Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types

Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud

***Abstract*—Security can be provided at different levels using different settings with different security algorithms, which can consume different levels of energy. The security settings can be different in many factors, but the main factors are the choice of ciphers used to provide security functions, the key length, and the number of operational rounds, packet size, and data types. These factors also have a significant impact on the energy consumption for providing security. A security algorithm is a function that is commonly used to provide security services such as encryption and message authentication. Many ciphers have been created, but only few are known to be strong and secure, which means no loophole or backdoor is known. The study of the energy consumption of the encryption schemes in wireless devices is essential in design of energy efficient security protocols. The major contributions of this paper are energy-security trades off then, some suggestions for design of secure communications systems. 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.**

***Index Terms*—Encryption techniques, Computer security, AES, DES, RC2, 3DES, Blowfish, RC6**

I. INTRODUCTION

Encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. 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). 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].

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. Strength of Symmetric key encryption depends on the size of the 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 uses various (128, 192, 256) bits keys [1-5]. The most common classification of encryption techniques can be shown in Fig. 1.

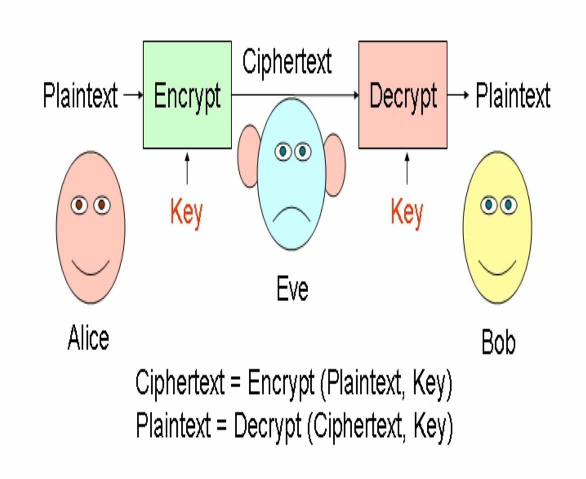
Plaintext
Encrypt
Ciphertext
Decrypt
Plaintext
Key
Key
Alice
Eve
Bob
Ciphertext = Encrypt (Plaintext, Key)
Plaintext = Decrypt (Ciphertext, Key)

Fig.1 Symmetric Key Encryption algorithms

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

DES: (Data Encryption Standard) was the first 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 64-bits block cipher with a variable key size that -bit block - can be used as a replacement for the DES algorithm ranges from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [3].

Blowfish is block cipher 64. 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 (previously called Rijndael) [18], [19], [20] 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 [21], [22], [23] 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 on power consumption and encryption time. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. 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. We examine a method for analyzing trade-offs between energy and security. The goal is to aid the design of energy efficient secure communication schemes for the wireless environment in the future. 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, video data, and Pictures data- 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. Experimental results are shown in section 4. Finally the conclusions are drawn in section 5.

II. RELATED WORK

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

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).

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 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.

A study in [13] is conducted for different popular secret key algorithms such as RC4, AES, and XOR. They were implemented, and their performance was compared by encrypting for real time video streaming of varying contents. The results showed; encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Therefore, AES is a feasible solution to secure real time video transmissions.

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

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.

In [17] Crypto++ Library is a free C++ class library of cryptographic schemes. It evaluates the most commonly used cryptographic algorithms. Also it is shown that Blowfish and AES have the best performance among others. And both of them are known to have better encryption (i.e. stronger against data attacks) than the other two.

III. EXPERIMENTAL DESIGN

For our experiment, a laptop IV 2.4 GHz CPU is used, 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 8, 262 Kbytes for audio data, from 28 Kbytes to 131 Kbytes for pictures(Images) and from 4, 006 Kbytes to 5, 073 Kbytes for video files using.NET environment. These implementations are thoroughly tested and are optimized to give the maximum performance for the algorithms. Several performance metrics are collected:

8- Power consumption.
9- Encryption time.
10- CPU process time.
11- CPU clock cycles

