Theoretical Overview of various Encryption Techniques on Data Security

Priyamvada Saxena
Department of Electrical Engineering, Centre of Excellence, Veermata Technological Institute, Mumbai, India-4000019

***Abstract*- Data Security is an important element in data communication. Numerous encryption techniques play a key role in securing the data. The techniques strengthen data privacy by making it unreadable or impossible to break the data which can be understandable. By using the techniques discussed in the paper security can be provided against eavesdropping. The techniques that protects data is called cryptography which converts a plain-text into incomprehensible form and the back process produces data in lucid form. The above process is defined as encryption of data and decryption of data. This paper discusses various encryption techniques that can be used for data security.**

***Index Terms*- Encryption, Decryption, Public-key encryption, Private-key encryption, plain-text, cipher-text Introduction (Heading 1).**

I. INTRODUCTION

Data preservation is an important condition in data communication .As we live in the age of internet or the "information age" data security over the network has been a serious issue because a large part of population choose internet for data communication. When data is conveyed to sender there may be a possibility of eavesdropping or intruder taking part in the communication and data is modified by a third person. The popular technique of data protection is cryptography. Cryptography is merger of words such as crypto meaning unknown or hidden and graphy is an art of writing. This can be cited as an art which involves conversion of data in an unreadable form. It is a major functional block in information scheme. It is the study of mathematical techniques for data security. In cryptography techniques few words are constantly used they are, the data that can be fully understandable is called the plain-text. The process by which a plain-text is modified called encryption. This result in a text called cipher-text. The process of recovering the text back is called decryption. A system which provides encryption and decryption is known as cryptosystem. Another term that is most commonly used is crypto-analysis. A Crypto-analysis focuses on how the data that is meant to be secured can be attacked by outsiders. As need for data security increased various encryption techniques are developed. The oldest technique is the Caesar's cipher. This technique was developed during Second World War. It is known as substitution cipher, in this each letter is replaced by another letter .For example, we consider a shift of 3 then A is substituted by E and so on.

There are two keys associated with the cryptography technique that is private and public keys.

Fig 1:Basic cryptography process

Cryptography is branched into three sections. They are symmetric encryption process, Asymmetric encryption process and hash function. In Symmetric Encryption process encryption uses the same key for encrypting and decrypting data. This can be observed in the below fig2.

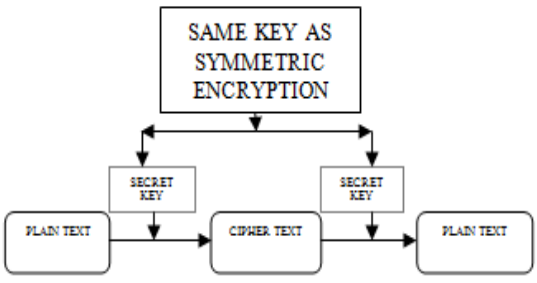


Fig 2: Symmetric Encryption Process

In Asymmetric Encryption process the encryption demands different keys to be used for encryption and decryption process. This process can be seen in fig 3.

Fig 3.Asymmetric Encryption process.

Hash function is known as one way cryptography. It does not have any key to recover the plain text from the cipher text. The text obtained can also be called as hashed text as seen in fig 4.

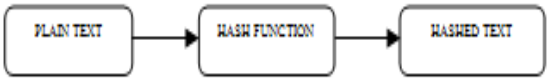


Fig 4.Hashing algorithm.

On the basis of data lump , cryptography is divided into two sectors they are:-

a) Stream Ciphering system:-In this encryption of the data is done byte-by-byte at a time.

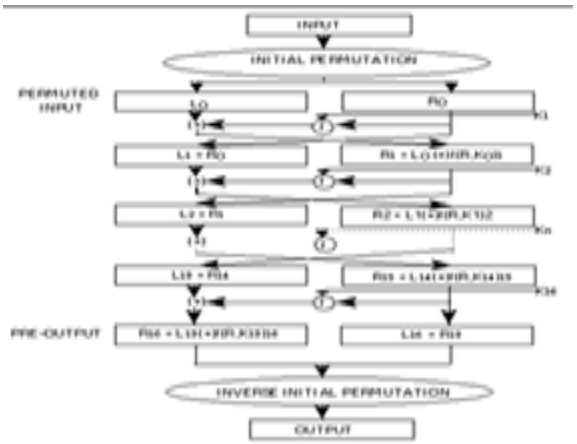
b)Block Ciphering System:-In this encryption of data is done by considering number of particular bits at a time.

