Volume 3, No. 8, August 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

PERFORMANCE EVALUATION OF SYMMETRIC ALGORITHMS

S. Pavithra[*1] and Mrs. E. Ramadevi[2]

[1]Research Scholar, Department of Computer Science, NGM College, Pollachi, India.
Pavisou010@gmail.com
[2]Assistant Professor, Department of Computer Science, NGM College, Pollachi, India.
ramajus@hotmail.com

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. . In this paper, we compare the various cryptographic algorithms. On the basis of parameter taken as time various cryptographic algorithms are evaluated on different video files. Different video files are having different processing speed on which various size of file are processed. Calculation of time for encryption and decryption in different video file format such as .vob, and .DAT, having file size for audio and for video 1MB to 1100MB respectively. Encryption processing time and decryption processing time are compared between various cryptographic algorithms which come out to be not too much. Overall time depend on the corresponding file size. Throughput analysis also done.

Keywords - AES, BLOWFISH, DES, Cryptography, Decryption, Encryption, Security

INTRODUCTION

There are number of cryptographic algorithms used for encryption data and most of all fall into two generic categories – Public key system and secret key system. Symmetric key algorithm is known as secrecy key or shared key algorithm. Because in symmetric key algorithm a shared key does both the encryption and decryption. Only one key is used for doing everything, so the success of algorithm depends on two factors-secrecy of the key and its distribution. Symmeric algorithms are: Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption algorithm (IDEA), Blowfish, Advanced Encryption Standard (AES). Asymmetric key algorithm is also known as public key algorithm. In this algorithm, there are two keys public and private used for encryption and decryption. Public key is used to encrypt the message and private key is used to decrypt the message. Asymmetric algorithms are: Diffe-Hellman and RSA Public Key Encryption.

SYMMETRIC ALGORITHM

Des:

DES is a block cipher. It encrypts data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The key length is 64 bits [10]. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

DES results in a permutation among the 2^64 possible arrangement of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and right half R.

The DES [3] algorithm turns 64-bit messages block M into a 64-bit cipher block C. If each 64-bit block is encrypted individually, then the mode of encryption is called Electronic Code Book (ECB) mode. There are two other modes of DES encryption, namely Chain Block Coding (CBC) and Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation.

Aes:

AES is based on a design principle known as a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [1]. AES operates on a 4×4 column-major order matrix of bytes, termed the state. Most AES calculations are done in a special finite field.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. The number of cycles of repetition are as follows:

a. 10 cycles of repetition for 128 bit keys.
b. 12 cycles of repetition for 192 bit keys.
c. 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: SubBytes, ShiftRows, MixColumns, XorRoundkey. Decryption is the reverse process of encryption and using *inverse* functions: InvSubBytes, InvShiftRows, InvMixColumns[4].

Blowfish:

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data- encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes [8].

The data encryption occurs via a 16-round Feistel network [9] . It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

RELATED WORK

This section discusses the performance of the compared algorithms.

In this paper [6] consider the performance of encryption algorithm for text files, it uses AES, DES and RSA algorithm and is evaluated from the following parameters like Computation time, Memory usage, Output bytes.

First, the encryption time is computed. The time is taken to convert plain text to cipher text is known as encryption time. Comparing these three algorithms, RSA takes more time for computation process. The memory usage of each algorithm is considered as memory byte level. RSA takes larger memory than AES and DES. Finally, the output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

In this paper [7], the selected algorithms are AES, 3DES, Blowfish and DES. By using these algorithms the performance of encryption and decryption process of text files is calculated through the throughput parameter.

Encryption time is calculated as the total plaintext in bytes encrypted divided by the encryption time. Decryption time is calculated as the total plaintext in bytes decrypted divided by the decryption time.

As a result mentioned in the paper [7], it is said that Blowfish algorithm gives the better performance than all other algorithms in terms of throughput. The least efficient algorithm is 3DES.

In this paper [9], discuss the performance evaluation of AES and BLOWFISH algorithms, and the parameters are Time consumption of packet size for 64 bit encodings and hexadecimal encodings, encryption performance of text files and images are compared with these two algorithms and calculate the throughput level,
Throughput of encryption = Tp/Et
where
Tp: total plain text (bytes)
Et: encryption time (second)

The simulation results shows that Blowfish has better performance than AES in almost all the test cases.

EXPERIMENTAL RESULTS

In this section, the AES, DES and Blowfish algorithms can be implemented to different audio and video files. Comparison of encryption and decryption time for video files has been given in the following table 1 and table 2, and it shows the Throughput of AES, DES BLOWFISH algorithm for different video files.