The method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery. The experiments note the number of iteration or runs over the file and the battery life. Change in battery life divided by the number of runs gives the battery life consumed in percentage for one run. The flow chart for the software code used in the experiment is presented in (figure 4.3). The battery and computational trade-off of encryption schemes under different scenarios are considered in various experimental setups but the underlying setup remains the same. Initialization in case of encryption would be to establish the keys required while in case of data transmission it would include establishing a wireless connection. Processing in experiment for encryption without data transmission is to read data from the file encrypt the data and put it in another file. In case of encryption with data transmission the data is read from the file encrypted and the send to the second laptop. This is done till the battery drains to 30% of the lifetime left. We stop at 30% because after that the systems alarm and data recovery mechanisms become active and the performance of the schemes change. After a few runs of processing on the file the battery life left and the system time is recorded. The average battery life consumed per run and the time taken to do so is the calculated for the results. It is expected that the computation time would be closely related to the battery requirements; however, since the CPU utilization of power depends on parameters like voltage supply and capacitive load. The capacitive load on the CPU depends on the switching demand, which again depends on the instructions being executed. Hence, measurements for both the parameters are considered.

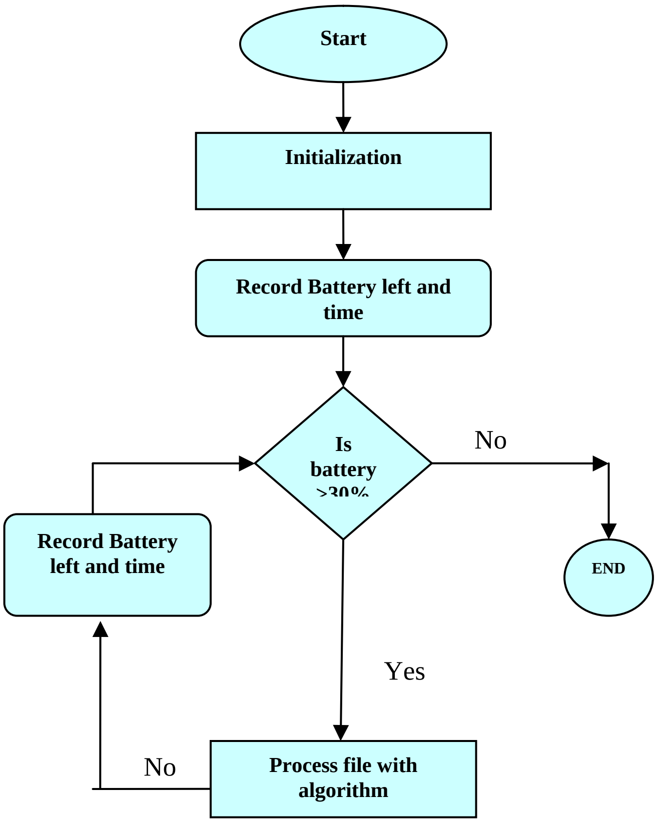
Start
Initialization
Record Battery left and time
Is battery >30%
No
END
Record Battery left and time
Yes
No
Process file with algorithm

Fig.2: Flowchart for software code

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 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:

1. A comparison is conducted between the results of the selected different encryption schemes in terms of the encryption time, battery power and throughputs.
2. A study is performed on the effect of changing packet size on power consumption, throughput, and CPU work load for each selected cryptography algorithm.
3. A study is performed on the effect of changing data types -such as text or document, Audio file, Video file and images- for each cryptography selected algorithm on power consumption.
4. A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

IV. EXPERIMENTAL RESULTS

A. The effect of changing packet size for cryptography algorithm on power consumption (text files)

a Encryption of different packet size

1 CPU work load

In Figure 3, we show the performance of cryptography algorithms in terms of sharing the CPU load for encryption process. With a different data block size

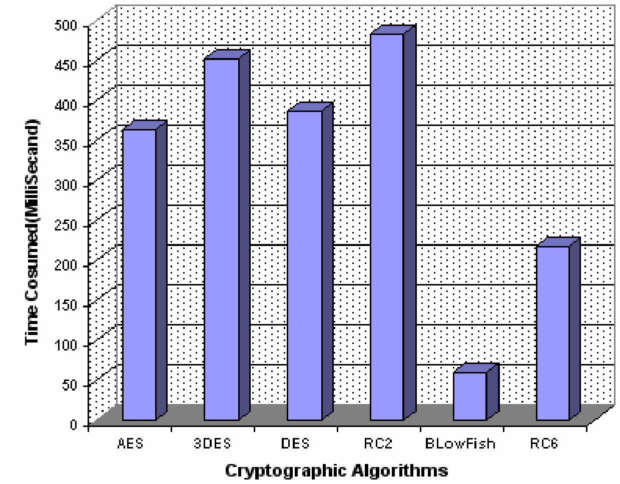

Fig. 3 Time consumption for encrypt different Text Data (Millisecond)

2Encryption throughput

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.

