Energy Efficiency of Encryption Schemes for Wireless Devices

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

Abstract—**Encryption algorithms are known to be computationally intensive.They 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 tries to present a fair comparison between the most common and used algorithms in data encryption field according to power consumption. It 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, and finally encryption/decryption speed. Experimental results are given to demonstrate the effectiveness of each algorithm.**

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

I. INTRODUCTION

Security can be provided at different settings with different security algorithms. The security settings can be different in many factors, but the main factors are the choice of ciphers used to prove security functions, packet size, and data types. Data encryption procedures are mainly into two categories depending on the type of security keys used to encrypt/decrypt the secured data.the two categories are: Symmetric and Asymmetric 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 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 ECC). 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].

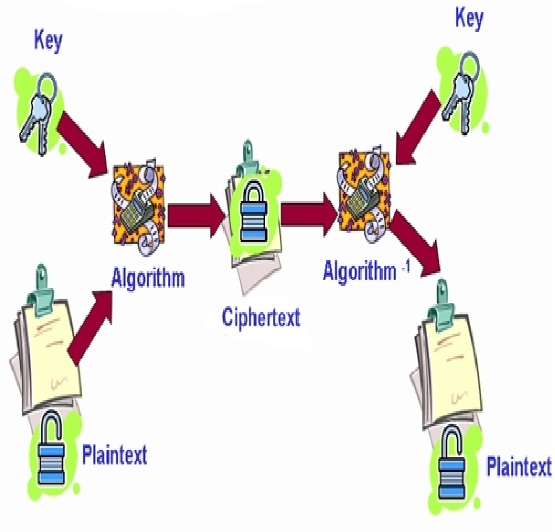

Fig. 1 Overview of the field of cryptography

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.

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 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, audio file, video files, and images using different settings such as changing packet size for the selected cryptographic algorithms. This paper is organized as follows. Related work is described in Section 2. A view of Experimental design is given in section 3. Experimental results are shown in section 4. Finally the conclusions are drawn 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 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.

III. Experimental Design

For our experiment, a laptop IV 2.4 GHz CPU is used, in which performance data are collected. In the experiments, the laptop encrypts a different file size that range from 321 Kilobyte 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:

5- Encryption time and throughput.
6- Power consumption (Micro joule/bytes)
7- Power consumption (Percent of battery consumed)

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 which can consider as a good indicator for power consumption [15].

The first 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 second method for computation of the energy cost of encryption, we use the same techniques as described in [16]. We present a basic cost of encryption represented by the product of the total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The basic encryption cost is in unit of ampere-cycle. To calculate the total energy cost, we divide the ampere-cycles by the clock frequency in cycles/second of a processor; we obtain the energy cost of encryption in ampere-seconds. Then, we multiply the ampere-seconds with the processor's operating voltage, and we obtain the energy cost in Joule. By using the cycles, the operating voltage of the CPU, and the average current drawn for each cycle, we can calculate the energy consumption of cryptographic functions. For example, in average, each cycle consumes approximately 270 mA on an Intel 486DX2 processor [16] or 180 mA on Intel Strong ARM [17]. For a sample calculation, with a 700 MHz CPU operating at 1.35 Volt, an encryption with 20, 000 cycles would consume about 5.71 x 10-3 mA-second or 7.7 μ Joule. Since for a given hardware Vcc are fixed.

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

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

-A study is performed on the effect of changing data types -such as text or document, Audio file, Video file and images- for each selected cryptographic algorithms 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 Encryption throughput

As the throughput value is increased, the power consumption of this encryption technique is decreased. Experimental results for this compassion point are shown Fig.2

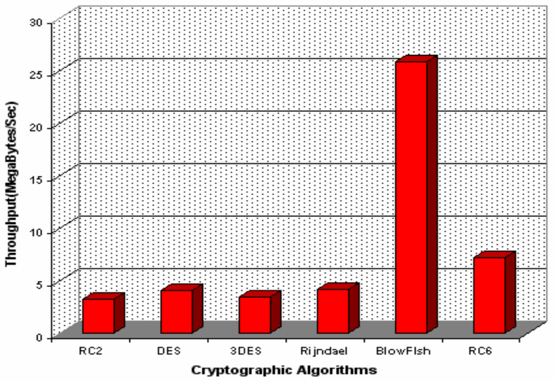

Fig. 2 Throughput of each encryption algorithm (Megabyte/Sec)