II.OVERVIEW OF ALGORITHMS

The algorithms selected for implementation are DES, AES, TWOFISH, SALSA20, CAMELLIA and RSA.

A.DES

DES is known as Data Encryption Standard. It is included in region of symmetric-key block cipher. It was a first encryption standard that was recommended by National Institute of Standards and Technology. It was developed around 1974 by IBM.DES algorithm has considered block- size of 64 bits and a key length of 56 bits for its algorithm. DES can be operated in different forms that are CBC, CFB, ECB, and OFB. The flow of above algorithm is shown in the fig 5.



Algorithm begins with an initial permutation, a sixteen rounds of block cipher and final permutation. DES is mostly benefited in military and other domains. There are variants of DES and they are 3DES,AES.

B.AES

AES is Advanced Encryption Standard .It is a replacement for DES. In 1998 the US NIST recommended use of AES.AES was refined by Joan Daemen and Vincent Rijmen. It is similar to DES. It uses a key length which is variable they are 128,192,256 . AES is a fast and flexible encryption method than DES. The algorithm flow is shown in the fig 6.

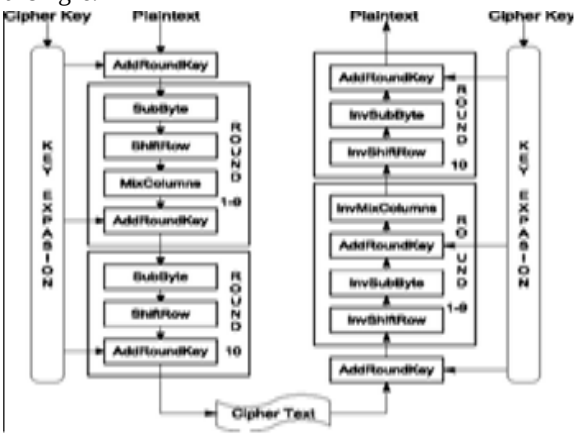


Fig 6.AES Encryption process.

Each processing round in the above figure associates four steps:-

a)Substitute bytes:-It consists of a S-box for performing a byte by byte substitution of the block.

b)Shift rows:-It involves in performing a simple permutation.

c)Mix column:-It is a substitution method where data in each column from the above shift row is multiplied by the algorithm matrix.
d)Add round key:-It involves the key for the processing round is XORed with the data.

C.TWOFISH
Twofish was not selected as standardization but was one of the finalists in the AES contsest. It is designed by Bruce Schneier, Dough Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall. It is similar to AES a symmetric key block cipher. It deals with a block size of 128 bit and key size to 256 bit. The algorithm is shown in fig 7.

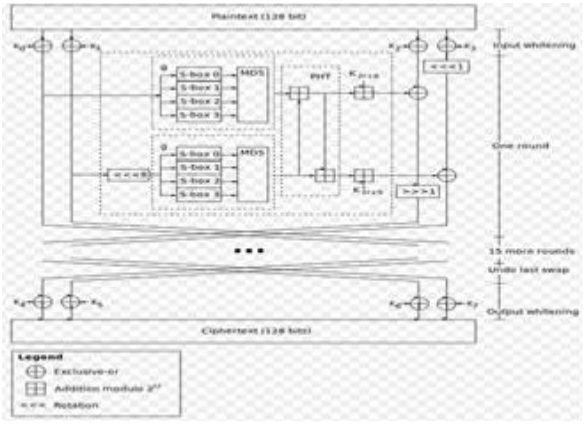


Fig 7:TWOFISH Encryption process.

D.SALSA20
It is developed by DanielJ. Bernstein. It is stream cipher.It is based on add-rotate-xor operations a 32 bit addition ,bitwise addition(XOR) and rotation operations. SALSA20 uses a 256 bit key ,a 64 bit nonce(it is an arbitrary number that can be used only once),64 bit stream position mapped to a 512 bit block of the key stream. The cipher uses bitwise addition ⊕ , a 32 bit addition mod 232 ⊞, and distance operations <<<.This process can be summarized from the figure 8.

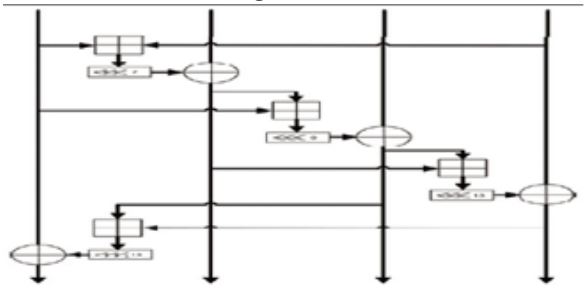


Fig 8: SALSA20 Encryption process.

