OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Survey on Symmetric Key Cryptographic Algorithms

[1]Sabitha S
Assistant Professor, Department of Information Technology, K R Gouri Amma College of Engineering, Alappuzha, Kerala, India.
[2]Binitha V Nair
Assistant Professor, Department of Computer Science & Engg., K R Gouri Amma College of Engineering, Alappuzha, Kerala, India.

ABSTRACT : Information is needed in every aspect of our life. So it is needed to be secured. To be secured, information needs to be protected from unauthorized access, unauthorized alterations and should be available to authorized entity when needed. Cryptography is an essential and effective method to secure these information's. There are several cryptographic algorithms that provide more security, accuracy and efficiency. In this paper, certain symmetric key encryption algorithms such as DES, 3DES, IDEA, AES and blowfish, their security aspects and the processes involved in design and implementation of these algorithms are examined.
Keywords – Cryptography, DES, 3DES, IDEA, AES and blowfish

Date of Submission: 28-02-2020 Date of acceptance: 08-03-2020

I. INTRODUCTION

Security plays an important role in transmitting and storing information. Secure communication is the basic requirement of transaction through any network. The three major goals of security are confidentiality (protecting data from unauthorized access), data integrity (protecting data from unauthorized modifications) and availability (information must be available to authorized entities when needed). Cryptography is the science and art of transforming messages or information to make them secure and immune to attacks. There are various cryptographic algorithms that use different mathematical processes. Right selection of the algorithm is important to achieve high security and to prevent cryptanalytic attacks. According to Kerckhoff's principle [1], all the crypto algorithms must be public, only the keys are secret. The two basic building blocks of all the encryption techniques are – substitution ciphers (replaces one symbol with another) and transposition ciphers (changes the location of the symbols).

A. Basic terms used in cryptography

- Plaintext – The original message that is to be transmitted between the two communicating parties.
- Ciphertext – The message that cannot be understood by anyone.
- Encryption – The process of converting plaintext to cipher text.
- Decryption – The process of converting ciphertext to plaintext.
- Key – key may be numeric, alphanumeric text or may be a special symbol that is used for encryption and decryption.

B. Classification of cryptographic algorithms

Cryptographic algorithms can be divided into two main categories – keyed cryptosystem and keyless cryptosystem [2]. In keyless cryptosystem, the plaintext and cipher text exclusively depends on the cryptographic algorithm. Anyone who has access to the algorithm can decrypt the message. Therefore, keyless cryptosystem is less secure. In keyed cryptosystem, the plaintext and cipher text depends on the cryptographic algorithm and a secret key. The keyed cryptosystem can be divided into two broad categories – Symmetric key (secret key) encryption and asymmetric (public key) encryption.

- Symmetric Key Encryption / secret key cryptography

The symmetric key encryption uses the same secret key for both encryption and decryption. The strength of the encryption scheme depends on the secrecy of the shared secret key. Symmetric ciphers can be classified in to two – stream cipher and block cipher. In stream cipher the encryption and decryption are done typically on one symbol at a time whereas in block ciphers, a group of plaintext symbols are encrypted together creating a group of ciphertext of the same size. Additive cipher, Vigenere cipher, Mono-alphabetic substitution cipher etc. are the examples of stream ciphers. Playfair cipher and Hill cipher are the examples of block ciphers.Examples of symmetric key encryption algorithm are DES [3], 3DES [2], IDEA [1], Blowfish [8], AES [4] etc.

- Asymmetric Key Encryption / Public Key Cryptography

  Here different keys are employed for encryption and decryption. A public key is used for encryption and a private key or a secret key is used for decryption. The most common public key algorithm is the RSA algorithm[10] which uses variable key size and is used for key exchange, digital signatures and encryption of small blocks of data.

C. Properties of Ciphers

- Diffusion – hides the relationship between the ciphertext and the plaintext.
- Confusion – hides the relationship between the ciphertext and the key.

