

SEMIARID JOURNAL OF ACADEMIC RESEARCH AND DEVELOPMENT (SJARD)

Security Algorithm in Internet Environment Problem Analysis, Description and Evaluation

^{1*}Muhammad Umar Diginsa, ²Muhammad Idris, ¹Sabi'u Usman Suleiman and ¹Nazifi Musa

¹Department of Computer Engineering, Binyaminu Usman Polytechnic Hadejia

²Department of Computer Science, Binyaminu Usman Polytechnic Hadejia

ABSTRACT

With the fast evolution of digital data exchange, security information is very important in data storage and transmission. Data encryption is widely used to ensure security in open networks such as the internet. Security is a very important factor in every field such as Government Agencies (EFCC, CBI, and FBI), Research Organization, E-commerce and etc. where internet is being used. Each type of data has its own features; therefore, different techniques should be used to protect confidential image data from unauthorized access. Cryptography is a technique use to secure data on the network from unauthorized user. The two major types of cryptographic algorithms are Symmetric cryptography and Asymmetric cryptography. In this paper another technique has been produce to improve the security of cryptographic algorithm by implementing Meta-Morphic cipher using c programming language and compare the algorithms and know which of the algorithms provides better (security, efficiency, accuracy and effectiveness).

Keywords: Cryptography, Encryption, Symmetric, Asymmetric, Meta-Morphic function.

Introduction

The Metamorphic-Enhanced MARS Cipher is a metamorphic cipher that improves the MARS Cipher. The user key is first encrypted then the encrypted key is used to generate the sub-keys. The Meta-MARS encryption function is built using the four low-level operations in the MARS encryption cipher. All operations are at the bit level composing the basic Crypto Logic Unit (CLU) .Where the operation selection bits can be chosen from any two sub-key consecutive bits [4].

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 [2]. Its design to take 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 [1].

<i>Mnemonic</i>	<i>Operation</i>	<i>Select Operation code</i>
XOR	$C_i = K_i \oplus P_i$	00
INV	$C_i = \neg(P_i)$	01
ROR	$P_i \leftarrow P_j$	10
NOP	$C_i = P_i$	11

Table1.0: The basic cipher engine (encryption function) operations [4]

The basic crypto logic unit (CLU) is shown in Table 4.1. All operations are at the bit level. The unit is to be repeated a number of times depending on the required word or blocksize. The rotation operation, referred to by the circular arrow, is performed using multiplexers. In this table, if we change the output cipher bit to become an input plain text bit, the new output will be the same as the old plain text bit. Obviously, this is a feature of the applied functions namely XOR, INV or NOP. The only exception is in the case of ROR, the decryptor will use ROL [3].

1.2 Meta-Morphic Algorithm

In this section, we provide the formal description of the Metamorphic MARS block cipher algorithm as follows:

Algorithm: METAMORPHIC MARS BLOCK CIPHER

INPUT: Plain text message P, User Key K

OUTPUT: Cipher Text C

Algorithm body:

Encryption Function

Begin

1. Read P message from the user.
2. Read user Key K.

3. Encrypt message plain text by calling the Meta-MARS encryption function.
4. Repeat step 3 till the P_i message encrypted.

End Encryption;

Function Meta-MARS Encryption

Begin

1. Read P_i message.
2. Read next k_i from sub-key;

End Meta-MARS
End Algorithm [44].

3. Read selection bits of sub-key;
4. Read rotation selection bits from sub-key.
5. Use selection & rotation bits to select and perform the operation: XOR, INV, ROR, NOP in Meta-h functions in Meta-MARS Algorithm;

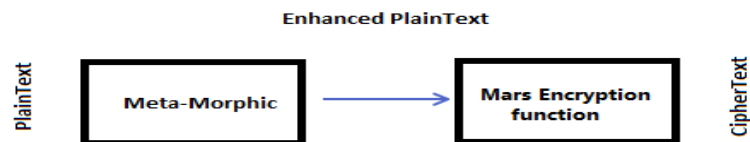


Figure 1.0:Encryption Processing Cycle



Figure 1.1:Decryption Processing Cycle

1.3 Metamorphic strategy

- We can use the Meta-MARS function before and after cipher process to improve ciphering, the plaintext is used to be an input to the Meta-MARS function.
- Then the output of the Meta-MARS function used to be
- input to the Encryption function.
- Finally the output of the ciphering process is used to be an input of the Meta-MARS function, the following figure 1.2 describes the ciphering process [1].