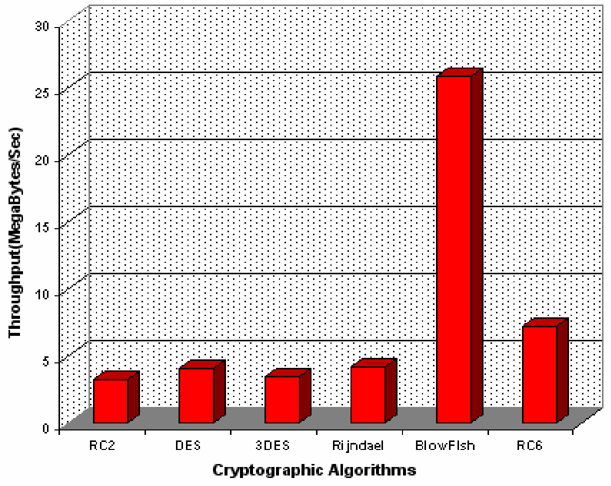

Fig. 4 Throughput of each encryption algorithm (Megabyte/Second)

3 Power consumption

In Figure5, we show the performance of cryptography algorithms in terms of Power consumption for encryption process. With a different data block size

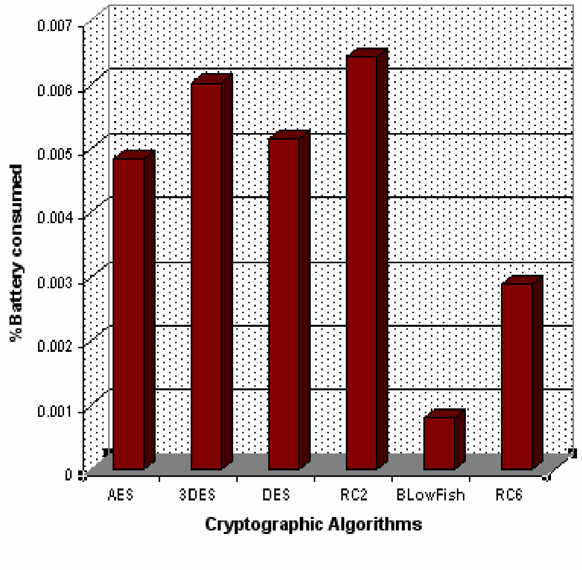

Fig. 5 Power consumption for encrypt different Text document Files

The results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time, and throughput (when we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 14% of the power which is consumed for AES). Another point can be noticed here that RC6 requires less power, and less time than all algorithms except Blowfish (when we encrypt the same data by using RC6 &AES, we found that RC6 requires approximately 56% of the power which is consumed for AES). A third point can be noticed here that AES has an advantage over other 3DES, DES and RC2 in terms of power consumption, 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.

B. The effect of changing file type (Audio files) for cryptographic algorithms on power consumption.

a Encryption of different Audio files (different sizes)

1 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 Fig. 6.