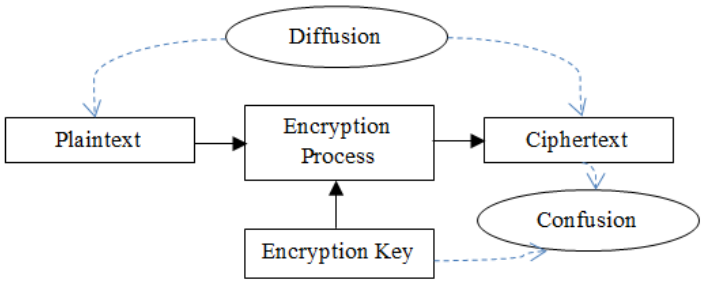

Figure 1. Relationship between Diffusion and Confusion

D. Evaluation Parameters

- Encryption time - It is the time required to convert the plaintext to ciphertext and is measured in milliseconds. It should be minimum.
- Decryption time - It is the time required to convert the ciphertext to plaintext and is measured in milliseconds. It should be minimum.
- Memory - memory requirements should be less as it affects the cost.
- Avalanche effect – a small change in plaintext or key should create a significant change in the cipher text.
- Entropy – measure of how unpredictable something is.

II. OVERVIEW OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

This section explains a review of the existing symmetric key cryptographic algorithms.

A. DATA ENCRYPTION STANDARD(DES)

DES is a block cipher algorithm which encrypts 64-bit plaintext block using 56-bit key. It processes the 64-bit input with initial permutation, 16 Fiestel rounds, swapping and final permutation. The general structure of the algorithm is shown in figure 2.The DES algorithm is based on Fiestel function, f, which divides the input block into two halves. The function (f) is based on four sections – expansion permutation box, key mixing, a group of eight substitution boxes and a straight permutation box. The output after the 16 Fiestel rounds undergoes inverse permutation and the 64-bit ciphertext is obtained. The Key generation process of DES involves straight permutation of 64-bit key to 56-bit cipher key. The key is then divided into two 28-bit halves and each half is shifted left one or two bits to the left. The two parts are then combined and a compression D-box changes the 58-bits to 48-bits round key. DES is vulnerable to Brute Force attack using 2^{55} encryptions, linear cryptanalysis using 2^{43} pairs of known plaintext and differential cryptanalysis using 2^{47} chosen plaintexts or 2^{55} known plaintexts.

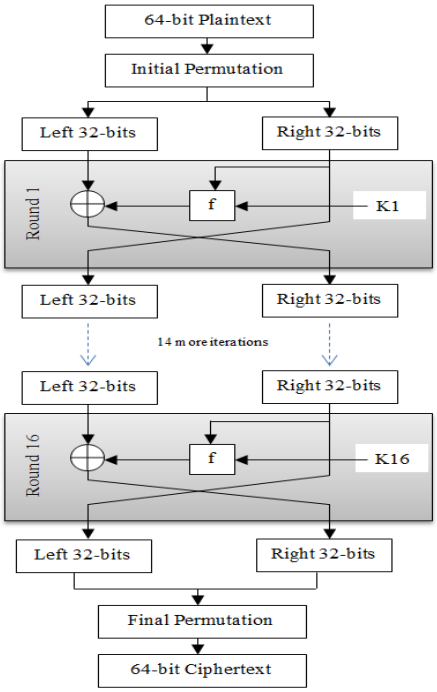

Figure 2. DES Encryption Process

B. TRIPLE DATA ENCRYPTION STANDARD (3DES)

Since DES is vulnerable to Brute Force attack, variations of DES called Multiple DES (2DES & 3DES) were introduced. In 3DES, triple encryption occurs using 2 or 3 keys. The key length of 3DES is 168-bits. There are 48 Fiestel rounds and the block size is 64-bits. 3DES is three times secure than DES as the key size is 2^{168} and thus it overcomes the vulnerability of brute force attack.

