Evaluating The Performance of Symmetric Encryption Algorithms

Diaa Salama Abd Elminaam[1], Hatem Mohamed Abdual Kader[2], and Mohiy Mohamed Hadhoud[2]
(Corresponding author: Diaa Salama Abd Elminaam)
Higher Technological Institute 10th of Ramadan City, Egypt[1]
Faculty of Computers and Information Minufiya University, Egypt[2]
(Email: {ds_desert, hatem6803, mmhadhoud}@yahoo.com
(Received Feb. 16, 2009; revised and accepted May 12, 2009)

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. Experimental results are given to demonstrate the effectiveness of each algorithm.

Keywords: 3DES, AES, blowfish, computer security, DES, encryption techniques, RC2, RC6

1 Introduction

Many encryption algorithms are widely available and used in information security [8, 9, 10]. 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. 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 ECC). Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [4, 6, 14]. 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 [2, 3, 5, 6, 8, 13, 14, 15, 17]. The most common classification of encryption techniques can be shown in Figure 1.

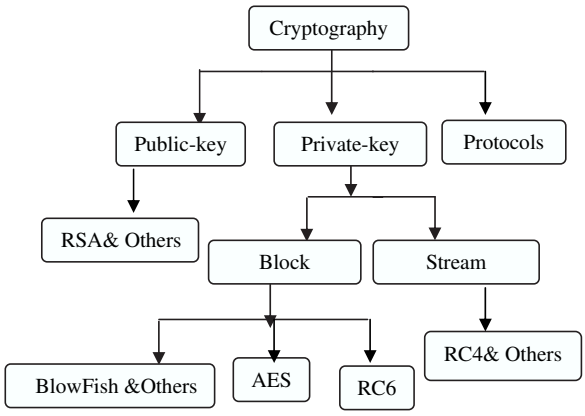

Figure 1: Overview of the field of cryptography

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" [1, 12]. 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, Audio data and video data- power consumption, changing packet size and changing key size for the selected cryptographic algorithms.

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 [14] that energy consumption of different common symmetric key encryptions on hand held 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 [7] 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.

A study in [19] 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 [20].

In [11] 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 Experimental 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 Byte139MegaBytes for text data, from 33 Kbytes to 8262 Kbytes for audio data, and from 4006 Kbytes to 5073 Kbytes for video files.

Several performance metrics are collected: 1) Encryption time; 2) CPU process time; and 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 [18].

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, audio file, and video file - 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 Experimental Results

4.1 Differentiate Output Results of Encryption (Base 64, Hexadecimal)

Experimental results are given in Figures 2 and 3 for the selected six encryption algorithms at different encoding method. Figure 2 shows the results at base 64 encoding while Figure 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.

Time consumption of encryption algorithm (base 64 encoding)

4.2 Effect of Changing Packet Size for Cryptographic Algorithms on Power Consumption

4.2.1 Encryption of Different Packet Size

Encryption time is used to calculate the throughput of an encryption scheme. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for

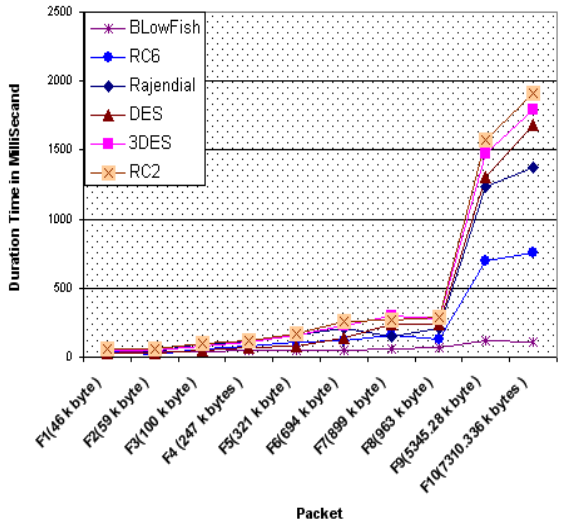

Figure 2: Time consumption of encryption algorithm (base 64 encoding)