E. CAMELLIA
CAMELLIA is also a symmetric-key block cipher. It has a block size of 128 bits and key sizes of 128,192 and 256 bits. It was advanced jointly by Mitsubishi Electric and NIT of Japan.

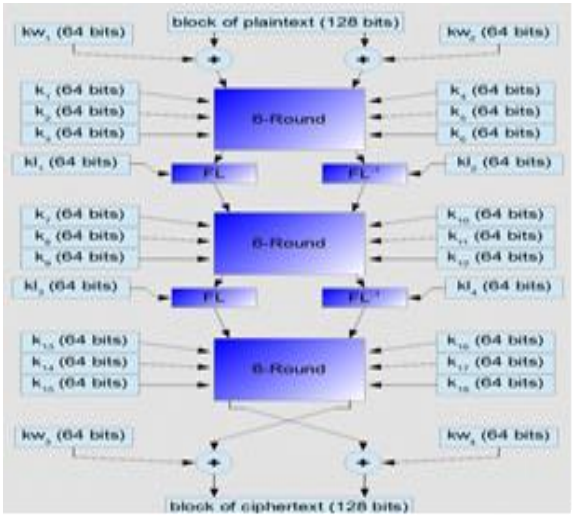


Fig 9: CAMELLIA Encryption process.

From the fig 9 the process can be described as the most important element of the process are F-functions. They are to be used during encryption-decryption .The F-function takes 128 input bits mixes them with sub keys and returns new 128 bits. F-function calls are gathered in blocks and each block contains 6 rounds. Both in encryption and decryption process are about to perform some repetitions of the 6-round blocks.

F.RSA
RSA was developed by Rivest, Shamir and Adelman and an asymmetric cryptographic algorithm. It is one of the best techniques of public key cryptosystems for key swap and encryption of blocks of data. It requires two keys, one is the public key for encryption and other is the private key to decrypt message. The encryption process contains three steps, first step is the key generation second and third step are encryption and decryption respectively. The key size is of 1024 to 4096 bits. It uses two prime numbers to generate a public-key and a private-key. Sender encrypts the message using Receiver's public key and at the decryption side the message is decrypted using Receiver's private key. This can be seen in the fig 10.

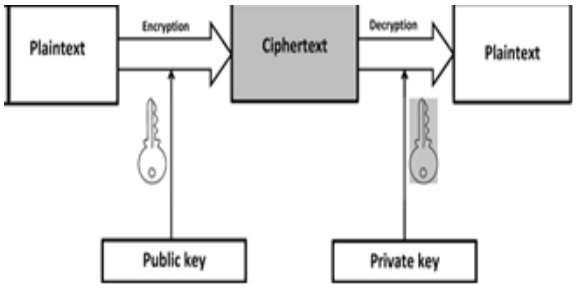


Fig 10: RSA Encryption process.

III.SIMULATION RESULTS AND ANALYSIS

Comparison is done in the performance of the algorithms was conduction with encryption and decryption of a string of data. The performance parameters that need to be calculated are a) Encryption time, b) Decryption time.

Simulation was conducted on Linux platform. A string of data was selected. Python language is used for implementation. For each encryption and decryption time was calculated and comparison is made.

The first technique is DES and data to be passed on is "Please encrypt my message". It is in CBC mode. The cipher text can be seen in the fig11.

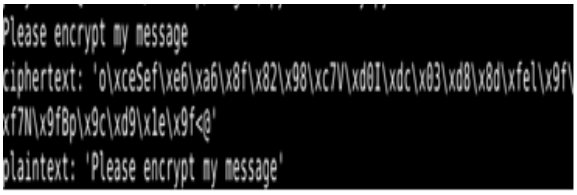


Fig 11: DES technique implementation.

The time taken for its encryption is 0.027111sec and for its decryption is 0.043025 sec.

The next technique is AES and data to be passed on is "Please encrypt my message". It is in CBC mode. The cipher text can be seen in the fig12

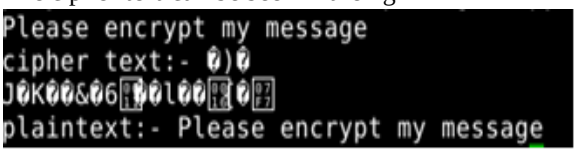


Fig12:AES technique implementation.