2 Power consumption (Micro joule/byte)

In Fig.3, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process with a different data block size (Micro joule/byte)

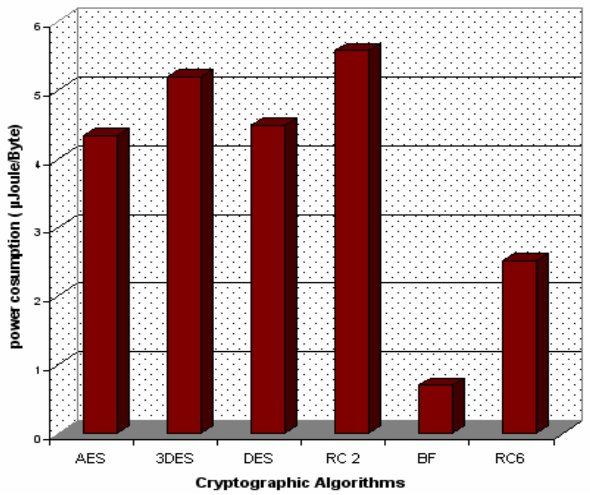

Fig.3 Power consumption for encrypt different Text document Files (micro Joule/Byte)

3 Power consumption (percent of power consumed)

In Fig. 4, we show the performance of cryptographic algorithms in terms of Power consumption by calculating difference in battery consumed for encryption process with a different data block size

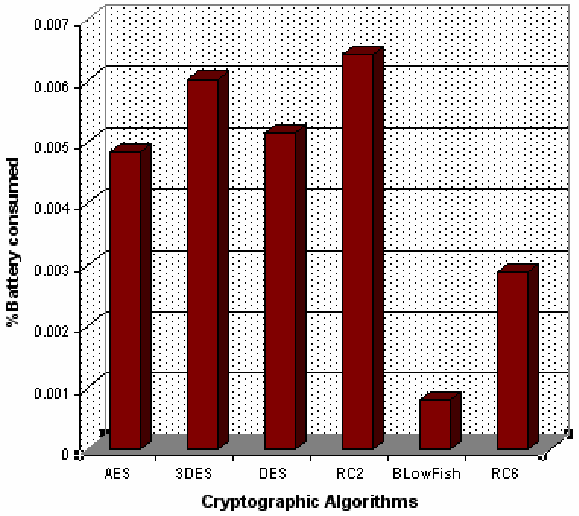

Fig. 4 Power consumption for encrypt different Text document Files

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 16% 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 and AES, we found that RC6 requires approximately 58% 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 Decryption of different packet size

Decryption throughput

Experimental results for this compassion point are shown Fig.5

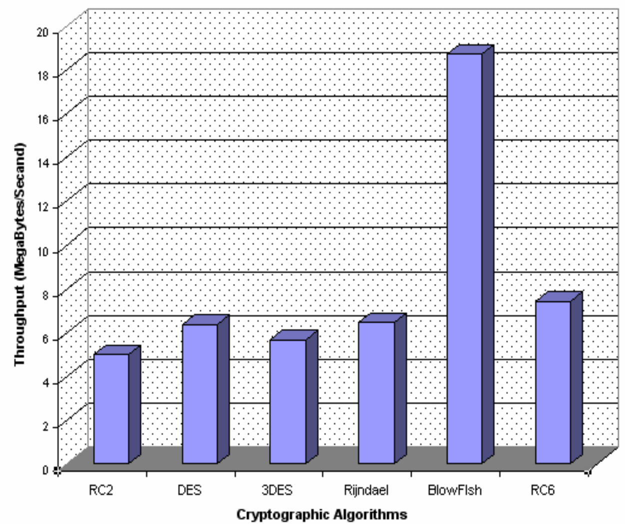

Fig. 5 Throughput of each decryption algorithm (Megabyte/Sec)

