Evolution of AES, Blowfish and Two fish Encryption Algorithm

[1]E.Jeevalatha, [2]Mr.S.SenthilMurugan

Abstract: Data is any type of stored digital information. Security is about to protection of assets. Network security involves covers a variety of computer networks, both public and private, that are used in everyday jobs. Cryptography is a concept to protect network and data transmission. Cryptography is a method of storing and transmitting data in a particular form. AES is one of the most powerful techniques. In this paper, we analyze and find an efficient encryption algorithm which takes less space, time and security among these encryption algorithms. These AES, Blowfish and Two fish algorithms are outlined.

Keywords: Network Security, Cryptography, AES, Blowfish, Two fish

1 INTRODUCTION

Cryptography is the method to secure our personal data or information from the unauthorized users. Cryptography means "secret writing" which means is the science and art of transforming messages to make them secure and immune to attacks by unauthorized users. In cryptography two types of operation can be performed,

- Encryption and
- Decryption.

The Encryption and Decryption operation can do by using key management. An encryption is the process of converting the original data into another format is known as cipher text, which is not easy to understand and unreadable.

2 CRYPTOGRAPHY MECHANISM

2.1 Key

It is used to change the format of data; it can be either private key or public key.

2.2 Plain text

Original message that is easy to understand by anyone.

2.3 Cipher text

Another format of data that cannot be understood by anyone.

2.4 Encryption

It is the process to convert the plain text into the cipher text.

2.5 Decryption

It is the process to reverse the encryption process i.e., cipher text into plain text.

2.6 Steps of cryptography

- The message can be encrypt by using either private or public key that becomes unreadable.
- It converts the plain text into the cipher text and send to the receiver.

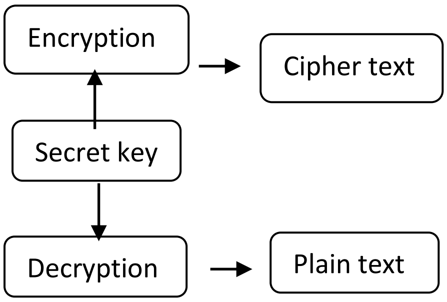
Then the receiver applies the reverse process of the encryption to back over the original message.

In the present era everyone needs fast processing and less space to store the result. There are many encryption algorithm in which some of the algorithm takes less computational time and some of takes more time, but all has their own advantages and disadvantages. Here, the aim to find which algorithm takes specific time for computation and more secure.

3 SYMMETRIC AND ASYMMETRIC ENCRYPTION

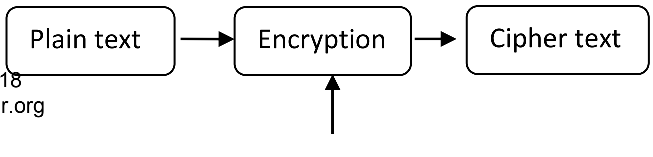
3.1 Symmetric Key Encryption

It is also known as private key encryption. A single key is used in both the sender and receiver side to encrypt and decrypt the message or data. The sender uses the secret key (private key) and encryption algorithm to encrypt the plain text and the receiver uses the same private key and corresponding decryption algorithm to decrypt the cipher text. Sometimes it is easy to crack the password by applying brute force method. There are two types of symmetric algorithms: stream cipher and block cipher algorithm. AES, DES, 3DES, IDEA, RC4, Blowfish and Two fish are some examples for this symmetric algorithm.

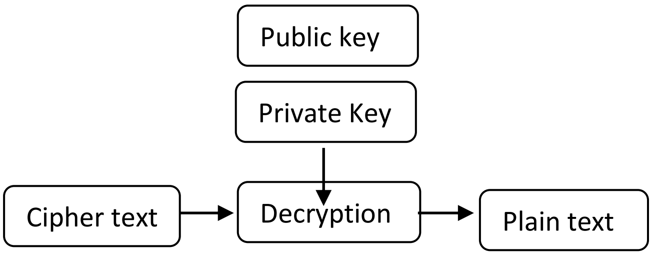


3.2 Asymmetric Key Encryption

It is also known as public key encryption. Adifferent key is used to encrypt and decrypt the data. The sender uses the public key to encrypt the plain text and the receiver uses the private key to decrypt the cipher text. It is not easy to crack and guess the password. RSA, Diffie-Hellman, Pailler, Elgamal are some examples of this asymmetric algorithm.



