Performance Analysis of AES and MARS Encryption Algorithms

Mohan H. S.[1] and A Raji Reddy[2]

[1] Research Scholar, Dr MGR University, Chennai, India

[2] Professor, Department of Electronics and Communication
Madanapalle Institute of Technology & Science, Angallu, Madanapalle, Chittoor, India

Abstract

Block ciphers are very important in communication systems as they provide confidentiality through encryption. The popular block ciphers are Advanced Encryption Standard (AES) and MARS algorithms. Each cipher uses several rounds of fixed operations to achieve desired security level. The security level is measured in terms of diffusion and confusion. The diffusion level should be at least equal to strict avalanche criterion (SAC) value. Therefore, the number of rounds are chosen such that the algorithm provides the SAC value. This paper presents measured diffusion value of AES and MARS algorithms. Diffusion values are compared for both the algorithms: AES and MARS. Similarly, speed of each algorithm is compared.

Keywords: *AES, MARS, SAC, block ciphers.*

1. Introduction

The principal goal in the design of any encryption algorithm must be security. It is required to achieve the desired security level at minimal cost or expenditure. In block ciphers, the cost can be reduced if the algorithm uses less number of rounds. Therefore, it is required to do a trade-off between the security level and cost of the algorithm. This paper addresses these issues and makes comparative study of AES and MARS for diffusion analysis.

In the remaining section, it discusses symmetric algorithms, stream and block ciphers, cryptanalysis, key schedule and SAC. In section 2, it discusses AES and MARS algorithms. Diffusion analysis results are presented in section 3. Speed of each algorithm is also presented.

1.1 Symmetric Algorithms

There are two general types of key based algorithms: Symmetric and Public Key. In Symmetric algorithms encryption key can be same as the decryption key and vice versa. These are also called as secret key algorithms. Symmetric algorithms can be divided into two categories: i) some operate on the plaintext a single bit at a time which are called Stream ciphers, and ii) others operate on the plaintext in groups of bits, such groups of bits are called blocks and such algorithms are called Block ciphers.

1.2 Stream Ciphers and Block Ciphers

Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. Stream ciphers are more suitable for situations where transmission errors are highly probable.

Symmetric key block ciphers are the most prominent and important elements in many cryptographic systems. Individually, they provide confidentiality. The examples of block ciphers are DES, 3-DES, FEAL, SAFER, RC5 and AES. The implementation of any basic block cipher is generally known as Electronic Code Book (ECB) mode. In order to increase the security further additional modes are also defined. They are (1) Cipher Feed Back (CFB) mode (2) Output Feed Back (OFB) mode (3) Counter mode (CTR). The counter mode has become popular in IPSec and IPv6 applications.

1.3 Cryptanalysis

There are two general approaches for attacking a conventional encryption algorithm:

Cryptanalysis: This is used for deciphering a m essage without any knowledge of the enciphering details. Cryptanalysis is the science of recovering the plaintext of a message without the access to the key. Successful cryptanalysis may recover the plaintext or the key. It also finds weakness in the cryptosystem.

Brute – Force attack: The attack tries every possible key on a piece of cipher text until an intelligible translation into plain text is obtained. This is tedious and may not be feasible if key length is relatively long.

1.4 Confusion and Diffusion

These are the two important techniques for building any cryptographic system. Claude Shannon introduced the terms Confusion and Diffusion. According to Shannon, in an ideal cipher, "all statistics of the cipher text are independent of the particular key used". In Diffusion, each plaintext digit affects many cipher text digits, which is equivalent to saying that each cipher text digit is affected by many plain text digits.

All encryption algorithms will make use of diffusion and confusion layers. Diffusion layer is based upon simple linear operations such as multi-permutations, key additions, multiplication with known constants etc. On the other hand, confusion layer is based upon complex and linear operations such as Substitution Box (S-box).

1.5 Key Schedule Algorithm

A final area of block cipher design is the key schedule algorithm. A block cipher requires one sub-key for each round of operation. The sub-key is generated from the input master key. Generation of sub-key requires an algorithm. This algorithm should ensure that not sub-key is repeated. In general, we select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key.

1.6 Avalanche criteria

There are two different types of strict avalanche criteria: i) First order SAC: It is a change in output bit when a single input bit is flipped and ii) Higher order SAC: It is a change in output bit when many input bits are flipped.

