Evaluation and Performance Analysis of Cryptography Algorithms

B.Sandhya[1], K. Pratyusha[2], G.Devi priya[3], D.Sagar[4]
Computer Science and Engineering, Lendi Institute of Engineering and Technology, Jonnada, Vizianagaram, AP, India.
[1] *sandy.princess133@gmail.com*
[2] *pratyushakurada@gmail.com*
[3] *Devipriya330@gmail.com*
[4] *sagarmahesh3@gmail.com*

***Abstract*— In today's world most of the communication is done using electronic media. Data security plays a major role in communication; hence there is a need to protect our data from malicious attacks .This can be achieved by using cryptography, which is an algorithmic process of converting the plain text into chipper text. It is based on the algorithm that both the sender and receiver know the key and message can be returned into its original plain text form. There are number of algorithms for performing encryption and decryption but they differ in time complexity and space complexity. The algorithms are classified based upon the number of keys that are employed for encryption and decryption like secret key cryptography, public key cryptography and hash functions. Encryption algorithm plays a major role in the information security while on the other side these algorithms put additional CPU load and consume battery fast. The main] objective of our paper is to compare and analyse Different algorithms such as DES, 3DES, AES, BLOWFISH, IDEA, SERPENT on the basis of encryption time with the variation of various file like plain text, image of data different sizes.**

***Keywords*— Cryptography, Encryption algorithms, Encryption time**

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it [1-4].
Cryptography models:

Symmetric (secret key)
Asymmetric (public key)

Symmetric (Secret key): Cryptography schemes are generally categorized as being either *stream ciphers* or *block ciphers*

Asymmetric (public key): PKC depends upon the existence of so called one-way functions or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute.

DES: The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, [5] while making sure the operations can be performed in both directions (for decryption).The combination of substitutions and permutations is called a product cipher.

3DES: 3DES is an enhancement of Data Encryption standard. It uses 64 bit block size with 192 bits of key size. The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average time 3DES is slower than other block Cipher methods.

AES: AES is based on a design principle known a Substitution permutation net AES has 128-bit block size and a key size of 128,256 bits .[3] AES 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 is 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.

IDEA: In cryptography, the International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES).The algorithm was intended as a replacement for the Data Encryption Standard (DES). IDEA is a minor revision of an earlier cipher, Proposed Encryption Standard (PES).IDEA operates on 64-bit using a 128-bit key, and consists of a series of eight identical transformations and an output transformation.

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 totalling 4168 bytes .[9] 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.

SERPENT: The serpent cipher algorithm is a block cipher that encrypts a 128 bit block of plaintext using a 256 bit key.The algorithm consists of three basic functions.[10] These functions are an initial permutation of bits named IP a Round Function named R, and a final permutation of bits named FP The Key Schedule of this algorithm provides 33 128-bit keys to be mixed with the text blocks during the Round function of the algorithm.

ALGORITHM	BLOCK SIZE	KEYSIZE
DES	64	56
3DES	64	56/112/168
AES	128	128/192/256
BLOWFISH	64	32
IDEA	64	128
SERPENT	128	128/192/256

II. OUR WORK

This section discusses the performance of the compared algorithms. In this paper we consider the performance of encryption algorithm for text files and images. We used AES, DES,3DES,BLOW-FISH ,IDEA,SERPENT algorithms evaluated usng 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 six algorithms, SERPENT takes more time for computation process. The memory usage of each algorithm is considered as memory byte level.

DES takes larger memory than AES,3DES,BLOWFISH,IDEA and SERPENT . Finally, the output byte is calculated by the size of output byte of each algorithm.

The level of output byte is equal for AES,3DES,BLOWFISH,IDEA and SERPENT, but DES algorithm produces low level of output byte. In this paper , the selected algorithms are AES,DES ,3DES, Blowfish ,IDEA and SERPENT . By using these algorithms the performance of encryption and decryption process of text files and image is calculated through the throughput parameter.

Encryption time is calculated as the total plaintext in bytes encrypted divided by the encryption time. [7]Decryption time is calculated as the total plaintext in bytes decrypted divided by the decryption time. As a result mentioned in the paper , it is said that DES algorithm gives the better performance than all other algorithms in terms of throughput. The least efficient algorithm is DES.

In [8] paper ,we discuss the performance evaluation of AES,DES,3DES,BLOWFISH,IDEA and SERPENT 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 six 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 remaining algorithms in almost all the test cases.

III. TEST RESULTS

Encryption Time:

The six algorithms DES, 3DES, IDEA, AES, BLOWFISH and SERPENT are considered and the text file is given as an input and encryption. The encryption time is calculated and represented in the below table.

Table 1: Comparative execution times (in seconds) of secret key algorithms

Text File(bytes)	Des	3Des	Aes	Blowfish	Idea	Serpent
68060	0.31	0.577	0.31	0.265	0.31	0.9
106789	0.32	0.621	0.34	0.268	0.33	1.2
151246	0.4	0.624	0.342	0.266	0.41	1.4
173928	0.42	0.639	0.35	0.281	0.43	1.8

From the above calculated values Blowfish is executed in short period of time and then aes is executed is in faster way. Serpent takes more time to execute. Image file is given as an input to the six algorithms and encryption time is calculated.