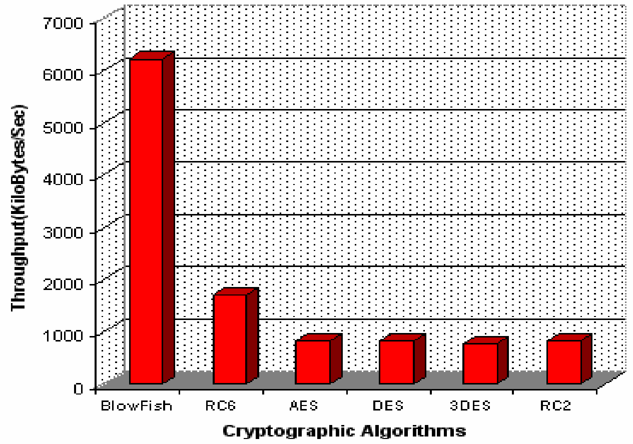

Fig. 6 Throughput of each encryption algorithm (Kilobytes/Second)

.2 CPU work load

In Figure 7, we show the performance of cryptographic algorithms in terms of sharing the CPU load for encryption process with a different audio block size

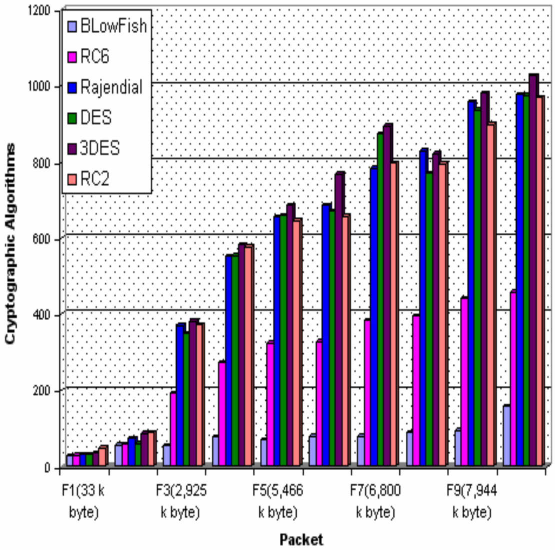

Fig. 7 Time consumption for encrypt different Audio Files (Millisecond)

3Power consumption

In Figure8, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process. With a different audio block size

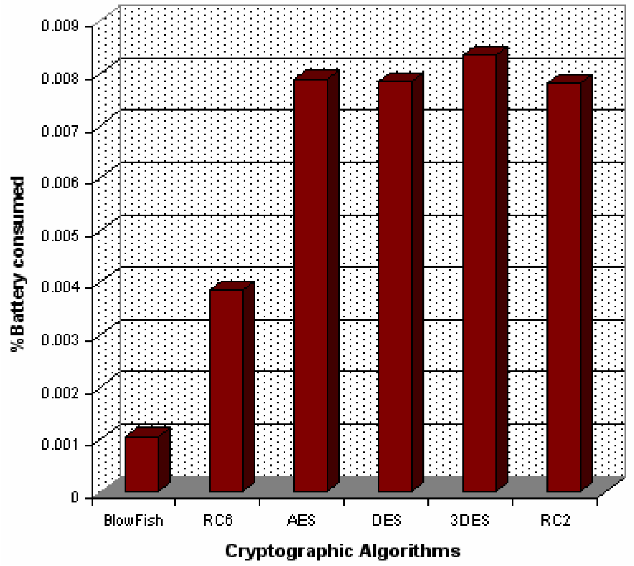

Fig. 8 Power consumption for encrypt different Audio Files

Results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time (CPU work load), and throughput (when we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 14% of the power which is consumed for AES). Another point that can be noticed here is that RC6 requires less power consumption and less time than all algorithms except Blowfish (when we encrypt the same data by using RC6 and AES, we found that RC6 requires approximately 45% of the power which is consumed for AES). A third point can be noticed here is 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 is that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES. Finally, it is found that RC2 has low performance and low throughput when compared to the other five algorithms in spite of the small key size used.

C. The effect of changing file type (Video files) for cryptographic algorithms on power consumption.

a Encryption of different Video files (different sizes)

1 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 Fig. 9 at encryption.

