Performance Evaluation of Symmetric Encryption Algorithms

Diaa Salama Abdul. Elminaam[1], Hatem Mohamed Abdul Kader[2] and Mohie Mohamed Hadhoud[3]
(Corresponding author: H. M. Abdul Kader*)*
Higher Technological Institute, 10th of Ramadan City, Egypt[1]
Faculty of Computers and Information, Minufiya University, Egypt[2]
Faculty of Computers and Information, Minufiya University, Egypt[3]

Abstract
Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types ,battery power consumption, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm. .

Key Word
Encryption techniques, Computer security, AES, DES, RC2, 3DES, Blowfish, RC6

1. Introduction

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then every one may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys [1-5].

Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1].

Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2].The most common classification of encryption techniques can be shown in Fig. 1.

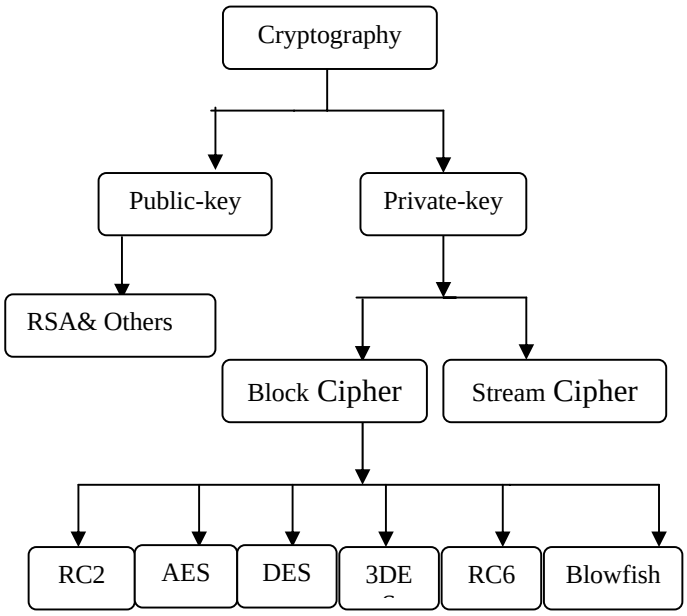

Fig. 1 Overview of the field of cryptography

Brief definitions of the most common encryption techniques are given as follows:

DES: (Data Encryption Standard), was the first

Manuscript received December 5, 2008
Manuscript revised December 20, 2008

encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) . Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [3],[4].

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [3].

RC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [3].

Blowfish is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish [5].

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [6]. Also, AES has been carefully tested for many security applications [3], [7].

RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard [8].

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies. This causes a “battery gap” [9], [10].We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices.

This study evaluates six different encryption algorithms namely; AES, DES, 3DES, RC6, Blowfish, and RC2. The performance measure of encryption schemes will be conducted in terms of energy, changing data types -such as text or document and images- power consumption, changing packet size and changing key size for the selected cryptographic algorithms. This paper is organized as follows. Related work is described in Section 2. A view of simulation and experimental design is given in section 3. Simulation results are shown in section 4. Finally the conclusions are drawn section 5.

2. Related Work

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

It was shown in [1] that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly.

It was concluded in [11] that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. The difference is not noticeable. Reducing the number of rounds leads to power savings but it makes the protocol insecure for AES and should be avoided. Seven or more rounds can be considered fairly secure and could be used to save energy in some cases.

A study in [12] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [13].

. In [14] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the

performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser.

3. Experimental Design

For our experiment, we use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 321 K byte to 7.139Mega Byte.

Several performance metrics are collected:

1- encryption time
2- CPU process time
3- CPU clock cycles and battery power.

The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [15].

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU.

The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy.

The following tasks that will be performed are shown as follows:

- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different encoding bases namely; hexadecimal base encoding and in base 64 encoding.

- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.

-A study is performed on the effect of changing data types -such as text or document and images- for each cryptography selected algorithm on power consumption.

- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

4. Simulation Results

A. differentiate output results of encryption (Base 64, Hexadecimal)

Simulation results are given in Fig. 2 and Fig. 3 for the selected six encryption algorithms at different encoding method. Fig. 2 shows the results at base 64 encoding while Fig. 3 gives the results of hexadecimal base encoding. We can notice that there is no significant difference at both encoding method. The same files are encrypted by two methods; we can recognize that the two curves almost give the same results.

