Analysis and comparison of symmetric key algorithms (Blowfish, DES, TEA, IDEA) in cryptography

G. Sindhu[1], P. Krithika[2]
[1, 2] Department of Computer Science
[1, 2] Cauvery College for Women, Trichirappalli, India.

Abstract- *The information being transmitted through a network is vulnerable to various types of passive and active attacks. So the information security is becomes a challenging aspects in network data transmission. Cryptography algorithms encrypt data and provide a security against the data intruders and secure the network communication. Symmetric key algorithms shared the secret keys to sender and receiver's side.*

Here a detailed analysis and comparison made on Blowfish, DES (Data Encryption Standard), TEA (Tiny Encryption Algorithm), and IDEA (International Data Encryption Algorithm) symmetric key algorithms. The analysis and comparison is based their parameters like structure of the algorithm, rounds, Key size, Encryption time, Decryption time, security against attacks and uniqueness of algorithm and the encryption and decryption time series is implemented for different size files.

Keywords- Encryption, Decryption, Brute force attack, Feistel network.

I. INTRODUCTION

The Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free.

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. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).

Encryption is the process of converting a message (or plaintext) into an 'unintelligible' form (called cipher text) and decryption is the reverse process. The cipher text is transmitted by the sender to the intended recipient of the plaintext, across an insecure communication channel (any third party can intercept data that flows through such a channel). The algorithm used for performing encryption and decryption is called the cipher.

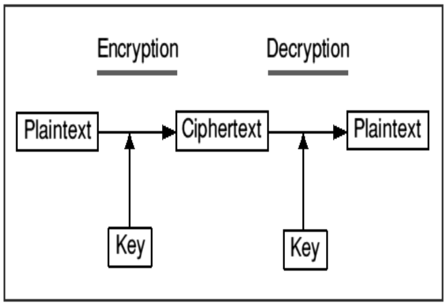


Figure-1 Encryption and Decryption Process

Plaintext: An original intelligible message or data that is fed into the algorithm as input.

Cipher text: The coded message is known as Cipher text. That is depends on plaintext and secret key.

Encryption: The process of converting from plaintext to cipher text that is known as Encryption.

Decryption: Restoring the plaintext from cipher text that is known as Decryption.

Cryptography: The many schemes used for enciphering constitute the area of study known as Cryptography. Such as a scheme is known as Cryptographic system or Cipher.

II. PERFORMANCE ANALYSIS

Performance analysis of Blowfish, DES, TEA, and IDEA is done to provide some measurement on the encryption and decryption. Various parameters such as number of rounds, file size, key length and key generation time are inquired. Effects of several parameters such as number of rounds, block size and the length of secret key on the performance evaluation criteria are investigated.

A. PERFORMANCE FACTORS

Key Length Value

In the encryption methodologies, the key management is the important feature to shows the how the data is encrypted. The symmetric algorithm uses a variable key length which is longer. So, the key management is a huge aspect in encryption processing.

Block size

Symmetric key ciphers are generally divided into stream ciphers and block ciphers. Block ciphers operate on a fixed length string of bits. The length of this bit string is the **block size**.

Security Issues

Cryptographic security defines whether encryption scheme is secure against brute force, time attack and different plaintext-cipher text attack

Encryption and Decryption time

The time essential by algorithm to total the operation depends on processor speed and algorithm Complexity. Less time algorithm take to entire its operation improved it is.

Structure

In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network. The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved.

III. IMPLEMENTATION AND RESULTS OF ENCRYPTION & DECRYPTION TIME

These encryption and decryption of Blowfish, DES, TEA, and IDEA algorithms were implemented in java in NetBeans IDE 6.9.1. Performance was measured on Intel(R) Core(TM) i3 CPU M 370 @ 2.40 Ghz 2.39 Ghz 32 bit system with 4 GB of RAM running Windows 7 Ultimate.

A. Encryption Time

The encryption time of different size of files are implemented. The process encryption screen is given below.

