STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS

S. Pavithra
Research Scholar, Department of Computer Science,
NGM College, Pollachi, India.
Email: Pavisou010@gmail.com

Mrs. E. Ramadevi
Assistant Professor, Department of Computer Science,
NGM College, Pollachi, India.
Email: ramajus@hotmail.com

Abstract **- Today's world, for secure data transmission via Internet or any public network, there is no alternative to cryptography. The role of Cryptography is most important in the field of network security. The main goal of cryptography is Confidentiality, Integrity, Authentication, Nonrepudiation. Cryptography is widely used by governmental and intelligence agencies around the world to safe transmission of any format of messages online or offline. In this study is made for the cryptography algorithms, particularly algorithms are compared and performance is evaluated.**

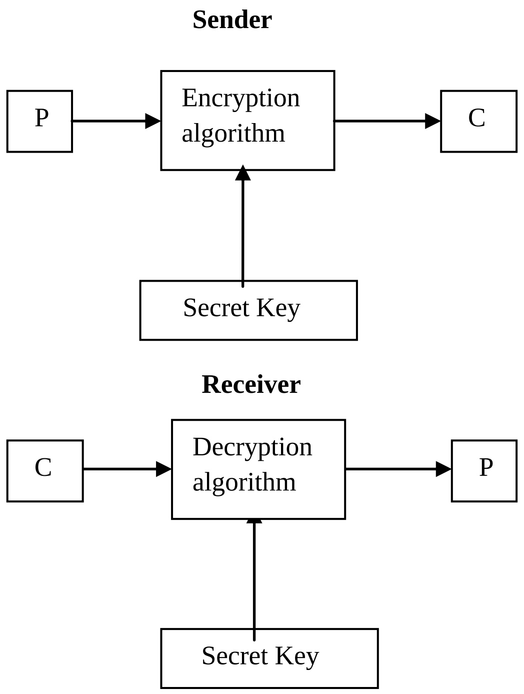
Keywords **- AES, BLOWFISH, Cryptography, Decryption, Encryption, Security**

I. 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.

II. SYMMETRIC KEY ALGORITHMS

Symmetric key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.



A. 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 [3]. 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 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.

B. 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 [2]. 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:

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 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.

C. IDEA:

IDEA is one of the strongest cryptographic algorithms. Idea is a block cipher. It works on 64-bit plain text blocks. The key is longer and consists of 128 bits. IDEA is reversible of DES.[2]

The 64-bit plaintext block is partitioned into four 16-bit sub blocks. Four 16-bit key sub-blocks are required for the subsequent output transformation, and its generated from the 128-bit key. The key sub-blocks are used for the encryption and the decryption.[10] IDEA was used in Pretty Good Privacy (PGP).

D. 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 . 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.

E. Triple DES:

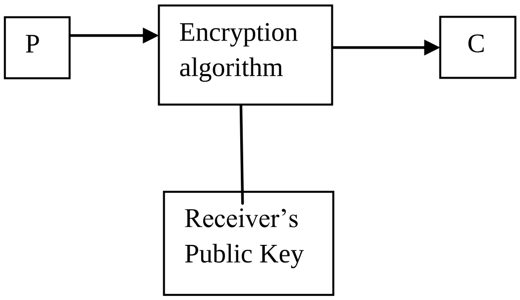
Triple DES is an alternative to DES. 3DES takes a 64-bit block of data and performs the operations encrypt, decrypt and encrypt. The key is always presented as a 64-bit block, every 8th bit of which is ignored. Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times.

we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows: [2] Encrypt with K1-> Decrypt with K2 -> Encrypt with K3 Decryption is the reverse process: Encrypt with K3-> Decrypt with K2 -> Encrypt with K1

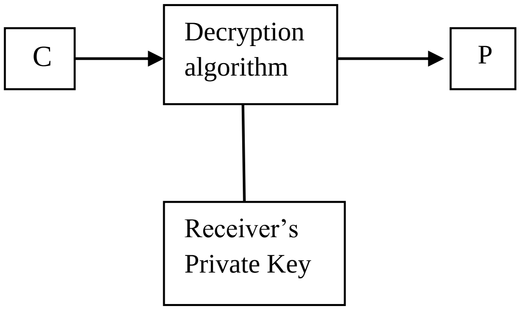
III. ASYMMETRIC KEY ALGORITHM

Asymmetric key algorithm uses private key and public key. It is used to easily encrypt and decrypt the message when the relevant key is known. In crypto system one key to encrypt and different key to decrypt.