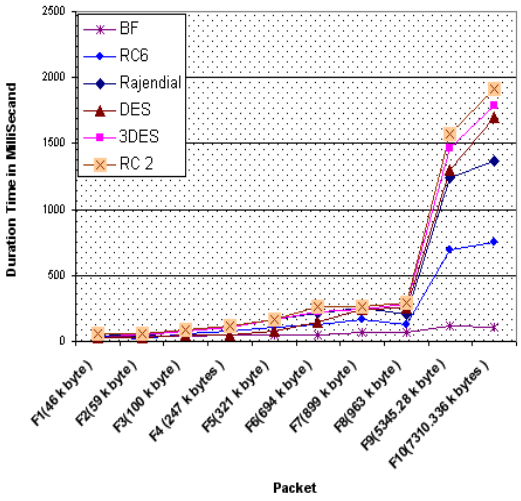

Figure 3: Time consumption of encryption algorithm (Hexadecimal encoding)

each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased.

Experimental results for this compassion point are shown Figure 4 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 always requires 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.

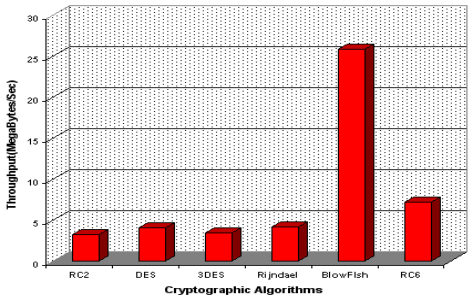

Figure 4: Throughput of each encryption algorithm (Megabyte/Sec)

4.2.2 Decryption of Different Packet Size

Experimental results for this compassion point are shown Figure 5 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 noticed 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.

4.3 The Effect of Changing File Type (Audio Files) for Cryptography Algorithm on Power Consumption

4.3.1 Encryption of Different Audio Files (Different Sizes)

Encryption Throughput

In the previous section, the comparison between encryption algorithms has been conducted at text and document data files. Now we will make a comparison between other types of data (Audio file) to check which one can perform better in this case. Experimental results for audio data type are shown Figure 6 at encryption.

CPU Work Load

In Figure 7, we show the performance of cryptographic algorithms in terms of sharing the CPU load. With a different audio block size

Results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time (CPU work load) and throughput. Another point can

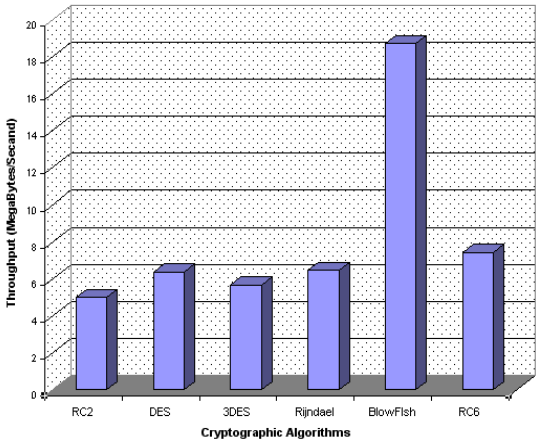

Figure 5: Throughput of each decryption algorithm (Megabyte/Sec)

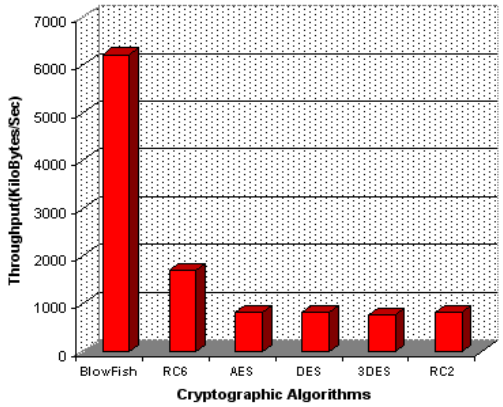

Figure 6: Throughput of each encryption algorithm (Kilobytes/Second)

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 especially in small size file. A fourth point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It always requires more time than DES. 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.

4.3.2 Decryption of Different Audio files (Different Sizes)

Decryption Throughput

Experimental results for this compassion point are shown Figure 8.