- [1]E.Jeevalatha, Second Year Master of Computer Applications in Priyadarshini Engineering College, Vaniyambadi, E-mail: jeevaethirai1013@mail.com
- [2]S.SenthilMurugan, Assistant Professor Master of Computer Applications in Priyadarshini Engineering College, Vaniyambadi, E-mail: mailmurugan.78@mail.com



4 COMPARED ALGORITHM

Before comparison of AES, Blowfish and Two fish encryption algorithm, there is some description about these algorithms:

4.1 AES(AdvancedEncryption Standard)

In this paper, the author explained that AES is a block cipher algorithm, it supports 128 bit block and key size is 128, 192, 256 bits. The original name of AES is Rijindeal and published in 1977. Maximum there is 14 processing round is processed in the AES and the number of round is depends upon the key size. If the key size is 128 bits 10 rounds is processed, if the key size is 192 12 rounds is processed and if the key size is 256 14 rounds is processed. In AES there are four major steps are followed:

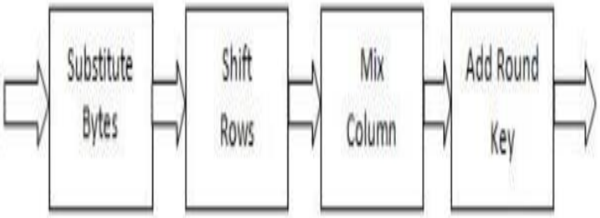
4.1.1 Sub Bytes

each byte (ai,j) of matrix is replaced with a sub byte (si,j), that is Rijindeal S-box.

4.1.2 Shift Rows-Shift each row with certain constraint. That is first row of matrix is left same, the second, third, fourth rows are shifted to one place left.

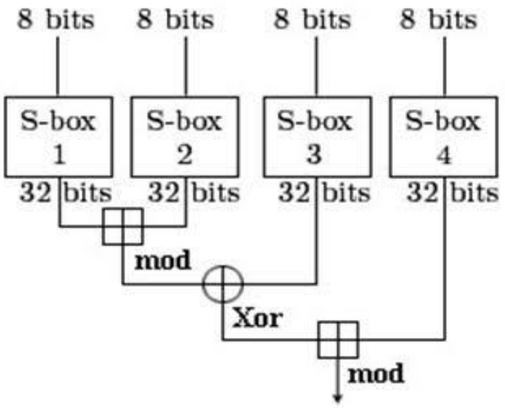
4.1.3 Mix Columns-The each column is multiplied with a fixed polynomial and the new value of the columns is placed.

4.1.4 Add Round Key- This sub key is derived from the main key and the sub key is added into this step by applying XOR to the matrix.



4.2 Blowfish

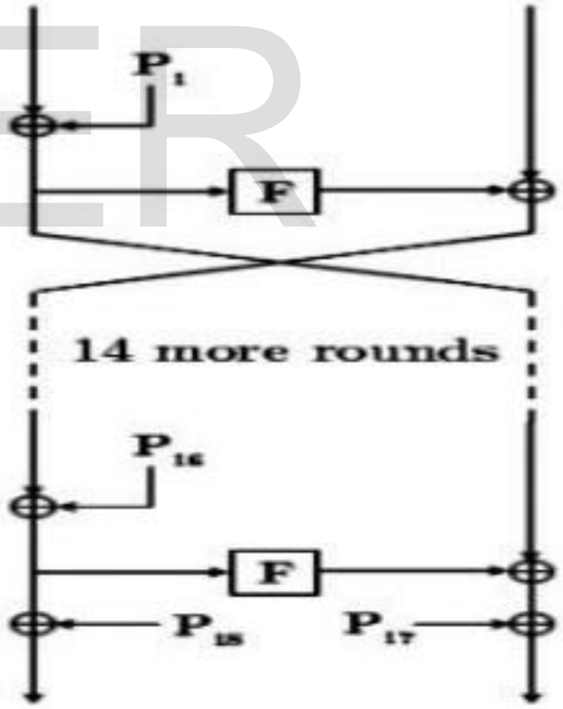
Blowfish is a symmetric block cipher algorithm for encryption and decryption. It is 64-bit block cipher. It optimized for 32-bit processors with large data caches, it is faster than DES. It takes a variable-length key, from 32 bits to 448 bits, making it for securing data. This algorithm is designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It is a 16-roound Feistel cipher and uses large key-dependent S-boxes. This S-boxes has 8-bit input and to produce 32-bit output. The merits of this algorithm is secure and easy to implement but the demerit is requires more space for cipher text because of difference in key size and block size.



