A PERFORMANCE EVALUATION OF COMMON ENCRYPTION TECHNIQUES WITH SECURE WATERMARK SYSTEM (SWS)

Ashraf Odeh[1], Shadi R.Masadeh[2], Ahmad Azzazi[3]

[1]Computer Information Systems Department, Isra University, Amman, Jordan
[2]Computer Networks Department, Isra University, Amman, Jordan
[3]Computer Information Systems Department, Applied Science University, Amman, Jordan

ABSTRACT

Ciphering algorithms play a main role in information security systems. Therefore in this paper we are considering the important performance of these algorithms like CPU time consumption, memory usage and battery usage. This research tries to demonstrate a fair comparison between the most common algorithms and with a novel method called Secured Watermark System (SWS) in data encryption field according to CPU time, packet size and power consumption. It provides a comparison the most known algorithms used in encryption: AES (Rijndael), DES, Blowfish, and Secured Watermark System (SWS).

For comparing these algorithms with each other variations of data block sizes, and a variation of encryption-decryption speeds where used in this research.

In addition a comparison with different platforms such as Windows 8, Windows XP and Linux has been conducted. Finally the results of the experimentation demonstrate the performance and efficiency of the compared encryption algorithms with different parameters.

KEYWORDS

AES, DES, Blowfish, Secured Watermark System (SWS) and Computer Security.

1.INTRODUCTION

Security of information systems could be implemented with many widely known security algorithms, which can be adjusted with different settings for these algorithms [1],[2],[11],[12]. There are a lot of factors for security settings [3],[5] with main important factors like the type of cipher, which proves the security functionality, the processor time consumption, the size of packets, the general power consumption, the data type used and the battery power consumption [6],[10],[13].

A brief description of the most common ciphering algorithms like AES, DES, Blowfish and 3DES are discussed below:

1- DES: - The Data Encryption Standard is one of the most common used encryption mechanism introduced in the year 1977.Using this algorithm data are encrypted using a 64 bit blocks with an encryption key of 56 bit length. The DES with 64 bit input as steps applied in series gives an output of 64 bits. The decryption of the cipher data is done with the reversed steps of the

DOI : 10.5121/ijnsa.2015.7303

encryption mechanism with the same key. Using the same key for the encryption and for the decryption mechanisms gives the attackers of the cipher data a big opportunity to attack the encryption system, which forms an important weakness of this algorithm [20],[19],[22].

2- 3DES: The 3DES encryption algorithm has the block of the size 64 bits. It uses an encryption key of 192 bits. This algorithm is similar to the original Data Encryption Standard, but with the difference that the 3DES is to be applied 3 times. The repeated application of 3 times of the algorithm should give the encryption more complexity to increase security level of it and to increase the safe time when trying to decrypt it. The 3DES is therefore slower than the traditional block encryption algorithms [23],[24],[25].

3- AES: - Which stands for the Advanced Encryption Standard. This standard was introduced in the year 2001.The AES algorithm was developed to overcome the weaknesses of the Data Encryption Standard. It is a block cipher standard with a symmetric key solution. It provides an encryption method better than the 3DES one with improved security level and improved security efficiency. A variation of the AES is called the "Rijindael" with a variable key length of 128 bits, 192 bits or 256 bits, which is specified independent of the block length. The block length should be limited in the standard to 128 bits [7]-[9],[11].

4-Blowfish: - This newly developed encryption mechanism is a symmetric block cipher standard. It should be fast for encrypting data with a 32 bit processor at the clock speed of 18 cycles per byte. It should use a compact memory size of 5K of less. This standard has a simple structure, which is easy to implement and use. Therefore the strength of the standard could be easily determined. The length of the key of the Blowfish standard is variable and can have the length of 448 bits. This gives the user of this mechanism to get higher security, but the user should consider the speed issues when deploying higher values of the key length. The Block size of the Blowfish is usually 64 bits [5],[22].

