ISSN:2249-5789
E Surya et al , International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477

A Survey on Symmetric Key Encryption Algorithms

E. Surya
Research Scholar
DR.G.R.D College of Science
Coimbatore.
suryaelango89@gmail.com

C.Diviya
Assistant professor
DR.G.R.D College of Science
Coimbatore.
mercy_twin@yahoo.com

Abstract

Security is the most challenging aspects in the internet and network applications. Internet and network applications are growing fast. So the importance and the value of the exchanged data over the internet or other media types are increasing. The better solution to offer the necessary protection against the data intruders is cryptography. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form by using Encryption and Decryption Techniques. The Cryptography ensures that the message should be sent without any alternations and only the authorized person can be able to open and read the message. A numbers of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography-Symmetric and Asymmetric. This paper presents a detailed study of the symmetric encryption techniques over each other.

Keywords: *Cryptography, Encryption, Decryption, AES, DES, TRIPLEDES, Blowfish.*

1. Introduction

Cryptography[1] is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from reader and only the intended recipient will be able to convert it into original text. Its main goal is to keep the data secure from unauthorized access. Data can be read and understood without any special measures is called plaintext. The method of disguising plaintext in such a way as to hide its substances is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext.The process of reverting cipher text to its original plaintext is called decryption. A system provides encryption and decryption is called cryptosystems. Cryptography provides number of security goals to ensure the privacy of data, on-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

1.1. Confidentiality

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

1.2. Authentication

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

1.3. Data Integrity

Ensuring the information has not been altered by unauthorized or unknown that means no one in between the sender and receiver are allowed to alter the given message.

1.4. Non Repudiation

Prevents either sender or receiver from denying a message. Thus when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received the message.

1.5. Access Control

Only the authorized parties are able to access the given information.

2. Overview of Algorithms

Brief definitions of the most common encryption techniques are given as follows:

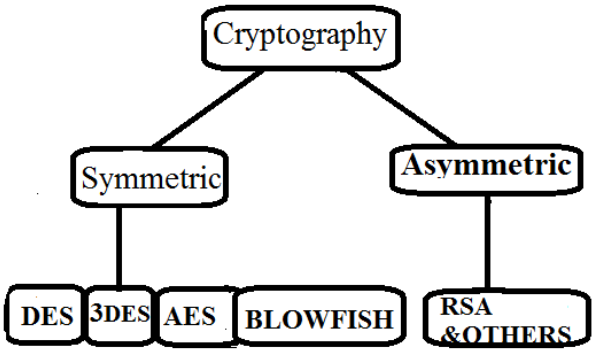

Fig.1.Classification of cryptography

The symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively. There are various symmetric key algorithms such as DES, TRIPLEDES, AES, and BLOWFISH.

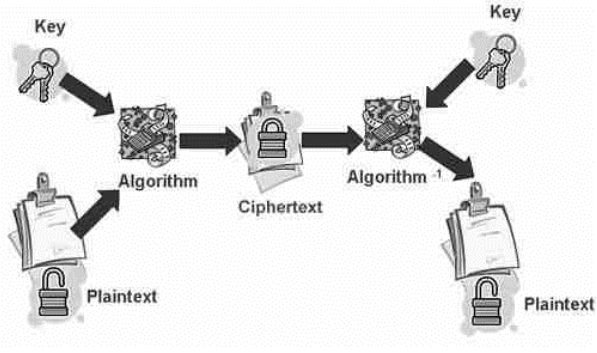

Fig.2.Symmetric key encryption

2.1. Data Encryption Standard (DES)

DES was the first encryption standards to be published by NIST[2] (National Institute of Standards and Technology).It was designed by IBM based on their Lucifer Cipher. Initially,56 bits of the key are selected from the initial 64 by permuted choice(1).the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves, each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected by permuted choice(2),24 bits from the left half and 24 from the right. The key schedule for decryption is similar, the sub keys are in reverse order compared to encryption.

2.2. Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher published by National Institute of Standards and Technology (NIST) in December 2001.AES is a non-Feistel cipher[5] that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size which can be 128,192, or 256 bits, depends on the number of rounds. If both block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are 192 bits, AES will perform 11 processing rounds. If the block and key are 256 bits, then it performs 13 processing rounds. Each processing rounds involves four steps:

- Substitute bytes: Uses an S-box to perform a byte by byte substitution of the block.
- Shift rows: A simple permutation.
- Mix column: A substitution method where data in each column from the shift row is multiplied by the algorithm's matrix.
- Add round key: The key for the processing round is XORed with the data.

2.3. Triple DES

In cryptography, TRIPLE DES[3] is the common name for Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks. It takes three 64-bit keys, for an overall key length of 192 bits. In Triple DES the data is encrypted with the first key, decrypted with the second key, and finally encrypted with the third key. Triple DES runs three times slower than DES, but it much more secure. The procedure for decrypting is the same as the procedure for encryption, except it is executed in reverse.

2.4. Blowfish

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993[2] by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and key can be any length up to 448 bits. It is

significantly faster than most encryption algorithms when implemented on 32- bit microprocessors with large data caches. The algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub keys arrays totaling 4168 bytes.

3 Comparison of Symmetric key Algorithms

Table 1. Comparison table

Factors	***AES***	***3DES***	***DES***	***BLOW FISH***
Key length	128,192, 256	K1,k2,k3 168 bits	56 bits	32-448 bits(128 by default)
Cipher type	Symmetric block cipher	Symmetric	Symmetric	Symmetric
Block size	128,192, 256	64	64	64
Created by	Joan Daemen &Vincent Rijmen in 1998	IBM in 1978	IBM in 1975	Bruce Schneier in 1993
Possible Keys	2^128, 2^192 2^256	2^112 or 2^168	2^56	2^32 to 2^448
Algorithm Structure	Substitution Permutation Network	Fiestel Network	Fiestel Network	Fiestel Network
Rounds	9,11,13	48	16	16
Effectiveness	Effective in Both S/W & H/W	Slow especially in S/W	Slow	Efficient in S/W
Attacks	Side channel Attacks	Theoretically possible	Brute Force Attack	Not Yet

4. Conclusions

This paper gives a detailed study of the symmetric key encryption algorithms like AES, DES, TRIPLEDES and BLOWFISH. Among those algorithms the Blowfish algorithm uses a variable number of bits ranging from 32 to 448 bits and encrypts the data 16 times. So it is impossible for a hacker to decrypt it.

5. References

[1] W. Stallings, Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009.
[2] Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.
[3] Singh, S preet, and Maini, Raman "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communication,vol.2,No.1,January-June 2011,pp.125-127.A.
[4] Atul khate, Cryptography and Network Security, 2nd Ed, Tata Mcgraw hill, 2009, pp.87-2004.
[5] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology vol.3,No.12,December 2012.