2. Encryption Algorithms

2.1 Evaluation of Advanced Encryption Standard

In 1997, the National Institute of Standards and Technology (NIST) announced a program to develop and choose an Advanced Encryption Standard (AES) to replace the aging Data Encryption Standard (DES).In 1998, NIST announced the acceptance of fifteen candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this preliminary research and selected MARS, RC6, Rijndael, Serpent and Twofish as finalists. An interesting performance comparison of these algorithms can be found in [3]. On October 2000 and having reviewed further public analysis of the finalists, NIST decided to propose Rijndael as the Advanced Encryption Standard (AES). Rijndael, designed by Joan Daemen (Proton World International Inc.) and Vincent Rijmen (Katholieke Univeriteit Leuven) of Belgium, is a block cipher with a simple and elegant structure [2].The Advanced Encryption Standard (AES), also known as the Rijndael algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys of 128, 192 or 256 bits. AES was introduced to replace the Triple DES (3DES) algorithm used for a good amount of time universally. Though, if security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come. The main drawback was its slow software implementation. For reasons of both efficiency and security, a larger block size is desirable. Due to its high level security, speed, ease of implementation and flexibility, Rijndael was chosen for AES standard in the year 2001.

2.2 Rijndael Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) as show in the diagram. These rounds are governed by the following transformations:

	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Fig 1. Key-Block-Round Combinations.

(i) Bytesub transformation: Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

(ii) Shiftrows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

(iii) Mixcolumns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column

vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

(iv) Addroundkey transformation: Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

The encryption procedure consists of several steps as shown by Fig. 2. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

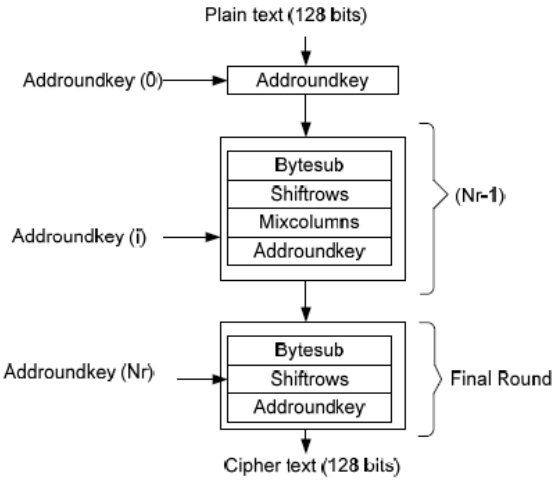


Fig 2 AES algorithm- Encryption Structure

2.3 MARS Algorithm

MARS is a shared-key block cipher, with a block size of 128 bits and a key size of 128 bits. It was designed to meet and exceed the requirements for a standard for shared-key encryption. It takes four 32-bit words plaintext as input and produces four 32-bit words ciphertext as output. The cipher itself is word-oriented, in that all the internal operations are performed on 32-bit words, and hence the internal structure is endian-neutral (i.e., the same code works on both little- endian and big-endian machines). When the input (or output) of the cipher is a byte stream, we use little endian byte ordering to interpret each four bytes as one 32-bit word.

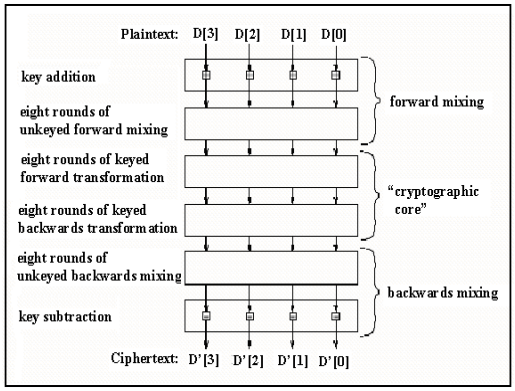


Fig 3. High-level structure of the cipher

The general structure of the cipher is depicted in Figure 3. The cipher consists of a "cryptographic core" of keyed transformation, which is wrapped with two layers of cryptographic cores providing rapid key avalanche.

The first phase provides rapid mixing and key avalanche, to frustrate chosen-plaintext attacks, and to make it harder to "strip out" rounds of the cryptographic core in linear and differential attacks. It consists of addition of key words to the data words, followed by eight rounds of S-box based, un-keyed type-3 Feistel mixing (in "forward mode").