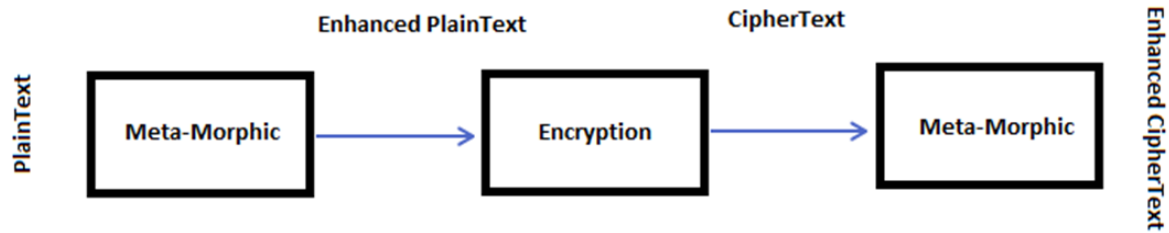


Figure 1.2:Encryption Processing Cycle [1].

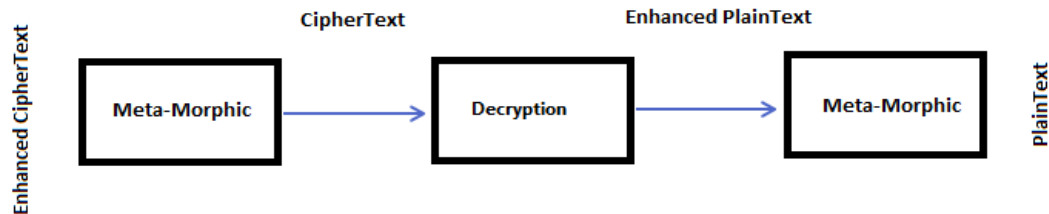


Figure 1.3 Decryption Processing Cycle

2.0 MATERIAL AND METHODS

2.1 Comparison of the Algorithms

This section intends to give the readers the necessary background to understand the key differences between the compared algorithms. Security level of the encryption algorithm should depend on the size of the key space, secrecy of the key, length of the key, initialization vector and how they all work together. Depending upon the number of keys used, cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). Symmetric-key system uses a single key that both the sender and recipient have. Asymmetric-key system uses two keys, a public key known to everyone and a private key that only the recipient of the messages uses. The symmetric key algorithms are further classified as block cipher (AES) and stream cipher (RC4).

DES: (Data Encryption Standard), was the first encryption standard to be recommended

by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher [6]

3DES: As an enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods [50].

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard. Brute force attack is the only effective attack known against it, in which the attacker tries to test

all the characters combinations to unlock the encryption. Both AES and DES are block

ciphers

[6].

	Comparison of DES, 3DES And AES Algorithm		
	Symmetric Encryption Algorithms		
	DES	3DES	AES
Block Size	64 bit	64 bit	128 bit
Key Size	56 bit	168 bit	128, 192, 256 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network
Rounds	16	48	9,11,13
Attacks	Brute Force Attack	Theoretically Possible	Side Channel Attacks

Table 1.2: Comparison of different Algorithms

2.2 Space Time Complexity

The better the time complexity of an algorithm is, the faster the algorithm will carry out its work in practice. Apart from time complexity, its space complexity is also important: This is essentially the number of memory cells which an algorithm needs. A good algorithm keeps this number as small as possible, too.

There is often a time-space-tradeoff involved in a problem, that is, it cannot be solved with few computing time and low memory consumption. One then has to make a compromise and to exchange computing time for memory consumption or vice versa, depending on which algorithm one chooses and how one parameterizes it.

