Volume: 02, Issue: 05, Pages: 796-803 (2011)

How Good Is The DES Algorithm In Image Ciphering?

Said F. El-Zoghdy
Computer Science Dep. College of Computers & Information Technology,
Taif University, Kingdom of Saudi Arabia (KSA).
Email: Elzoghdy@yahoo.com
Yasser A. Nada
Computer Science Dep. College of Computers & Information Technology,
Taif University, Kingdom of Saudi Arabia (KSA).
Email: Y_nada@yahoo.com
A. A. Abdo
Department of Mathematics & Computer Science,
Faculty of Science, Menoufia University, Egypt
Email: azza2asd@yahoo.com

----------**ABSTRACT**----------
Digital Images and video encryption plays an important role in today's multimedia world. Many encryption schemes have been proposed to provide security for digital images. Usually the symmetric key ciphering algorithms are used in encrypting digital images because it is fast and use the techniques for block and stream ciphers. Data Encryption Standard is symmetric key encryption algorithm. In spite of the successful cracking of the data encryption standard by massive brute force attacks, data encryption standard algorithm is an entrenched technology and still useful for many purposes. In this paper, we use some of the image quality encryption measuring factors to study the effect of data encryption standard algorithm in image ciphering. The results show that the data encryption standard algorithm is fast and it achieves a good encryption rate for image ciphering using different modes of operation.

Keywords: Image Encryption, Key Ciphering Algorithms, DES.
Date of Submission: 26 December 2010 Revised:15 February 2011 Date of Acceptance: 30 March 2011

I. INTRODUCTION

Network and Internet Security (NIS) is a very crucial aspect in today's world where computers and electronic media are used for transferring sensitive information like bank accounts, electronic cash and so on. NIC involves protecting this delicate information in transit. For any information system to be secure, it should be able to provide the following services [7,8]:

- **Confidentiality:** Information should only be accessible for authorized parties.
- **Authentication:** The sender of a message should be correctly identified.
- **Integrity:** Transmitted information can be modified by only the authorized parties.
- **Non-repudiation:** Neither the sender nor the receiver of a message can be able to deny the transmission of the message.
- **Access Control:** Access to information must be controlled by the system.

As far as confidentiality is concerned, conventional encryption has been used, but could not provide authentication. In symmetric encryption a single key is used for both encryption and decryption. The two communication parties have to share that key [7,8,9,10]. The encrypted data in symmetric key cryptography can only be read by parties who have been given the necessary key to decrypt the cipher text back into its original plaintext form. The key used for encryption is the same used in deciphering. There are a lot of symmetric key cryptography algorithms. The Data Encryption Standard (DES) is a famous one. It uses a shared secret key of length 64 [1,14,15].

On the other hand, RSA named after its founder (Revisit; Shamir; and Adleman) [7,8,11] and Elliptic Curve Cryptography (ECC) systems provide both confidentiality

Volume: 02, Issue: 05, Pages: 796-803 (2011)

and authentication [7,8,12]. This kind of encryption involves the use of two keys, one publicly known to everyone and other known only to the user/owner. This later kind of encryption eliminates the problems involved with conventional encryption, namely:

- Difficulty of key distribution.
- Lack of digital signature to provide authentication.

The keys are used to provide confidentiality and the private key is used for digital signatures [2,7,8]. A variety of encryption algorithms have been proposed [1,3,4,5,6,13].

Encrypting data means converting it to an unintelligible form called cipher. Decrypting cipher means converting the data back to its original form called plaintext [7,8]. The algorithms described in this standard specify both enciphering and deciphering operations which are based on a binary number called a key.

Security of the data depends on the security provided for the key used to encipher and decipher the data. Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically.

In this paper we use some image quality of encryption measuring factors to study the effect of DES algorithm in image ciphering. The results show that the DES algorithm achieves a good encryption rate for image ciphering using different modes of operation.

The reset of this paper is organized as follows: In Section II we explain the DES algorithm. Section III presents some experimental results. Section IV presents other tests and Finally, Section V summarizes this paper.

II. DES ALGORITHM

Simplified DES, developed by Professor Edward chaefer of Santa Clara University [1]. The algorithm is designed to encipher and decipher blocks of data consisting for 64 bits under control of a 64-bit key of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection [1,7,8,14,15]. Its output is 64-bit block of ciphertext. Decryption takes 64-bit input of ciphertext analog with a 56-bit key and produces a 64-bit output of plaintext. The encryption process takes 16 rounds in which a round function, defined in terms the S-boxes, is applied over various subkeys of 56-bit input key, which are generated according to a well defined scheme. The diagram in Fig. 1 shows the flowchart of DES.

