Comparative Study of Different Symmetric and Asymmetric Algorithms of Cryptography

Md Imran Alam

Lecturer, Department of Computer Engineering & Networks, Jazan University, Jazan Saudi Arabia

imran.amu2008@gmail.com

***Abstract*— Nowadays Data Security has emerged as a challenging field in both academic and industry fields. Security of data or information is a major concern nowadays. To transmit data through unsecured networks like Internet or any public networks there is no alternative to Cryptography. When we transfer sensitive information across insecure networks like internet we want that this information cannot be read by anyone except the person whom we want to send it. This is the situation where we use Cryptographic Algorithms for security of our valuable information. This paper is a comparative study of different Symmetric and Asymmetric Cryptographic algorithms like AES, IDEA, DES,RC4 and RSA. Cryptographic algorithms have been compared based on the following factors: input size of data (in the form of texts), encryption time, and decryption time, throughput of encryption and decryption of each algorithm. From Simulation results, we compares these Cryptographic algorithms (AES, IDEA, DES, RC4 and RSA).**

***Keywords*—Security, Cryptography, Symmetric, Asymmetric, Algorithm, AES, IDEA, DES, RC4 and RSA, Throughput**

I. INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. [2]
Overview of some basic terms involved in Cryptography:

Plaintext and Cipher text:
The original message, before being transformed, is called plaintext. After the message is transformed, it is called cipher text. An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the cipher text back into plaintext.

Cipher: We refer to encryption and decryption algorithms as ciphers. The term *cipher* is also used to refer to different categories of algorithms in cryptography.

Key: A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext. These create the cipher text. To decrypt a message, we need a decryption algorithm, a decryption key, and the cipher text. These reveal the original plaintext.

Cryptography is divided in two parts:

(i) Symmetric key cryptography

(ii) Asymmetric key cryptography.

(i)Symmetric key Cryptography uses only key to encrypt and decrypt data. Symmetric algorithms are of two types:

A. Block ciphers

B. Stream ciphers.

A. Block Cipher: A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. [15]
Examples of Block Ciphers are: DES, 3DES, CAST, AES, BLOWFISH, IDEA and RC2.

B. Stream ciphers: A stream cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.[9]
RC4 is an example of stream cipher algorithm.

(ii). In Asymmetric key Cryptography, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption. Public key is known to the public and private key is known only to the user. Examples of Asymmetric cryptographic algorithms are: RSA,Diffie-Hellman, and DSA.

An overview of different fields of Cryptography.

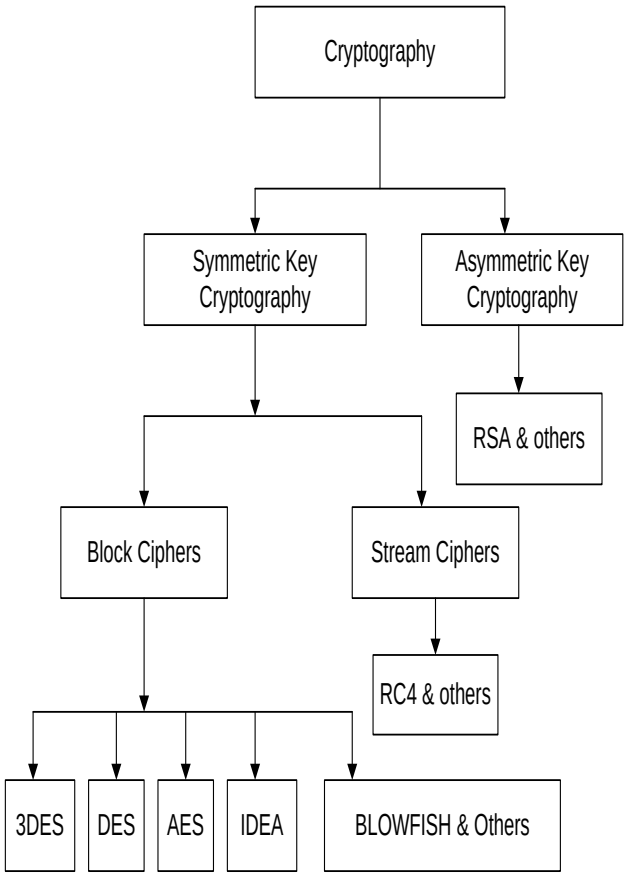

Fig.1 An overview of different fields of Cryptography

This paper is organized as follows: In section I Introduction part of cryptography is discussed. Section II covers the literature reviews. In section III the different types of Encryption algorithms are discussed. In section IV the various performance factors for the algorithms are given. In section V Simulation results and the discussions are presented. With the section VI the final conclusion of paper is provided.