Most of these algorithms (i.e. the block ciphers DES, Triple DES, AES, Blowfish) are normally only working on a **fixed block size**, and take approximately the same time independently of input, thus they are $O(1)O(1)$.

If you put them into a mode of operation to encrypt longer messages, you usually get an $O(m)O(m)$ complexity, where m is the message size, having $O(m)O(m)$ blocks of data to encrypt.

(One could design modes of operations with different complexity, but they have to touch at least each input bit once to be reversible, thus $O(m)O(m)$ is a minimum. Also, with $O(m)O(m)$ block cipher calls you can do enough to make it secure, so there is no point of making it slower.) [7]

Two more notes to specific ciphers:

- Yes, Triple-DES usually needs thrice the computing power as DES, but this then becomes $O(1)O(1)$ or $O(m)O(m)$, too.
- Blowfish is known for its quite slow key schedule (which takes as long as encrypting about 4 KB of data), but this is still $O(1)O(1)$.

Thus, OO-notation is not really an interesting thing to look at in block ciphers.

It gets a bit more interesting when we look at algorithms with a **varying input size**. For the asymmetric algorithm RSA, we have the public (and private) key modulus n , and its size $k = \lceil \log_2 n \rceil$ in bits can be considered a security parameter. (The private exponent d is of similar size, while the public exponent e is usually some small number like 33 or 65537 = 216 + 165537 = 216 + 1.) The message size is then limited by $O(k)O(k)$, too.

Encryption and decryption are both modular exponentiations of plaintext or cipher text modulo n , with the respective

exponents. With the square-and-multiply algorithm, encryption needs $O(1)O(1)$, decryption $O(k)O(k)$ multiplications and a similar number of modular reductions, each of k -bit or $2k$ -bit numbers ... which means about $O(k^2)O(k^2)$ or $O(k^3)O(k^3)$ elementary operations (with a quite small factor, as you use the word size build into your processor).

Decryption can be speed up by storing the factors of n , but this still gives only a constant factor, I think (i.e. it reduces the k in the formulas).

RSA also uses one of various padding schemes, but this should be in $O(k)$ and thus not contribute to the complexity.[8

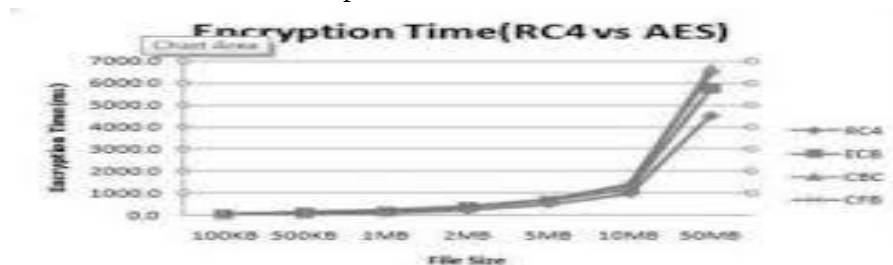


Figure 1.4: Encryption Time

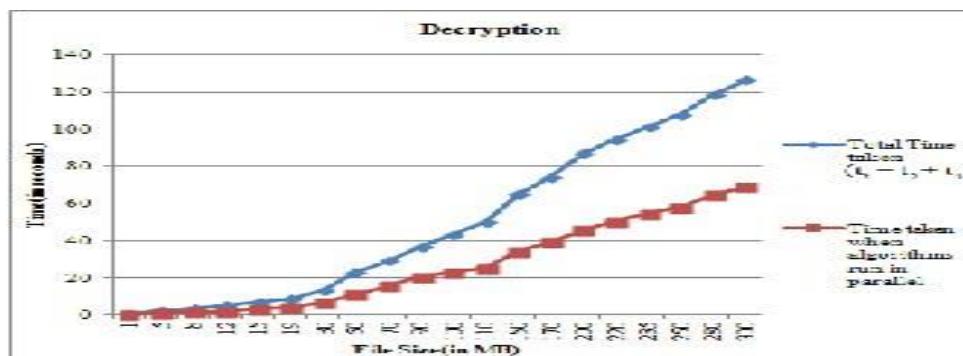


Figure 1.5: Decryption Time.