1 Power consumption (Micro joule/byte)

Experimental results for this compassion point are shown Fig.6

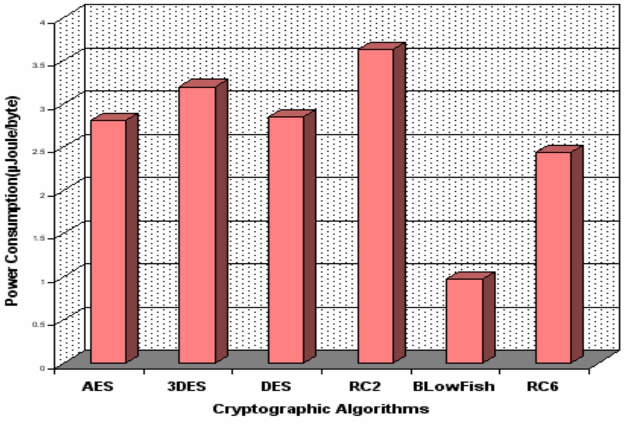

Fig. 6 Power consumption for Decrypt different Text document Files (Micro Joule/Byte)

It is found that in decryption stage Blowfish is better than the other algorithms in throughput and power consumption (when we decrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 34% of the power which is consumed for AES). The second point which should be noticed here is that RC6 requires less time than all algorithms except Blowfish (when we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 87% of the power which is consumed for AES). A third point that can be noticed is 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.

b The effect of changing file type (Audio files) for cryptography algorithm on power consumption.

4.2.1 Encryption of different Audio files (different sizes)

1. Encryption throughput

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. 7 at encryption.

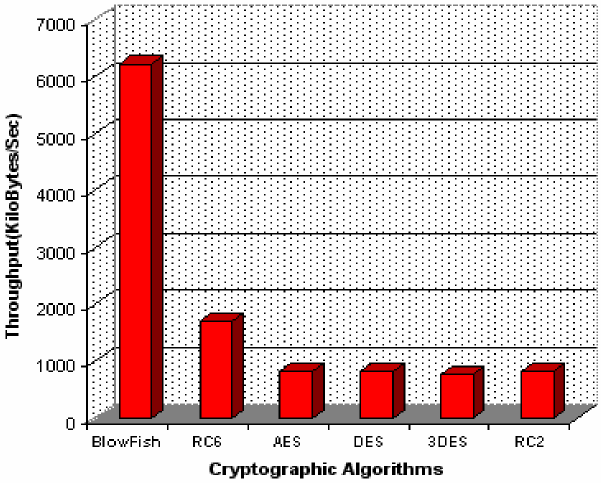

Fig. 7 Throughput of each encryption algorithm (Kilobytes/Second)

2. Power consumption (Micro Joule/Byte)

Experimental results for this compassion point are shown Fig.8

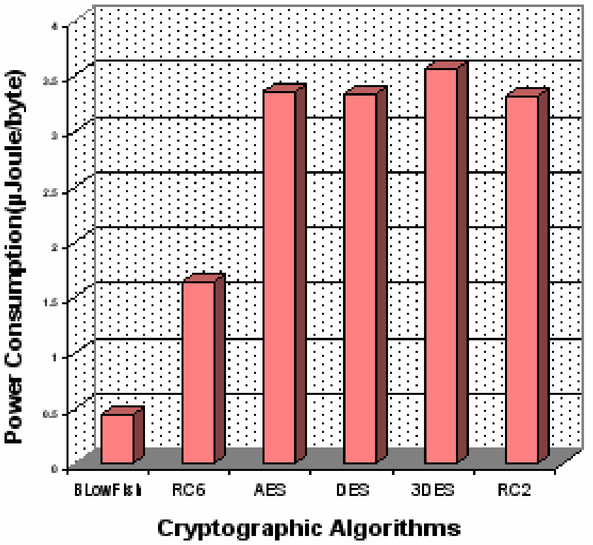

Fig. 8 Power consumption for encrypt different Audio Files (Micro Joule/Byte)