In our Research, we developed a novel algorithm to provide data security which is called the Watermark System (SWS) algorithm. The newly developed algorithm SWS was tested through the evaluation of the four mentioned algorithms for encryption (i.e. AES, DES and Blowfish) compared with the developed (SWS) algorithm in term of time and power consumption. The SWS adopts asymmetric encryption technique.

2. Related Works

There are many research studies related to the comparison of the commonly used security algorithms like DES,AES,3DES, Blowfish and others [15].Different studies implement these algorithms with different input files of different content and different sizes to compare the performance of these algorithms with each other[15].

From pervious studies results show that the performance of Blowfish algorithm is the better algorithm compared with the other mentioned algorithms. It showed also that the AES Algorithm is efficient and faster than the other algorithms [16]. The transmission of data where considered also in the pervious studies, with the conclusion that the AES has the best performance among the compared encryption algorithms. It follows that; the DES encryption algorithm is faster 3 times more than the 3DES algorithm for the same size of encrypted data.

In [14], the authors gave some assumptions about the most common security algorithms like AES, XOR, and RC4. They compared the encryption algorithms by encrypting video streams in real time and not text data only. They concluded; that the delay overhead of the AES encryption algorithm is less than the overhead of the XOR algorithm and the RC4 algorithm when encrypting real time video stream data. Thus, the AES is a better solution when transmitting real time video data streams.

In [18] the authors made a performance study to get results about the usability of security algorithms within the scripting languages of web based programming languages. They analysed the performance of the encryption algorithms when using web browser data.

Another study done in [17] has been done to compare the consumption of energy of the different available symmetric key encryption algorithms on handheld devices. It shows that only about 45% of the battery power is remaining when encrypting a file of about 5MB using the 3DES,that means, the no further encryption is [possible after that size of data because the battery died at all.

In the study [21], the authors used the free c++ encryption library (Cryto++ library).They have done an evaluation of the most know encryption algorithms. They showed that the Blowfish and the AES algorithms have the best security performance results. They showed also that both have better security level against attacks than the of DES and 3DES security algorithms.

3. THE SECURE WATERMARK SYSTEM (SWS)

The functionality overview of the proposed system (SWS) consists of two phases. The first phase is called the encoding phase. The steps of encoding phases are as follows:

1. Read Dataset.
2. Divide Dataset into subset (64 blocks)
3. Convert Watermark image into decimal equivalent (array of 8 elements)
4. Embedded each of array element into each block
5. Encrypt the embedded dataset using private key
6. The data in this model is read serially from an input stream or file as a block of 64- bits as a plain text. The 4 blocks numbered from b1 – b4, and then the blocks are divided into constituent bytes where each block yields 2 bytes that represent the left and Right of the block.
7. The bytes are swapped into constituent.
8. All Block's after swapping process are shifted in a symmetrical way.
9. The first block in the left side is X-oring with key1 .The key1 was received from key generation process as shown figure 2.
10. Do step 4 for all other blocks in order but each block has different key.
11. Combined all blocks in order then send the 64-bits cipher text to receiver side

Key generation process as illustrated as shown below:

1. Read the plain text as a key (16-bits)
2. Split the key (16-bits) into two bytes as left and right.
3. Use the logical shift to the right for the first two bits in the left portion of the key.
4. Use the logical shift to the right for the first two bits in the right portion of the key.
5. Concatenate the new result after the logical shift from step 3 and 4.
6. Use the (16-bit key) round 1 for the key1 shown in Fig 3.

Repeat all steps before for all the keys (4- Rounds).

To clarify in further the watermark embedding in the first phase, the watermark embedding procedure consists of the following operational steps as illustrated as shown below:

Step 1: Arrange the watermark image into b strings each of n bits length.
Step 2: Make a logical division of the dataset into sub-sets of blocks. A sub-set has m blocks.
Step 3: Embed the n-bit binary string in the corresponding m block of a sub-set as follows:

- Find the decimal equivalent of the string. Let the decimal equivalent d.
- The decimal number d must be embedded into a pre selected block.