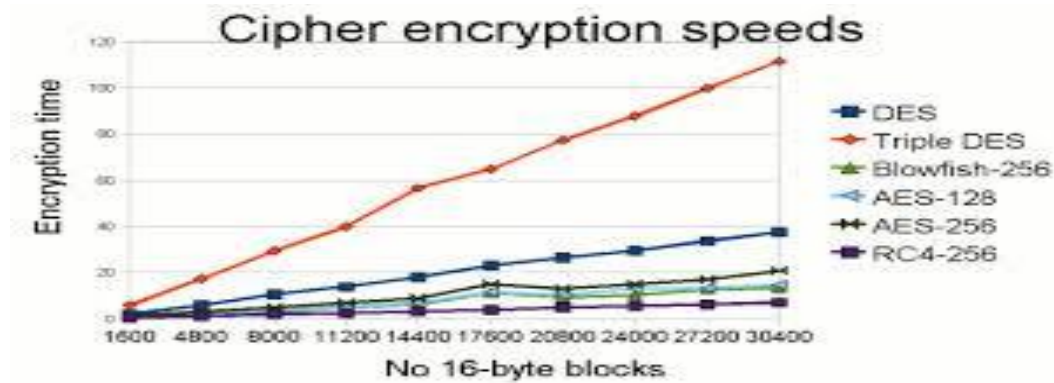


Figure 1.6: Encryption Speed.

2.3 Performance

As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. [9]

This section tries to present comparison between Security algorithms in the data encryption field. Since our main concern here is the performance of these algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. [10] [11].