The second phase is the "cryptographic core" of the cipher, consisting of sixteen rounds of keyed type-3 Feistel transformation. To ensure that encryption and decryption have the same strength, we perform the first eight rounds in "forward mode" while the last eight rounds are performed in "backwards mode".

The last phase again provides rapid mixing and key avalanche, to protect against chosen-ciphertext attacks. This phase is essentially the inverse of the first phase, consisting of eight rounds of the same type-3 Feistel mixing as in the first phase (except in "backwards mode"), followed by subtraction of key words from the data words.

3. Performance Analysis

The performance analysis can be done with various measures such as 1) Diffusion analysis of MARS and AES 2) Speed comparison with encryption and decryption cycles, key setup and key initialization, analysis of various key sizes, fair speed/security. The performance analysis will be presented in the form of tables and figures below.

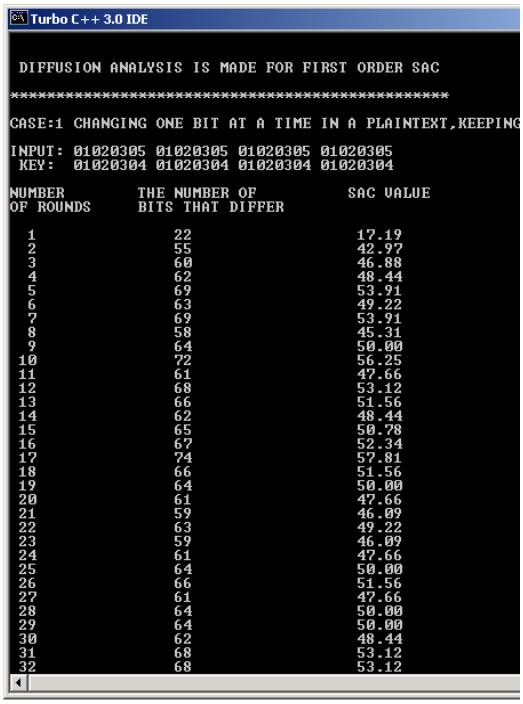
3.1 Diffusion analysis

Diffusion is made for AES and Mars algorithm that exhibits a strong avalanche effect for First order SAC and Higher order SAC taking the following cases.

1. Changing one bit at a time in a plaintext, keeping key as constant.
2. Changing one bit at a time in a key, keeping plaintext as constant.
3. Changing many bits at a time in a plaintext, keeping key as constant.
4. Changing many bits at a time in a key, keeping plaintext as constant.

a) Diffusion of MARS

Table 1: Results of Avalanche Effect of MARS



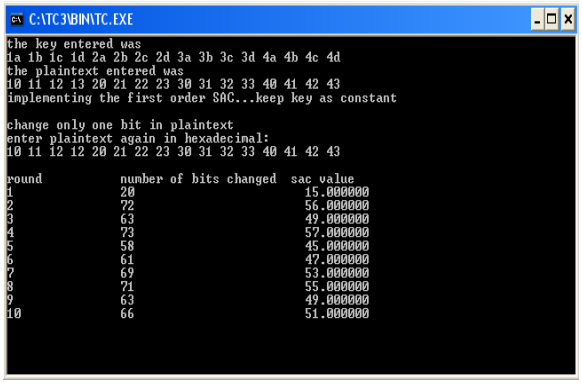
As shown in Table 1, at the end of first round, 22 bits of cipher value have changed out of 128-bit cipher text. This resulted an Avalanche value of 17.19%. As we observe in the Table1, SAC is achieved at the end of 5th round and Avalanche values changes around the SAC value for the remaining rounds. The final round has an Avalanche value of 53.12%.

Similar kind of results is obtained for the remaining three cases.

b) Diffusion of AES

As shown in Table 2, at the end of first round, 20 bits of cipher value have changed out of 128-bit cipher text. This resulted an Avalanche value of 15%.As we observe in the Table2, SAC is achieved at the end of 2nd round and Avalanche values changes around the SAC value for the remaining rounds. The final round has an Avalanche value of 51%.