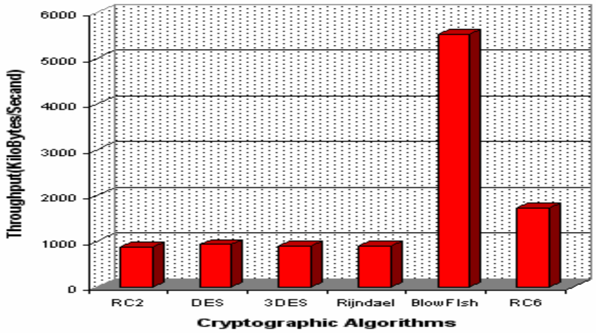

Fig. 9 Throughput of each encryption algorithm (Kilobytes/Second)

2 CPU work load

In Figure 10, we show the performance of cryptographic algorithms in terms of sharing the CPU load. With a different video block size

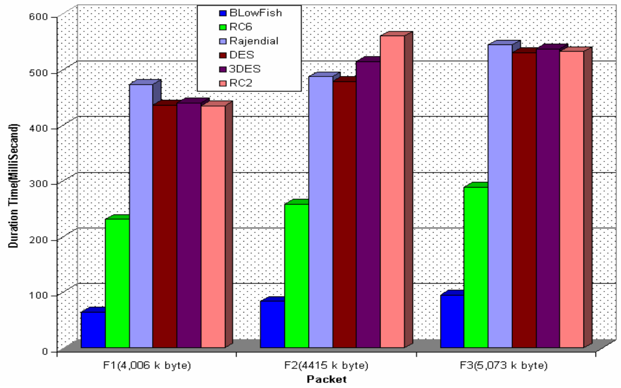

Fig. 10 Time consumption for encrypt different video Files (millisecond)

3 Power consumption

In Figure11, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process with a different video block size

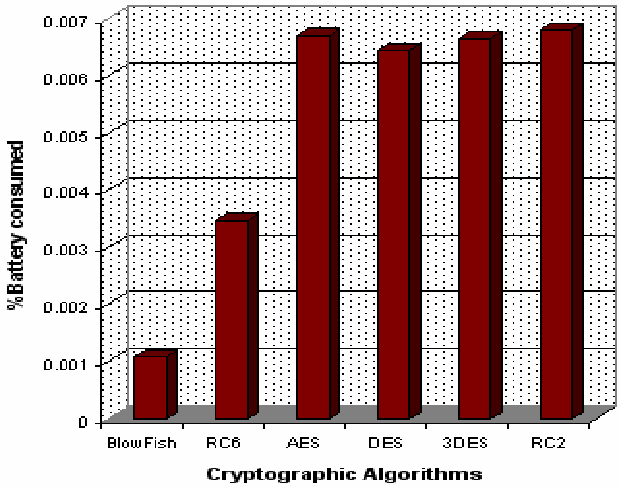

Fig. 11 Power consumption for encrypt different Video Files

The result is the same as in text and audio data.The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time, power consumption, and throughput (when we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 18% of the power which is consumed for AES). Another point that can be noticed here is that RC6 requires less power consumption and less time than all algorithms except Blowfish (when we encrypt the same data by using RC6 and AES, we found that RC6 requires approximately 54% of the power which is consumed for AES). A third 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. Finally, it is found that RC2 has low performance and low throughput when compared to the other five algorithms

D. The effect of changing file type (Images) for cryptography algorithm on power consumption.

Here too we performed the same operation which was conducted on text files, audio, and video files in encryption and decryption images files. Experimental results for image data type (JPEG images) are shown Fig. 12 at encryption.

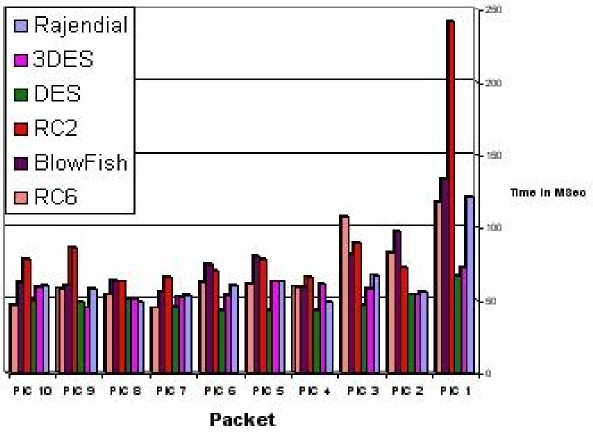

Fig. 12 Time consumption for encrypt different images (Millisecond)

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 the decryption process over other algorithms in terms of time consumption and serially in throughput. It is found that 3DES still has low performance when compared to DES.

