 20 69 73 20 6F 6E 6C 79 20 70
61 72 74 20 6F 66 20 61 20 77 68 6F 6C 65 3F 00
```

CT :

```
08 C8 B0 8B 68 5A 19 93 F0 7A C1 29 E2 69 E4 53
4A FE D1 FD D6 3E D6 47 F5 C7 EF 97 1B 22 4A 69
38 00 44 0A 88 C9 91 20 31 DA DA 56 84 19 87 C9
```

AD 7B 3F 22 84 E7 5E F7 28 3D 44 12 01 21 E5 D9
81 71 C5 EB 6B A4 B0 EB D9 DF 71 26 5A C0 A4 D5
19 37 05 7C 09 7E B5 3E FB 45 8B FA 0A 46 BA 0C
D9 36 F7 96 05 1E 48 31 D0 AD E1 B3 CC 47 D4 71
6D 67 10 B2 6D FF 67 31 E1 AE 23 22 17 2F A9 80
30 4D 00 25 AA 69 5B 7A 21 9F 36 ED 0C C1 0A CC
43 89 DA 7C 63 17 89 02 6F C9 1A 68 34 B5 C9 EF
45 6F 10 30 10 28 86 82 47 DD 68 7F 0C 09 1F A8
41 8B A6 72 FB 3E 53 5A 52 35 EF 53 08 94 83 A9
28 6A 5E A5 AF A2 0C 6F C8 10 80 1C 79 D6 1A 3A
12 19 7D A0 61 D6 F2 5E EA C9 9B 3C 30 A1 B7 4B
9B EA 2E 80 79 38 AA 64 FE 0D 21 A1 98 16 2E EF
27 9D AC E1 2D 89 9B A6 C8 FC A0 EF 32 06 F9 0A
F8 4E B0 FC 40 9C 52 40 BC 70 99 21 C5 8C 2C 04
71 28 2A 61 FD EB CC 43 B5 AD F5 81 1C 9D EE 00
29 B1 8C A1 8D 7E 0A D3 37 DB 5C 9E 5A 7C B3 47
0E 7F 24 C5 9B 40 41 D7 A8 9D 35 FE 8A 91 CC 49
20 FB A4 47 CF 96 1E E2 3E C7 3A E9 77 49 2B 19
F7 D9 32 72 87 74 73 88 70 B2 C9 61 36 A0 53 60
DA 6C 3B C1 A3 53 5E 35 6F CB F2 03 AB D2 A6 F4
19 47 28 89 93 15 6F 9B 01 3A 00 5B A0 8B 03 E2
20 67 14 DA D3 85 93 AB 23 C5 F8 FA AB D7 A4 FC
38 B9 BB 4B 2D 5E FB D2 87 3F 28 5F 10 90 98 1A
3F 50 BF 0D 34 FE CB 8E D7 81 CD B8 89 BD 88 9C
48 CD CA 3F 28 3E 6A 16 F4 7F DF 60 02 C0 61 42
E1 D3 59 37 A2 18 F4 63 DE 00 7B 54 EE 7F 66 2F
1A 17 99 48 61 EA 29 A0 02 1F 5A 4B 1D CE A0 61
5C 13 3C 02 5A 43 D2 53 70 7A 0D E8 85 C9 69 2E
2B CB B4 A9 BA 91 11 E6 54 6B 09 A9 8C AE 3C 92
FC 68 1D 4B 98 ED F8 CF 54 5F 90 DC A2 DC 64 D3
0E BD 93 D7 DB 20 CA F2 D1 10 39 81 D3 49 CC 62
6D 8C E5 B6 D8 9C D9 CF A8 F5 8A 7F BB EC BE 62
74 FA 24 DD 20 4A 7E 9B B6 70 CF 43 EA AC 12 DD
D5 54 5A 51 36 FD 56 DF 7D FF 93 D6 1A 49 B2 2D
61 AB 38 35 6F 08 4A DE 20 A9 37 AE DA F8 37 B1
8E 59 00 3A 2D 11 31 22 B4 51 2F 80 3F 35 3F 41
82 AF 21 D9 4D 1C FC EE 07 9E 35 92 89 24 AE 51
54 67 62 10 22 80 23 77 31 EB DA F9 1D 73 00 AF
32 4F C5 87 6B 98 81 2C 81 96 68 19 31 ED FC FB
CF 2C DF 22 2E 79 DB 43 6A 2B C8 30 9E 11 D2 C2
63 F6 75 25 83 42 99 48 E8 01 54 C5 86 CA 56 52
FA EE 4D 9A 9D 70 17 69 F1 EE 81 BC 1A 8D C9 43
36 29 5E 89 1E D7 2A E4 A3 B9 73 84 AA C6 4F 51
8D B0 B4 E2 2E 0F AF 90 6D EB 45 50 99 A0 5C 6D
0F DA 32 4A 7E 94 CA EC D8 A0 FB C5 36 33 1B A8
5B D4 A8 FC BD E1 CB 0C EF C5 25 E5 FE 3E AF 6F
35 C2 35 B0 78 98 FB 8F 3F C3 E2 1C 6E AB 8E 19
08 5B AD 8D 70 F4 CA 3E 62 F2 90 CB 6D EC 9B B9
B6 ED 24 78 E8 2C C0 28 A8 CF 40 F1 6D E1 40 E4

4 Performance Estimates

No specific test data was gathered for performance because there are a significant number of things that can affect the overall throughput of nearly any block cipher algorithm. However, the performance for both XBC-1 and XBC-2 should be nearly identical to any block algorithm's sequential ECB and CBC performance results, because neither XBC-1 nor XBC-2 are doing any sort of heavy weight calculation. At most, there should only be a few extra assembly instructions per run of the block cipher algorithm.

5 Intellectual Property Statements / Agreements / Disclosures

There are no patents or patent applications for either XBC-1 or XBC-2 as far as the author is aware. The author also releases all intellectual property for XBC-1 and XBC-2 to the public domain. Therefore, there is no licensing obligation of any kind and XBC-1 and XBC-2 may be used freely by anyone.

6 References

1. Crowdsourcing via Wikipedia, "Two-man rule", http://en.wikipedia.org/wiki/Two-man_rule.

2. W. Dai, "Crypto++ Library", http://www.eskimo.com/weidai/cryptlib.html.

3. NIST, "Advanced Encryption Standard", FIPSPUB 197, November 26, 2001.