Table 2: Results of Avalanche Effect of AES



3.2 Speed Analysis

The performance of the algorithm is measured in terms of the speed, i.e., number of cycles required for the completion of the function. The speed of the algorithm can be characterized by measuring the time required for key scheduling, encryption and decryption. These parameters are measured for both the algorithms: AES and MARS.

a) Speed and Key Setup Comparisons

Table 3: Speed

	Speed		Key Setup		
Cipher	Encrypt (Cycles)	Decrypt (Cycles)	Encrypt	Decrypt	Init
MARS	1600	1580	4780	5548	18
Rijndael	1276	1276	17742	18886	28

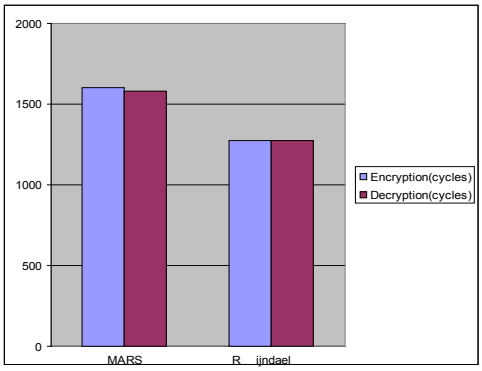


Fig. 4 Graph for Encryption and Decryption(cycles)

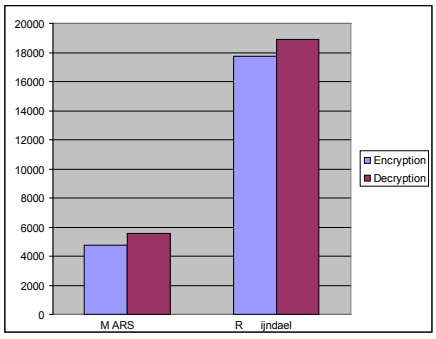


Fig. 5 Graph for key setup Encryption and Decryption

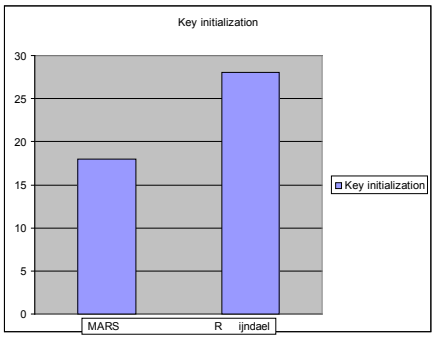


Fig. 6 Key initialization

b) Analysis using variable key sizes

i) Encryption

Table 4: Encryption

Algorithm	Encrypt 128	Encrypt 192	Encrypt 256
MARS	3738	3707	3733
Rijndael	4855	4664	4481

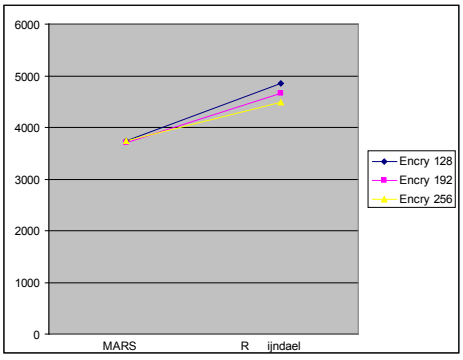


Fig. 7 Encryption

ii) Decryption

Table 5: Decryption

Algorithm	Decrypt 128	Decrypt 192	Decrypt 256
MARS	3965	3965	3936
Rijndael	4819	4624	4444

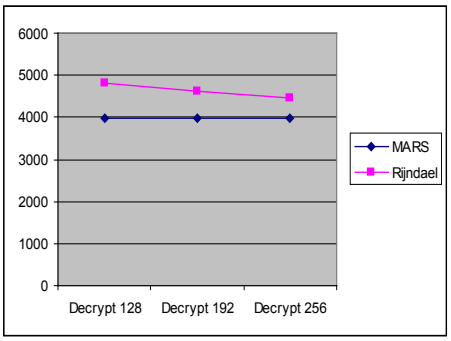


Fig. 8 Decryption

c) Fair Speed and Security Comparisons

Table 6: Speed/Security comparison

Cipher	Original (Cycles)	Rounds	Minimal Rounds	Time (Cycles)
MARS	1600	32	20	1000
Rijndael	1276	10	8	1021

