International Journal of Engineering, Science and Metallurgy

(Full length research article)

Comparative Performance of DES and AES in Wireless Security for Brute Force Attack

M A Khan[a], Tazeem A Khan[b] and M. T Beg[b]

[a*]*Electrical Engg Section, F/o Engg & Tech., JMI*
[b]*E & C Deptt., F/o Engg & Tech., JMI*

Received 19 April 2012; accepted 2 May 2012, Available online 1June 2012

Abstract

The Security involves mechanism used to protect the different shareholders, like subscriber and service providers. The aspects of the security that this paper covers are mainly anonymity, authentication and confidentiality. The important aspects of the system that need protection are described along with the implementation of mechanisms used for protection. It appears that many of the very valuable aspects of the GSM can be attacked. The most obvious threat against communication system is eavesdropping on conversation. The privacy of GSM conversation is protected using some version of A5 algorithm. There are several impressive cryptanalysis attacks against these algorithms like linear attack, differential attack and brute force attack etc. that break the encryption and make it possible to eavesdrop in real time. The main focus of this paper is investigations of brute force attack on DES and AES. In the presence of these threats and vulnerabilities it is justified to wonder whether GSM provides sufficient security for users with very valuable information to communication. These users may be military organizations, senior management personal in large companies etc. GSM's current security model does not provide sufficient protection for these entities.

Keywords: *A5, DES, AES.*

1. Introduction

Security plays a more important part in wireless communication system than in the systems that use wired communication. This is mainly because of the ubiquitous nature of the wireless medium that makes it more susceptible to secure attacks than the wired communications. In the wireless medium, anyone can listen to whatever is being sent over network. Also, the presence of communication does not uniquely identify the originator (as it does in the case of a pair of coaxial cable or optical fibers). To make the things worse, any tapping or eavesdropping cannot even be detected in a medium as ubiquitous as the wireless medium. Thus security plays a vital role for the successful operation of a mobile communication system

2. Security Issues in Wireless Systems

Wireless systems contain all vulnerabilities of wired systems, plus they may have extra vulnerabilities according to their physical behavior [1]. It is so easy to follow the information traffic without being spotted by the system owners. Everybody may capture the radio signals with the suitable equipments over air. Because of the wireless devices are usually mobile, they have less storage capability and memory. Also network bandwidth of the wireless systems is relatively smaller than wired systems. As a result, codes working on mobile devices should be located in a small portion of the hard drive and use less memory, also because of the less computation power cryptographic operations should be selected carefully. For the reason which stated above, elliptic curve cryptography suits on restricted mobile devices. Elliptic curve cryptosystem needs less storage and computation for equivalent security level than other alternatives like RSA [2]

In GSM systems authentication is much more important than privacy, because authentication is a mandatory issue in the standard; however, people usually don't want to pay more for privacy. GSM uses secret key operations in cryptographic functions. Two main reason of the non-usage of public key operations are:

- The processors of mobile devices are small.
- The data transfer rate of the mobile devices is small.

Corresponding author's email: makhan@ieee.org

3. GSM Encryption

After authentication of the mobile subscriber, the communications between the system and the subscriber must be protected against fraudulent access. This is provided by encrypting the data on the radio interface using a key Kc and the A5 encryption algorithm. There are up to seven variants of A5 and mobile subscriber and operator agree on one of the A5 algorithms.

3.1 Cryptographic Algorithms of GSM

There are three common encryption algorithms used in GSM security: A3, A5, and A8. A5 is a stream cipher used for encryption in GSM, A3 and A8 are one-way functions take place in the authentication phase. A3 algorithm is used by a GSM network to authenticate the mobile subscriber. It is a one way function implemented in the SIM. The A5 is the algorithm used for encryption in GSM mobile phones. It can be used on both voice and data connections. It is a stream cipher that uses a 64-bit secret key. A5 is designed to be efficiently implemented in hardware. There are two versions of the A5 algorithm: A5/1, which is used in Europe, and A5/2, which is used in export systems A8 is used to exchange a session key that can be used to encrypt voice or data. A8 is also one-way function implemented in SIM.