II. LITERATURE REVIEW

In this section various performance factors and Encryption techniques used by different papers are discussed.

In paper[3] it is discussed that Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES and RSA algorithms are used for performance evaluation. Based on the text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

In Paper[5] it is discussed that in symmetric key encryption techniques the AES algorithm is specified as the better solution then follows the blowfish algorithm. In the Asymmetric encryption technique the RSA algorithm is more secure key generation. since it uses the factoring of high prime number hence, the RSA algorithm is found as the better solution in this method.

In paper[6] it was concluded that In Data communication, encryption algorithm plays an important role . Our research work surveyed the existing encryption techniques like AES, DES and RSA algorithms along with LSB substitution technique. Those encryption techniques are studied and analysed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. but RSA consume more encryption time and buffer usage is also very high . we also observed that decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

Paper[7] presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. In the case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption.

Paper[8] presents the superiority of Blowfish algorithm with others in terms of the throughput, processing time and power consumption. More the throughput, more the speed of the algorithm & less will be the power consumption. Secondly, AES has advantage over the other 3DES and DES in terms of throughput & decryption time. Third point is that 3DES has the least performance among all the algorithms mentioned here. Finally we can conclude that Blowfish is the best of all. In future we can perform same experiments on image, audio & video and developing a stronger encryption algorithm with high speed and minimum energy consumption changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption.

Paper[11] presents comparative analysis of existing Encryption algorithms like DES, 3DES, AES, RSA and BLOWFISH. By analyzing experimental results it was concluded that BLOWFISH algorithm takes least encryption and decryption time as compared to DES, 3DES, AES and RSA algorithms. Throughput value of BLOWFISH is the highest as compared to DES, 3DES, AES and RSA algorithms.

Power consumption value of AES is higher than BLOWFISH but lesser than DES, 3DES and RSA algorithms.

Paper[18] presents a performance and efficiency analysis of different block cipher algorithms (3DES, DES, CAST-128, BLOWFISH, IDEA and RC2) of Symmetric Cryptography based on different performance factors. By analyzing experimental results several points can be concluded. We find that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Throughput of CAST-128 is better than DES, 3DES and IDEA. RC2 is faster for smaller sizes of input data as compared to BLOWFISH algorithm because of it has only one P-box for key expansion loaded into memory as compared to BLOWFISH which has one P-box and four S-boxes. Throughput value of BLOWFISH is greater than 3DES, DES, CAST-128, IDEA and RC2. Power Consumption value of BLOWFISH is least. 3DES having the least throughput value and maximum Power Consumption value as compared to all block ciphers discussed in this paper. From the experimental results it is also concluded that by taking input data in the form of text, audio as well as video throughput of Encryption and Decryption of all block ciphers discussed here is almost same in all three forms of data.

III.CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

***A.* DES (Data Encryption Standard)** is the most popular computer encryption algorithm. DES is a U.S. and international standard. It is a symmetric algorithm; the same key is used for encryption and decryption. "Reference[5] shows" Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses using a 56-bit. DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

***B.* AES:** The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. The Advanced Encryption Standard (AES) was designed because DES's key was too small.[2] Although Triple DES ODES) increased the key size, the process was too slow. The National Institute of Standards and Technology (NIST) chose the Rijndael algorithm, named after its two Belgian inventors, Vincent Rijmen and Joan Daemen,

as the basis of AES. AES is a very complex round cipher. AES is designed with three key sizes: 128, 192, or 256 bits. Below Table shows the relationship between the data block[2]

Size ofData Block	*Number ofRounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

***C.* IDEA(International Data Encryption Algorithm):** IDEA is a block cipher; it operates on 64-bit plaintext blocks. The key is 128 bits long. The same algorithm is used for both encryption and decryption. As with all the other block ciphers we've seen, IDEA uses both confusion and diffusion. The design philosophy behind the algorithm is one of "mixing operations from different algebraic groups." [1]
Three algebraic groups are being mixed, and they are all easily implemented in both hardware and
software:
— XOR
— Addition modulo 2^{16}
— Multiplication modulo 2^{16} + 1. (This operation can be viewed as IDEA's S-box.)
All these operations (and these are the only operations in the algorithm—there are no bit-level
permutations) operate on 16-bit sub-blocks. This algorithm is even efficient on 16-bit processors.