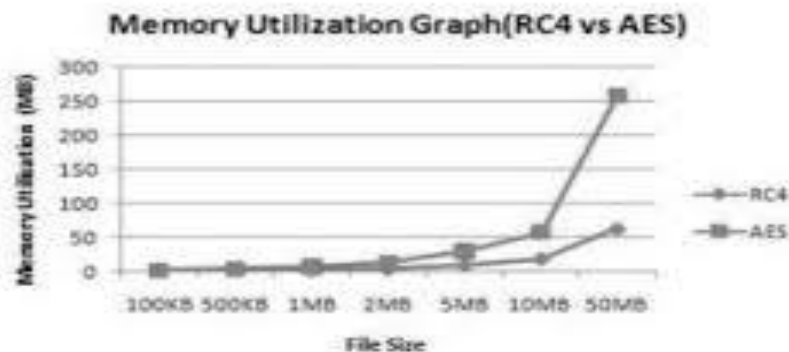


Figure 1.7: RC4 and AES Memory Utilization

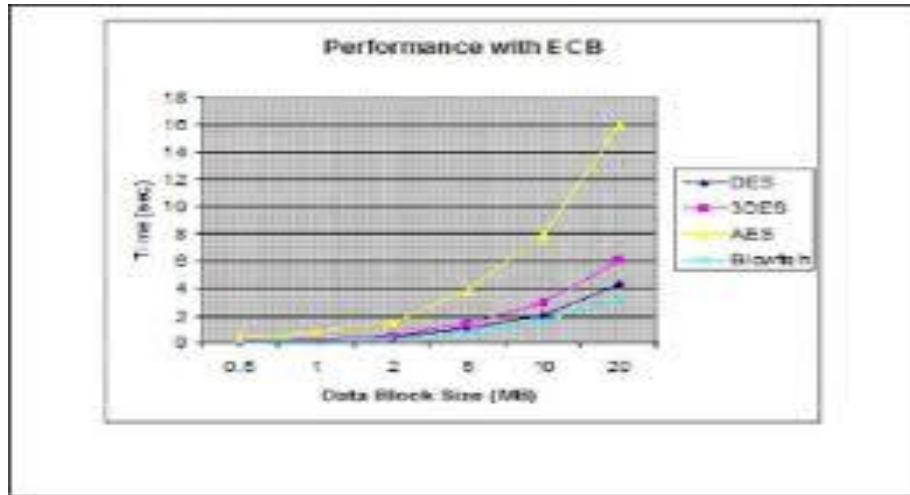


Figure 1.8: AES, DES, 3DES ECB performance curve

Implementation of Security Algorithms Using C Language

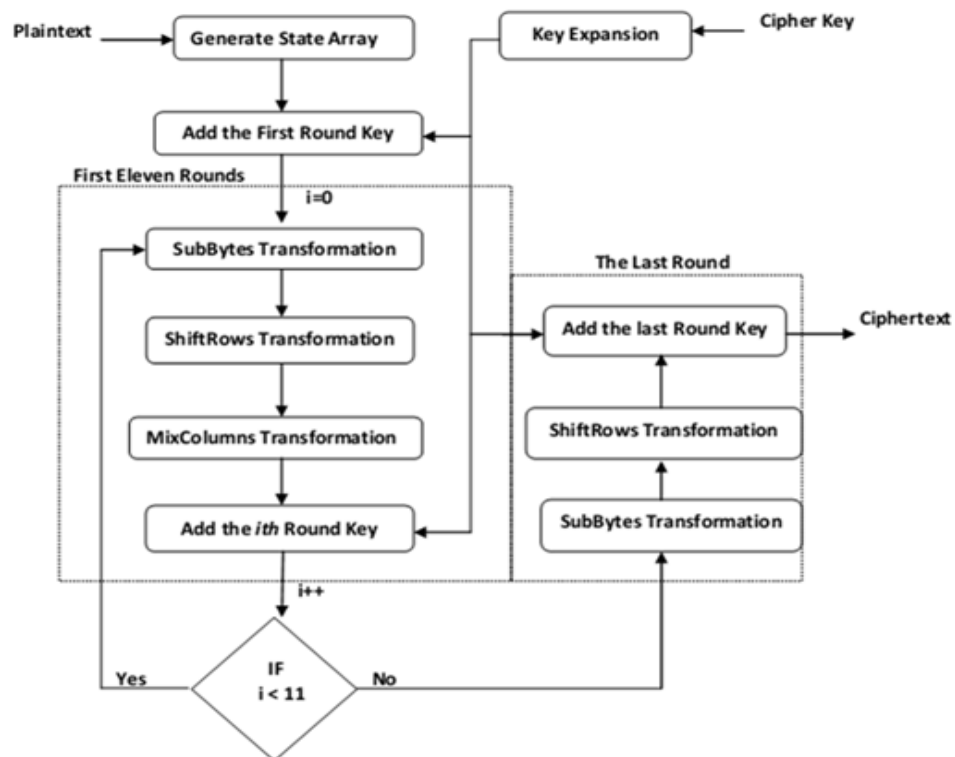


Figure 1.9: DES Flowchart

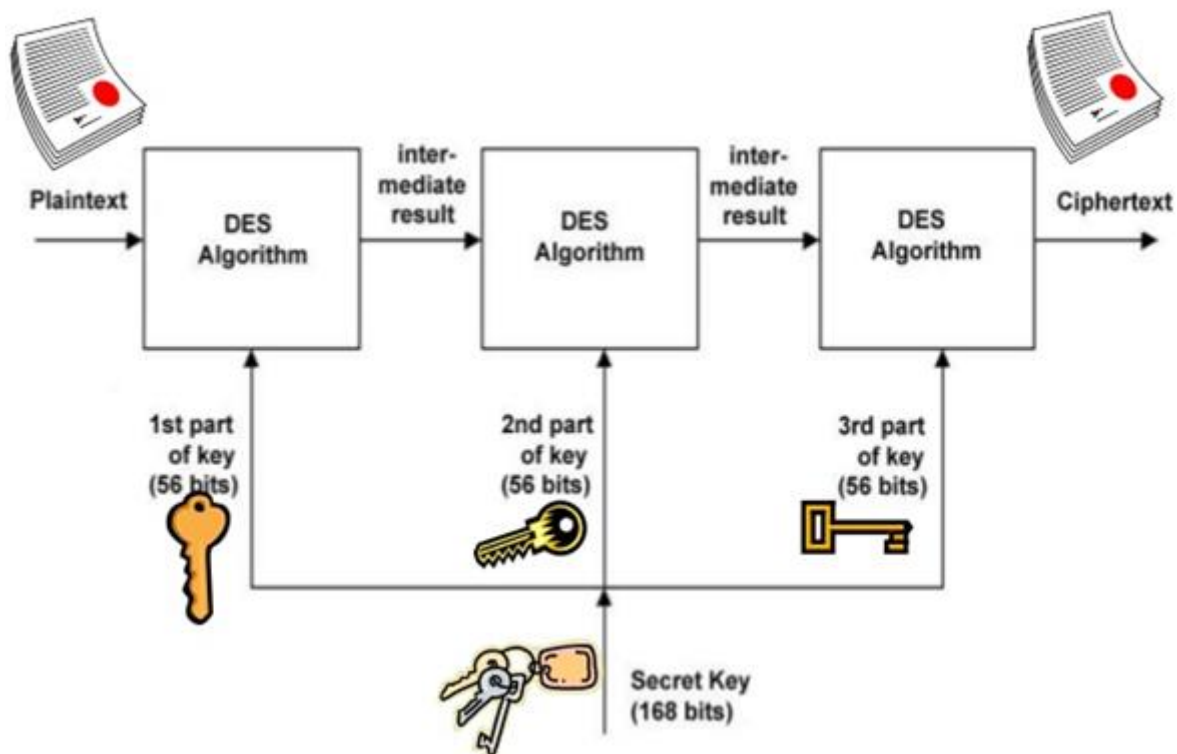


Figure 2.0: Triple Des

3.0 RESULTS AND DISCUSSION

A new comparative study between DES, 3DES RC4 and AES were presented in to factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, keys, time required to check all these eligible proved the AES is better than DES and 3DES[10].

There are a variety of different types of encryption methods, they can be classified according to the way in which the plaintext

is processed which can be either stream cipher or block cipher, or according to the type of operations used for transforming plaintext to Ciphertext. Also, encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption but most commonly used is Symmetric key encryption.

The most common Symmetric-block ciphers are DES, 3DES, AES and others. The current Digital Encryption Standard (DES) does no longer satisfy the need for data security because of its short 56-bit key. Such short keys can today be broken by brute force attacks.