Table 2: Comparative execution times (in seconds) of secret key algorithms

Image File(bytes)	Des	3Des	Aes	Blowfish	Idea	Serpent
4605	0.23	0.14	0.281	0.2	0.31	0.97
845924	0.3	0.624	0.297	0.268	0.33	1.29
879365	0.32	0.64	0.328	0.4	0.41	1.49
879368	0.93	0.702	0.42	0.48	0.43	1.98

Decryption Time: The six algorithms DES, 3DES, IDEA, AES, BLOWFISH and SERPENT are considered and the text file is given as an input and encryption. The decryption time is calculated and represented in the below table.

For decryption the cipher text file is given as an input and decrypted.

Table 3: Comparative execution times (in seconds) of secret key algorithms

File(bytes)	Des	3Des	Aes	Blowfish	Idea	Serpent
68060	0.31	0.31	0.3	0.26	0.31	0.9
106789	0.32	0.39	0.3	0.31	0.33	1.2
151246	0.47	0.655	0.342	0.34	0.41	1.4
173928	0.49	0.67	0.35	0.342	0.43	1.8

From the above calculated values Blowfish is executed in short period of time and then aes is executed is in faster way. Serpent takes more time to execute. Image file is given as an input to the six algorithms and encryption time is calculated.

Table 4: Comparative execution times (in seconds) of secret key algorithms

File(bytes)	Des	3Des	Aes	Blowfish	Idea	Serpent
4605	0.31	0.577	0.31	0.265	0.31	0.978
845924	0.32	0.621	0.34	0.268	0.33	1.298
879365	0.4	0.624	0.342	0.266	0.41	1.436
173928	0.42	0.639	0.35	0.281	0.43	1.829

IV. FIGURES

Fig.1 Chosing an algorithm

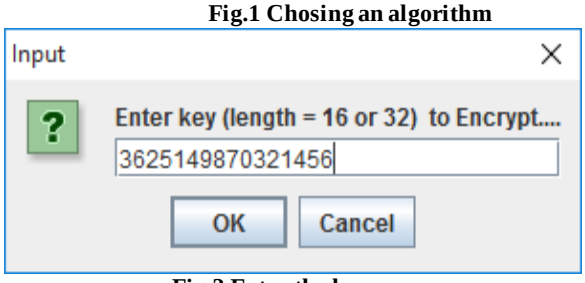

Fig.2 Enter the key

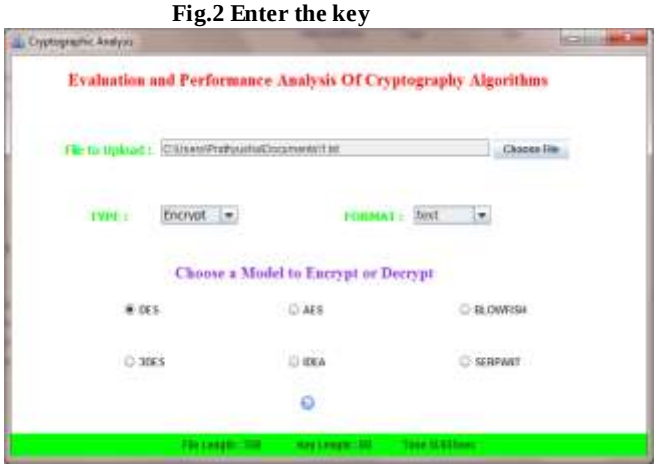

Fig.3 Output text

Fig.4 Text encrypted

Fig.5 Text decrypted

Fig.6 Image encrypted

Fig.7 choose the model

Fig.8 Image decrypted

V. CONCLUSIONS

In this paper we compared Six Cryptographic algorithms those are DES, 3DES ,IDEA,AES, BLOWFISH AND SERPENT and implemented in JAVA. We implemented and tested these encryption algorithms, under different scenario with different data sizes. To measure the performance of these six algorithms, we use different metrics like encryption time, decryption time, file size. Finally we find 3DES need more time to encrypt/decrypt, and also it use very high memory. AES and BLOWFISH have the similar time for encrypt and decrypt and better throughput but AES need more memory than BLOWFISH. DES needs similar memory as 3DES but it takes minimum time to encrypt and decrypt and also having higher throughput than 3DES. When compared to all algorithms and find BLOWFISH encryption/decryption algorithm has better performance related to remaining algorithms.

REFERENCES

[1] BRUCE SCHNEIER applied cryptography, second edition.
[2] William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", National Institute of Standards and Technology, NIST Special Publication 800-67, 2008.
[3] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)",Federal Information Processing Standards Publication 197, Nov. 200
[4] Fundamentals of computer security, springer publications "Basic cryptographic algorithms", an article available at www.itse.state.md.us/oldsite/info/internet security/crypto/cryptointro.html#Algorithms.
[5] Amandeep singh, ManuBansal "FPGA Implementation of DES encrypted algorithm" computer networks and information security,2012
[6] Apoorva, Yogesh, kumar "comparative study of different symmetric key cryptography algorithms" International Journal of Network security & its applications(IJNSA).Vol. no 1 2013
[7] Elliptic Curve Cryptography, Certicom Research, 2000
[8] G.Rameshi, Dr.R.Umarani "performance analysis of most comman symmetric encryption algorithms" International Journal Of Power Control Signal and Computation(IJPCSC)
[9] Amit Jain, Ravindra Patel, "An Efficient Compression Algorithm (ECA) for Text Data", icsps, pp.762-765, 2009 International Conference on Signal Processing Systems, 2009
[10] Farina, A.; Navarro, G.; Parama, J.R., "Word-Based Statistical Compressors as Natural Language Compression Boosters", Data Compression Conference 2000