D. RC4: RC4 is a variable-key-size stream cipher developed in 1987 by Ron Rivest for RSA Data Security, Inc. [1]
RC4 is simple to describe. The algorithm works in OFB: The keystream is independent of the plaintext. It has a 8 * 8 S-box: *S*0, *S*1,..., *S*255. The entries are a permutation of the numbers 0 through 255, and the permutation is a function of the variable-length key. It has two counters, *i* and *j*, initialized to zero.
To generate a random byte, do the following: [1]
i = (*i* + 1) mod 256
j = (*j* + *S*i) mod 256
swap *S*i and *S*j
t = (*S*i + *S*j) mod 256
K = *S*t
produce plaintext. Encryption is fast—about 10 times faster than DES.
Initializing the S-box is also easy. First, fill it linearly: *S*0 = 0, *S*1 = 1,..., *S*255 = 255. Then fill another

256-byte array with the key, repeating the key as necessary to fill the entire array: *K*0, *K*1,..., *K*255.
Set the index *j* to zero. [1]
Then:
for *i* = 0 to 255:
j = (*j* + *S*i + *K*i) mod 256
swap *S*i and *S*j
RC4 is in dozens of commercial cryptography products, including Lotus Notes, Apple Computer's
AOCE, and Oracle Secure SQL.

E. **. RSA:**This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is the most popular public-key algorithm. It can be used for both encryption and digital signatures. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key [18].

RSA algorithm:
Select two different prime numbers p and q ,for security aim, the integers p and q must be prime numbers.

- Compute n = p*q
- Let m=(p-1)(q-1)
- Choose an integer *e*, co prime to m
- Compute the secret exponent *d*

Such that de=(1+Nm) for N greater than equal to zero

- d=(1+Nm)/e
- The public key is (e,n) and the private key (d, n).
- Plain text message=P
- Cipher text: C =(P^e)MOD n
- Decrypted text=(C^d)MOD n

IV. PERFORMANCE FACTORS

For our experiment, we used a laptop with i5, 2.53 GHz CPU and 4 GB RAM. We used the Microsoft Visual Studio .Net and Compact Framework as the software development environment. Code of block Ciphers algorithms was written using C# language. In the experiment, the laptop encrypts a different file size ranges from 61 KB to 11165KB.

In this paper, the following factors are used as the performance criteria:

i. Input data (in the form of texts)
ii. Encryption Time of each algorithm
iii. Decryption Time of each algorithm
iv. Throughput of Encryption of different algorithms with text data
v. Throughput of Decryption of different algorithms with text data

Encryption time: The time which an algorithm takes to convert plain text to a cipher text is called encryption time.

Decryption time: The time which an algorithm takes to get plain text from a cipher text is called decryption time.

Throughput of an encryption: It is defined as total plain text in Megabytes divided by total encryption time of each algorithm.

Throughput of a decryption: It is defined as total plain text in Megabytes divided by total decryption time of each algorithm.

If throughput value of an encryption is increased then power consumption of that encryption is decreased.

Similarly if throughput of an encryption is decreased then power consumption of that encryption is increased and hence the battery consumption is also increased.

V. EXPERIMENTAL RESULTS & ANALYSIS

Experimental results for different Cryptographic Algorithms DES, AES, RC4 ,IDEA and RSA are shown in Table1 and Table 2.
Table 1 shows the encryption time of different Cryptographic Algorithms where input data is in the form of text of different sizes. In this table encryption throughput of different Cryptographic Algorithms is also calculated.

Table 2 shows the decryption time of different Cryptographic Algorithms where input data is in the form of text of different sizes. In this table decryption throughput of different Cryptographic Algorithms is calculated.