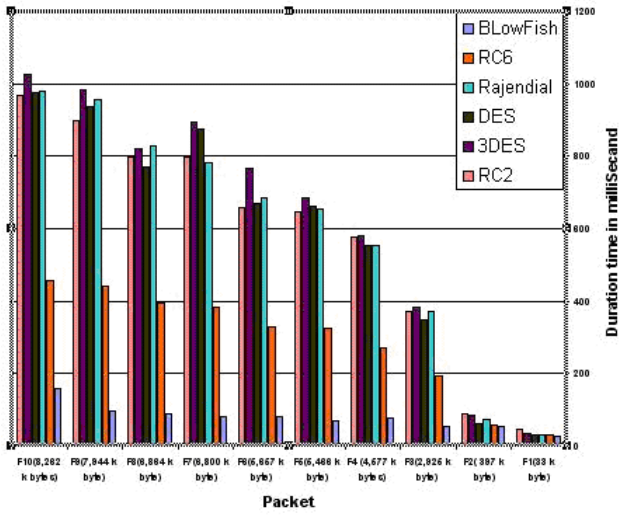

Figure 7: Time consumption for encrypt different audio files

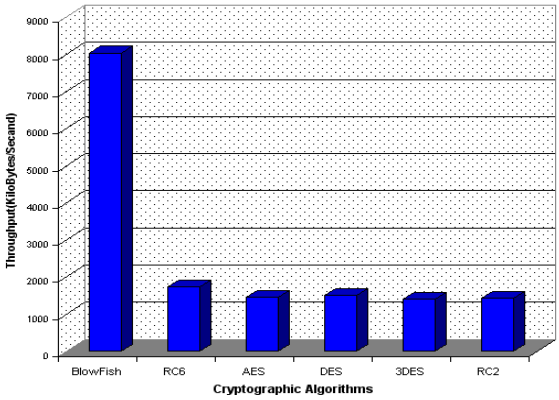

Figure 8: Throughput of each Decryption algorithm (Kilobytes/Second)

CPU Work Load

Experimental results for this compassion point are shown Figure 9.

From the results we found the result as the same as in encryption process for audio files.

4.4 The Effect of Changing File Type (Video Files) for Cryptography Algorithm on Power Consumption

4.4.1 Encryption of different video files (different sizes)

Encryption Throughput

Now we will make a comparison between other types of data (video files) to check which one can perform better in this case. Experimental results for video data type are shown Figure 10 at encryption.

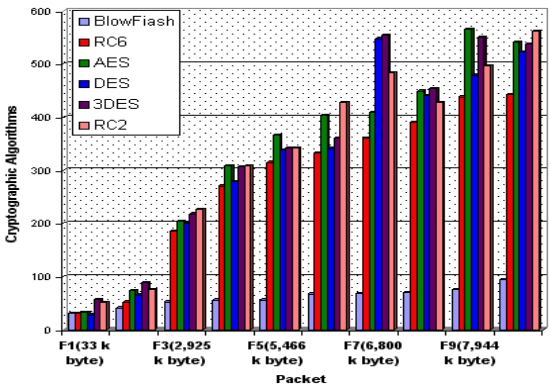

Figure 9: Time consumption for decrypt different audio files

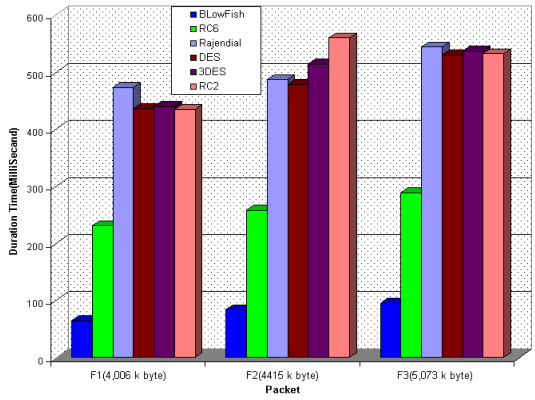

Figure 11: Time consumption for encrypt different video files

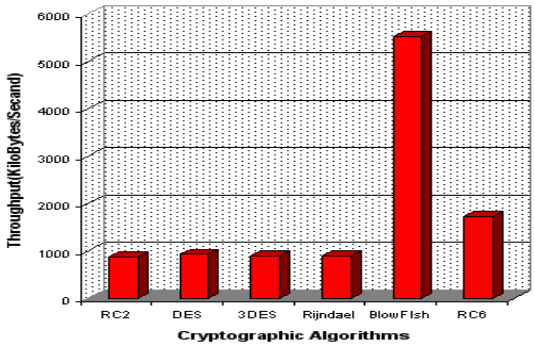

Figure 10: Throughput of each encryption algorithm (Kilobytes/Second)