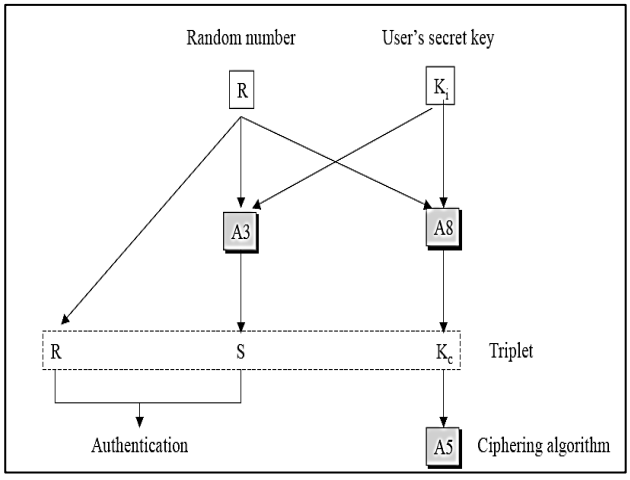

Fig. 1 Cryptographic Algorithms of GSM

4. Encryption Algorithms

4.1 Encryption algorithm of GSM (A5)

A partial source code implementation of the GSM A5 algorithm was leaked to the Internet in June, 1994. More recently there have been rumors that this implementation was an early design and bears little resemblance to the A5 algorithm currently deployed. Nevertheless, insight into the underlying design theory can be gained by analyzing the available information. The details of this implementation, as well as some documented facts about A5, are summarized below: [20]

- A5 is a stream cipher consisting of three clock-controlled LFSRs of degree 19, 22, and 23.
- The clock control is a threshold function of the middle bits of each of the three shift registers.
- The sum of the degrees of the three shift registers is 64. The 64-bit session key is used to initialize the contents of the shift registers.
- The 22-bit TDMA frame number is fed into the shift registers.
- Two 114-bit keystreams are produced for each TDMA frame, which are XOR-ed with the uplink and downlink traffic channels.
- It is rumored that the A5 algorithm has an "effective" key length of 40 bits.
-

4.2 Data Encryption Standard (DES)

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standard, now the National Institute of Standards and Technology (NIST), as the federal Information Processing Standard 46 (FIPS PUB 46). The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption. [19]

4.2.1 DES Encryption

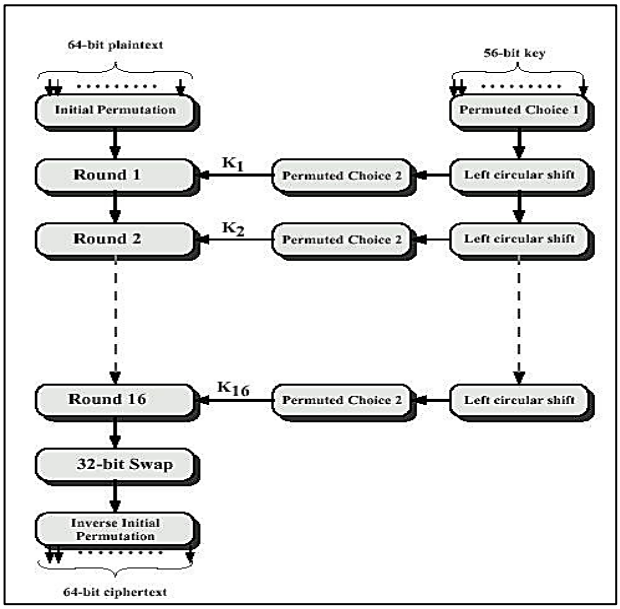

Fig. 2 DES Encryption & Decryption

In the Data Encryption Standard (DES) method, there are two inputs to the encryption function: the plaintext to be encryption and the key. In the case, the plaintext must be 64-bits in length and the key is 56-bit in length.

The right hand side of the figure shows that the processing of the plaintext proceed in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 round of the same function, which involves both permuted and substituted function. The output of the last (sixteen) round consists of 64 bits that are a function of the input plaintext and key. The left and right halves of the output are swapped to produce the preoutput. Finally, the preoutput is passed through a permutation (Inverse IP) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

The right-hand portion of the figure shows the way in which the 56-bits key is used. Initially, the key is passed through a permutation function. Then, for each of the 16 round, a subkey (ki) is produced by the combination of the right circular shift and a permutation. The permutation function is same for each round, but a different subkey is produced because of the repeated iteration of the key bits.