After analyzing Table1 and Table 2, it is concluded that encryption and decryption time of RSA algorithm is much higher than encryption and decryption time of DES, AES, RC4 and IDEA algorithm. We also noticed here that encryption and decryption time of RC4 algorithm is the lowest as compared to DES, AES, IDEA and RSA algorithms.

Table 1: Comparisons of DES, AES, RC4 ,IDEA and RSA based on Encryption Time (in Milliseconds)

Input Size (KB)	DES	AES	RC4	IDEA	RSA
61	43	51	9	54	126
255	57	58	13	76	178
572	78	71	21	98	239
925	122	112	29	147	387
5620	389	375	81	657	1249
11165	956	929	210	1089	3014
Throughput (MB/Sec)	11.30	11.65	51.23	8.76	3.58

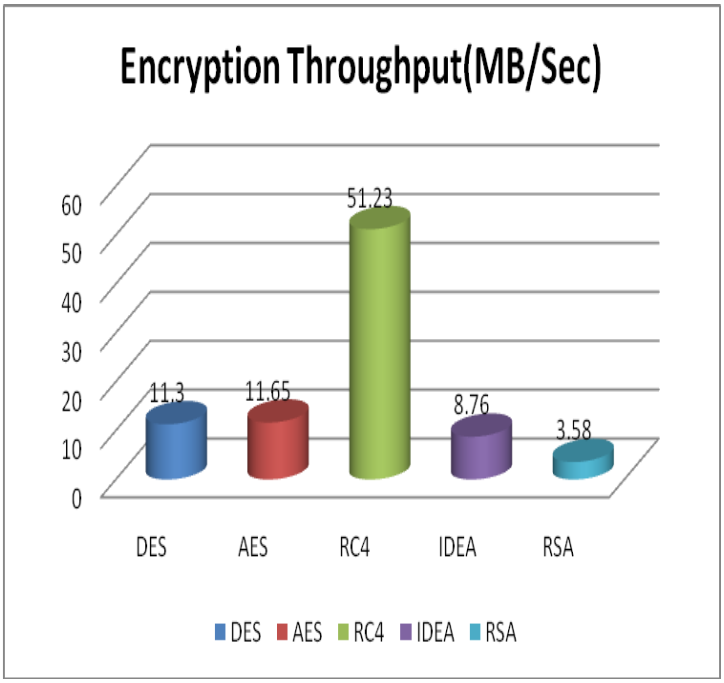

Fig. 2 Encryption Throughput of each Algorithm

Table 2: Comparisons of DES, AES, RC4 ,IDEA and RSA based on Decryption Time (in Milliseconds)

Input Size (KB)	DES	AES	RC4	IDEA	RSA
61	39	49	7	55	114
255	59	53	15	74	169
572	82	69	22	97	241
925	121	98	26	124	372
5620	367	359	76	635	1239
11165	968	908	197	1053	2994
Throughput (MB/Sec)	11.36	12.11	54.22	9.12	3.62

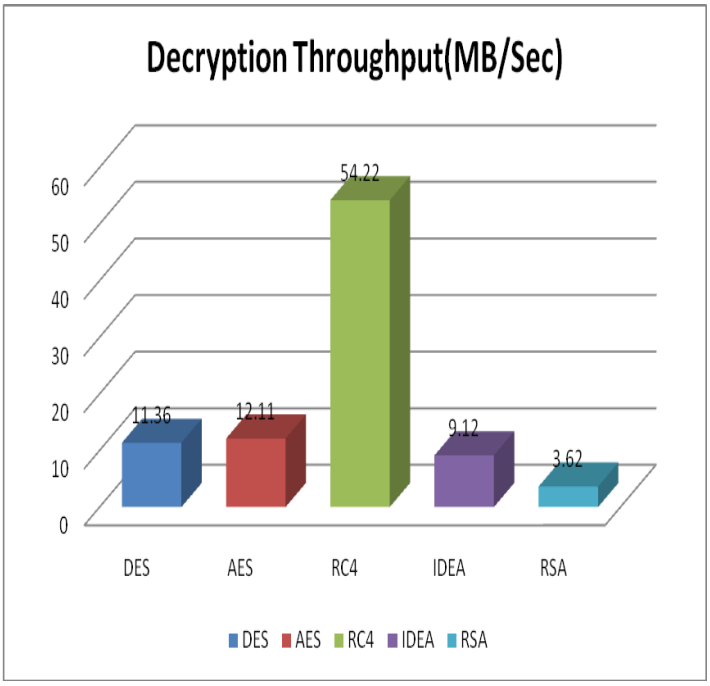

Fig. 3 Decryption Throughput of each Algorithm

After analyzing Fig 2 we conclude that throughput of RC4 algorithm is higher than throughput of all other algorithms like DES, AES and IDEA and RSA. It is also noticed here that AES algorithm has advantage over DES and IDEA algorithm in terms of the processing time.

