Fişa suspiciunii de plagiat / Sheet of plagiarism's suspicion	Indexat la: 49/06

Opera suspicionată (OS) Suspicious work	Opera autentică (OA) Authentic work

OS	MANG, E., MANG, I. An FPGA-based implementation of the key transformation procedure in the MARS algorithm. *Journal of Computer Science and Control Systems*. **3**(1), 2010, 119-122.
OA	* * *, MARS Encryption, Disponibil la: http :// www . tropsoft . com / strongenc / mars . htm.

Incidenţa minimă a suspiciunii / Minimum incidence of suspicion	
p.119:01s – p.119:04s	p.02:33 – p.02:35
p.119:19s – p.119:31s	p.02:35 – p.02:45
p.119:42d - p.119:47d	p.02:45 – p.02:47

Tropical Software

PC Security
Private Desktop
Private Pix
Private Encryptor
Secure Browser
Strong Encryption
Winvestigator
Ergotimer

Download
Buy Now
Technical Support
Prices
Join Mailing List
About Us
Links
Site Map

Purchase | Product Information | Screen Shots | Technical Information

MARS Encryption

Overview

About the Advanced Encryption Standard (AES)

The DES algorithm has become obsolete and is in need of replacement. To this end the National Institute of Standards and Technology (NIST) has been holding a competition to develop the Advanced Encryption Standard (AES) as a replacement for DES. Triple DES has been endorsed by NIST as a temporary standard to be used until the AES is finished sometime in 2001.

NIST has been working very closely with industry and the cryptographic community during the development of the Advanced Encryption Standard. The overall goal is to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm (or algorithms) capable of protecting sensitive government information well into the next century. The algorithm(s) is expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.

On January 2, 1997, NIST announced the initiation of the AES development effort and made a formal call for algorithms on September 12 of that year. The call stipulated that the AES would specify an unclassified, publicly disclosed encryption algorithm(s), available royalty-free, worldwide. In addition, the algorithm(s) must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128 bits and key sizes of 128, 192, and 256 bits.

On August 20, 1998, NIST announced a group of fifteen AES candidate algorithms at the First AES Candidate Conference (AES1). These algorithms had been submitted by members of the cryptographic community from around the world. At that conference and in a simultaneously published Federal Register notice, NIST solicited public comments on the candidates. A Second AES Candidate Conference (AES2) was held in March 1999 to discuss the results of the analysis conducted by the global cryptographic community on the candidate algorithms. The public comment period on the initial review of the algorithms closed on April 15, 1999. Using the analyses and comments received, NIST selected five algorithms from the original fifteen submissions.

The AES finalist candidate algorithms are MARS, RC6, Rijndael, Serpent, and Twofish. Four of the algorithms (MARS, Rijndael, Serpent, and Twofish) are supported by Private Encryptor. NIST has developed a Round 1 Report describing the selection of the finalists.

These finalist algorithms received further analysis during a second, more in-depth review period prior to the selection of the final algorithm(s) for the AES. The comment period on the remaining algorithms ended on May 15, 2000. Comments and analysis were actively sought by NIST on any aspect of the candidate algorithms, including, but not limited to, the following topics: cryptanalysis, intellectual property, comparative analyses of all of the AES finalists, and overall recommendations and implementation issues. An informal AES discussion forum was also provided by NIST for interested parties to discuss the AES finalists and relevant AES issues.

Near the end of Round 2, NIST sponsored the Third AES Candidate Conference (AES3), which was an open, public forum for discussion of the analyses of the AES finalists. AES3 was held April 13-14, 2000 in New York. Submitters of the AES finalists were invited to attend and engage in discussions regarding comments on their algorithms.

At the time this document is being written, the Round 2 public analysis period is just ending. Over the next few months NIST intends to study all available information from the Round 2 analysis and make a selection for the AES from among one or more of the finalists. Currently, NIST anticipates that it will announce the AES selection by late summer or early fall of 2000. No date has yet been set for this announcement. Following the announcement, NIST intends to publish a Round 2 Report that will summarize information from Round 2 and explain the algorithm selection.

Shortly thereafter, a draft Federal Information Processing Standard (FIPS) for the AES will be published for public review and comment. Following the comment period, the standard will be revised by NIST in response to those comments. A review and approval process will then follow. If all steps of the AES development process proceed as planned, it is anticipated that the standard will be completed by the summer of 2001.

About MARS

MARS is a block cipher designed by IBM as a candidate algorithm for the Advanced Encryption Standard (AES). It has been selected as one of the five finalists in the AES competition. MARS has a very high level of security and is much more efficient than many older algorithms. The algorithm is resistant to all known shortcut attacks. Its design takes advantage of the powerful capabilities of modern computers to allow a much higher level of performance than can be obtained from less optimized algorithms such as DES. MARS is unique in that it combines virtually every design technique known to cryptographers in one algorithm. But it does so in a way that is easy to analyze so that the properties of the algorithm are more completely understood, decreasing the probability that any loopholes exist which might weaken the algorithm.

The MARS cipher actually consists of a mixture of two very different structures, so that an attack that works against one portion of the algorithm wouldn't be able to affect the other. More importantly, this mixed structure is likely to provide better resistance against new, as yet undiscovered attacks that might be used in the future. This design strategy makes sense in light of the fact that MARS, like all AES algorithms, is intended to have a useful lifetime of a few decades at least. The combination of high security, high speed, and flexibility makes MARS an excellent choice for the encryption needs of the information world well into the 21st century.

In Depth

MARS is a 128-bit block cipher, meaning that data is encrypted and decrypted in 128-bit chunks. The key length can vary from 128 to over 400 bits, but for the purposes of the AES it is defined to be either 128, 192, or 256 bits. This block size and variable key length is standard among all AES candidates and was one of the major design requirements specified by NIST. The main cryptographic core uses 16 rounds, or iterations, to encrypt and decrypt data. This inner core is wrapped by a layer of mixing rounds using an entirely different structure. This is the second structure that was mentioned above. These "wrappers" don't actually perform encryption or decryption, but merely mix up the input data and prepare to feed it to the cryptographic core. Eight mixing rounds are executed before the input data is fed to the main algorithm, and eight more mixing rounds are performed on the resulting ciphertext to complete the process. It is possible to turn off these mixing rounds and pass the plaintext directly through the cryptographic core, but this is not advisable because it would significantly weaken the security of MARS.

Private Encryptor's implementation of MARS uses a 448-bit key. We decided to use the largest possible key size to ensure that the user always enjoys the best possible security. Our design philosophy is that security always comes before speed. If a shorter key is provided by the user, Private Encryptor pads the key in a special, seemingly random, way to make it 448 bits long. Such a large key size may seem like overkill, but the algorithm supports it and there are no significant costs in terms of encryption speed, so why not use a large key?

The detailed description of the actual algorithm is contained in the official MARS paper submitted for the AES competition by IBM. The paper is rather technical and a certain degree of mathematical proficiency is required of the reader in order to understand it.

Download the MARS algorithm specification: MARS.pdf

Buy Strong Encryption Package™ Now!

Back to Product Information

Purchase | Product Information | Screen Shots | Technical Information

PC Security	Private Encryptor	Strong Encryption Package	Winvestigator
Private Pix	Private Desktop	Ergotimer	Secure Browser
Home	Download	Order	Tech Support	Prices	About Us