Blowfish Function F

The Blowfish encryption algorithm steps are as follows:

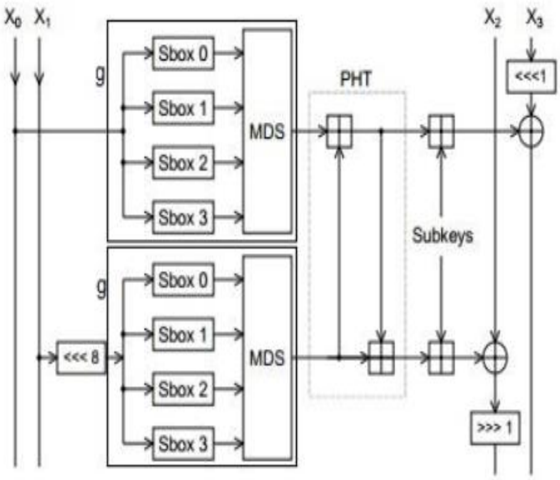
- X is 64 bit input data
- X is divided into two equal parts x1 and x2
- for i=0 to 15
- x1=x1 XOR pi
- x2=f(x1)XOR x2
- swap x1 and x2
- swap x1 and x2(undo the previous swap)
- x1=x2 XOR P18
- x2=x2 XOR P17
- Combine x1 and x2.



Blowfish procedure

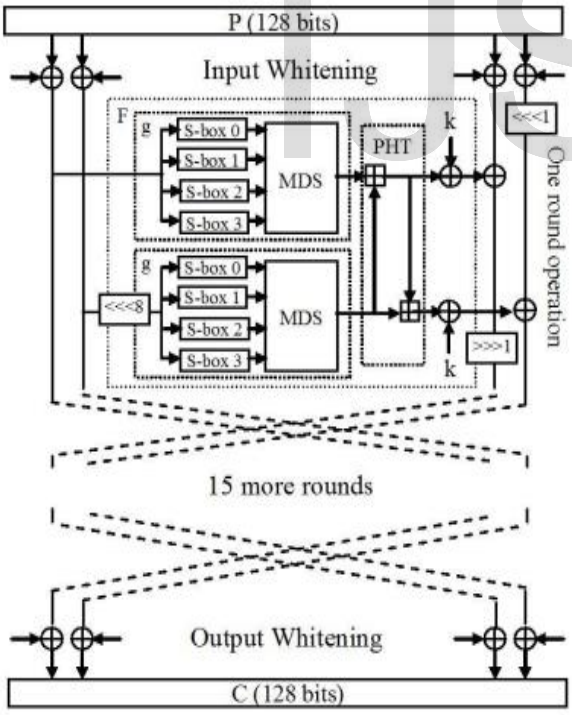
4.3 Two fish

Two fish is a symmetric block cipher encryption algorithm, derived from Blowfish. It uses 128 bit block size and key size is 128, 192, 256 bits. It is designed to be highly secure and highly flexible. The feature of two fish is key-dependent S-boxes and complex key schedule. The key is dividing into two halves; one half of the key is used as actual encryption key, and the other key is used to modify the encryption algorithm. In Two fish the number of processing round is same as Blowfish.