By analyzing fig. 3, it is noticed here that RC4 algorithm is far better than other algorithms (DES, AES and IDEA and RSA) based on throughput value. Throughput value of AES is higher than DES, RSA and IDEA algorithm but lesser than RC4 algorithm.

VI. CONCLUSIONS

This paper is a comparative study of existing Symmetric Key Cryptographic Algorithms**(DES,AES,IDEA and RC4)** and Asymmetric key Cryptographic Algorithm like **RSA.** By analyzing experimental results several points can be concluded. Throughput of AES is better than throughput of DES, IDEA, and RSA but lesser than RC4. RC4 algorithm takes least encryption and decryption time as compared to DES, AES,IDEA and RSA. Throughput value of RC4 is the highest as compared to DES,AES, IDEA and RSA .Throughput of DES is better than IDEA and RSA but lesser than AES and RC4.

From the experimental results, we finally conclude that RSA has least performance efficiency as compared to DES,AES,IDEA and RC4 algorithm. We also conclude that performance of RC4 algorithm is best as compared to all other algorithms discussed in this paper.

ACKNOWLEDGMENT

The author would like to thank to all authors that are listed below in the reference lists as well as anonymous reviewers for their valuable comments and suggestions that improved the presentation of this paper.

REFERENCES

[1] Bruce Schneier ”Applied Cryptography, Protocols, Algorithms and Source Code in C”.

[2] Behrouz A. Forouzan “Data Communications and Networking ”

[3] Shasi Mehlrotra seth, Rajan Mishra “ Comparative Analysis of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011

[4] Ali Makhmali, Hajar Mat Jani” Comparative Study On Encryption Algorithms And Proposing A Data Management Structure”INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 6, JUNE 2013 ISSN 2277-8616

[5]AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram” COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS “ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

[6] B. Padmavathi1, S. Ranjitha Kumari2 “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique” International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064Volume 2 Issue 4, April 2013 www.ijsr.net

[7] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader,Mohly Mohamed Hadhoud, “Evalution the Performance of Symmetric Encryption Algorithms”, international journal of network security vol.10,No.3,pp,216-222,May 2010.

[8] Pratap Chnadra Mandal’ Superiority of Blowfish Algorithm” International Journal of Advanced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201

[9] . http://en.wikipedia.org/wiki/Stream_cipher

[10] Diaasalama, Abdul kader, MohiyHadhoud, “Studying the Effect of Most Common Encryption Algorithms”, International Arab Journal of e-technology, vol 2,no.1,January 2011.

[11] Md Imran Alam” A Comparative Analysis of Different Encryption Techniques of Cryptography” International Journal of Advanced and Innovative Research (2278-7844) / # 160 / Volume 2 Issue 9 2013

[12] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar “A modified RSA cryptosystem based on ‘n’ prime numbers” International Journal of Engineering and Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66

[13] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,’’ The Third IEEE Workshop on Wireless LANs – September 27-28, 2001- Newton, Massachusetts.

[14] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."I BM Journal of Research and Development, May 1994,pp. 243 -250.

[15] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha” A Study of New Trends in Blowfish Algorithm” / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 2, pp.321-326

[16] http://en.wikipedia.org/wiki/Block_cipher

[17] W. Stallings. Cryptography and Network Security, Prentice Hall, 1999.

[18] Md Imran Alam*, Mohammad Rafeek Khan/ “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography”/ International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013

[19] Md Imran Alam, Mohammad Rafeek Khan” Performance Evaluation of Different Cryptographic Algorithms: DES, 3DES, AES,IDEA & BLOWFISH”/ International Journal of Advanced and Innovative Research (2278-7844) / #203 / Volume 2 Issue 10, 2013