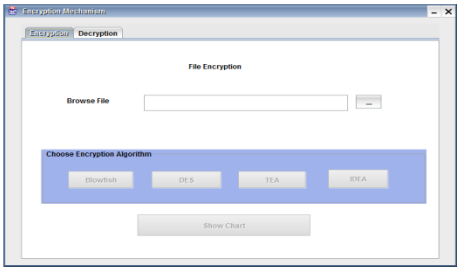
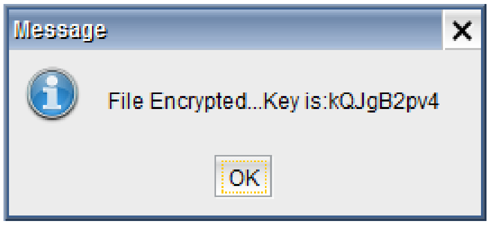


Figure-2 Encryption home Screen

The screen contains select the file option and algorithms name button and show chart button for displays the encryption time of file with different algorithms.

In this screen, first the select the file and click the algorithms name. The encryption is displayed for each and every algorithm. The key must be same in decryption process.



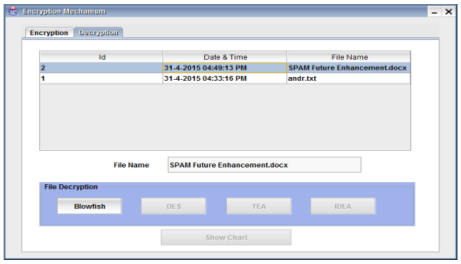
File Encrypted...Key is:kQJgB2pv4

Figure-3 Encryption key value

Show chart button also displayed this option is used to show the encryption time of a file in graph format. The x axis contains the algorithms names. The Y axis contains the time series of encryption time.

B. Decryption time

The decryption screen is displayed as follows.



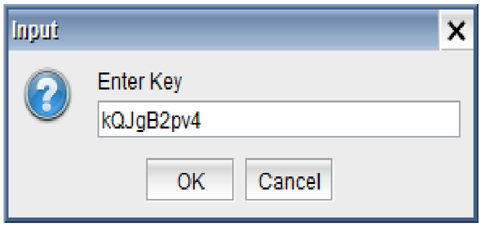
Id	Date & Time	File Name
2	31-4-2015 04:49:13 PM	SPAM Future Enhancement.docx
1	31-4-2015 04:33:16 PM	andr.txt

File Name: SPAM Future Enhancement.docx

Figure-4 Decryption home screen

It contains which file is encrypted with their time of encryption and it contains the file name option for select a file for decryption process.

The Blowfish, DES, TEA, IDEA algorithm buttons are used to do the decryption process. During the decryption process key value is needed, this key must be same to encryption process time of key.


Input

Enter Key

kQJgB2pv4

Figure-5 Decryption key value

Show chart button also displayed this option is used to show the decryption time of a file in graph format. The x axis contains the algorithms names. The Y axis contains the time series of decryption time.

C. RESULT OF DIFFERENT SIZE OF FILES

The different size of files are implemented that results are displayed as follows.

4.3.1 150kb size of file

The text file with 150kb size is implemented. Their results are displays as follows.

Encryption

The IDEA algorithm's encryption process has low encryption time and range. Next the TEA algorithms process the next level and the Blowfish algorithm has the next level of encryption time. At last the DES algorithm has high time of encryption process.

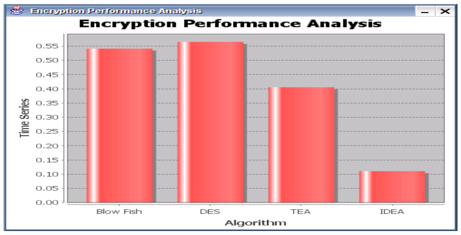


Figure-6 Encryption performance analysis of a file with 150kb size

So the IDEA algorithm has less time series value from BLOWFISH, DES, TEA, and IDEA with file size 150kb.

Decryption

The blowfish algorithm's Decryption process has low decryption time. Next the TEA algorithms process the next level and the DES algorithm has the next level of decryption time. At last the IDEA algorithm has high time of decryption process.