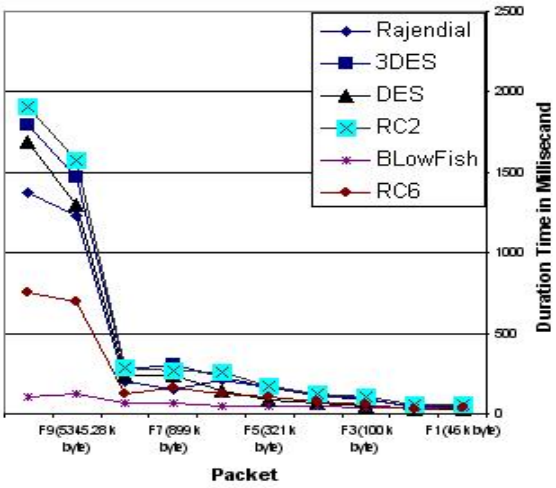

Fig. 2. Time consumption of encryption algorithm (base 64 encoding)

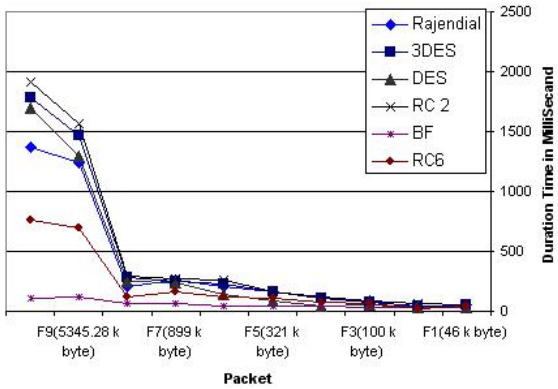

Fig. 3 Time consumption of encryption algorithm (Hexadecimal encoding)

B- The effect of changing packet size for cryptography algorithm on power consumption.

-Encryption of different packet size

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased.

TABLE 1
Comparative execution times (in milliseconds) of encryption algorithms with different packet size

Input size in (Kbytes)	AES	3DES	DES	RC6	Blow Fish	RC2
49	56	54	29	41	36	57
59	38	48	33	24	36	60
100	90	81	49	60	37	91
247	112	111	47	77	45	121
321	164	167	82	109	45	168
694	210	226	144	123	46	262
899	258	299	240	162	64	268
963	208	283	250	125	66	295
5345.28	1237	1466	1296	695	122	1570
7310.336	1366	1786	1695	756	107	1915
Average Time	374	452	389	217	60.3	480.7
Throughput (Megabytes/sec)	4.174	3.45	4.01	7.19	25.892	3.247

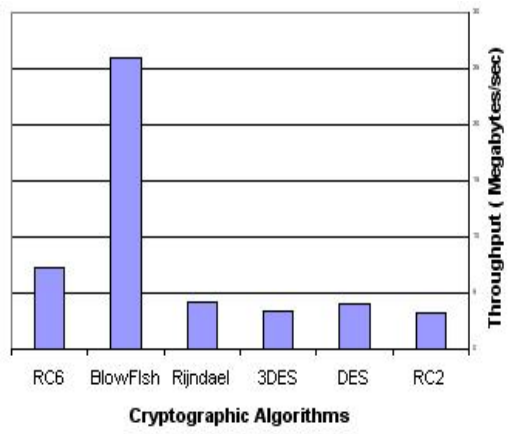

Fig. 4 Throughput of each encryption algorithm (Megabyte/Sec)

Simulation results for this compassion point are shown Fig. 4 and Table1 at encryption stage . The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Another point can be noticed here; that RC6 requires less time than all algorithms except Blowfish. A third point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. A fourth point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used.

-decryption of different packet size

TABLE 2
Comparative execution times (in milliseconds) of decryption algorithms with different packet size

Input size in (Kbytes)	AES	3DES	RC6	Blow fish	DES	RC2
49	63	53	35	38	50	65
59	58	51	28	26	42	59
100	60	57	58	52	57	90
247	76	77	66	66	72	95
321	149	87	100	92	74	161
694	142	147	119	89	120	165
899	171	171	150	102	152	183
963	164	177	116	80	157	194
5345.28	655	835	684	149	783	904
7310.336	882	1101	745	140	953	1216
Average Time	242	275.6	210	83.4	246	313.2
Throughput (Megabytes/sec	6.452	5.665	7.43	18.72	6.347	4.985