First we introduce the following notations:
Let *L(x)* denote the left half of a 64-bit string x, let R(x) denote the right half of x, and let C(x) be given by

$$C(x) = R(x) \,||\, L(x) \quad (1)$$

In other words C(x) changes the right and left halves of x. We explain this algorithm in the following steps:

1. An initial permutation, designated as IP, this applied to 64 bits of plaintext. You can see the IP, and its inverse in Fig. 2(a), 2(b) respectively.

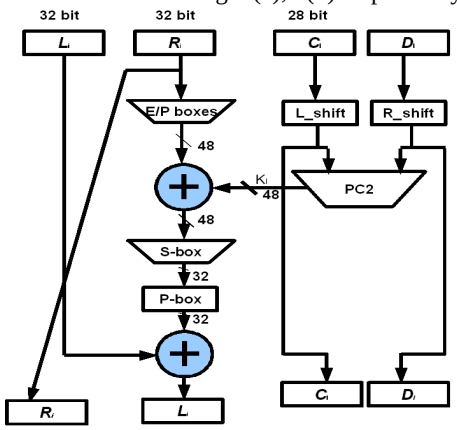


Figure 1: Data Encryption Standard Flowchart

2. This bits is split into two 32-bit halves designated L(left) and R(right).
3. At the same time, the first subkeys K_1, a 48-bit string is generated.
4. The subkey K_1 analog with the right halve R are used as inputs to the round function F(K;R(x)) to produce a 32-bit output, blow we explain briefly the steps of the round function F:
   - Expand x from 32 bits to 48-bit, by using the expansion box E, see Fig. 3(a).
   - Apply the modulo 2 addition of E(x) and K, the output is also 48-bit.
   - Where the later is concatenation of eight bit string B_i of length six, say
   - $E(R(x)) \oplus K = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$.
     Enter each B_i into S-box where S-box is generated from a linear function, witch takes six bits as an inputs and get four outputs. Fig. 4 illustrates the S-boxes design.
   - The output of the pervious step has a 32-bit length is entered into the permutation function P, which is defined as P box. See Fig. 3 (b).
5. The output from the round function F is XOR-ed with the left half of the plaintext.
6. Finally, the left old half of the plaintext is replaced by the old right half, and the output of the XOR replaces the old value of R. The function f represents this step.

$$f_k(x) = (L(x) \oplus F(k,R(x)) || R(x) \quad (2)$$

where

$$F_k(x) = P(S(E(R(x)) \oplus L(x)) \quad (3)$$

7. This completes one round of the DES. The same procedure is applied 15 more times, the only

difference being the subkeys K_2, K_3,…,K_{15} generated by the subkey schedule are used as inputs to the round function f. Notice that when F_{K16} is applied the right and left halves of the pre-output are not switched.

8. The last step of encryption is to reassemble the L and R output by the last round of f_{k16} of 64-bit string and apply the inverse of initial permutation IP^{-1}.

DES has the feature that the decryption of the ciphertext y produced with a key who corresponding subkeys are K_1, K_2,…,K_{16} is achieved by applying exactly the same algorithm that was used to encrypt except that the subkeys are used in reverse order K_{16}, K_{15},…,K_1.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(a)

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(b)

Figure 2: (a) *IP*, (b) IP^{-1}

A. Security Analysis

The level of security provided by DES fall into two areas namely, key size and the nature of the algorithm.

1. **Using a 56-bit key:** with 56-bit key, there are 2^{56} possible keys, which approximately $7.2x10^{16}$keys. In 1998, DES has been proved insecure when the Electronic Frontier Foundation (EFF) broke a DES encryption using a special-propose DES-Cracker machine [18]. Also, in 1993 there was a deferential attack on DES [19]. Fortunately, there are a number of alternatives to DES, the most important of witch are Advanced Encryption Stander (AES), and triple DES [16,17].
2. **The nature of DES Algorithm:** DES depends on eight substitution boxes (S-BOX). Each box is generated from non-linear function, which made the powerful of DES against any attack for a long time. There are modified algorithms depend on the substitution boxes with more powerful as AES algorithm [21,22].

