IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.274

A Comparative Study of Symmetric Key Encryption Algorithms

[1] Amit Jain, [2] Divya Bhatnagar

[1] Computer Science and Engineering Department, Sir Padmapat Singhania University
Udaipur, Rajasthan 323601, India

[2] Computer Science and Engineering Department, Sir Padmapat Singhania University
Udaipur, Rajasthan 323601, India

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 five of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2 and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, battery power consumption, different key size and finally encryption/decryption speed.

Keywords - *Encryption Techniques, Computer Security, AES, DES, RC2, 3DES, RC6.*

1. Introduction

Information security plays a pivotal role nowadays. The requirement of information security is increasing because of widespread use of distributed systems, network and communication facilities for carrying information between terminal user and computer system and from one computer to another computer [1]. Hence to provide confidentiality authentication, integrity and non-repudiation, information security has proposed.

Large number of algorithms and techniques are designed for secure transmission of data. Cryptographic algorithms play a key role in information security systems. There are two general types of key-based algorithms: Symmetric and Asymmetric algorithms. Symmetric algorithm(also called secret-key algorithms) are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption and decryption key are the same. Both the sender and receiver agree on a key before they can communicate securely. 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 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 while RC6 is used various (128,192,256) bits keys [1-5]. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Asymmetric algorithm (also called public-key algorithms), two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. The decryption key (private key) cannot be calculated from the encryption key (public key). So, keys play an important role in the security of any cryptographic algorithm. If weak key is used in algorithm, then any intruder may decrypt the data.

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

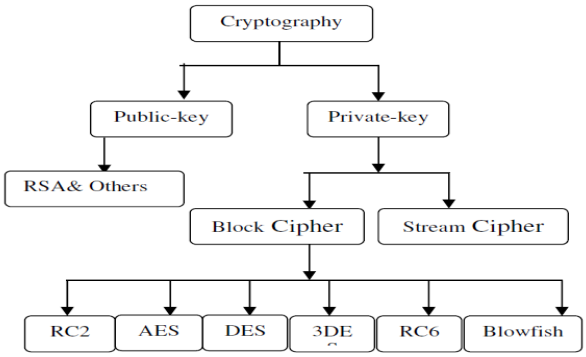

Fig. 1 Overview of the field of cryptography

Brief definitions of the most common symmetric key 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 to 128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [3].

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].

Table 1 : Summary of some symmetric block cipher algorithms

S. No.	Algorithm	Block Size	Key Length
1.	DES	64 bits	56 bits
2.	3DES	64 bits	168, 112, 56 bits
3.	RC2	64 bits	8- 128 bits (variable length key)
4.	AES	128 bits	128, 192, 256 bits
5.	RC6	128 bits	128, 192, 256 bits

This paper examines a method for evaluating performance of various symmetric key encryption 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 five different encryption algorithms namely; AES, DES, 3DES, RC6 and RC2. The performance measure of encryption schemes will be conducted in terms of energy, encryption and decryption time, changing packet size and changing key size for the selected cryptographic algorithms.

This paper is organized as follows. Related work is described in Section II. A view of simulation and experimental design is given in section III. Simulation results are shown in section IV. Finally the conclusions are drawn section V.

2. Related Work

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

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

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

A study in [12] is conducted for different popular secret key algorithms such as DES, 3DES, AES and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They

had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [13].

In [14] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser.

3. Experimental Design

For our experiment, we use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 49 K byte to 7310 K Byte. Several performance metrics are collected: encryption time, CPU process time, and CPU clock cycles and battery power. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [15]. The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy.

The following tasks that will be performed are shown as follows:
- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time and decryption time.

- 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 key size for cryptography selected algorithm on power consumption.

4. Simulation Results

4.1 Differentiate Output Results of Encryption & Decryption

Simulation results are given in Fig. 2 and Fig. 3 for the selected five encryption algorithms for different size of document. Fig. 2 shows the results of encryption while Fig. 3 gives the results of decryption. We can notice that there is no significant difference in both encryption and decryption time. In both encryption and decryption, the time required by RC2 is higher than all other methods and time required by RC6 is lower than all other methods.