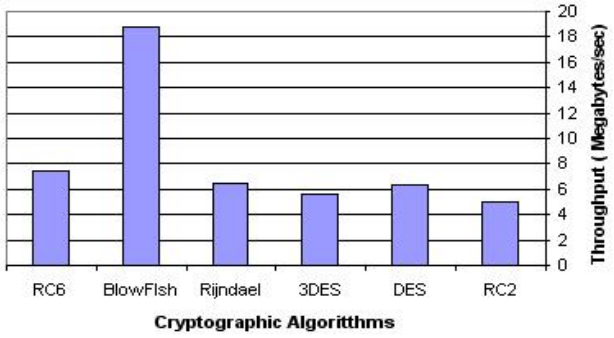

Fig. 5 Throughput of each decryption algorithm (Megabyte/Sec)

Simulation results for this compassion point are shown Fig. 5 and Table2 decryption stage. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. The second point should be notice here that RC6 requires less time than all algorithms except Blowfish. A third point that can be noticed that AES has an advantage over other 3DES,DES RC2.The fourth point that can be considered is that RC2 still has low performance of these algorithm. Finally, Triple DES (3DES) still requires more time than DES.

C- The effect of changing file type for cryptography algorithm on power consumption.

In the previous section, the comparison between encryption algorithms has been conducted at text and document data files. We found that Blowfish has a performance greater than other the other five types .Now we will make a comparison between other types of data

(Images) to check which one can perform better in this case. Simulation results for image data type (JPEG images) are shown Fig. 6 and Fig 7 at encryption and decryption respectively.

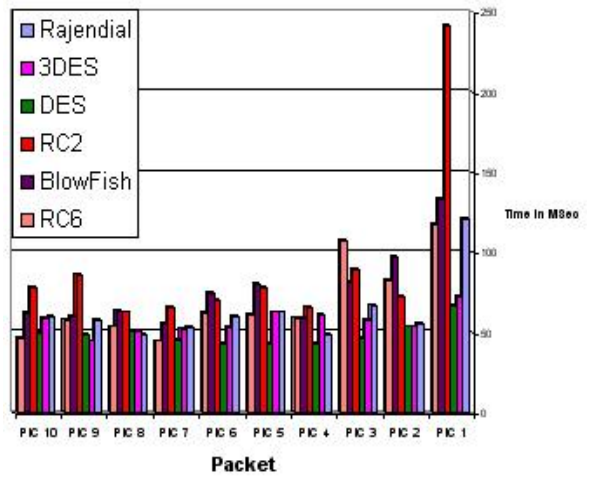

Fig. 6 Time consumption for encrypt different images

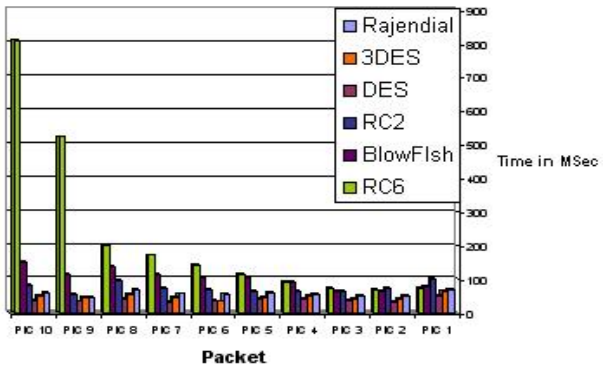

Fig. 7 Time consumption for decrypt different images

From those results, it is easy to observe that RC2 still has disadvantage in encryption process over other algorithms in terms of time consumption and serially in throughput. On the other hand, it is easy to observe that RC6 and Blowfish have disadvantage in decryption process over other algorithms in terms of time consumption and serially in throughput. We find that 3DES still has low performance when compared to DES.

D- The effect of changing key size of AES on power consumption.

The last performance comparison point is the changing different key sizes for AES and RC6 algorithm. In case of AES, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. The simulation results are shown in Fig. 8 and Fig. 9.

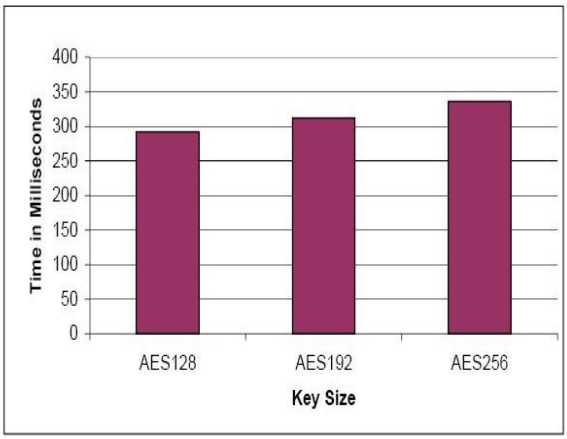

Fig. 8 Time consumption for different key size for AES

In case of AES it can be seen that higher key size leads to clear change in the battery and time consumption. It can be seen that going from 128 bits key to 192 bits causes increase in power and time consumption about 8% and to 256 bit key causes an increase of 16% [9].