4 .3 AES (Advanced Encryption Standard)

There are many drawbacks in DES (Data encryption Standard)

1. DES (Data Encryption Standard) is slow.

2. DES (Data Encryption Standard) uses only 64-bits block size.

For reason of both efficiency and Security, a large block size is desirable. Because Of these drawbacks, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard(AES), Which should have a security strength equal to or Better than DES. In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length 128 bits and support for key lengths of 128, 192, and 256 bits.

In the first round of evaluation, 15 proposed algorithms were accepted. A second round narrowed the field to 5 Algorithms. NIST completed its evaluation process and published a final standard In November of 2001. NIST selected Rijndael as the proposed AES algorithm.[19]. Fig3. shows the overall structure of AES. The input to the encryption and decryption algorithm is a single 128 bits block, this block is depicted as a square matrix of bytes. This block is copied into the state array, which is modified at each state of encryption and decryption. After the final stage, state is copied to an output matrix.

Table1 AES Parameters

Key size (word/ bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size(word/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size(word/byte/bits)	4/16/128	4/16/128	4/16/128
Expanded key size(word/bytes)	44/176	52/208	60/240

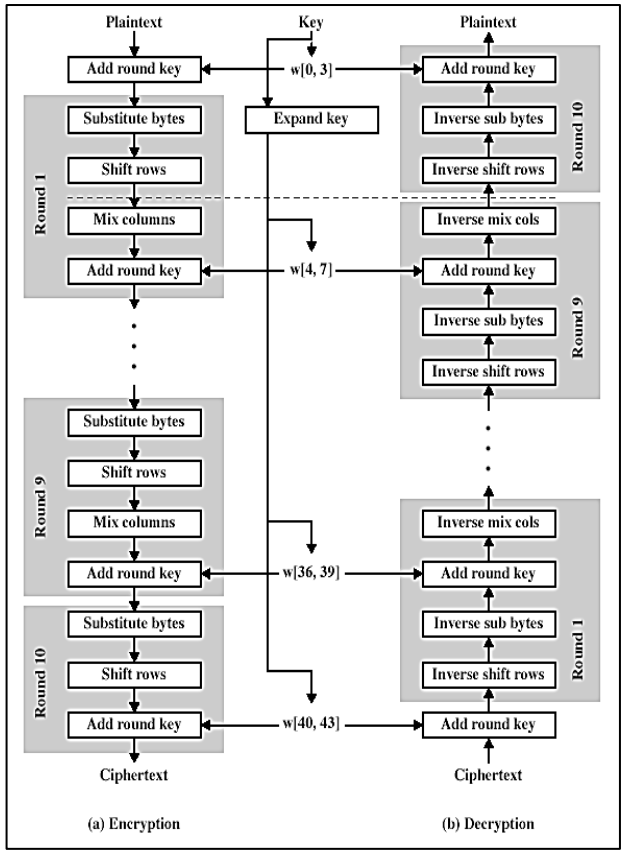

Fig. 3 AES Encryption and Decryption

4.3.1 Steps of AES

1. One noteworthy feature of this structure is that it is not a Feistel structure. In Feistel structure, the half of the data block is used to modify the other half of the data block and then halves are swapped. But the AES do not use a feistel structure but the process the entire data block in parallel during each round using substitution and permutation.

2. The key that is as an input is expanded into array of forty- four 32-bit word, w[i]

Four distinct words (128 bits) serve as round key for each round.

3. Four different stages are used, one of the permutation and three are substitution;

- **Substitution bytes**- Uses an S- boxes to perform a byte- byte substitution of the block
- **Shift rows** – A simple permutation
- **Mix column**- A Substitution that makes use arithmetic cover.
- **Add round key**- A simple bitwise XOR of the current block with a portion of expanded key.