The encryption algorithm is given by, $C = Encrypt_{K3}(Decrypt_{K2}(Encrypt_{K1}(P)))$

The decryption algorithm is given by, $P = Decrypt_{K3}(Encrypt_{K2}(Decrypt_{K1}(P)))$

The major drawback of 3DES is that it takes more time for both encryption and decryption process.

C. INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)

IDEA is a symmetric key, Fiestel block cipher which was intended as a replacement of DES. The size of the plaintext is 64-bits which is divided into 4 blocks (P1, P2, P3and P4) of 16-bits each. It uses 128-bit key. It consists of 8 rounds and a half round (output transformation). Each round uses six 16-bit sub-keys, while the half round uses 4 sub-keys. Thus a total of 52 sub-keys (K1 to K52) are used in IDEA. The general structure of the algorithm is shown in figure 3. Operations needed in the first 8 rounds are multiplication modulo, addition modulo and bitwise XOR. Operations needed in output transformation are multiplication modulo and addition modulo.

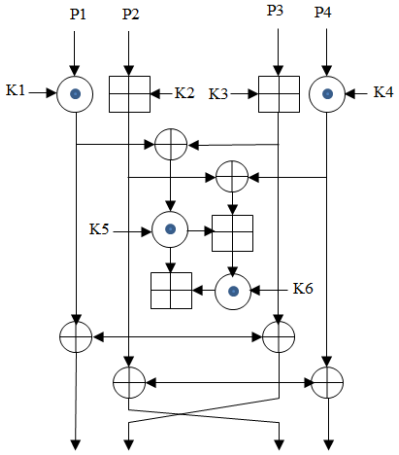

Figure 3. IDEA Encryption Process

D. ADVANCED ENCRYPTION STANDARD (AES)

AES is a symmetric key, non Fiestel, block cipher. AES is available in three versions – AES-128 (uses 128-bit key and 10 rounds), AES-192(uses 192-bit key and 12 rounds) and AES-256(uses 256-bit key and 14 rounds). AES operates on 128-bit block size. AES is 6 times faster than DES. The different AES parameters are based on key length is shown in the table.

Table I. AES Parameters

Key Size (bits)	Block Size (bits)	No. of Rounds	Round key size (bits)
128	128	10	128
192	128	12	128
256	128	14	128

The Encryption process in AES is shown in Figure 4.

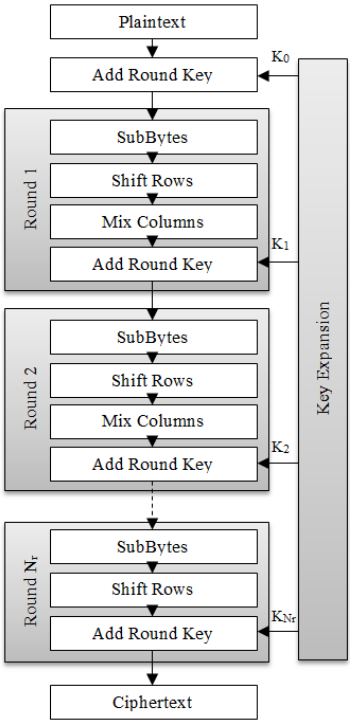

Figure 4. AES Encryption Process

The operations in each round are:

- SubBytes – Each byte of the block is replaced by its substitute in the substitution box (S-box).
- Shift Rows – Bytes in the last three rows are cyclically shifted to the left over different number of offsets.
- Mix Columns – Each column is multiplied with a known matrix. Multiplying by 1 means leaving unchanged, by 2 means shifting byte to the left and by 3 means shifting byte to the left and then performing XOR with the initial unshifted value.
- Add Round Key – XOR with the input data and the round key.

In the final round, the Mix Columns operation is not performed.
The decryption process involves Inverse SubBytes, Inverse Shift Rows, Inverse Mix Columns and Add Round Key.