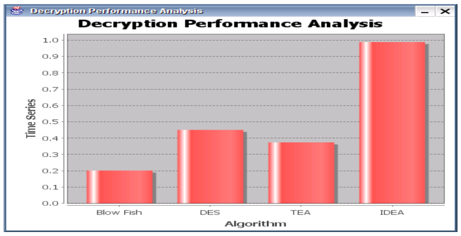


Figure-7 Decryption performance analysis of a file with 150kb size

So the blowfish algorithm has less time series value from BLOWFISH, DES, TEA, and IDEA with 150 kb.

4.3.2. 55kb size of file

The text file with 55kb size is implemented. Their results are displays as follows.

Encryption

The blowfish algorithm's encryption process has low encryption time. Next the IDEA algorithms process the next level and the TEA algorithm has the next level of encryption time. At last the DES algorithm has high time of encryption process.

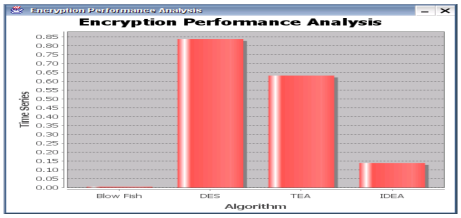


Figure-8 Encryption performance analysis of a file with 55kb size

So the blowfish algorithm has less time series value from BLOWFISH, DES, TEA, and IDEA with 55kb.

Decryption

The blowfish algorithm's Decryption process has low encryption time. Next the DES algorithms process the next level and the TEA algorithm has the next level of decryption time. At last the IDEA algorithm has high time of decryption process.

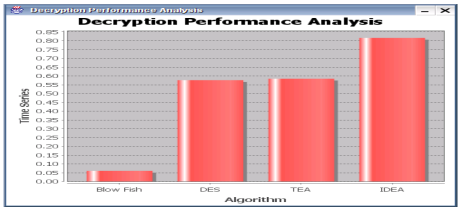


Figure-9 Decryption performance analysis of a file with 55kb size

So the blowfish algorithm has less time series value from BLOWFISH, DES, TEA, and IDEA with 55 kb file size.

4.3.3. 20kb size of file

The text file with 20kb size is implemented. Their results are displays as follows.

Encryption

The DES algorithm's encryption process has low encryption time. Next the TEA algorithms process the next level and the Blowfish algorithm has the next level of encryption time. At last the IDEA algorithm has high time of encryption process.

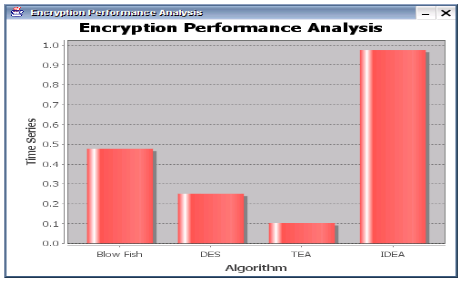


Figure -10 Encryption performance analysis of a file with 20kb size

So the TEA algorithm has less time series value from BLOWFISH, DES, TEA, IDEA with 20 kb file size.

Decryption

The DES algorithm's Decryption process has low encryption time. Next the TEA algorithms process the next level and the IDEA algorithm has the next level of decryption time. At last the Blowfish algorithm has high time of decryption process.

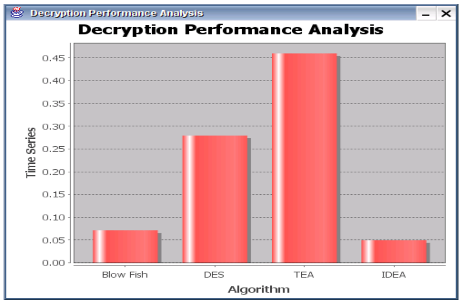


Figure-11 Decryption performance analysis of a file with 20kb size

So the IDEA algorithm has less time series value from BLOWFISH, DES, TEA, and IDEA with 20 kb file size.

Table-1 The Encryption time series of different size files

Algorithm names	Encryption time of different files		
	150kb	55kb	20kb
Blowfish	0.54	0.01	0.43
DES	0.56	0.83	0.25
TEA	0.40	0.62	0.10
IDEA	0.10	0.14	0.90

As per the implementation of three files the IDEA algorithm has the lowest level of values. So for encryption the IDEA algorithm is best for encrypted a file quickly.