4. The structure is quite simple. For both encryption and decryption, the cipher begins with add round key stage, followed by nine round that each includes all four stage, followed by a tenth round of three stage.
5. Only the Add Round Key stage makes use of key. For this reason, cipher begins and end with Add Round Key stage. Any other stages applied at beginning or end, is reversible without knowledge of key and so would add no secure.
6. The Add Round key stage is, in effect, a Vernam cipher and by itself would not be formidable. The other three stages together provide confusion, diffusion and nonlinearity, but by themselves would provide no secure because they do not use the key. We can view the cipher as alternative operation of XOR encryption (Add Round Key) of the block, followed by XOR encryption, and so on.This scheme is both efficient and highly secure .
7. Each stage is easily reversible. For the substitution Byte , shift row , and mix column stages , and inverse function is used in the decryption algorithm. For the Round Key stage, the inverse is achieved by XORing the same round key to the block.
8. Decryption process is reversible process of the encryption process.[19]

5. Attacks on Encryption Algorithms

5.1 Differential and Linear Cryptanalysis

The prime concern with DES has been its vulnerability to brute- force because its relatively short (56 bits) key length. However, there has also interest in finding cryptanalytic attacks on DES. With increasing popularity of block cipher with long key length, including triple DES, brute- force attacks have become increasingly impractical.

Thus there has been increased emphasis on cryptanalytic attacks on DES and other symmetric block ciphers. I will consider two attacks on AES and DES plaintext.

1. Differential attack
2. linear attack

5.1.1 Differential attack

The differential cryptanalytic attack is complex. In differential cryptanalytic first we consider the original plaintext block m to consist of two halves m_o and m_1.Each round of DES maps the right-hand input into the left-hand output and sets the right- hand output to be a function of the left-hand input and the subkey for this round. So, at each round, only one new 32-bits block is created.

If we label each new block m_i , Then the intermediate message halves are related as follows:

If we label each new block m_i , Then the intermediate message halves are related as follows:

$$M_{i+1} = M_{i-1} \oplus f(m_i, k_i),\ I = 1, 2, ...16. \quad (1)$$

In differential cryptanalysis, we start with the two message m and m', with a known XOR Difference

$$\triangle M = M \oplus M' \quad (2)$$

and consider the difference between the intermediate message halves

$$\triangle M_i = M_i \oplus M_i' \quad (3)$$

Then we have

$$\triangle M_{i+1} = M_{i+1} \oplus M'_{i+1} \quad (4)$$

Put equation no (1) in equation no (4) then we get

$$= [M_{i-1} \oplus f(M_i, K_i)] \oplus [M'_{i-1} \oplus f(M'_i, K_i)]$$

$$= \triangle M_{i-1} \oplus [f(M_i, K_i) \oplus f(M'_i, K_i)]$$

Now, suppose that many pairs of inputs to f with the same difference yield the same output difference if the same subkey is used.[5] , [6]

5.1.2 Linear Cryptanalysis

A more recent development is linear cryptanalysis; This attack is based on finding linear approximation to describe the transformations performed in DES. This method can be found a DES key given 2^{47} know plaintext, as compared to 2^{47} chosen plaintexts for differential cryptanalysis. Although this is a minor improvement, because it may be easier to acquire known plaintext rather than the chosen plaintext.

In linear cryptanalysis, For a cipher with n- bits plaintext and cipher text blocks and an m- bits key, let the plaintext blocks labeled P[1] ,.....P[n], the cipher text Blocks C[1].....C[n], and the key K[1].....K[m]. then defined

$$A[i, j, \ldots k] = A[i] \oplus A[j] \oplus \ldots \oplus A[k] \quad (5)$$

The objected of linear cryptanalysis is to find an effective linear equation of the form

$P[\alpha_1, \alpha_2, .. \alpha_a] \oplus C[\beta_1, \beta_2, ... \beta_b] = K[\gamma_1, \gamma_2, ., \gamma_c]$ (6)

Where X= 0 or 1 ; $1 \leq a, b \leq n$, $1 \leq c \leq m$, and where α ,β ,γ term represent fixed, unique bit locations.[5] , [6]

5.2 Brute Force Attack

A brute force attack is defined as a brute- force search to break a cipher by trying each possible key. In most cases, a cipher is considered secure if it can only be broken by brute force .The attacks depend on the block cipher, or the key length of any encryption algorithm. A typical brute force attack involves exhaustive key search, equivalent to a situation where a thief tries every possible combination in the lock of safe.

