Volume 2, No. 7, July 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

ANALYZING THE SUPERLATIVE SYMMETRIC CRYPTOGRAPHIC ENCRYPTION ALGORITHM (ASCEA)

Srinivasarao D[*1],Sushma Rani N[2], Ch.Panchamukesh[3] and S.Neelima[4]

[1] Department of Computer Science, HITS, Hyderabad, India.
[2] Department of Computer Science, MVGR, Vizianagaram, India.
[3]Department of Computer Science, HITAM, Hyderabad, India.
panchamukesh.yadav@gmail.com
[4]Department of Computer Science, Pydha College, Kakinada, India.

Abstract: Cryptology is a science that deals with codes and passwords. Cryptology is alienated into cryptography and cryptanalysis. The Cryptography produces methods to protect the data, and cryptanalysis hack the protected data. Cryptography provide solutions for four different security areas - confidentiality, authentication, integrity and control of interaction between different parties involved in data exchange finally which leads to the security of information .Encryption algorithms play a key role in information security systems. This paper provides critical analysis of six most common encryption algorithms namely: DES, 3DES, RC2, Blowfish, AES (Rijndael), and RC6. A comparative study has been carried out for the above six encryption algorithms in terms of encryption key size ,block size, Number of Rounds ,Encryption/decryption time ,CPU process time, CPU clock cycles (in the form of throughput), Power consumption. And these comparisons are used to conclude the best Symmetric Cryptography Encryption algorithm.

Keywords: Cryptography, Encryption Algorithm, Symmetric keys, Performance, Analysis, DES, 3DES, AES, Blowfish, RC2 and RC6.

INTRODUCTION

Now a day's sensitive information is stored on computers and transmitted over the Internet, and there is need to ensure information security and safety. Hence, encryption is mainly used to ensure secrecy. Encryption is the process of conversion of data into a form, called a cipher text and so preventing any unauthorized recipient from retrieving the original data. Many encryption algorithms are extensively available and used in information security. They can be categorized into Symmetric or private key and Asymmetric or public key encryption. In Symmetric 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 key used.

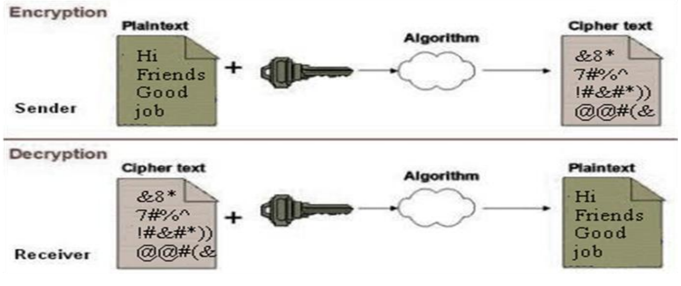

Figure. 1 Encryption and decryption process

Asymmetric key encryption is used in resolve the problem of key distribution. In Asymmetric key encryption, two keys are used they are public and private keys. Public key is used for encryption and private key is used for decryption of data .Where public key, which is known to the every one and private key which is known only to the user, so there is no need for distributing them earlier to transmission.

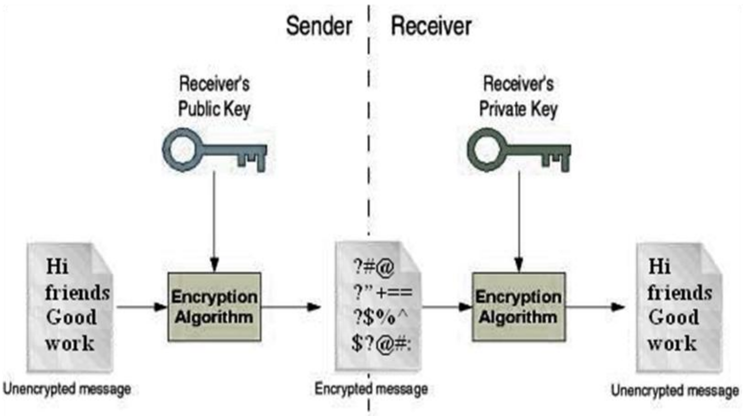

Figure. 2 Roles of Public and Private Keys in Encryption

Considering the computational processing power, Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques .

BACKGROUND

The most commonly used Symmetric Encryption Techniques are discussed below.

A. *DES Technique*

Data Encryption Standard (DES), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).The Data Encryption Standard

(DES) was developed and authorized by the U.S. government in 1977 as an official.. It is based on the IBM proposed algorithm called Lucifer.