Step 4: Repeat step 3 for each block in the dataset.

4. EXPERIMENTAL RESULTS

For our experiment, we used a laptop IV 1.5 GHz CPU, in which performance data is collected.

As hardware for the different experiments a personal computer with a CPU speed of 1.5GHz was used.

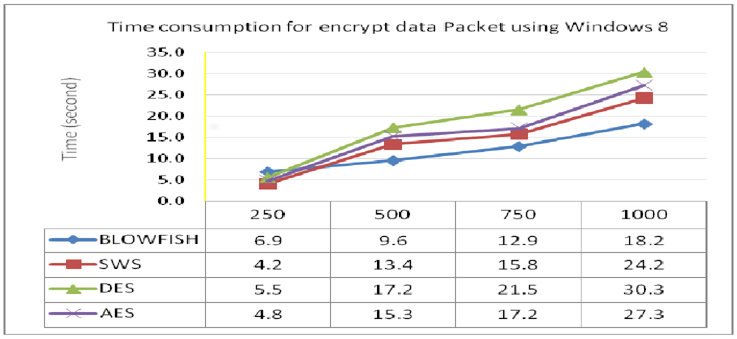
The following criteria that will be achieved are shown as follows:

- ❖ The different selected algorithms were compared with each, to see the time and power consumption of each when encrypting or decrypting data.
- ❖ A research is performed on the effect of changing packet size on CPU time for each selected cryptography algorithm.

In the experiments, the laptop encrypts a different the size ranges from 250 MB to 1GB for text data only and compared with different platforms such as Windows XP, Windows 8 and Linux in term of time and power consumption. Several performance metrics are collected as below:

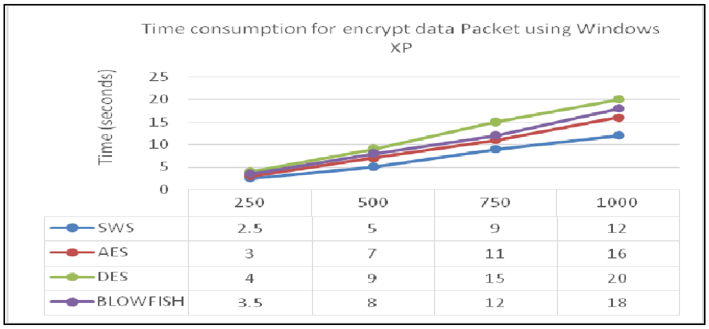
4.1 Time Consumption

Figure 1, Figure 2 and Figure 3 show the four encryption algorithms namely the Blow Fish, The AES-128, the DES and SWS algorithms. They are showing the time consumption of each compared algorithm in seconds when varying the size of data samples. The data sizes are 250MB, 500MB, 750MB and 1000MB. Different operating systems where used when applying these algorithms such as Windows 8, Windows XP and Linus OS.



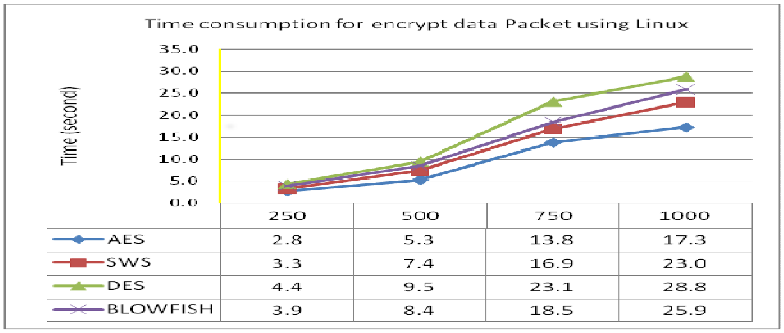
	250	500	750	1000
BLOWFISH	6.9	9.6	12.9	18.2
SWS	4.2	13.4	15.8	24.2
DES	5.5	17.2	21.5	30.3
AES	4.8	15.3	17.2	27.3

Figure 1. Time consumption results of the comparison on OS Windows 8 for encryption of different sizes of data Packet.