Table 2 shown below summarizes how long it would take to decrypt a message with a given key length, assuming a cracking machine capable of one million encryptions per second.[20]

Table 2 Brute force key search time for various key sizes

Key length in bits	32	40	56	64	128
Time required to test all possible keys	1.19 hours	12.7 days	2,291 years	584,542 years	10.8x 10^24 years

The time required for a 128-bit key is extremely large; as a basis for comparison the age of the Universe is believed to be 1.6x10^10 years. An example of an algorithm with a 128-bit key is the International Data Encryption Algorithm (IDEA). The key length may alternately be examined by determining the number of hypothetical cracking machines required to decrypt a message in a given period of time.

Table 3 Number of machines required to search a key space in a give time

Key length in bits	**1 day**	**1 week**	**1 year**
40	13	2	-
56	836,788	119.132	2,291
64	2.14x10^8	3.04x10 ^6	584,542
128	3.9x10^27	5.6x10^ 26	10.8x10^24

A machine capable of testing one million keys per second is possible by today's standards. In considering the strength of an encryption algorithm, the value of the information being protected should be taken into account. It is generally accepted that DES with its 56-bit key will have reached the end of its useful lifetime by the turn of the century for protecting data such as banking transactions. Assuming that the A5 algorithm has an effective key length of 40 bits (instead of 64) and brute force attack can break it with a work factor of 2^{40}.

It currently provides adequate protection for information with a short lifetime. A common observation is that the "tactical lifetime" of cellular telephone conversations is on the order of weeks.

The objective of this paper is to study the effectiveness of AES and DES algorithm against brute force attack. This is covers only brute force attack on AES and DES because Brute force attack is more dangerous as compare to linear and differential and other attacks.

6. Results

6.1 Brute Force attack on DES

In DES, Data are encrypted in 64-bit blocks using 56 bit key and transform 64-bit input in a series of steps into 64-bit output. Brute force can break DES with work factor of 2^{56}. This thesis represented breaking time of DES when the last two bits of ciphering key are unknown. Matlab will be used to write simulation scripts for DES.

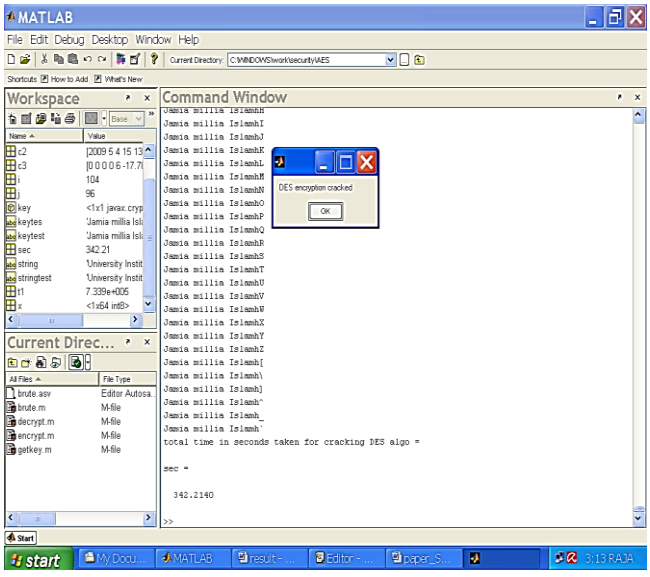

Fig.4 Brute force attack on DES

6.2 Brute force attack on AES

In AES, Data are encrypted in 128 -bit blocks using 128 bit key and transform 128 -bit input in a series of steps into 128-bit output. Brute force can break DES with work factor of 2^{128}. This thesis represented breaking time of

AES when the last two bits of ciphering key are unknown.