1 Power consumption (percent of power consumed)

Experimental results for this compassion point are shown Fig.9

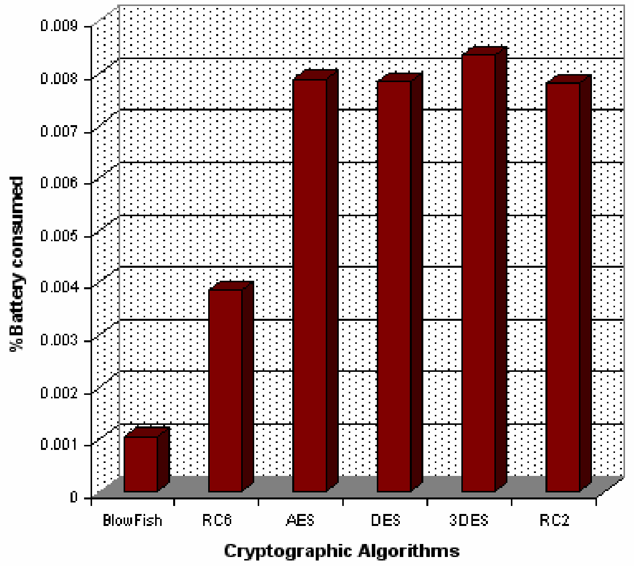

Fig. 9 Power consumption for encrypt different Audio Files

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 13% 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 48% 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 Decryption of different Audio files (different sizes)

1 Decryption throughput

Experimental results for this compassion point are shown Fig.10

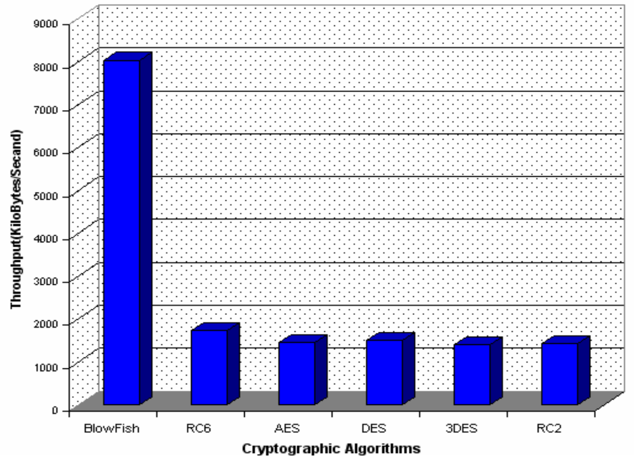

Fig. 10 Throughput of each Decryption algorithm (Kilobytes/Second)

2 Power consumption for decryption

Experimental results for this compassion point are shown Fig. 11

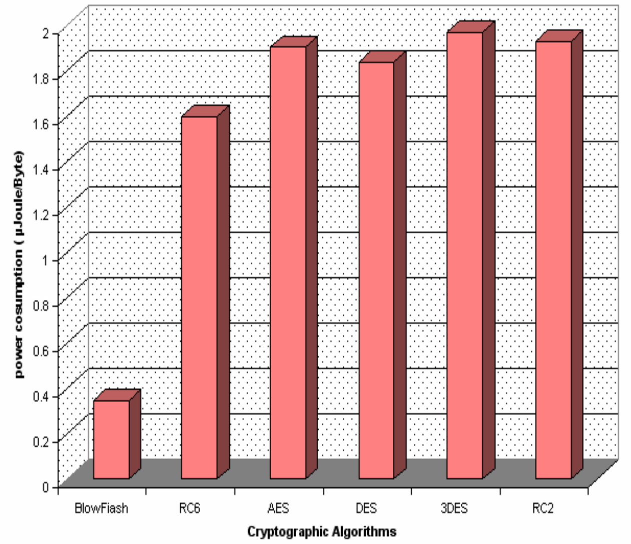

Fig. 11 Power consumption for decrypts different Audio Files (Micro Joule/Byte)

From the results we found that the result is the same as in encryption process for audio files. When we decrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 18% of the power which is consumed for AES. When we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 84% of the power which is consumed for AES

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

4.3.1 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 to calculate throughput for video data type is shown Fig. 12 at encryption.