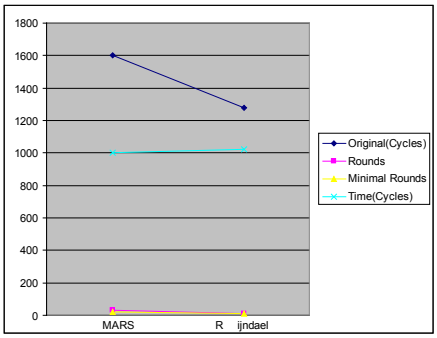


Fig. 9 Security comparison

4. Conclusions

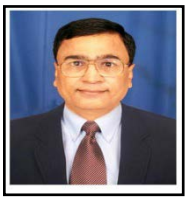
The results of diffusion analysis indicates that required diffusion level is achieved at the end of 5th round in the MARS encryption algorithm. No major improvement is achieved in the rounds from 6 to 32. Whereas the results of AES indicate that the diffusion level is achieved at the end of 2nd round itself. Rijndael is well suited to be implemented efficiently on a wide range of processors and in dedicated hardware on both the Pentium and Pentium Pro processors is about 320 clocks per block. Unlike RC6 and Mars, there are no known CPU platforms (8-bit or 32-bit) on which Rijndael's relative performance would be unduly negatively affected or on which timing attacks would be possible. Mars is not suitable for Smart card implementation whereas Rijndael is very much suitable for widespread smart card implementation. By the analysis of various factors we can conclude from the results tabulated

that Rijndael is more secure and strong when compared to MARS algorithm.

References

[1] W Stallings, CRYPTOGRAPHY AND NETWORK SECURITY, Printice Hall, 2003.
[2] AES page available via http://www.nist.gov/CryptoToolkit.4
[3] Computer Security Objects Register (CSOR): http://csrc.nist.gov/csor/.
[4] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999, available at [1].
[5] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.
[6] B. Gladman's AES related home page http://fp.gladman.plus.com/cryptography_tetechnolo/.
[7] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.
[8] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997, p. 81-83.
[9] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.
[10] Mohan H.S and A. Raji Reddy. "Diffusion Analysis of Mars Encryption Algorithm", International conference on current trends of information technology,MERG-2005,Bhimavaram, Andhrapradesh.
[11] N. Penchalaiah , "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010, pp.1641-1645.
[12] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27 2007
[13] B.D.C.N.Prasad, P E S N Krishna Prasad, "A Performance Study on AES algorithms", International Journal of Computer Science and Information Security, Vol. 8, No. 6,September 2010,pp 128-132.
[14] Mohan H.S and A. Raji Reddy. "Generating the New S-box and Analyzing the Diffusion Strength to Improve the Security of AES Algorithm", International Journal of Computer and Network Security, Vol. 2, No. 9, September 2010.
[15] B. Schneier and D. Whiting, A Performance Comparison of the Five AES Finalist, 15 March 2000.

Mohan H.S. received his Bachelor's degree in computer Science and Engineering from Malnad college of Engineering, Hassan during the year 1999 and M . Tech in computer Science and E ngineering from Jawaharlal Nehru National College of Engineering, Shimoga during the year 2004. Currently pursing his part time Ph.D degree in Dr. MGR university,Chennai. He is working as a professor in the Dept of Information Science and Engineering at SJB Institute of Technology, Bangalore-60. He is having total 12 years of teaching experience. His area of interests are Networks Security, Image processing, Data Structures, Computer Graphics, finite automata and formal languages, Compiler Design. He has obtained a best teacher award for his teaching during the year 2008 at SJBIT Bangalore-60. He has published and presented papers in journals, international and national level conferences.



A. Raji reddy received his M.Sc from Osmania University and M.Tech in Electrical and Electronics and c ommunication Engineering from IIT, Kharagpur during the year 1979 and hi s Ph.D degree from IIT, kharagpur during the year 1986.He worked as a senior scientist in R&D of ITI Ltd, Bangalore for about 24 years. He is currently working as a pr ofessor and head i n the department of Electronics and C ommunication, Madanapalle Institute of Technology & Science. Madanapalle. His current research areas in Cryptography and its application to wireless systems and net work security. He has published and presented papers in journals, international and national level conferences.