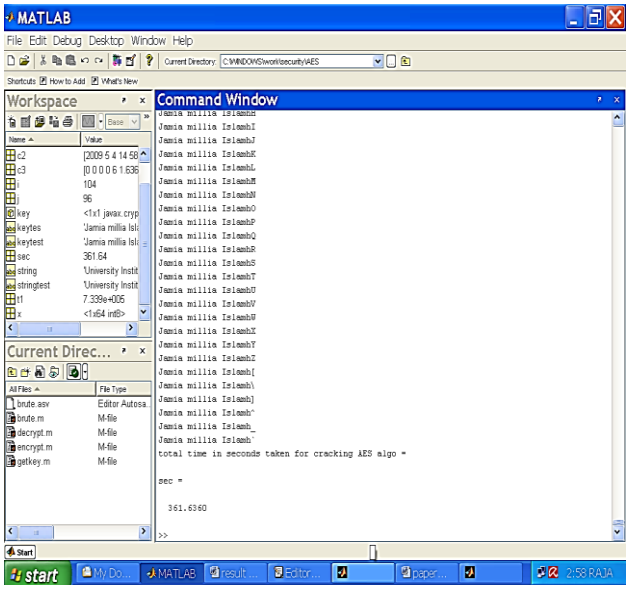

Fig. 5 Brute force attack on AES

Table 4.Comparison table

Algorithm	DES	AES
Key length in bits	56	128
Time required to test last two bits of key	342.2seconds	362.6 seconds
Speed	Slow	Fast
Complexity	High	Low
Round	16	10
Security	Low	High

7. Conclusion

GSM, which is one of mobile system that most people use in the world, found to have some possible vulnerability which concerned among many them are weakness in algorithm used in both authentication to mobile user and encryption to communication data (A5). In the past, these algorithms are considered to be secure. However, now nowadays technology, it makes many attacks become possible. The cipher key of A5 is 64 bits although we know that the last 10 bits are set to be zero. This key reduced the key space from 2^{64} to 2^{54} (1024 times smaller key space) and brute force attack break it with a work factor 2^{40}.This thesis covers only the brute force attack on DES and AES when the last two bits of key are unknown and table 6 show that the breaking time of AES is large than the breaking time of DES because of large key length (128 bits) and strong round of AES as compare to DES. This paper concludes that AES is more secure as compare to A5 and DES. If AES would be used on GSM network then GSM would be more secure.

References

1. Sebastian Nanz and Chris Hankin (2006), A framework for security analysis of mobile wireless networks, *Computer Science*, In Press, Accepted Manuscript.
2. Yun Zhou, Yanchao Zhang and Yuguang Fang (2006), Access control in wireless sensor networks, *Ad Hoc Networks*, In Press.
3. Bruce Potter (2004), GSM Security, *Network Security*, Volume 2004, Issue 5, Pages 4-5
4. Rijndael (2005), Cryptanalysis of S-box and improvement, *Applied Mathematics and Computation*, Volume 170, Issue 2, 15 Nov., Pages 958-975
5. Liu Jing-mei, Wei Bao-dian, Cheng Xiang-guo and Wang Xin-mei (2003), Differential and linear cryptanalysis for 2-round SPNs , *Information Processing Letters*, Volume 87, Issue 5, 15 September, Pages 277-282
6. Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung and Seonhee Yoon (2001), Linear and Differential Cryptanalysis of Russian GOST, *Electronic Notes in Discrete Mathematics*, Volume 6, April, Pages 538-547
7. Vitaly V. Shorin, Vadim V. Jelezniakov and Ernst M. Gabidulin (2005), Evolutionary computation based cryptanalysis: A first study, *Nonlinear Analysis*, Volume 63, Issues 5-7, 30 November , Pages e823-e830
8. E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou and M.N. Vrahatis (2001), National Institute of Standards and Technology: Specification for the Advanced Encryption Standard(AES),http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
9. Aamer Nadeem, Dr M. Younus Javed (2009), A Performance Comparison of Data Encryption Algorithms , *IEEE International Conference on Networking*.
10. Diaasalama, Abdul kader, MohiyHadhoud (2011), Studying the Effect of Most Common Encryption Algorithms, *International Arab Journal of e-technology*, vol 2,no.1, January .
11. Diaasalama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud (2010), Evalution the Performance of Symmetric Encryption Algorithms, *International journal of network security*, vol.10,No.3,pp,216-222,May.