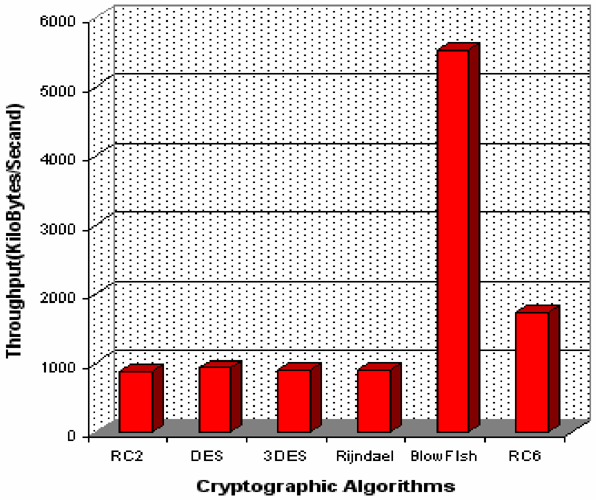

Fig. 12 Throughput of each encryption algorithm (Kilobytes/Second)

2 Power consumption (Micro joule/byte)

Experimental results for this compassion point are shown Fig. 13

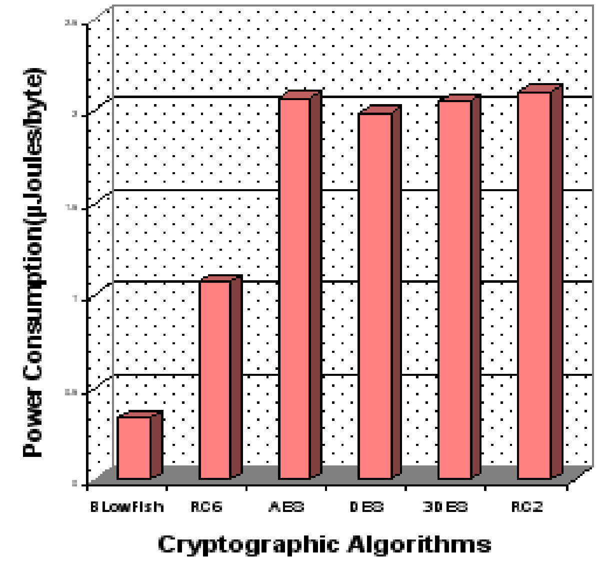

Fig. 13 Power consumption for encrypt different Video Files (micro Joule/Byte)

3 Power consumption (percent of power consumed)

In Figure14, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process with a different video block size

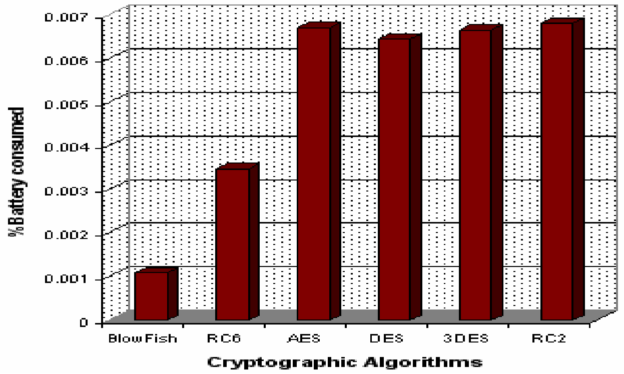

Fig. 14 Power consumption for encrypt different Video Files

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 16% 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 51% 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 Decryption of different Video files (different sizes)

1 Decryption throughput

Experimental results for this compassion point are shown Fig. 15

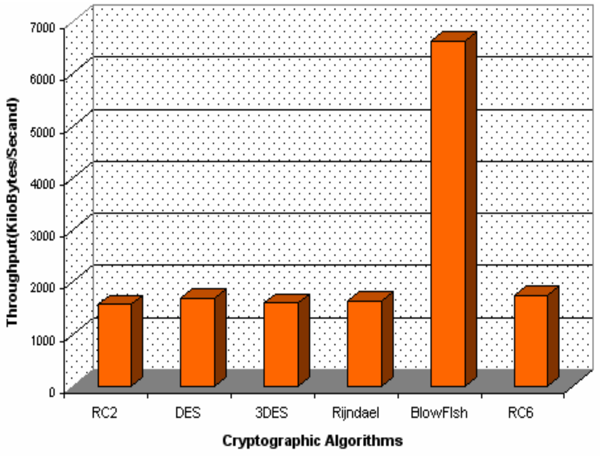

Fig. 15 Throughput of each Decryption algorithm (Kilobytes/Second)

