International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Comparative Study of Security Algorithms

Mr. Sagar Yashwant Jadhav
Bharti Vidyapeeth Institute of Management and Information Technology,
CBD Belapur, Navi Mumbai, Maharashtra, India

ABSTRACT

At present, through internet lots of confidential data is send across the world and though it is confidential it needs protection from unauthorized person who will try to read that data so to protect the data from unauthorized person security algorithms are used through which the original data can be able to convert into encrypted format and only the legitimate person or receiver can be able to read that data after decrypting it. Algorithms which protect the data and maintain the privacy of data are called Cryptography Algorithms.

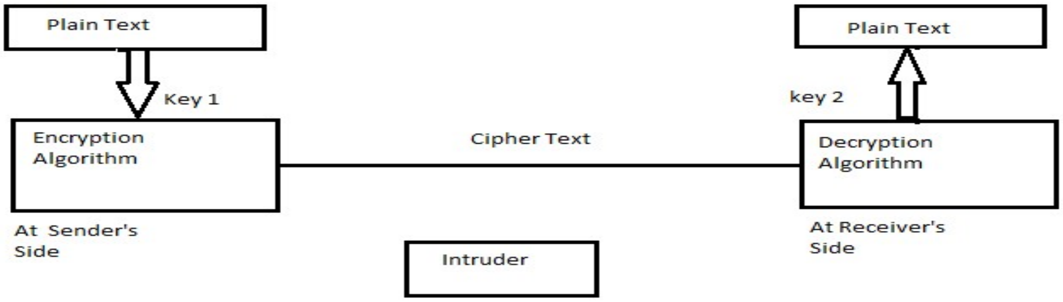
Cryptography has been very useful for sending the data safer over the internet. Comparative study of security algorithms means analyzing the better performance which has the low cost comparatively and analyzing which is the widely used algorithm through which we can able to understand the best algorithm for secure transmission. [2]

Keywords: *Cryptography, Encryption, Decryption, Symmetric Algorithms, Asymmetric Algorithms, DES, 3DES, Blowfish, RSA.*

INTRODUCTION

Cryptography does the hiding of data so that it cannot be accessible to the intruder but only the authorized person who have the access to the information. Data Encryption Standard(DES), Triple Data Encryption Standard(3DES), Rivest Shamer Adlemen(RSA) and Blowfish are the types of cryptography algorithms.

Working Overview:



In Cryptography the plain text is the actual data or information the sender wants to send to the receiver through the help of encryption algorithm the plain text and the key 1(no of characters) are taken as an input and cipher text is produced. Cipher text is nothing but the data to be send which is in encrypted format. Similarly, at the receiver side the receiver will be provided by key 2 for the decryption by taking the cipher text and receiver key as input and produces the plain text as output. Both the keys used are secret so be kept secured otherwise one can steal it and read the data in between transmission.

In this both the keys 1 & 2 are same therefore it is called symmetric key algorithm. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Blowfish are examples of symmetric key algorithm. [2]

Data Encryption Standard(DES)

1. Data Encryption Standard is a type of symmetric key encryption technique published in1977 and updated in 1993.
2. DES encodes plain text of 64 bit using 56 bit key.
3. DES consists of two permutation steps in which all 64 bits are permuted and 16 rounds are used by DES.
4. The operation in each round is identical taking the output of previous round as input.
5. After doing all this cipher text is obtained by the XOR operation.
6. Decryption works by reversing the algorithm’s operation.[1]

Triple Data Encryption Standard(3DES)

1. Triple Data Encryption Standard(3DES) is also a type of symmetric key encryption technique.
2. 3DES also encodes the plain text of 64 bits with 56 bits of key length.
3. Compare to DES the 3DES is more secure.
4. It performs the same DES algorithm but three times to each block.
5. The same XOR operation is performed for obtaining the cipher text. Decryption is done by reversing the operations of algorithm.[1]

Blowfish Encryption Technique

1. Blowfish algorithm is third type of symmetric key encryption technique. Blowfish is designed in 1993 by Bruce Schneier.
2. Blowfish uses key sizes from 32 to 448 bits for block size of 64 bits.
3. Blowfish also uses 16 rounds for encryption. Blowfish was developed for faster encryption of data.
4. Blowfish is used in many applications but later blowfish got a successor named Twofish.
5. Blowfish consists of two phase, In first phase key expansion is done. 448 bit key is converted into number of sub keys totalling 4168 bytes.
6. In second phase encryption is done. The function is executed 16 times and encrypted text is obtained by performing XOR operation.

Rivest Shamir Adlemen (RSA)

1. RSA is the type of asymmetric key encryption technique it means the keys used for this are not similar.
2. Asymmetric key uses different key such as public key and private key for encryption.
3. The sender encrypts the plain text and obtain the cipher text by public key which is visible to everyone.
4. The receiver decrypts the cipher text with the private key which is only known to the receiver. RSA is the best algorithm of asymmetric key encryption type.
5. RSA use C = M^E mod(n) Formula for calculating the cipher text. RSA use P = M^D mod(n) Formula for calculating the plain text. Where E and D are the public and private keys and n is the value obtained through mathematical operations in RSA.[2]

CONCLUSION:

Each encryption technique is best at their time also has strong and weak points to look out. DES is the encryption technique which was developed for encryption but it gives less security to the data which is overcome by 3DES encryption technique which runs 3 times and gives more security to the data compare to DES which is required for transmission. Blowfish has small requirement of memory and it gives faster encrypted data which is also well secured. RSA requires more memory compare to Blowfish but it is also good algorithm of asymmetric type encryption. Though Blowfish requires less memory it can used for applications which has small memory such as embedded applications. [2]

REFERENCES

1. W. Stallings, Cryptography and Network Security.
2. Pradeep Senwal and M K Sharma, “ Comparative study of different algorithms”.