B. 3DES Technique

(Triple Data Encryption Standard), is a variation of DES. In this model 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.

C. AES Technique

Advanced Encryption Standard is a winning algorithm, Rijndael, which was developed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen. AES provides strong encryption and was selected by NIST as a Federal Information Processing Standard in November 2001 (FIPS-197) which can be used to protect electronic data.

D. Blowfish Technique

Can be used as a replacement for the DES algorithm, and was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms .Blowfish has a Feistel Network, iterating a simple encryption function 16 times. Though there is a complex initialization segment required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors Blowfish is unpatented, license-free, and is available free for all uses. Blowfish is successor to Twofish.

E. RC2 Technique

Is a variable-key-length cipher, Designed by Ronald Rivest in 1987 for RSA Data Security, Inc. "RC" stands for "Rivest Cipher", alternatively, "Ron's Code".

F. RC6 Technique

Is block cipher consequent from RC5. It was designed to meet the necessities of the Advanced Encryption Standard. It was designed by four analysts named Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin.

RELATED WORK

To asses the best symmetric algorithm, this section discusses the results obtained from other resources like Encryption/decryption time, CPU processing time and Battery consumption.

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 algorithms.

IMPLEMENTATION AND EXPERIMENTAL DESIGN

Table [1] contains the speed benchmarks for some of the most commonly used symmetric cryptographic algorithms. All were coded in C++, compiled with Microsoft Visual C++ .NET 2003 (whole program optimization, optimize for speed, P4 code generation), and ran on a Pentium IV of 2.4 GHz CPU Speed.

Table [1] Algorithms Key and Block Sizes in Bits

Algorithm	**Key Size (Bits)**	**Block Size (Bits)**
DES	**64**	**64**
3DES	**168**	**64**
Rijndael	**128,192 or 256**	**128**
Blowfish	**From 8 to 448**	**64**
Rc2	**64**	**64**
Rc6	**128,192 or 256**	**128**

Longer key lengths mean more effort must be put forward to break the encrypted data security. So, here Blowfish has the longer key size as compared to other algorithms. Since the evaluation test is meant to evaluate the results when using block cipher, due to the memory constraints on the test machine (1 GB) the test will break the load data blocks into smaller sizes .The load data are divided into the data blocks and they are created using the Random Number Generator class available in System.

Table [2] Algorithms Number Of Rounds

Algorithm	Number Of Rounds
DES	16
3DES	48
Rijndael	18
Blowfish	16
Rc2	18
Rc6	16

This section we discusses the result obtained from added resources, to give more potential about the performance of the all the above described algorithms. To asses all the algorithms in this paper, the performance data is collected using a laptop with Pentium IV of 2.4 GHz CPU Speed, by which we encrypt a different range of file size from 49 K byte to 7.310Mega Byte which were displayed in Table[3] A number of performance metrics are calculated based on the following :

(a) Encryption/decryption time.
(b) CPU process time – in the form of throughput
(c) CPU clock cycles and battery power.

The Encryption time is the time taken by an Encryption algorithm to generate a cipher text from a given plaintext. Encryption time is used to calculate the throughput of an encryption method which indicates the speed of encryption.

$$\text{Throughput} = \frac{\underline{\text{Total Plain Text in Bytes}}}{\text{Encryption time}}$$

Table [3.a] Algorithms Throughput (Mbytes/Sec)

Input size in (Kbytes)	DES		3DES		Rijndael	
	ENC	DEC	ENC	DEC	ENC	DEC
49	29	50	54	53	56	63
59	33	42	48	51	38	58

100	49	57	81	57	90	60
247	47	72	111	77	112	76
321	82	74	167	87	164	149
694	144	120	226	147	210	142
899	240	152	299	171	258	171
963	250	157	283	177	208	164
5345.28	1296	783	1466	835	1237	655
7310.336	1695	953	1786	1101	1366	882
Average Time	389	246	452	275.6	374	242
Throughput (Mbytes/sec)	4.01	6.35	3.45	5.67	4.174	6.45

Table [3.b] Algorithms Throughput (Mbytes/Sec)

Input size in (Kbytes)	**Blowfish**		**Rc2**		**Rc6**	
	ENC	DEC	ENC	DEC	ENC	DEC
49	36	38	57	65	41	35
59	36	26	60	59	24	28
100	37	52	91	90	60	58
247	45	66	121	95	77	66
321	45	92	168	161	109	100
694	46	89	262	165	123	119
899	64	102	268	183	162	150
963	66	80	295	194	125	116
5345.28	122	149	1570	904	695	684
7310.336	107	140	1915	1216	756	745
Average Time	60.3	83.4	480.7	313.2	217	210
Throughput (Mbytes/sec)	25.89	18.72	3.25	4.985	7.19	7.43

RESULTS

As the throughput value is increased, the power consumption of this encryption technique is decreased. Simulation results for the above obtained point for both encryption and decryption are shown below in the form of both encryption and decryption using throughput.