2 Power consumption for Decryption

Experimental results for this compassion point are shown (Fig.16)

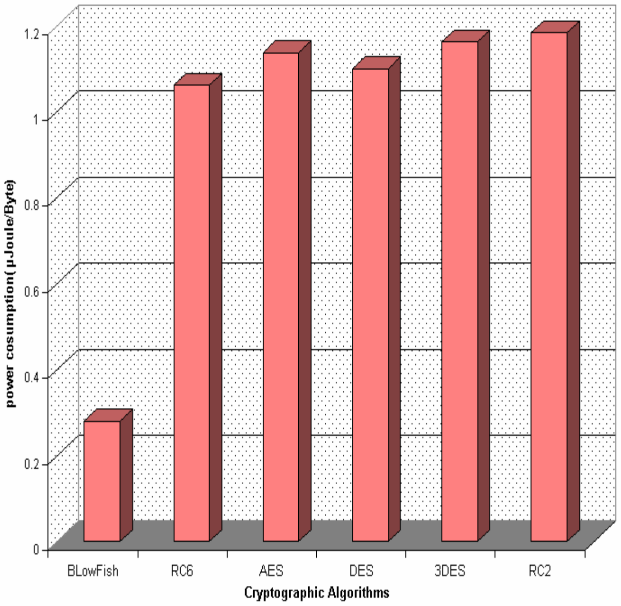

Fig. 16 Power consumption for Decrypt different Video Files in (micro joule/Byte)

From the results we found that the result is the same as in the encryption process for Video, audio files, and text data. When we decrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 24% of the power which is consumed for AES. When we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 93% of the power which is consumed for AES.

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

a Encryption of different images files (different sizes)

Now we will make a comparison between other types of data (Images) to check which one can perform better in this case. Experiment results for image data type (JPEG images) are shown Fig. 17, Fig 18, and Fig 19 respectively.

1 CPU work load

In Figure 17, we calculated the performance of cryptography algorithms in terms of sharing the CPU load to encrypt different Images files with a different data block size with out data transmission.

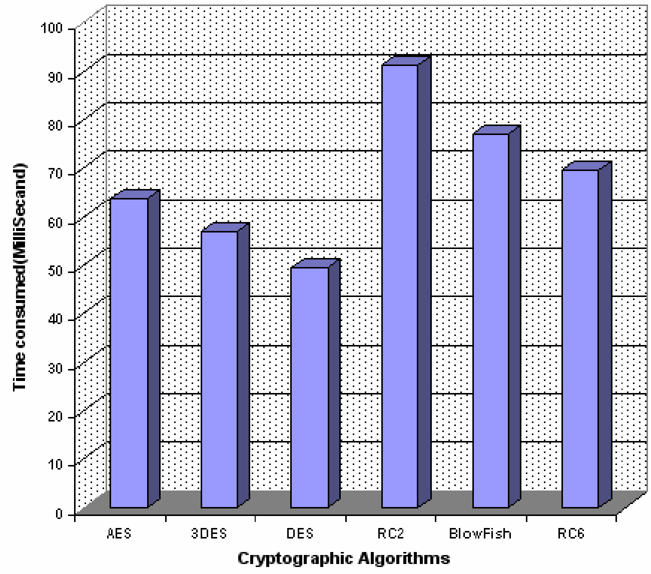

Fig. 17 Time consumption for encrypt different Images (Millisecond)

2 Encryption throughput

In fig 18 Throughput of each encryption algorithm to encrypt different text data (Kilobytes/Sec).