Also in case of RC6, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. The result is close to the one shown in the following figure

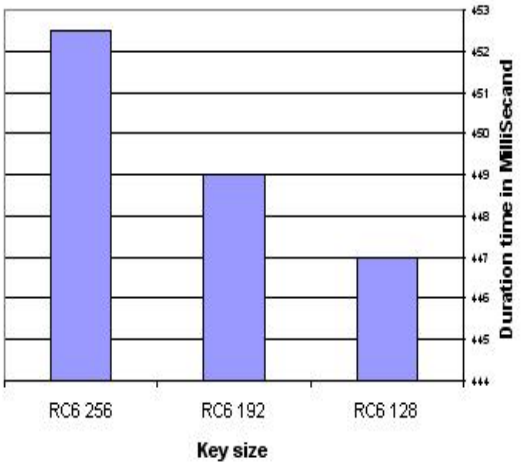

Fig. 9 Time consumption for different key size for RC6

In case of RC6 it can be seen that higher key size leads to clear change in the battery and time consumption.

5. Conclusions

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms

are AES, DES, 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results. First; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Third; 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. Also, we find that 3DES still has low performance compared to algorithm DES. Finally -in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.

Acknowledgment

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

References

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

[2] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.

[3] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

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

[5] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html

[6] K. Naik, D. S.L. Wei, Software Implementation Strategies for Power-Conscious Systems," Mobile Networks and Applications - 6, 291-305, 2001.

[7] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.

[8] N. El-Fishawy , "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, , Nov. 2007, PP.241–251

[9] K. McKay, "Trade-offs Between Energy and Security in Wireless Networks Thesis," Worcester Polytechnic Institute, April 2005.

[10] R. Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9 , Issue 2 ,May. 2006.

[11] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9,2003. Retrieved October 1, 2008, at: portal.acm.org/citation.cfm?id=383768

[12] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.

[13] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark- . Retrieved October 1, 2008, from: http://www.eskimo.com/~weidai/benchmarks.html

[14] S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,PP 20-25.

[15] A.A. Tamimi, "Performance Analysis of Data Encryption Algorithms. Retrieved October 1, 2008 from http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html

[16] A. Sinha and A.P. Chandrakasan, JouleTrack, "A Web Based Tool for Software Energy Profiling, ," proceedings of the 38th Design ,Las Vegas ,2001 DAC ,Conference. utomation ,NV , USp.p 220-225

Diaa Salama Abdul. Elminaam was born on November 23, 1982 in Kafr Sakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig Univeristy, Egypt in 2004. He is working in Higher Technological Institute,10th of Ramadan city as Demonstrator at Faculty of Computer and informatics. He majors in Cryptography and Network Security.

Dr. H. M. Abdul-kader obtained his B.S. and M.SC. (by research) both in Electrical Engineering from the Alexandria University , Faculty of Engineering , Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University , Faculty of Engineering , Egypt in 2001 specializing in neural networks and applications. He is currently a Lecturer in Information systems department , Faculty of Computers and Information, Menoufya University, Egypt since 2004. He has worked on a number of research topics and consulted for a number of organizations. He has contributed more than 30+ technical papers in the areas of Neural networks, Database applications , Information security and Internet applications .

Prof. ***Mohiy Mohamed Hadhoud***, Dean, Faculty of Computers and Information, head of Information Technology Department, Menoufia University, Shebin Elkom, Egypt. He is a member of National Computers and Informatics Sector Planning committee, University training supervisor. He graduated, from the department of Electronics and Computer Science, Southampton University, UK, 1987. Since 2001 till now he is working as a Professor of Multimedia, Signals and image processing and Head of the department of Information Technology (IT), He was nominated by the university council for the national supremacy award, years 2003, and 2004. He is the recipient of the university supremacy award for the year 2007. He, among others are the recipient of the Most cited paper award form the Digital signal processing journal, Vol. 18, No. 4, July 2008, pp 677-678. ELSEVIER Publisher. Prof. Hadhoud has published more than 110 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Digital Signal Processing, 2-D Adaptive filtering, Digital Image Processing, Digital communications, Multimedia applications, and Information security and data hiding.