The time taken for its encryption is 0.000224 sec and for its decryption is 0.000418 sec.

The next technique is TWOFISH and data to be passed on is "MESSAGENCRYPTION". The cipher text can be seen in the fig13.

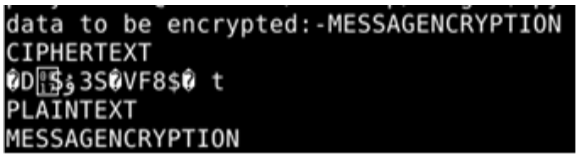


Fig13: TWOFISH technique implementation.

The time taken for its encryption is 0.000211sec and for its decryption is 0.0009sec.

The next technique is SALSA20 and data to be passed on is "MESSAGEENCRYPTION". The cipher text can be seen in the fig14.

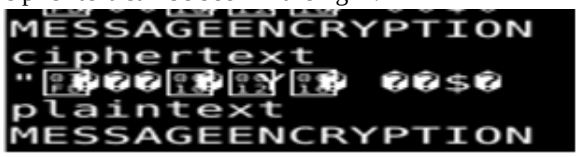


Fig14:SALSA20 technique implementation.

The time taken for its encryption is 0.271191sec and for its decryption is 0.271389sec.

The next technique is CAMELLIA and data to be passed on is "This is a data". The cipher text can be seen in the fig15.

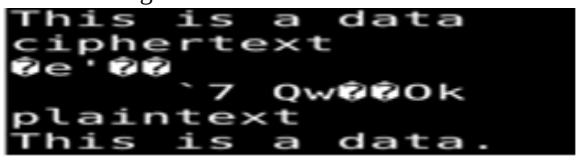


Fig15: CAMELLIA technique implementation.

The time taken for its encryption is 0.000667 sec and for its decryption is 0.000968 sec.

The next technique is RSA and data to be passed on is "Please encrypt my message". The cipher text can be seen in the fig16.

Fig16: RSA technique implementation.

The time taken for its encryption is 0.002287 sec and for its decryption is 0.002545 sec.

TECHNIQUE	ENCRYPTION(in sec)	DECRYPTION(in sec)
DES	0.02711	0.043025
AES	0.000224	0.000418
TWOFISH	0.000211	0.0009

SALSA20	0.271191	0.271389
CAMELLIA	0.000667	0.000968
RSA	0.002287	0.002545

From the results it is clearly visible that AES technique takes less time to encrypt and decrypt the data. But RSA technique is the best technique for protection of data.

IV.CONCLUSION

This paper presents the performance characteristics of some algorithms. From the results it can be seen that AES technique is the best technique in account of less time for encryption and decryption. RSA is the best technique for data protection. In future it can be extended for image and video files, also it can be used to send data from one place to another.

REFERENCES

[1] Madhumita Panda, "Performance Analysis of encryption Algorithms for Security," IEEE,International conference on Signal Processing,Communication,Power and Embedded System(SCOPES)-2016.

[2] Aasif Hasan,Neeraj Sharma,"A New Method Towards Encryption Schemes",IEEE,International conference on Reliability,Optimization and Information Technology-ICROIT 2014.

[3] Javier Sanchez,Ronny Correa,Hernando Buenano,Susana Arias,Hector Gmoez,"Encryption Techniques:A Theoretical Overview and Future Proposals",IEEE.

[4] Madhumita Panda,Atul Nag,"Plain Text Encryption Using AES,DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux ",IEEE,2015 Second International Conference on Advance in Computing and Communication Engineering.

[5] Dr.Sanjay Kumar,"Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication :A Review on RSA Algorithm",IEEE.

[6] Shaify Kansal,Meenakshi Mittal,"Performance Evaluation of various Symmetric Encryption Algorithms",IEEE,2014 International Conference on Parallel,Distributed and Grid computing.

[7] Kaibin Huang,Raylin Tso,Yu-Chi Chen,"One-Time-Commutative Public Key Encryption",IEEE,Computing confrence July 2017.

[8] Krishna Keerthi Chennam,Lakshmi Muddana,Rajani Kanth Aluvalu,"Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for securing Data in Cloud",IEEE,International Conference on Recent Trends in Electronics Information and Communication Technology,May 2017.

[9] Abhishek Vichare,Tania Jose,"Data Security using Authenticated Encryption and Decryption Algorithm for Android Phones",IEEE,International Conference on Computing,Communication and Automation 2017.