Two fish function

The Two fish encryption algorithm steps as follow as:X0 and X1 on the left the inputs to the g functions after the rotation by 8bits of one of them.The g function consists of 4 byte key-dependent S-boxes follow by a linear mixing step.The result of the two g functions are combined using a PHT(Pseudo-Hadamard Transform).After that two keywords are added. One right among them is rotated by one bit and then both of these keywords are XORed into the result on the left.For next round, right and left halves swapped.

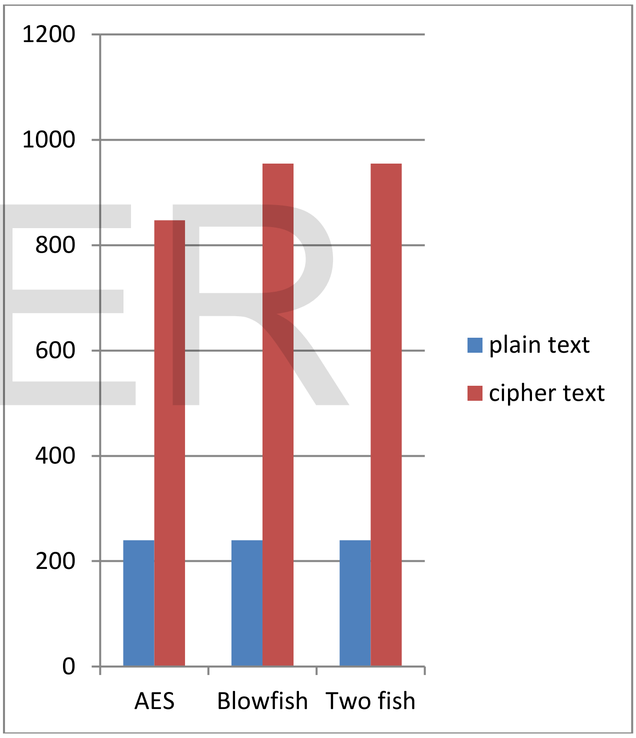


Two fish procedure

5 EXPERIMENT AND RESULT ANALYSIS

By using these three encryption algorithm of AES, Blowfish and Two fish is to encrypt the 240KB of data (plain text). The result is shown below:

Algorithm	AES	Blowfish	Two fish
Original text	240KB	240KB	240KB
Cipher text	847KB	955KB	955KB
Plain text	240KB	240KB	240KB
Speed	Faster	Very fast	Fast
Space	Less than Blowfish and Two fish	More than AES	Same as Blowfish
Security	Excellent security	Highly secure	Secure



From the above result, the AES requires less space among these algorithms. Blowfish encryption algorithm consists maximum space than AES. Two fish encryption algorithm is similarly same space consists of Blowfish because the Two fish algorithm is derived from the Blowfish algorithm.

6 CONCLUSION

Cryptographic algorithms play a very important role in Network security. In this paper, we have analyzed three encryption algorithms: AES, Blowfish and Two fish. We discussed the basic design and performance issues of these three algorithms. In the above result, we have found AES is better than other algorithms. In future, the experiment is in various hardware and software environment to evaluate the performance of these algorithms.

REFERENCES

[1] Prof.MukundR.Joshi, RenukaAvinashKarkade "Network Security with Cryptography", January-2015

[2] Dr.SandeepTayal, Dr.Nipin Gupta, Dr.Pankaj Gupta, Deepak Goyal, Monika Goyal "A Review paper on Network Security and Cryptography"-2017

[3] Sonia Rani, Harpreet Kaur "Technical Survey on Cryptography Algorithms for Network Security", September-2016

[4] SaritaKumari "A research paper on Cryptography Encryption and Compression Techniques", April-2017

[5] ShyamNandan Kumar "Review on Network Security and Cryptography", March-2015

[6] DeepaliD.Rane "Superiority of Twofish over Blowfish"-2016

[7] RajdeepBhanot and Rahul Hans "A Review and Comparitive Analysis of Various Encryption Algorithms"-2015