From: "Carl Meyer" <CARLHMEYER@email.msn.com>
To: <AESround2@nist.gov>
Subject: AES vote for MARS
Date: Sun, 9 Apr 2000 22:08:10 -0400
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3612.1700
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3612.1700

To whom it may concern,
I have attached a memo giving my reasons for voting.
I would like to point out that I was not biased due to the fact that I am one of the inventors of DES.
At first I actually leaned toward RC6 and RIJNDAEL. But after extensive study of the finalists I came to the MARS decision. I have also attached MARStalk which gives more details of my decision process.
Carl H. Meyer carlhmeyer@msn.com

Carl H. Meyer
27 Lafayette Ave.
Kingston, NY 12401, U.S.A.
Phone: (914) 331-3506
e-mail: CarlHMeyer@msn.com

Saturday, April 8, 2000

Subject: "AES: Justifying Vote for MARS" foil presentation

I think that innovative ideas and concepts employed in the MARS design will only be appreciated by one who is willing to spend considerable time to study it. I am afraid that not many people will do that and hence will look at each of the finalists with an equal amount of limited time. This will put MARS at a considerable disadvantage. In order to highlight the essential MARS design concepts and building blocks I have prepared a foil presentation.

Let me start out to report on my "reviewing experience" which might be representative of others too. I was right away impressed about the brilliant ideas (one-way function and data dependent rotations, to name a few) employed in RC6. It is also easily understood. The RIJNDAEL algorithm, although not as easily comprehended as RC6, is a mathematical beauty which combines individual mathematical operations in a cryptographically secure way. Once the fundamental idea of how the polynomial representation of the byte(s) is used to define the individual operations (addition, multiplication, inverse operations) is grasped, everything falls neatly in place. I would not be surprised if RC6 and RIJNDAEL will become strong contenders for first place. TWOFISH as well as MARS lacks this aura of brilliance. Initially I almost agreed with the statement (I read somewhere) "IBM put everything into the algorithm but the kitchen sink."

By studying design details of all finalists I became more and more impressed about the thoughts which went into the MARS design and how "resistance against future cryptographic breakthroughs" became the guiding principle to connect the different building blocks together. I think that MARS deserves to be selected to become the next standard, but I am deeply concerned that the final decision will be made on "brilliance combined with simplicity" of the design. I think by making "resistance against future attacks" the criteria, a certain degree of structural complexity is required and should be taken into account in selecting the next standard.

The first impression of MARS could be that it is complicated due to the presence of several crypto design ideas which are then replicated. To guide me in my evaluation process as well as to make it easier for others to evaluate the MARS design I am preparing a foil presentation about the key ideas employed in MARS to achieve the main design goal: "Provide not only strong resistance to all known cryptanalytical attacks, but also to protect the cipher against future advances in cryptanalytical

techniques." The presentation uses a high level, top down approach and concentrates on explaining the major building blocks which provide crypto strength, especially with respect to future attacks. By justifying the different methods to achieve that goal the audience might appreciate how much thought went into the designs of the different building blocks.

MARS will not win the simplicity contest against Rijndael or RC6, but could win if the complexity of the design is justified on security grounds.

Individual Topics of Foil presentation

Choosing a Feistel Network Approach for MARS: To justify the choice of a Feistel network for the MARS design we show that it is an evolution from the classical stream cipher to a block cipher. Using a Feistel network has thus the inherent advantage that it evolved from the time proven stream cipher design and thus is preferable to experimenting with new design approaches using non-Feistel networks.

More Details on Feistel Networks: To show that a Feistel network can be considered an evolution from the classical stream cipher let us list the properties of such a cipher: *(1) An identical cryptographic pseudo-random bit stream (defined key stream in the literature) is employed in the encipher/decipher process. (2) The operation generating this key stream does not have to have an inverse since the same bit stream must be generated at the encipher and decipher port. (3) In the enciphering process plaintext is combined with the key stream to generate ciphertext, in the deciphering process ciphertext is combined with the key stream to recover plaintext. The combining operation must thus have an inverse. (In the Vernam stream cipher that operation is an XOR.)*

In a Feistel scheme a source word generates, together with key material, the cryptographic bit stream. This in turn operates on a target word to "encipher it in the stream cipher mode." In the simplest approach, there is one source and one target word. In a general Feistel network there could be "s" source words and "t" target words, resulting in a block size of (s+t) words. A general Feistel network is therefore determined by the number of source and target words defined here as F(s,t). The design could be made more precise by introducing additional parameters which indicate how the transformed source words operate on the target words. One possibility is to form the Cartesian product (S x T) and indicate which of the source words in the set S influence which of the target words in the set T. The designation would in that case be F[(s,t), (subset of S x T)]. If s=1 it is customary to use Mft where MF stands for modified Feistel network.

Since the stream cipher concept has been established as a sound cryptographic operation, it could be argued that the Feistel network structure should also be cryptographically sound.

One Source vs. Two Source Word Approaches in Feistel networks: All finalists define the 128-bit block cipher input by four 32-bit words. Three of them (RC6, TWOFISH, and MARS} are Feistel networks. They use two, two, and one target word(s), respectively as can be observed in Fig. 1 in Ref.[1], Fig. 1 in Ref.[2], and Fig. 2 and 3 in Ref.[3], respectively. The reason why the MARS designers chose one source word is that it is easier to analyze and thus less prone to errors.

MARS Design Principle - Remain Resilient even in the Face of New Crypt analytical Techniques: All of the finalists defend against presently known attacks, but the MARS design concentrates also on designing structures which most likely provide better resistance against as yet undiscovered attacks. As a result, a heterogeneous structure was invented, e.g., the splitting up of the 32 rounds into eight pre- and post-mixing rounds (forward and backwards mixing wrapper layer, respectively) and 16 middle rounds which are split up into two eight round sections (forward and backwards transformation cryptographic core). The middle rounds are designed differently than the top and bottom rounds. The wrapper layers provide rapid avalanche of key bits and the cryptographic core provides good resistance to cryptanalytical attacks. The cipher has the same resistance to attacks launched from the encipher or decipher port (e.g., chosen plaintext/ciphertext attacks} since the forward/backwards operations are essentially inverses of each other.

MARS looks more complex than the other contenders as a consequence of this design approach; but it should be realized that the complexity is not in the different building blocks, which were designed to permit extensive analysis, but in the way these building blocks are interconnected.

References

[1] R. L. Rivest, M. J. B. Robshaw, R. Sydney, and Y. L. Yin, *The RCA Block Cipher*, RSA Data Security, May 28, 1998.

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, Two fish: *A 128-Bit Block Cipher*, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, June 15, 1998.

[3] C. Burwick, D Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, *The MARS Encryption*

Algorithm, IBM (represented by N. Zunic), 522 South Road - MS P330, Poughkeepsie, NY 12601-5400, August 27, 1999 (revised).