Hadhoud Mohiy Mohamed,
“Performance Evaluation of Symmetric
Encryption Algorithms” IJCSNS
International Journal of Computer
Science and Network Security, VOL.8,
No.12, pp 280-286, December 2008.

[8] Shashi Mehrotra Seth, Rajan ishra,
“Comparative Analysis of Encryption
Algorithms for Data Communication”,
International Journal of Computer Science
and Technology, Vol. 2, Issue 2, pp.
292-294, June 2011.

[9] Dhawan2002] Priya Dhawan.,
"Performance Comparison: Security
Design Choices," Microsoft
Developer Network October
2002. [http://msdn2.microsoft.com/en-
us/library/ms978415.aspx](http://msdn2.microsoft.com/en-us/library/ms978415.aspx)

[10] Hamdan.O. Alanazi, B.B.Zaidan,
A.A.Zaidan, Hamid A.Jalab, M.Shabbir and
Y. Al- Nabhani, "New Comparative Study
between DES, 3DES and AES within Nine
Factors", Journal of Computing,
Volume 2, ISSUE 3, pp. 152-157, MARCH
2010

[11] Allam Mousa and Ahmad Hamad
Evaluation of the RC4 Algorithm for Data
Encryption: International Journal of
Computer Science and Applica- tions. Vol 3,
No 2, (2006)