E. BLOWFISH

Blowfish is a symmetric block cipher based on Fiestel function. It operates on 64-bit plaintext and uses variable key length which can be increased from 32 to 448-bits. It is faster than DES. The algorithm has two parts – round structure and key expansion function. There are 16 rounds, eighteen 32-bit sub keys and four S-Boxes each of which maps an 8-bit input to 32-bits. The Encryption process in Blowfish is shown in Figure 5.Let the input to F be x_L. Divide x_L into four 8-bit parts – a,b,c,d. Then the Fiestel function, F is given by,
$F[x_L] = ((S_1[a] + S_2[b] \bmod 2^{32}) \text{ XOR } S_3[c]) + S_4[d] \bmod 2^{32}$
Blowfish is used for applications like communication links or file encryptions.

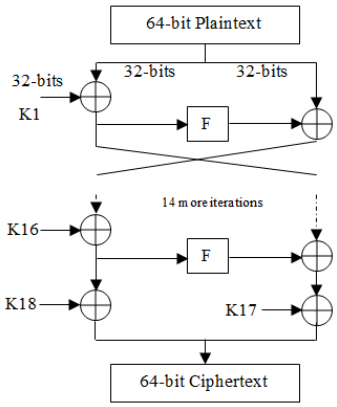

Figure 5. Blowfish Encryption Process

III. COMPARATIVE ANALYSIS

Table II. Comparative Analysis of Symmetric Key Algorithms

Algorithm / Parameters	DES	3DES	IDEA	AES	Blowfish
Developed by	IBM in 1975	IBM in 1978	James Massey in 1991	Joan Daeman & Vincent Rijmen in 1998	Bruce Schneiner in 1993
Algorithm Structure	Fiestel	Fiestel	Substitution - Permutation	Substitution - Permutation	Fiestel
Block size	64-bits	64-bits	64-bits	128-bits	64-bits
Key length	56 bits	168 bits	128 bits	128/192/256 bits	32 to 448 bits
No. of Rounds	16	48	8.5	10/12/14	16
Level of Security	Adequate security	Adequate security	Adequate security	Excellent Security	Excellent Security
Attacks	Brute force attack, Dictionary attack	Brute force attack, Known plaintext, Chosen plaintext	Meet-in-the middle attack, bicliques attack	Side channel attack	Dictionary attack

IV. CONCLUSION

In this paper, a review based on different symmetric key algorithms is presented. A detailed summary of algorithms such as DES, 3DES, IDEA, AES & Blowfish is analyzed. Each algorithm has different applications. According to research studies by various researchers, Blowfish and AES provide high security. Blowfish can be used in applications where encryption/decryption time is of major concern. AES can be used in applications where integrity and confidentiality is of major concern. Based on the survey, cryptanalysis attacks are possible on all these algorithms. So there is a need to develop more secure algorithm considering the different parameters affecting the algorithm.

REFERENCES

[1]. Behroz A. Forouzan, "Cryptography & Network Security", McGraw Hill Publication,2008, New Delhi.
[2]. W. Stallings, Cryptography and network security: principles and practices. Prentice Hall, 2005.
[3]. National Bureau of Standard. "Data Encryption Standard," Federal Information Processing Standards, NBS, 1977
[4]. N. I. of Standards-(NIST), Advanced Encryption Standard (AES). Federal Information Processing Standards Publication197, 2001.
[5]. W. Diffie and Y. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. 22, pp. 644-654, 1976.
[6]. "The Data Encryption Standard: Past and Future" by M.E. Smid and D.K. Branstad. Proc. of the IEEE, Vol. 76 No. 5 pp. 550-559, May 1988.
[7]. J. Daemen, V. Rijmen, and K. U. Leuven, AES Proposal: Rijndael. (NIST), National Institute of Standards, 1999.
[8]. B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," Proc. Fast Softw. Encryption Cambridge Secur. Work. Cambridge, U. K., pp. 191–204, 1994.
[9]. J. Daemen and V. Rijmen, the Design of Rijndael - The Advanced Encryption Standard. Springer-Verlag Berlin Heidelberg, New York, 2002.
[10]. S. Burnett and S. Paine, RSA Security's Official Guide to Cryptography. McGraw-Hill, 2001.