Expantion Table *E* Box					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(a)

P Permutation Table			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

(b)

Figure 3: (a) Expantion Table *E* Box, (b) *P* Permutation Table

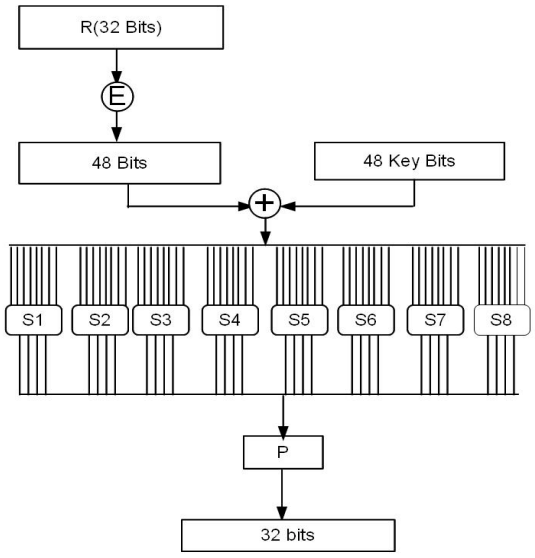


Figure 4: Substitution Box S-BOX

B. Statistical Analysis

Statistical analysis has been performed on the proposed image encryption algorithm to demonstrate its superior confusion and diffusion properties which strongly resist statical attacks. This is shown by a test of histograms on the enciphered images and on the correlations of adjacent pixels in the ciphered image.

1. Histogram of the encrypted images: Select a several 256 grey-scale of size 256x256 that have different contents, and calculate their histograms. One typical example among them is shown in Fig. 5. From that figure one can notice that the histogram of the ciphered image is fairly uniform and is significantly from that of the original image.

2. Correlation of two adjacent pixels: To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a ciphered image, the following procedure was carried out. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate the correlation coefficient of each pair by using the following two formulas:

$$Cov(x, y) = E(x-E(x)) -E(y - E(y)) \quad (4)$$

$$r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5)$$

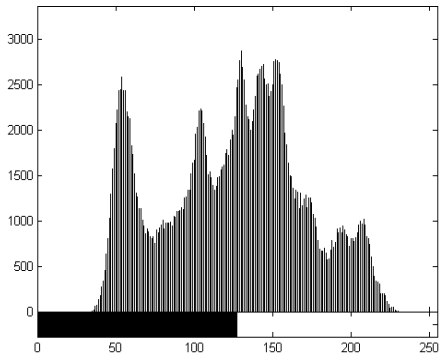
Where x, y are grey scale values of two adjacent pixels in the image. In numerical computation, the following formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (6)$$

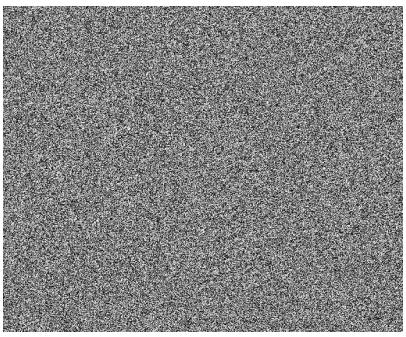
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (7)$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - D(x)) \quad (8)$$

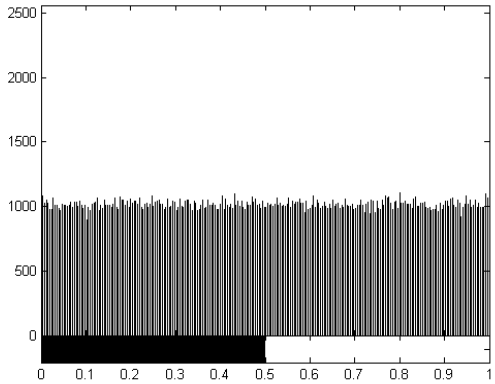
(a) Lena original image



(b) Lena original image histogram



(c) Lena ciphered image



(d) Lena ciphered image histogram

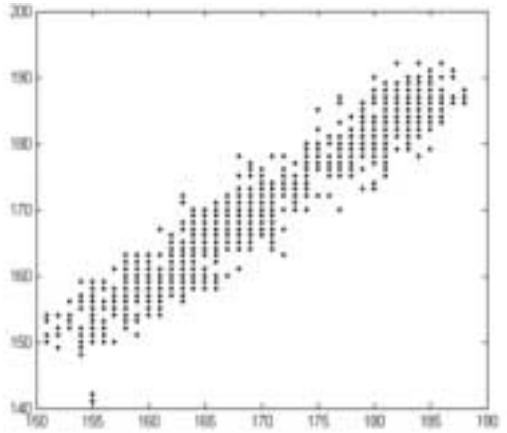
Figure 5: Histogram of the original image and that of the cipher-image