Table-2 The decryption time series of different size files

Algorithm names	Decryption time of different files		
	150kb	55kb	20kb
Blowfish	0.20	0.06	0.07
DES	0.43	0.57	0.28
TEA	0.38	0.58	0.45
IDEA	0.98	0.81	0.05

As per the implementation of three files the Blowfish algorithm has the lowest level of values. So for decryption the Blowfish algorithm is best for decrypted a file quickly.

IV. CONCLUSION

Different symmetric key algorithm have been analyzed for various file features like data size and key size, and analyzed the variation of encryption time for different selected cipher algorithms.. The encryption and decryption time of different sizes of files are implemented in NetBeans 6.9.1 using java coding for Blowfish, DES, TEA, IDEA symmetric algorithms.

The result of the implementation is, for encryption the IDEA symmetric algorithm has the less time interval and for decryption process Blowfish symmetric algorithm has the less time interval. So the IDEA algorithm is better for encryption process and blowfish algorithm is better for decryption process.

In future, the researchers implement the more symmetric algorithms with their different parameters like throughput, end to end delay and memory utilization for each algorithm.

REFERENCES

[1] International journal of engineering sciences & research technology**," comparative study of different authentication and identification algorithms in secured cryptography"** by nitin gupta, dr. Manoj kumar- January 2015.

[2] International journal of advance foundation and research in computer (ijafrc),"**Comparative study of symmetric and asymmetric cryptography techniques**." by ritu tripathi, sanjay agrawal.,- june 2014.

[3] International journal of computer applications, "**performance evaluation of rc6, blowfish, des, idea, cast-128 block ciphers**" by Kirti Aggarwal, Jaspal Kaur Saini , Harsh K. Verma - april 2013.

[4] International journal of innovative research in computer and communication engineering, **-"a comparative performance analysis of des and blowfish symmetric algorithm**" by Srinivas B.L , Anish Shanbhag, Austin Solomon D'Souza.- october 2014.

[5] International journal of network security & its applications (ijnsa), **"analysis and comparison of symmetric key cryptographic algorithms based on various file features "** by ranjeet masram, vivek shahare, jibi abraham, rajni moona- july 2014.

[6] Ijret: international journal of research in engineering and technology **, "Implementation of aes and blowfish algorithm"** by chaitali haldankar, sonia kuwelkar-may 2014