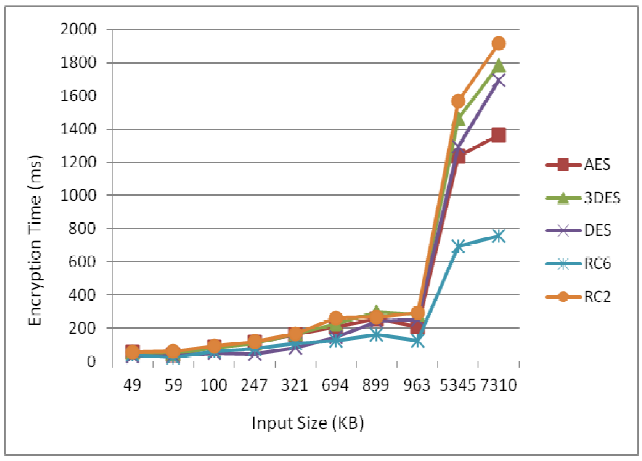

Fig. 2 Time consumption of encryption algorithm

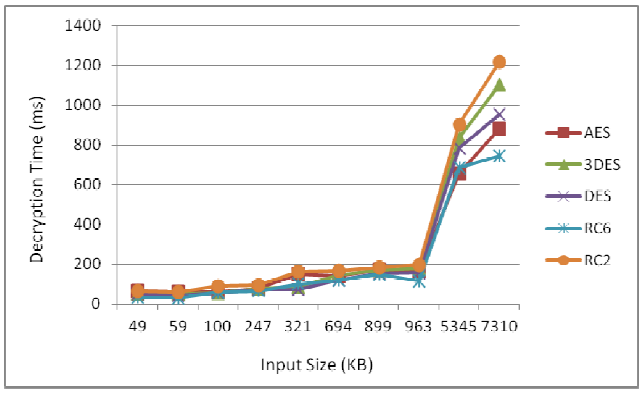

Fig. 3 Time consumption of decryption algorithm

4.2 The Effect of Changing Packet Size for Cryptography Algorithm on Power Consumption.

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by

dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. The formula used for calculating average data rate is:

$$AvgTime = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{Mi}{Ti}Kb/s$$

Where

AvgTime = Average Data Rate (Kb/s)
Nb = Number of Message
Mi = Message Size (Kb)
Ti = Time taken to Encrypt Message Mi

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 using the following formula:

$$ThroughPut = \frac{Tp}{Et}$$

Where

Tp = Total plain text
Et = Encryption Time

It is very important to calculate the throughput time for the encryption algorithm to know better performance of algorithm. Simulation results for this comparison are shown Fig. 4 and Table 2 at encryption stage.

Table 2 : Comparative execution times (in ms) of encryption algorithm with different packet size

Input Size (in KB)	AES	3DES	DES	RC6	RC2
49	56	54	29	41	57
59	38	48	33	24	60
100	90	81	49	60	91
247	112	111	47	77	121
321	164	167	82	109	168
694	210	226	144	123	262
899	258	299	240	162	268
963	208	283	250	125	295
5345	1237	1466	1296	695	1570
7310	1366	1786	1695	756	1915
Avg Time	374	452	389	217	480.7
Throughput (MB/S)	4.174	3.45	4.01	7.19	3.247

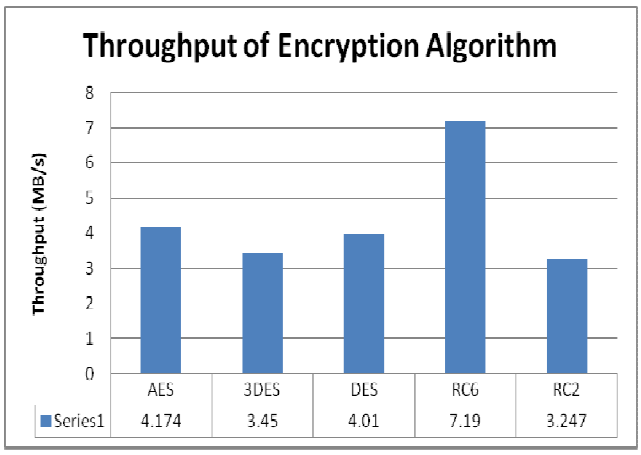

Fig. 4 Throughput of each encryption algorithm

The results show the superiority of RC6 algorithm over other algorithms in terms of the processing time. A Second point can be noticed here; that RC6 requires less time than all algorithms. A third point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. A fourth point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other four algorithms in spite of the small key size used.

Table 3: Comparative execution times (in ms) of decryption algorithm with different packet size

Input Size (in KB)	AES	3DES	DES	RC6	RC2
49	63	53	50	35	65
59	58	51	42	28	59
100	60	57	57	58	90
247	76	77	72	66	95
321	149	87	74	100	161
694	142	147	120	119	165
899	171	171	152	150	183
963	164	177	157	116	194
5345	655	835	783	684	904
7310	882	1101	953	745	1216
Avg Time	242	275.6	246	210	313.2
Throughput(MB/S)	6.452	5.665	6.347	7.43	4.985