	250	500	750	1000
SWS	2.5	5	9	12
AES	3	7	11	16
DES	4	9	15	20
BLOWFISH	3.5	8	12	18

Figure 2. Time consumption results of the comparison on OS Windows XP for encryption of different sizes of data Packet.

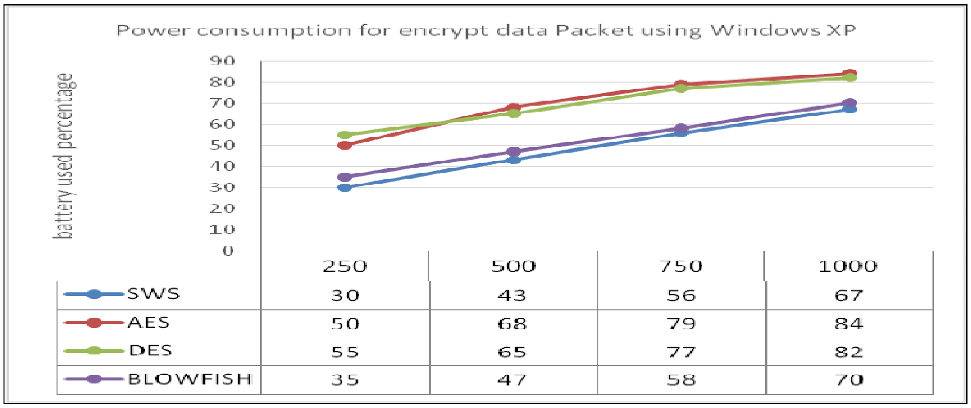


	250	500	750	1000
AES	2.8	5.3	13.8	17.3
SWS	3.3	7.4	16.9	23.0
DES	4.4	9.5	23.1	28.8
BLOWFISH	3.9	8.4	18.5	25.9

Figure3. Time consumption results of the comparison on OS Linux for encryption of different sizes of data Packet.

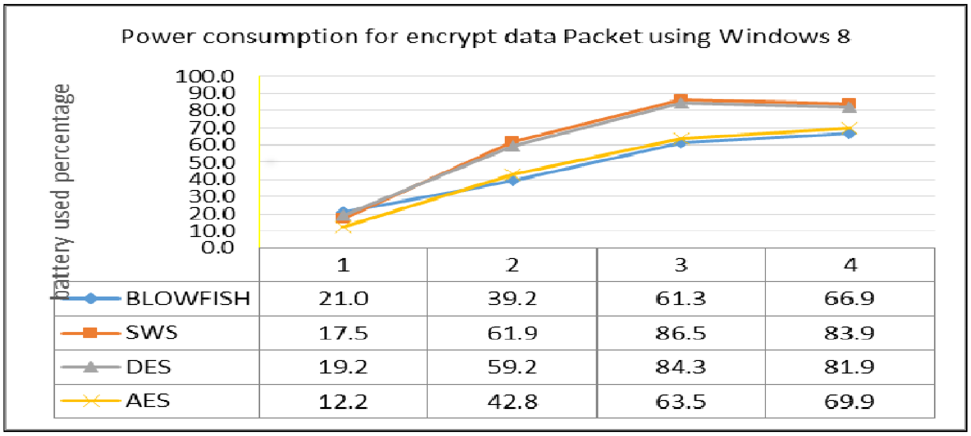
4.2 The results of the power Consumption

Figure 4, Figure 5 and Figure 6 show the power consumption of each encryption algorithms when varying the data size.