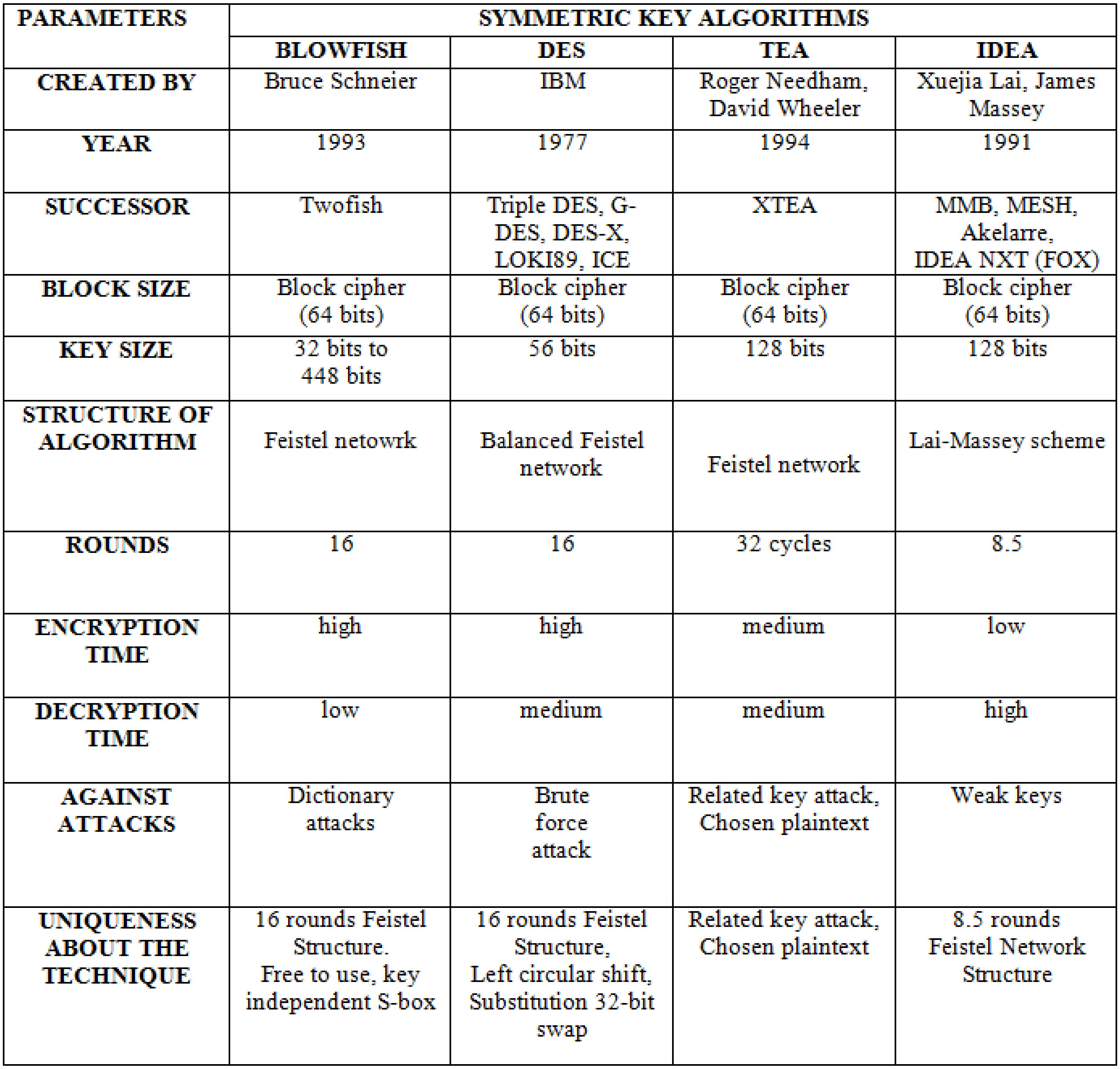
[7] International journal of science, engineering and technology research (ijsetr), **" a review on symmetric key encryption techniques in cryptography"** By saranya k mohanapriya r udhayan j, march 2014

[8] International journal of advanced research in Computer science and software engineering, **"comparative analysis of symmetric key encryption algorithms",** By narender tyagi anita ganpati , August 2014

[9] International journal of computer science and mobile computing, **"comparison of asymmetric algorithms in cryptography"** By neha garg partibha yadav, april 2014

[10] International journal of security (ijs) singaporean journal of scientific research(sjsr) "**a survey on variuos encryption and decryption algorithms",** m.chanda mona, s.banu chitra, v.gayathri, October 2014.

TABLE-3 COMPARISONS AND ANALYSIS OF SYMMETRIC KEY ALGORITHMS (BLOWFISH, DES, TEA, IDEA).



PARAMETERS	SYMMETRIC KEY ALGORITHMS			
	BLOWFISH	DES	TEA	IDEA
CREATED BY	Bruce Schneier	IBM	Roger Needham, David Wheeler	Xuejia Lai, James Massey
YEAR	1993	1977	1994	1991
SUCCESSOR	Twofish	Triple DES, G-DES, DES-X, LOKI89, ICE	XTEA	MMB, MESH, Akelarre, IDEA NXT (FOX)
BLOCK SIZE	Block cipher (64 bits)	Block cipher (64 bits)	Block cipher (64 bits)	Block cipher (64 bits)
KEY SIZE	32 bits to 448 bits	56 bits	128 bits	128 bits
STRUCTURE OF ALGORITHM	Feistel netowrk	Balanced Feistel network	Feistel network	Lai-Massey scheme
ROUNDS	16	16	32 cycles	8.5
ENCRYPTION TIME	high	high	medium	low
DECRYPTION TIME	low	medium	medium	high
AGAINST ATTACKS	Dictionary attacks	Brute force attack	Related key attack, Chosen plaintext	Weak keys
UNIQUENESS ABOUT THE TECHNIQUE	16 rounds Feistel Structure. Free to use, key independent S-box	16 rounds Feistel Structure, Left circular shift, Substitution 32-bit swap	Related key attack, Chosen plaintext	8.5 rounds Feistel Network Structure