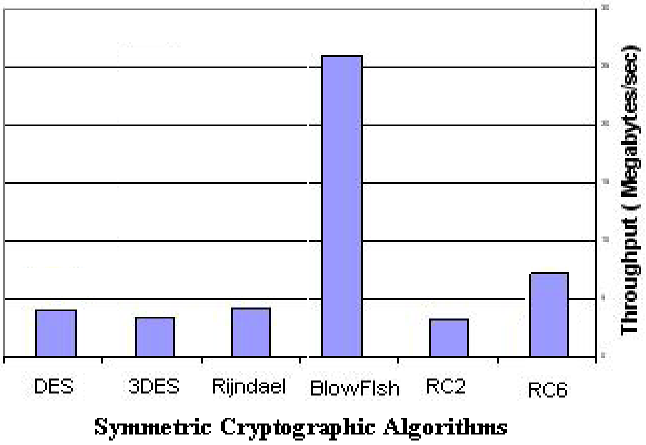

Figure.3 throughput and the processing time for encrypting a file

The results show the supremacy of Blowfish algorithm over other algorithms in terms of throughput and the processing time for encrypting a file. As compared to other algorithms RC6 requires less time except Blowfish and next AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. And 3DES has low performance in terms of processing time and throughput when compared with DES because of its triple phase encryption characteristics. Lastly, RC2 has low performance and low throughput when compared with other five algorithms because of its small key size.

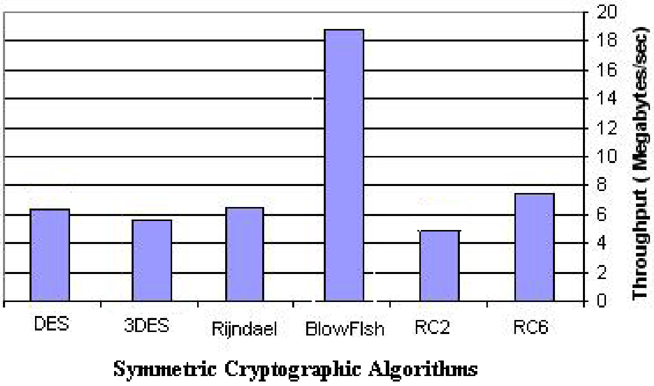

Figure.4 throughput and the processing time for decrypting a file

Again the results show the supremacy of Blowfish algorithm over other algorithms in terms of throughput and the processing time for decrypting a file. RC6 requires less time than all algorithms except Blowfish. AES has an advantage over other 3DES, DES RC2 in terms of throughput and processing time for decrypting a file. Triple DES (3DES) still requires more time than DES. And finally RC2 still has low performance of all the algorithm for decrypting a file.

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 utilization of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy. The following tasks are made to asses the performance of algorithms:

1. Two different encoding bases namely, hexadecimal base encoding and base 64 encoding are used to made a comparison between the results of different encryption and decryption algorithms in terms of Encryption Time.

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

A. Distinguish output results of encryption (Base 64, Hexadecimal)

Simulation results are given in Fig 5 and Fig 6 for the selected six encryption algorithms at base 64 encoding and hexadecimal base encoding. From the obtained results we can observe that there is no major difference in both encoding methods. The same files are encrypted by two methods, we can identify that the two curves almost display the same results.

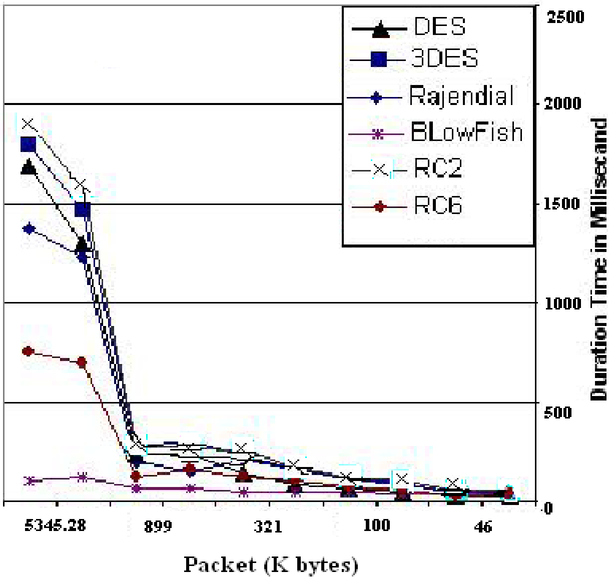

Figure5. Processing time of encryption algorithm (base 64 encoding)