Volume: 02, Issue: 05, Pages: 796-803 (2011)

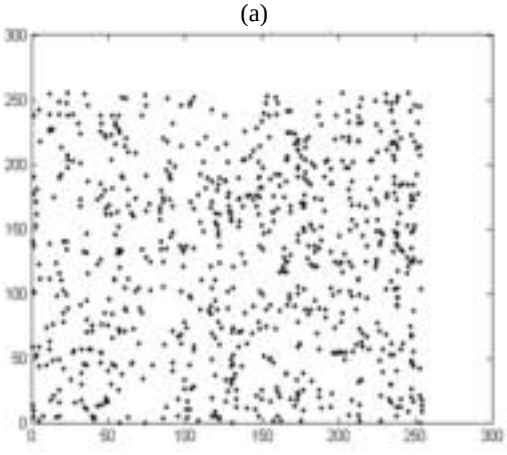
Fig. 6 shows the correlation distribution of two horizontally adjacent pixels in plain image and that in cipher image. The correlation coefficients are 0.9976 and 0.0275 respectively, witch are far apart. Similar results for diagonal and vertical directions were obtained, which are found in Table 1.

Table 1: Correlation coefficients of two adjacent pixels in two images

	Plain Image	Cipher Image
Horizontal	0.9974	0.0275
Vertical	0.9976	0.0411
Diagonal	0.8407	0.0572



(a)



(b)

Figure 6: Correlation of two horizontally adjacent pixels in the plain-image and that in cipher-image

III. EXPERIMENTAL RESULTS

The platform of our research is the Celeron 2.6 GHz processor, 2 GB Ram, windows XP professional system, and Matlab programming, A dope fotoshop7.0 as a graphical tool. In our experiments, we use two 256x256 gray images namely Lena, and cameraman. The results are shown in Fig. 7 and Fig. 8 respectively. Each figure shows the plain image, and the corresponding ciphering image in the three modes of operation Electronic Code Book (ECB), Cipher Block Chaining (CBC) and Cipher Feed Back Block (CFB). Table 2 shows the correlation between the plain image and the corresponding cipher text in the three modes of operation, respectively.

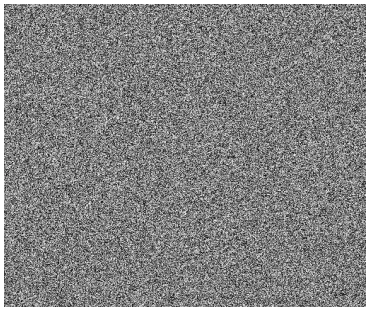
Table 2: Correlation between cipher and plain images.

	CBC Mod	ECB Mod	CFC Mod
Cameraman	0.00045967	0.0012	0.00072892
Lena	0.00081612	0.00011396	0.0026

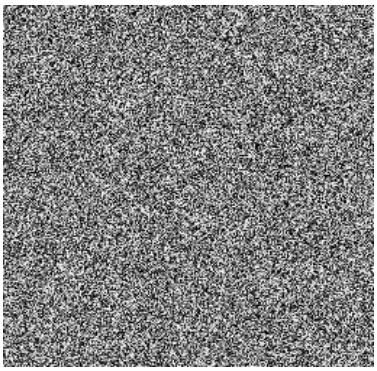
IV. OTHER TESTS

There are other important issues on an image encryption scheme including the running speed, practically for real time Internet applications. The results show that the proposed image encryption is fast enough. Simulation shows that the average enciphering and deciphering speed is 3.0 MB/s, on 2 GHz Pentium IV personal computer. Also the pre-calculations of the key scheduling increase the algorithm speed which significantly affects on the performance of the DES algorithm in image ciphering.