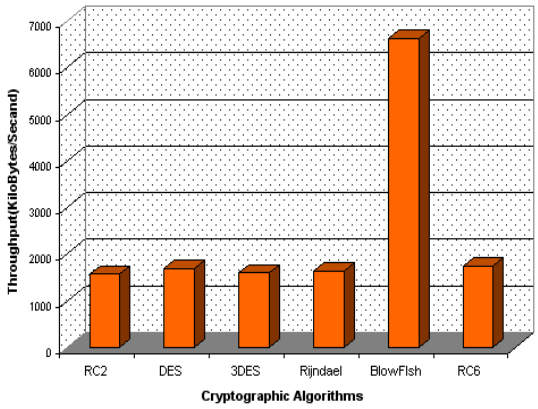

Figure 12: Throughput of each decryption algorithm (Kilobytes/Second)

CPU Work Load

In Figure 11, we show the performance of cryptography algorithms in terms of sharing the CPU load. With a different audio block size.

The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time and throughput as the same as in Audio files. Another point can be noticed here; that RC6 still requires less time has throughput greater than all algorithms except Blowfish. A third point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It always requires more time than DES. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms.

4.4.2 Decryption of Different Video Files (Different Sizes)

Decryption Throughput

Experimental results for this compassion point are shown Figure 12.

CPU Work Load

Experimental results for this compassion point are shown Figure 13.

From the results we found the result as the same as in encryption process for video and audio files.

4.5 The Effect of Changing Key Size of AES, And RC6 on Power Consumption

The last performance comparison point is 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-bit and 256-bit keys. The Experimental results are shown in Figures 14 and 15.

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-bit key to 192-bit causes increase in power and time consumption about 8% and to 256-bit key causes an increase of 16% [12].

Also in case of RC6, we consider the three different key

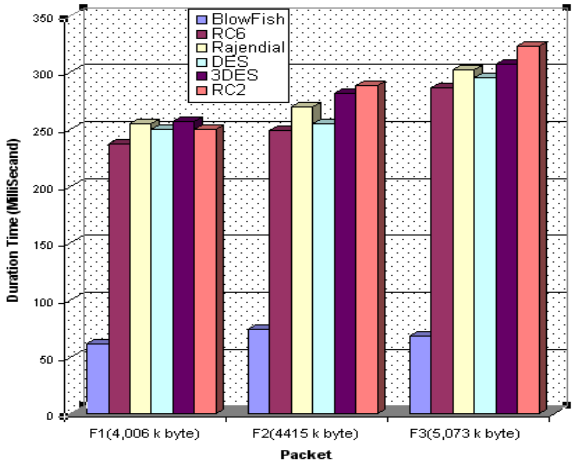

Figure 13: Time consumption for decrypt different video files

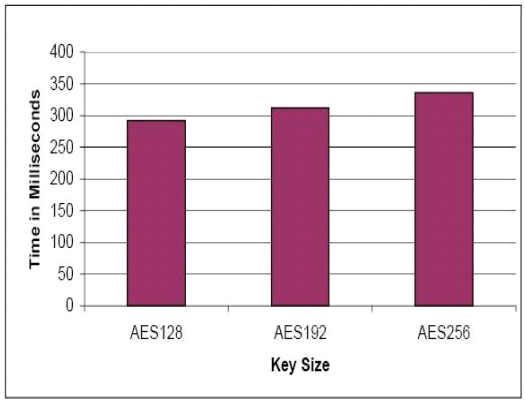

Figure 14: Time consumption for different key size for AES

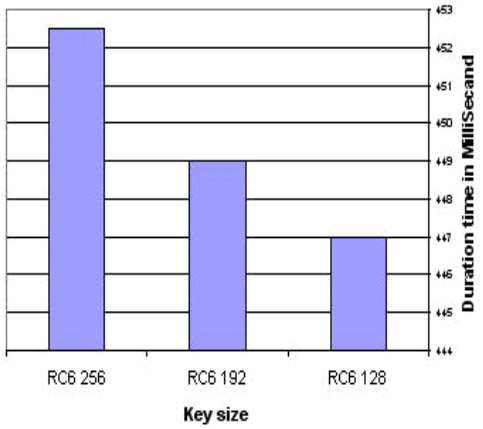

Figure 15: Time consumption for different key size for RC6

sizes possible i.e., 128-bit, 192-bit and 256-bit keys. The result is close to the one shown in the following figure:

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 Experimental results. Firstly; 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. Thirdly; we find that 3DES still has low performance compared to algorithm DES. Fourthly; we find RC2, has disadvantage over all other algorithms in terms of time consumption. Fifthly; we find AES has better performance than RC2, DES, and 3DES. In the case of audio and video files we found the result as the same as in text and document. 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.

Acknowledgments

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

References

[1] R. Chandramouli, "Battery power-aware encryption," *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 2, pp. 162-180, May 2006.

[2] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, pp. 243 -250, May 1994.

[3] J. Daemen, and V. Rijmen, "Rijndael: The advanced encryption standard," *Dr. Dobb's Journal*, pp. 137-139, Mar. 2001.

[4] P. Ding, "Central manager: A solution to avoid denial of service attacks for wreless LANs," *International Journal of Network Security*, vol. 4, no. 1, pp. 35-44, 2007.

[5] N. E. Fishawy, "Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms," *International Journal of Network Security*, pp. 241-251, Nov. 2007.

[6] Hardjono, *Security In Wireless LANS And MANS*, Artech House Publishers, 2005.

[7] S. Hirani, *Energy Consumption of Encryption Schemes in Wireless Devices Thesis*, University of Pittsburgh, Apr. 9,2003, Retrieved Oct. 1, 2008. (http://portal.acm.org/citation.cfm?id=383768)
[8] M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, 2005.
[9] M. H. Ibrahim, "A method for obtaining deniable public-key encryption," *International Journal of Network Security*, vol. 8, no. 1, pp. 1-9, 2009.
[10] M. H. Ibrahim, "Receiver-deniable public-key encryption," *International Journal of Network Security*, vol. 8, no. 2, pp. 159-165, 2009.
[11] S. Z. S. Idrus, and S. A. Aljunid, "Performance analysis of encryption algorithms text length size on web browsers," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no.1, pp. 20-25, Jan. 2008.
[12] K. McKay, *Trade-offs between Energy and Security in Wireless Networks Thesis*, Worcester Polytechnic Institute, Apr. 2005.
[13] K. Naik, "Software implementation strategies for power-conscious systems," *Mobile Networks and Applications*, vol. 6, pp. 291-305, 2001.
[14] P. Ruangchaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N," *The Third IEEE Workshop on Wireless LANs*, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.
[15] B. Schneier, *The Blowfish Encryption Algorithm*, Retrieved Oct. 25, 2008. (http://www.schneier.com/blowfish.html)
[16] A. Sinha, A. P. Chandrakasan, and JouleTrack, "A web based tool for software energy profiling," *Proceedings of the 38th Design Utomation Conference*, pp. 220-225, DAC Las Vega, US, 2001.
[17] W. Stallings, *Cryptography and Network Security*, Prentice Hall, pp. 58-309, 4th Ed, 2005.
[18] A. A. Tamimi, *Performance Analysis of Data Encryption Algorithms*, Retrieved Oct. 1, 2008. (http://www.cs.wustl.edu/∼jain/cse567-06/ftp/encryption_perf/index.html)
[19] A. Nadeem, "A performance comparison of data encryption algorithms," *IEEE Information and Communication Technologies*, pp. 84-89, 2006.
[20] *Results of Comparing Tens of Encryption Algorithms Using Different Settings- Crypto++ Benchmark*, Retrieved Oct. 1, 2008. (http://www.eskimo.com/ weidai/benchmarks.html)

Diaa Salama Abd Elminaam was born on November 23, 1982 in Kafr Sakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009. He is working in Higher Technological Institute, 10th of Ramadan city as teaching assistance at Faculty of Computer and informatics. He majors in Cryptography and Network Security. (Mobile: +20166104747; e-mail:ds_desert@yahoo.com)

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, and 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.

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.