Sender



Receiver



A. RSA

RSA is a most popular and proven asymmetric cryptography algorithm. RSA is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers. [2]

Encryption: compute $c = m\wedge e \bmod n$, where the e and n are the public key, and m is the message block. The c is the encrypted message.

Decryption: The private key d is used to decrypt messages. Compute: $m = c\wedge d \bmod n$, where n is the modulus and d is the private key.

In RSA, compare to encryption process, decryption process takes more time.

B. Diffe-Hellman Key Exchange

Diffie-Hellman key agreement is not based on encryption and decryption. Diffe-Hellman (DH) is a method for securely exchanging a shared secret between two parties in real time untrusted network. It is used by several protocols, including ***Secure Sockets Layer (SSl), Secure Shell (SSH) and Internet protocol security (IPSec).***

IV. 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.

V. EXPERIMENTAL RESULTS

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

Table 1: Average time of encryption

Audio Files (KB)	Encryption time of BLOWFISH (MS)	Encryption time of AES (MS)
8,282	970	1025
387	38	55
33	16	20
2,826	348	370
Average Time	343	367.5

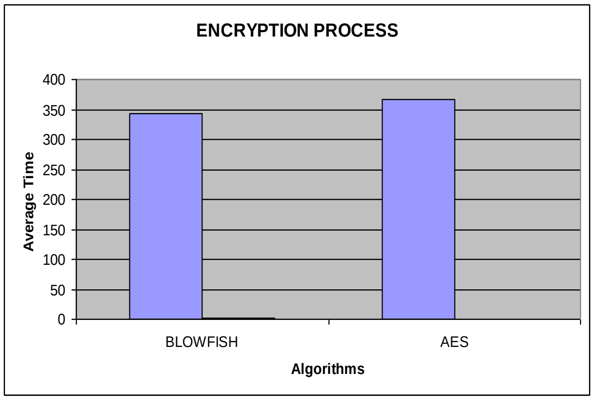


Figure 1 : Average Time of encryption

Figure 1 shows the result based on the average time of the encryption with different size of audio files. It shows that the average time is minimum for Blowfish when compared to that of AES. So from the experiment it proves that blowfish encryption algorithm consumes less time for encrypting the audio than that of AES.

Next, Comparison of decryption time has been given in the following table 2, and it shows the Average time of AES and BLOWFISH algorithm for different audio files decryption.

Table 2: Average time of decryption

Audio Files (KB)	Encryption time of BLOWFISH (MS)	Encryption time of AES (MS)
8,282	300	433
387	120	220
33	21	28
2,826	55	97
Average Time	124	194.5

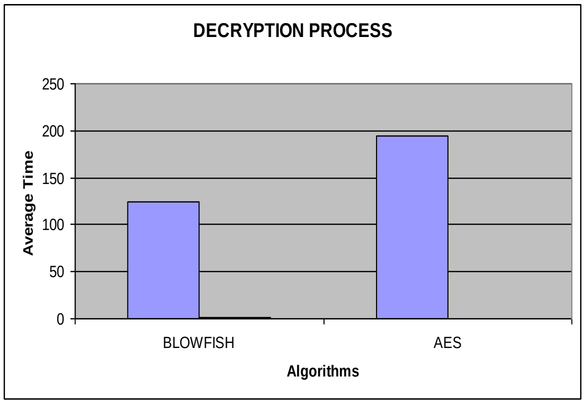


Figure 2: Average Time of decryption

Figure 2 shows the result based on the average time of the decryption with different size of audio files. It shows that the average time is minimum for Blowfish when compared to that of AES. So from the experiment it proves that blowfish decryption algorithm consumes less time for decrypting the audio than that of AES.

VI. CONCLUSION

Cryptography algorithm is the science in secret code. Rapidly rising cyber crime and the growing prospect of the internet being used as a medium for attacks create a major challenge for network security. In this paper

We studied the various cryptographic algorithms and majorly deals the encryption and decryption process for protecting the text files and images using some of the cryptographic algorithms.

The presented simulation results of audio files show the points. It was concluded that Blowfish has better performance than AES in terms of Average time.

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

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

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

[6] How-Shen Chang, "International Data Encryption Algorithms", 2004.

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

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

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

Authors:

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.

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.