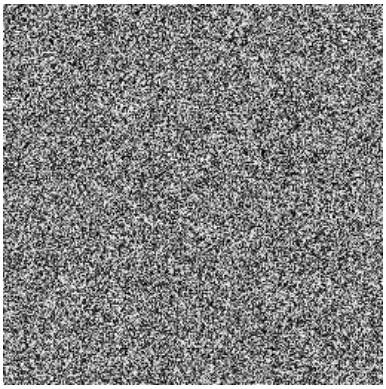
(a) Lena original image



(b) Lena encrypted in CBC mod



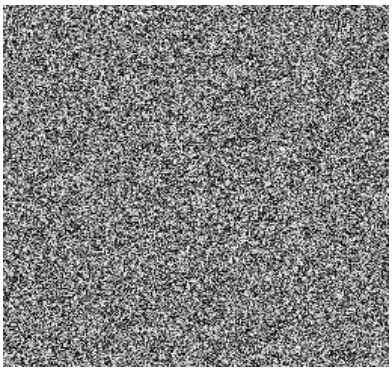
(c) Lena encrypted in ECB mod



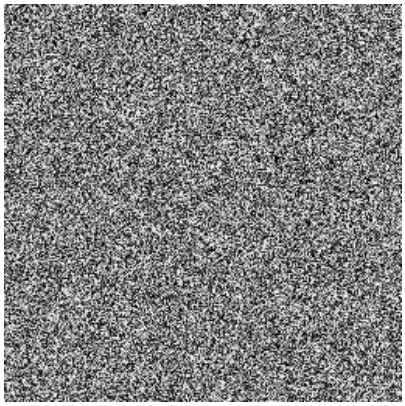
(d) Lena encrypted in CFC mod

Figure 7: Original Lena image and its ciphering image using CBC, ECB, and DFC modes

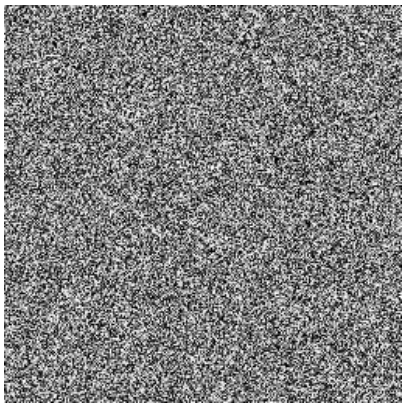
(a) Cameraman original image



(b) Cameraman encrypted in CBC mod



(c) Cameraman encrypted in ECB mod



(d) Cameraman encrypted in CFC mod

Figure 8: Original Cameraman and its ciphering image using CBC, ECB, and DFC modes

V. SUMMERY

In spite of the successful cracking of DES by massive brute force attacks, it will be several years before its widespread use declines significantly. DES is still useful for many purposes. In this paper, we study the effect of DES in image ciphering. DES is used with different modes of operations. The encryption quality of the DES algorithm is measured using different modes of operation. The results show that the DES algorithm is fast and it achieves a good image encryption rate.

REFERENCES

[1] Sauer.E. A simplified Data Encryption Stander Algorithm. Cryptologia.January 1996.

[2] P. Horster and H. Petersen. Verallgemeinerte elgamal signaturen. Sicherheit in In- formations systeme, Proceedings der Fachtagung SIS'94, pages 89-106, 1994. Verlag der Fachvereine Zu¨rich.

[3] H.U.Park I.Y.Lee, A digital nominative proxy signature scheme for mobile communication, in proceeding of international conference on information and communications security (ICICS'01), LNCS 2229, pp. 451-445, springer-verlag, 2001.

[4] Z.W.Tan Seo and S.H. Lee, Improvement on Nominative Proxy Signature Schemes , in Proceeding of the International Journal of Network Security(INS),Vol.7, No.2, PP.178-183,Sep.2008.

[5] S.H. Seo and S.H. Lee, New nominative proxy signature scheme for mobile communication, in Proceeding of the Security and Protection of Information (SPI'03), ISBN: 80-85960-50-8, pp. 149-154, springer-verlag, 2003.

[6] E. Van Herreweghen, Secure anonymous signature based transactions. In ESORICS 00: Proc. of the 6th European Symposium on Research in Computer Security, pages 5571. Springer-Verlag, 2000. LNCS 1895.

[7] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by RonaldL. Rivest.

[8] Stallings. W, Cryptography and Network Security, (Prentice Hall, New Jersey, 2003).

[9] Encryption And Decryption Algorithm http://homepages.uel.ac.uk/u0430614/Encryption%20index.htm

[10] A Comparison of Symmetric Key and Asymmetric Key Encryption Methods http://webupon.com/ security/a-comparison-of-symmetric-key-and-asymmetric-key-encryption-methods/

[11] Rivest, R. Shamir, A, and Adleman, l. A Method for obtaining digital signatures and public key cryptosystems. Communication of ACM. Vol. 21, No. 2, pp. 120-126, 1997.