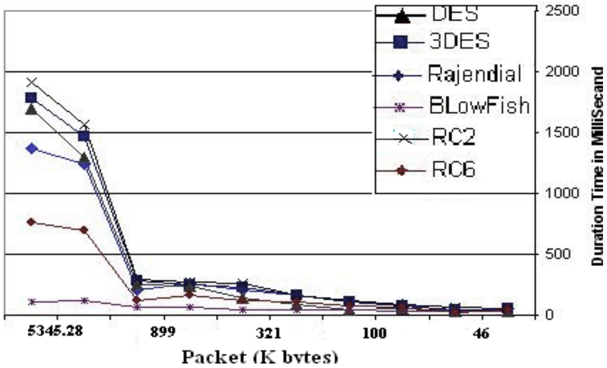

Figure 6. Processing time of encryption algorithm (Hexadecimal encoding)

B .Power consumption (Micro joule/byte)

In Fig 7, with a different data block size (Micro joule/byte) ,we show the performance of cryptographic algorithms in terms of Power consumption .

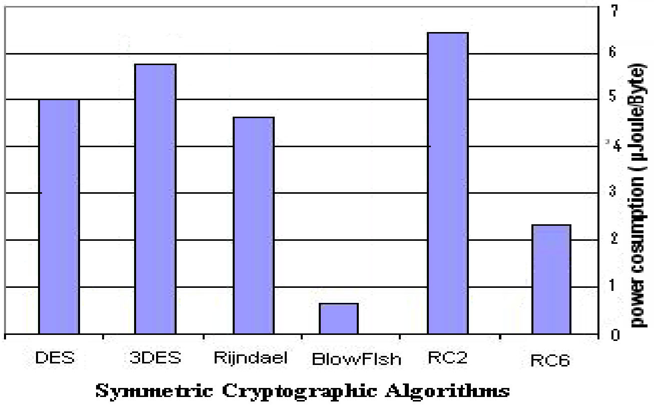

Figure 7. Power consumption for encrypt different Text document Files (micro Joule/Byte)

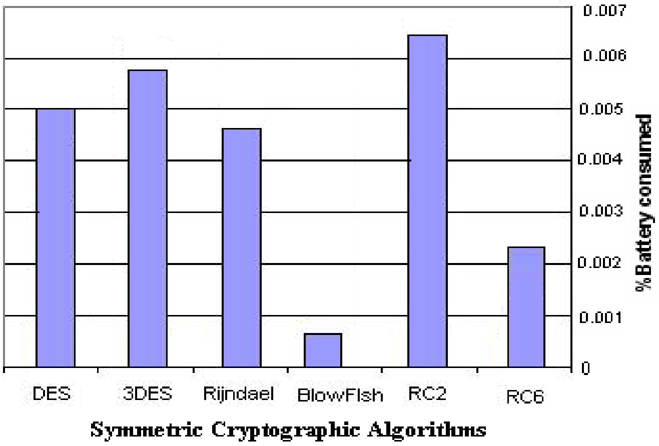

Figure 8. Power consumption for encrypt different Text document Files (in % Battery consumed)

All The above results shows the superiority of Blowfish algorithm on algorithms in terms of the throughput, processing time and power consumption (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) as in Fig 8 . 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.

CONCLUSIONS

This paper Analyzing the superlative symmetric cryptographic encryption algorithm .The selected algorithms are DES, 3DES, Rinjdal, Blowfish, RC2 and RC6. From the Experiment many points are concluded. First; in the case of using the key the Blowfish has the best use where the code is unbreakable it was concluded that Blowfish has best practice to avoid data misuse, followed by AES and RC6. Secondly; in the case of changing Encryption/Decryption Time again the Blowfish has the best performance which proves it has the best CPU Clock Cycles in the form of Throughput, so it was found that Blowfish has advantage 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 data files we found that Blowfish is again has a good performance as considered to other algorithms followed by 3DES and Rinjdal.

REFERENCES

[1] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.

[2] “DES Encryption.pdf” from http://www.tropsoft.

com/strongenc/des.htm.

[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 Algorithm Retrieved 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] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.

[10] 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.

[11] Limor Elbaz & Hagai Bar-El " Strength Assessment Of Encryption Algorithms.doc" from www.discretix.com.

[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/be nchmarks.html

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