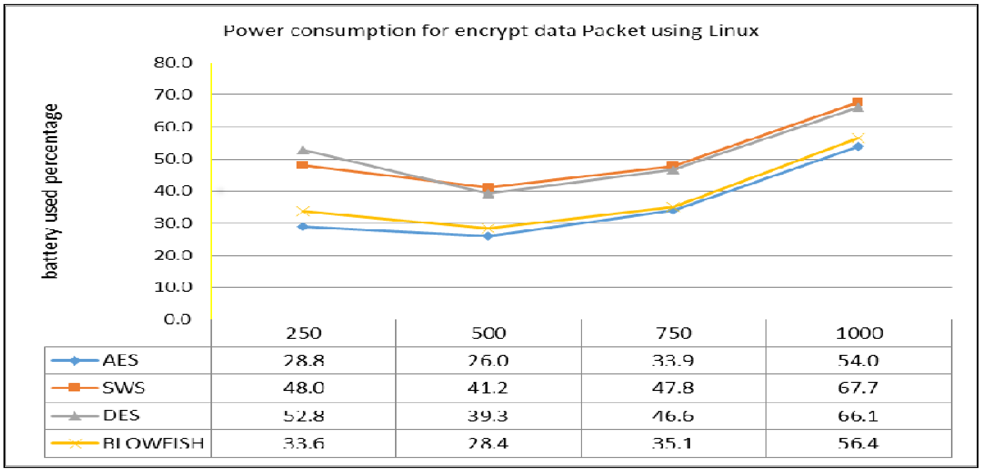
	250	500	750	1000
SWS	30	43	56	67
AES	50	68	79	84
DES	55	65	77	82
BLOWFISH	35	47	58	70

Figure 4. Power consumption for encrypt different data Packet size using windows XP



	1	2	3	4
BLOWFISH	21.0	39.2	61.3	66.9
SWS	17.5	61.9	86.5	83.9
DES	19.2	59.2	84.3	81.9
AES	12.2	42.8	63.5	69.9

Figure 5. Power consumption for encrypt different data Packet size using windows 8



	250	500	750	1000
AES	28.8	26.0	33.9	54.0
SWS	48.0	41.2	47.8	67.7
DES	52.8	39.3	46.6	66.1
BLOWFISH	33.6	28.4	35.1	56.4

Figure 6. Power consumption for encrypt different data Packet size using Linux

5. CONCLUSION AND FUTURE WORK

This paper presents a performance comparison of selected common encryption algorithms. The selected algorithms are AES, DES, Blowfish and Secure Watermark System (SWS).

Many conclusions can be done when analyzing the results of the experiments of this study. First; when varying the size of data packets, it can be shown that the SWS and the Blowfish algorithms have the best time consumption performance than the other compared algorithms.

Secondly; when varying the size of data, it can be shown that the DES algorithm have worst power consumption performance than the other compared algorithms.

Also, we find that DES still has low performance compared to algorithms used.

Finally; when varying the type of operating system used, it shows that the SWS has better time consumption under the Windows XP operating system than the other compared operating systems.
And we found (blowfish) result in time consumption in windows 8 is better than other operating system (Linux and Windows XP). And we found (AES) result in time consumption in LINUX is better than other operating system (Windows XP and Windows 8) and we conclude that the same result in the term of power consumption.

In our future work we will apply the same methodology on images and audio data, and we will work on a new methodology to make a reduction on the energy/power consumption of the security algorithms and to apply it on Wireless LANs to provide an energy efficient mechanism for the 802.11 WLAN protocol. We will try to replace all the primitives of the security algorithms with high energy consumptions with lower energy consumptions while keeping the security level of each.

REFERENCES

[1] S. Masadeh W.Salameh(2007). "End to end keyless self-encrypting/decrypting streaming cipher", Information Technology & National Security Conference 2007.

[2] A. Nadeem MYJ (2005)."A performance comparison of data encryption algorithms", First International Conference on Information and Communication Technologies, pp 84- 89.

[3] Hardjono(2005),"Security in wireless lans and wans", Artech House Publishers.

[4] N. Ruangch ,aijatupon and P. Krishnamurthy(2001),"Encryption and power consumption in wireless LANs-N",The Third IEEE Workshop on Wireless LANs, pp. 148-152.

[5] Schneier, Bruce (2012)."The Blowfish Encryption Algorithm". Blowfish, <http://www.schneier.com/blowfish.html>.