[12] Avi Kak, " Elliptic Curve Cryptography" http://cobweb.ecn.purdue.edu/~kak/compsec/NewLectures/Lecture14.pdf

[13] I. A. Ismail, S. F. El-Zoghdy, and A.A. Abdo, "A Secure Nominative Proxy Signature Scheme for Distributed Shared Object Systems", Int. J. Advanced Networking and Applications Vol. 02, No. 01, Pages: 411-418 (2010).

[14] Schaneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C(2nd ed) Wiley New Yourk [1996]

[15] Coppersmith. D, The data Encryption Standard (DES) and its Strength against attacks, IBM Journal of Research and Development,38 (1994).

[16] Daemen. J, and V. Rijmen. the block cipher Rijndael, Lecture Notes in Computer Science, 1820(2000), 288-296. (Smart Card Research and Applications)

[17] Daemen. J, and V. Rijmen. the Design of Rijndael. AES- Advanced Encryption Standard, Springer-Verlage, 2002.

[18] Electronic Frontier Foundation, Cracking DES, O'Reilly & Associates, 1998

[19] Biham.E, and A. Shamir Differential cryptanalysis of DES-like cryptosystems, Journal of cryptology, 4(1991),3-72.

[20] Biham.E, and A. Shamir Differential cryptanalysis of Data Encryption Stander, Springer-Verlage, 1993.

[21] Daemen. J, and V. Rijmen. the block cipher Rijndael, Lecture Notes in Computer Science, 1820(2000), 288-296. (Smart Card Research and Applications)

[22] Daemen. J, and V. Rijmen. the Design of Rijndael. AES- Advanced Encryption Standard, Springer-Verlage, 2002.

Authors Biography

Dr. Said Fathy El-Zoghdy Was born in El-Menoufia, Egypt, in 1970. He received the BSc degree in pure Mathematics and Computer Sciences in 1993, and MSc degree for his work in computer science in 1997, all from the Faculty of Science, Menoufia, Shebin El-Koom, Egypt. In 2004, he received his Ph. D. in Computer Science from the Institute of Information Sciences and Electronics, University of Tsukuba, Japan. From 1994 to 1997, he was a demonstrator of computer science at the Faculty of Science, Menoufia University, Egypt. From December 1997 to March 2000, he was an assistant lecturer of computer science at the same place. From April 2000 to March 2004, he was a Ph. D. candidate at the Institute of Information Sciences and Electronics, University of Tsukuba, Japan., where he was conducting research on aspects of load balancing in distributed and parallel computer systems. From April 2004 to 2007, he worked as a lecturer of computer science, Faculty of Science, Menoufia University, Egypt. From 2007 until now, he is working as an assistant professor of computer science at the Faculty of Computers

Volume: 02, Issue: 05, Pages: 796-803 (2011)

and Information Systems, Taif University, Kingdom of Saudi Arabia. His research interests are in load balancing in distributed/parallel systems, Grid computing, performance evaluation, network security and cryptography.

DR. Yasser Ahmed Nada Was born in Ismailia, Egypt, in 1968. He received the BSc degree in pure Mathematics and Computer Sciences in 1989 and MSc degree for his work in computer science in 2003, all from the Faculty of Science, Suez Canal University, Egypt. In 2007, he received his Ph.D. in Computer Science from the Faculty of Science, Suez Canal University, Egypt. From September 2007 until now, he worked as a lecturer of computer science, Faculty of Computers and Information Systems Taif University, KSA. His research interests include Expert Systems, Artificial Intelligence, Object Oriented Programming, Computer Vision, and Genetic Algorithms.

Azza Ahmed Abdo Ali Was born in Egypt, in 1982. She received the BSc degree in pure Mathematics and Computer Sciences in 2003, and MSc degree for her research in computer science in 2008, all from the Faculty of Science, Menoufia, Shebin El-Koom, Egypt. From 2005 to August 2008, she was a demonstrator of computer science at the Faculty of Science, Menoufia University, Egypt. From September 2008 to date, she is an assistant lecturer of computer science at the same place. Her research interests are in Image Processing, image Encryption, Symmetric Key Cryptography, and Multimedia Security.