E. 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 bits and 256 bit keys. The simulation results are shown in Fig.13 and Fig.14.

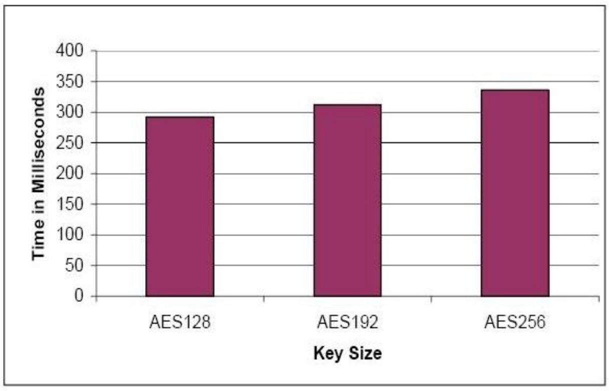

Fig.13 Time consumption for different key size for AES

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

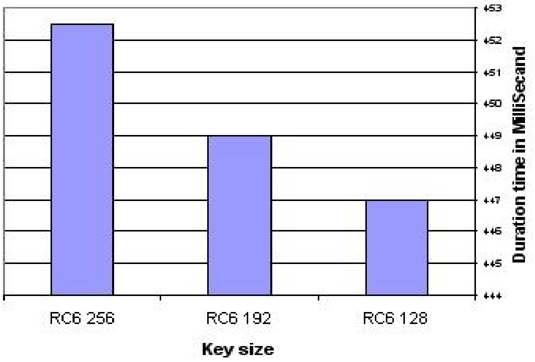

Fig. 14 Time consumption for different key size for RC6

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

V. CONCLUSION AND FUTURE WORK

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results. First, in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Secondly, it is found that 3DES still has low performance compared to algorithm DES. Thirdly, it is found that, RC2 has disadvantage over all other algorithms in terms of time consumption, and power consumption. Fourthly, it is found that, AES has better performance than RC2, DES, and 3DES. In the case of audio and video files we found that the result is 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.

For our future work, we will study the distribution of different packets sizes typically transmitted and received by wireless devices over wireless network. In our future research, we will suggest three approaches to reduce the energy consumption of security protocols and apply them to wireless local area networks (WLANs) to provide an energy efficient security schema for 802.11 WLANs by replacement of standard security protocol primitives that consume high energy while maintaining the same security level. Secondly, modification of standard security protocols appropriately. Finally, a totally new design of security protocol where energy efficiency is the main focus.

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 AlgorithmRetrieved 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] W.S.Elkilani, H.m.Abdul-Kader, "Performance of Encryption Techniques for Real Time Video Streaming, IBIMA Conference, Jan 2009, PP 1846-1850

[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, 2008Fromhttp://www.cs.wustl.edu/~jain/cse56706/ftp/encryption_perf/index.html

[16] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark-. Retrieved October 1, 2008,

[17] From: http://www.eskimo.com/~weidai/benchmarks.html

[18] J. Daemen and V. Rijmen. ”AES Proposal:Rijndael”. In National Institute of Standards and Technology, July 2001.

[19] J. Daemen and V. Rijmen. ”The Design of Rijndael”. In Springer-Verlag, 2002.

[20] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D.Wagner, and D.Whiting. ”Improved Cryptanalysis of Rijndael”. In Seventh Fast Software Encryption Workshop, page 19, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. Springer-Verlag.

[21] A. Elbirt, W. Yip, B. Chetwynd, and C. Paar. ”An FPGABased Performance Evaluation of the AES Block Cipher Candidate AlgorithmFinalists”, 2001.citeseer.nj.nec.com/elbirt01fpgabased.html.

[22] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar. ”An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists”. In AES Candidate Conference, pages 13–27, 2000.

[23] P. J. Robertson, E. L. Witzke, D. C. Wilcox, L. G. Pierson, and K. Gass. ”A DES ASIC Suitable for Network Encryption at 10 Gbps and Beyond”. In CHES, volume 1717, pages 37–48, 2000.

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 University, Egypt in 2004 with grade very good with honor. 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. (Mobile: +20166104747;
e-mail:ds_desert@yahoo.com)

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, 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.

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.