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 Vote for MARS

Before explaining the reasons for my vote on MARS I would like to describe, in my view, the distinguishing characteristics of the final five algorithms: (Each of them use four 32-bit input words.)

RC6: Brilliant, innovative, simple scheme. It is a Feistel network with two source words. Each operates, after a transformation process, on the two target words.

Rijndael: Translates fundamental mathematical ideas, based on polynomials, into a strong cryptographic approach. The design, which uses a purely mathematical approach, is a non-Feistel network. Consequently, all operations have an inverse.

Serpent: Highly conservative design which avoids the use of novel, untested ideas. This is in stark contrast to the other four finalists. It is a non-Feistel network. Consequently, all operations have an inverse.

Twofish: Creates four different key-dependent 8-by-8 bit S-boxes (permutations) by employing two fixed 8-by-8 bit S-boxes (permutations) and key material. It is a Feistel network with two source words. Each operates, after a transformation process, on the two target words.

Mars: Distinguishes between top/bottom (wrapper layer, which provides rapid avalanche of key bits) and middle rounds (cryptographic core, which provides resistance to cryptanalytical attacks). It is a Feistel network with one source word. It operates, after a transformation process, on the three target words.

Reasons for my vote choosing Mars for the AES:

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; however, 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.

To summarize, using "resistance against future crypto breakthroughs" as the main criteria to make the final selection I concluded that Serpent, RC6, Rijndael, and Twofish would not meet that criteria due to their simpler structures. Serpent could be criticized in addition for not using bigger S-boxes. (When we invented the DES we were limited in the S-box size due to chip requirements. The DES chip in the 1977 time frame was the densest chip IBM produced.)

Carl H. Meyer

PS If the selection criteria would be "ELEGANCE and novelty" I would have a hard time to choose between RC6 and RIJNDAEL.