Table1: Throughput of Video Files Encryption

Video Files (MB)	AES (ms)	DES (ms)	BLOW FISH (ms)
701	36688	63578	38641
2.74	125	29735	109
54.1	2187	235	2234
16.9	782	1500	891
372	14703	4844	25360
157	6031	14578	6562
892	42594	83219	48813
103	4094	8266	4344
89.2	3484	7078	3687
1013.76	57828	93781	56219
Average Time	168516	306814	186860
Throughput (KB / ms)	20.6	11.3	18.6

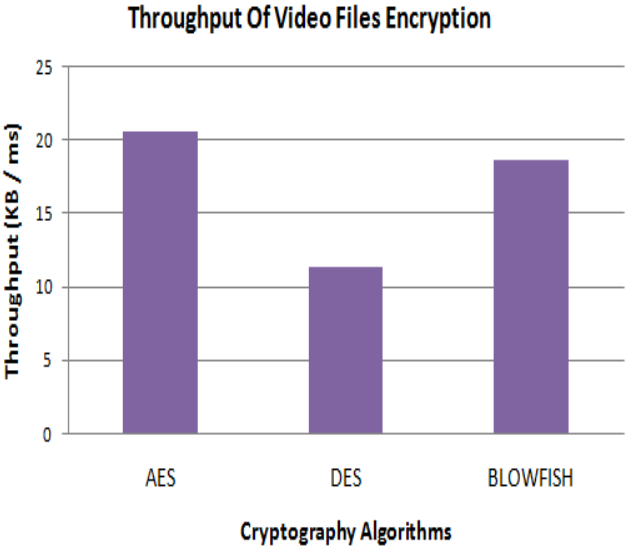

Figure 1: Throughput of Video Files Encryption

Table2: Throughput of Video Files Decryption

Video Files (MB)	AES (ms)	DES (ms)	BLOW FISH (ms)
701	32984	59406	33515
2.74	156	31890	141
54.1	2532	250	2563
16.9	828	1468	844
372	17172	4562	19718
157	7297	13297	7438
892	59859	87422	56281
103	4859	8906	4983
89.2	4156	7547	4303
1013.76	62140	99782	63594
Average Time	191983	314530	193380
Throughput (KB / ms)	18.2	11.0	18.0

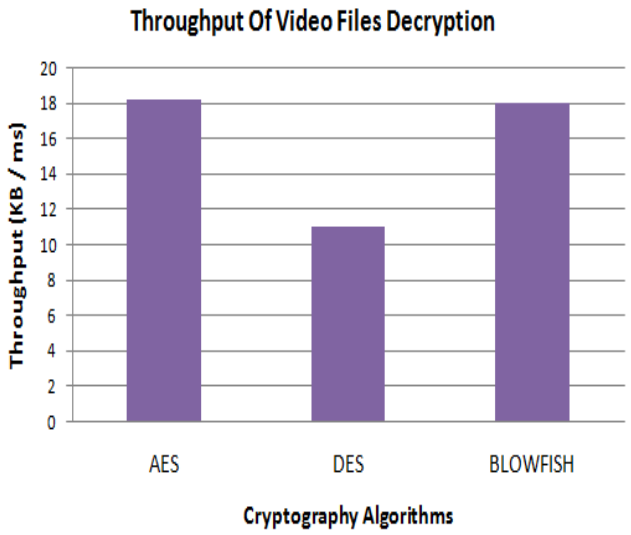

Figure2: Throughput of Video Files Decryption

The simulation results for this comparison shown in figure 3 and figure 4.The results shows the superiority of AES algorithm over the other algorithms in terms of the throughput of encryption and decryption (Video) process. Because more throughput and more speed.

CONCLUSION

In this paper presents the performance evaluation of cryptographic algorithms. AES algorithm is executed lesser processing time and more throughput level as compared to other algorithms. In future we can evaluate the performance of audio and video files for other parameters such as, memory usage and output byte.

REFERENCES

[1]. Atul Kahate, "cryptography and network security", Tata McGraw-Hill publishing company, New Delhi, 2008.

[2]. B. Schneier," Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption", Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[3]. Tingyuan Nie Teng Zhang, "A study of DES and Blowfish encryption algorithm", Tencon IEEE Conference, 2009.

[4]. William Stallings, "cryptography and network security", pearson prentice hall, 2006, 4th edition.

[5]. Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha, "Through Put Analysis of Various Encryption Algorithms", IJCST Vol.2, Issue3, September 2011.

[6]. Shashi Mehrotra Seth, Rajan Mishra, "Comparitive Analysis of Encryption Algorithms For Data Communication", IJCST Vol.2, Issue 2, June 2011

[7]. "Performance Analysis of AES and BLOWFISH Algorithms", National Conference on Computer Communication & Informatics", School of computer science, RVS college of arts and science, March 07, 2012.

[8]. "Blowfish Algorithm" Available : http://www.schneier.com/blowfish. html

[9]. "BLOWFISHalgorithm" http://pocketbrief.net/related/BlowfishEncryption.pdf

[10]. "DES algorithm" http://orlingrabbe.com/des.htm

Short Bio Data for the Author

S. Pavithra – S.Pavithra received M.Sc degree in Computer Science from Karpagam University, Coimbatore. Currently she is doing M.Phil Degree in Computer Science at Bharathiar University, Coimbatore. Her research interest lies in the area of Networking and Data Security. Published one research paper in International journal.

Mrs. E. Ramadevi - Mrs. E. Ramadevi received M.Phil degree in Computer Science from Bharathiar University, Coimbatore. Currently she is an Assistant Professor in Computer Science at NGM College, Pollachi, India. She has got 10 years of research experience and she has more than 15 years of teaching experience. Her research interest includes areas like Data Mining, Knowledge base System, Intelligent and Control Systems and Fuzzy Logic, presented various papers in National and International conferences. Published 2 research papers.