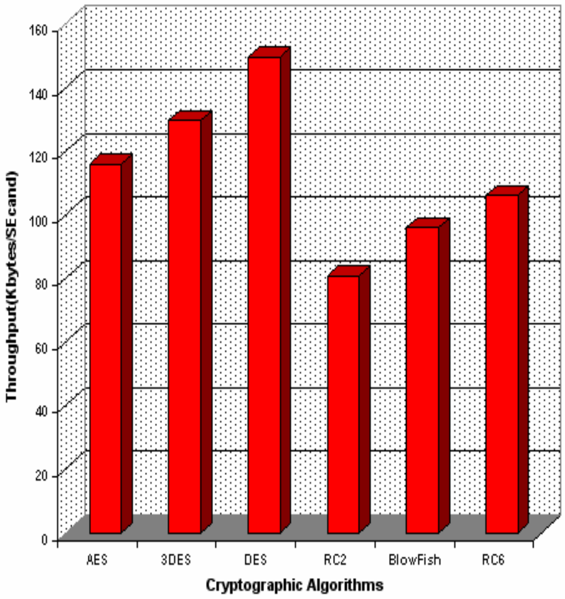

Fig.18 Throughput of each encryption algorithm (Kilobytes/Sec)

3 Power consumption (percentage of battery Consumed)

In Figure 19, we calculated the performance of cryptography algorithms in terms of Power consumption by calculating change in battery left for encryption process for text data with a different data block size.

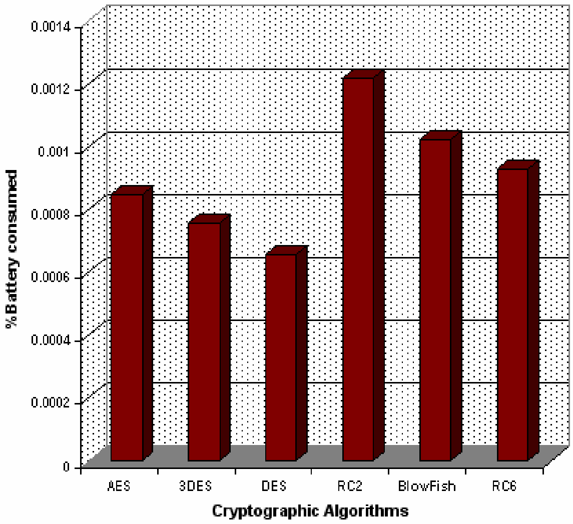

Fig.19 Power consumption for encrypt different Images Files

e Decryption of different Images files (different sizes)

4 CPU work load

Experiment results for this compassion point are shown Fig.20 to decrypt different text data with a different data block size with out data transmission.

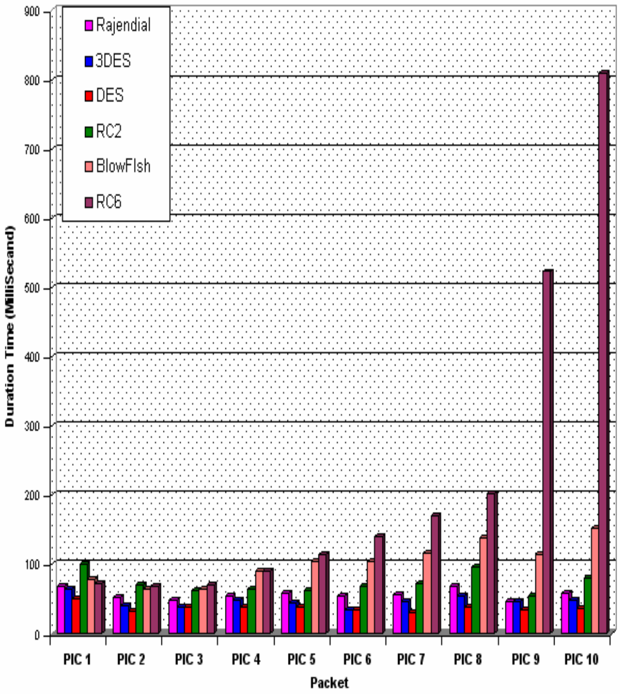

Fig. 20 Time consumption for decrypt different images (Millisecond)

V. 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. 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; 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 audio and video files we found the result as the same as in text and document.

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] 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. RetrievedOctober1, 2008From http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.htmlhttp://www.codeproject.com/KB/security/hexenc.aspx

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

[17] A. Sinha and A.P. Chandrakasan, “Joule Track- A Web Based Tool For Software Energy Profiling, ” Proceedings of the 38th Design Automation Conference, DAC 2001, Las Vegas, NV, USA, pp. 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 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.