[6] W. Stallings (2005),"Cryptography and Network Security", 4th Ed, pp. 58-309, Prentice Hall.

[7] Penchalaiah, N. and Seshadri, R. ffective (2010),"Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No.05.

[8] J. Daemen and V. Rijmen (2002),"The Design of Rijndael", Springer-Verlag.

[9] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M.Stay, D. Wagner, and D. Whiting(2000), Improved crypt-analysis of Rijndael,Seventh Fast Software Encryption Workshop, pp. 19, Springer-Verlag .

[10] K. Naik and D. S. L. Wei (2001),"Software implementation strategies for power-conscious systems, Mobile Networks and Applications", vol. 6, pp. 291-305.

[11] Singhal, Nidhi and Raina, J P S (2011)."Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[12] Singh, S Preet and Maini, Raman (2011)."Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, vol. 2, No. 1, pp. 125-127.

[13] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, T .Kohno (2003)."Helix fast encryption and authentication in a single cryptographic primitive", Fast Software Encryption, volume 2887 of LNCS. Springer-Verlag: 330-346.

[14] S. Hirani, Energy Consumption of Encryption Schemes in Wireless Devices Thesis(2008), University of Pittsburgh.

[15] A. Nadeem and M. Y. Javed,A performance comparison of data encryption algorithms(2005), Information and Communication Technologies, ICICT 2005, pp.84-89.

[16] Results of Comparing Tens of Encryption Algorithms Using Different Settings (2008), Crypto++ Benchmark. (http://www.eskimo.com/weidai/benchmarks.html)

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

[18] D. Salama, A. Elminaam and etal (2010),"Evaluating the Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.216–222.

[19] DES Overview, http://www.tropsoft.com/strongenc/des.htm [Explains how DES works in details, features and weaknesses].

[20] [Bruce1996] BRUCE SCHNEIER, Applied Cryptography, John Wiley & Sons, Inc. 1996.

[21] Crypto++ benchmark http://www.eskimo.com/~weidai/benchmarks.html.

[22] [Blowfish.NET] Coder's Lagoon, http://www.hotpixel.net/software.html

[23] http://en.wikipedia.org/wiki/Triple_DES.

[24] http://searchsecurity.techtarget.com/tip/Expertadvice-Encryption-101-Triple-DES-explained.

[25] Aamer Nadeem et al (2005),"A Performance Comparison of Data Encryption Algorithms", IEEE.

Authors

Ashraf Odeh was born in 24th February 1974 in Amman –Jordan he received a BSc degree in Computer Science in 1995 at Princess Summay University in Amman-Jordan and MSc degree in Information Technology in 2003 at Al-Nileen University in Sudan with a Thesis titled " Visual Database administrator Techniques " After that, he received PhD from department of Computer Information System in 2009 at Arab Academy in Amman-Jordan with a Thesis titled " Robust Watermarking of Relational Database Systems ". He interested in image processing, Watermarking, Relational Database, E-copyright protection, E-learning and Security Issues, Encryption and Decryption Systems. Dr. Odeh Currently, working at Al-ISRA University in Computer Information System Department as assistant Prof. and submitted a number of conference papers and journals.

Shadi R. Masadeh was born in 21th March 1977 in Amman –Jordan he received a BSc degree in Computer Science and Computer Information System in 2000 at Philadelphia University in Amman-Jordan and MSc degree in Information Technology in 2003 After that, he received PhD from department of Computer Information System in 2009 at Arab Academy in Amman-Jordan .He interests in many areas of research such as E-learning Management and Security Issues, Encryption and Decryption Systems, Networking and Wireless security. Dr. Masadeh Currently, working at Al-ISRA University in Computer Networks Department as assistant Prof. and submitted a number of conference papers and journals.

Ahmad Azzazi is an assistant professor in the Faculty of Information Technology at the Applied Science University. Dr. Azzazi’s research interests include Software security engineering, software engineering frameworks, natural language processing, security expert systems.