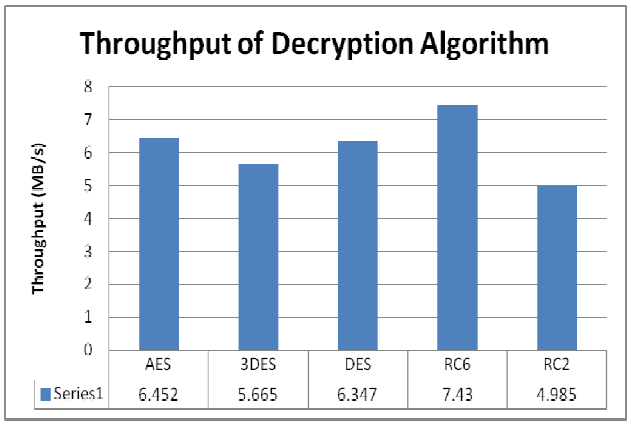

Fig. 5 Throughput of each decryption algorithm

Simulation results for this comparison are shown Fig. 5 and Table III decryption stage. We can find in decryption that RC6 is the better than other algorithms in throughput and power consumption. The second point should be notice here that RC6 requires less time than all algorithms. A third point that can be noticed that AES has an advantage over other 3DES, DES and 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 Key Size of AES on Power Consumption.

The last performance comparison point is the changing different key sizes for AES and RC6 algorithm. In case of AES, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. The simulation results are shown in Fig. 6 and Fig. 7.

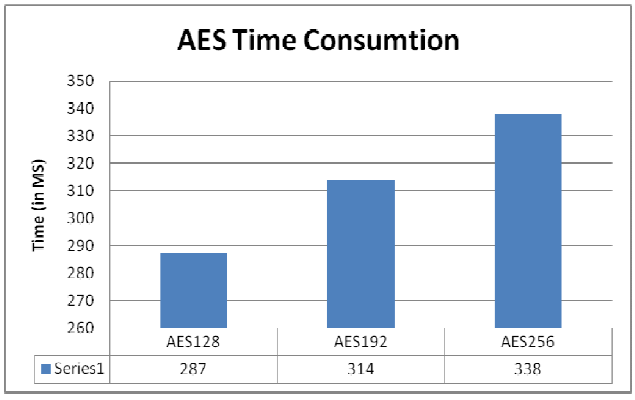

Fig. 6 Time consumption for different key size for AES

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.

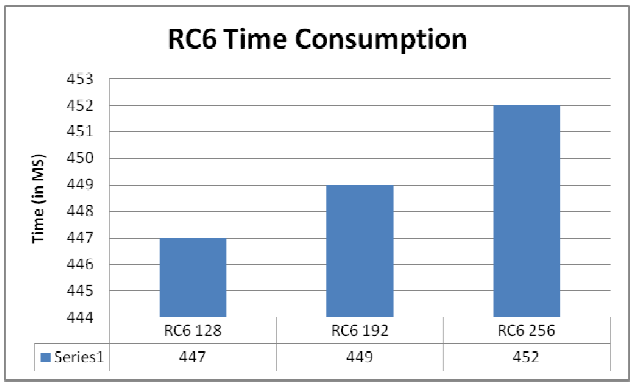

Fig. 7 Time consumption for different key size for RC6

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

5. Conclusions

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6 and RC2. Several points can be concluded from the simulation results. First; there is no significant difference when the results are displayed for encryption or decryption. Secondly; in the case of changing packet size, it was concluded that RC6 has better performance than other common encryption algorithms used. Third; 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. Also, we find that 3DES still has low performance compared to algorithm DES.

References

[1] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N'', The 3rd 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", IBM Journal

of Research and Development, May 1994, PP 243 - 250.

[5] Bruce Schneier, "The Blowfish Encryption Algorithm".

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

[7] Daemen, J. and Rijmen, V., "Rijndael: The Advanced Encryption Standard", Dr. 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.

[12] "A Performance Comparison of Data Encryption Algorithms", IEEE First International Conference, ICICT 2005, PP. 84- 89.

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

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

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

[16] Sinha, A.P. Chandrakasan, JouleTrack, "A Web Based Tool for Software Energy Profiling" proceedings of the 38th Design, NV, Las Vegas, US P.P. 220-225

Amit Jain is working as Assistant Professor in CSE Department at Sir Padampat Singhaniya University, Udaipur. He obtained M.Tech. Degree in Computer Science. His area of Research is "Information Security". He has published 4 papers in International Conference and 10 papers in national conference. At present he is pursuing Ph.D. in Computer Science from Sir Padampat Singhania University, Udaipur.

Divya Bhatnagar is presently working as Assistant Professor in the department of Computer Sc. & Engg. at Sir Padampat Singhania University, Udaipur, India. She was born in Gwalior, Madhya Pradesh, India. After completing her Master Degree in 1996 she received Post Graduate Diploma in Operations Management and thereafter, Doctoral Degree in Computer Application in 2012. She has a teaching and administration experience of 17 years in the field of Computer Science and Engineering, Computer Applications, IT, Management, and related fields. She has about 30 research publications in National, International Journals and Conferences. The major research areas of interest are data mining, neural network and privacy preserving data mining.