A STUDY ON DIFFERENT SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHM

Sumitra Samal
Asst. Professor,Department of Computer Science and Engineering (CSVTU), India
s.samal@ssipmt.com

Barkha Agrawal
Computer Science and Engineering (CSVTU), India
barkha.agrawal@ssipmt.com

Richa Parija
Computer Science and Engineering (CSVTU), India
richa.parija@ssipmt.com

Abstract – Cryptography is the art of transforming the information into unreadable or unintelligible format. Based on key, Cryptography is classified as symmetric key or asymmetric key. Since the use of internet has been increased over the last few years so the value of exchanged data has increased. Cryptography is one of the type of computer security that converts the data from normal form to coded form. The main task of cryptography is to increase the data confidentiality and security by hiding the information, so that it cannot be accessed by unauthorized user. This paper provides relative study of different symmetric key algorithms such as data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES) and blowfish.

Keywords – Cryptography, DES, 3DES, AES, Blowfish.

I. INTRODUCTION

With the rise in the use of Internet and network applications, need for protecting sensitive data has become important. Technique used to provide security is cryptography. Cryptography is the phenomenon of writing the data in the coded form so that it can be accessible only to the authorized user and no one else can access it. The whole phenomenon consists of two methods – encryption and decryption.

When the user defined input may in any of the format such as text, or an image which is plain, is converted into a scrambled or unintelligible form called as the cipher text or cipher image. This process is referred to as encryption. The reversible process in which the cipher text is converted in to the original form is called as the decryption process [1].

The data is said to be purely secure if it satisfies the main aspects of data security such as Authentication, Non Repudiation, Access Control, Confidentiality and Integrity of data [2]. The symmetric key cryptography is the method in which same key is used for performing the encryption and decryption [3].

Symmetric key algorithm requires lesser time for the execution. The symmetric key encryption modes are of two types: Block Cipher, Stream Cipher. Generally the block cipher is operated on a group of bits called blocks whereas stream cipher is operated on one bit at a time [3].

Generally key plays a very important role in hiding information. So, if weak key is used then anyone can easily access the data. The strength of the symmetric key depends upon the size of the key used. So longer keys are used, since they are hard to break as compare to the smaller key. Different algorithms uses different keys some of them are: AES(128,192,256 bit key), DES(64 bit key), Blowfish(32-448 bit key) [4-7].

In case of asymmetric key two key private key and public key are used. The public key of the receiver is used by the sender for encryption and receiver uses his private key for the decryption of the message. Various Algorithms are present to implement the asymmetric mechanism : RSA, Diffie Hellman and Digital Signature Algorithm [9]. Generally asymmetric key technique is slower than symmetric key technique, since it requires more computation processing power [8].

II. OVERVIEW OF ALGORITHMS

The overview of various symmetric key cryptography algorithms such as DES, 3DES, AES and Blowfish is as follows:

A. DES (Data Encryption Standard) –
DES was the first encryption standard which was developed by an IBM team around 1974. In 1977, it was adopted as a national standard.DES is a symmetric block cipher with 64-bit block size that uses a 56-bit key to encrypt and decrypt data. It takes a 64-bit block of plaintext as input and outputs a 64-bit

block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm [1]. It has 16 rounds, that means the algorithm is repeated 16 times to produce cipher text.

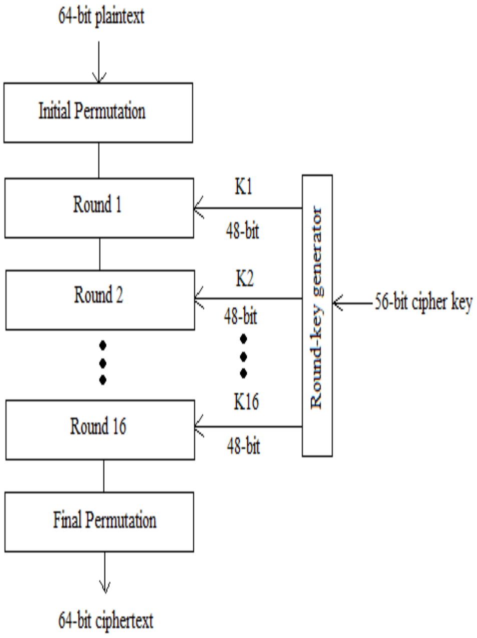

Fig. 1 DES Encryption Algorithm

B. 3DES (Triple Data Encryption Standard) –

Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. It uses as input 64-bit plaintext to produce 64-bit cipher text similar to DES. But unlike DES the combined key size is thus 192 bits with actually key size usage of 168 bits (three times 56) [2]. Triple DES is three times slower than DES, but it is much more secure than DES, as it applies the DES cipher algorithm 3 times to each data block.

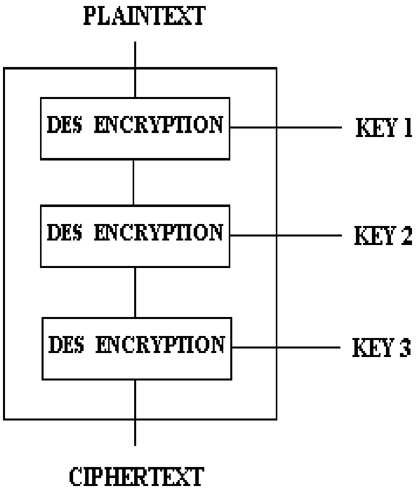

Fig. 2 Triple DES

C. AES (Advanced Encryption Standard) –

The two major problems faced by the earlier algorithms were the small key size (in case of DES algorithm) and slow speed (Triple des algorithm). To overcome these shortcomings; NIST (National Institute of Standards and Technology) published a new encryption algorithm known as AES (Advanced Encryption Standard). AES is a symmetric block cipher that has replaced DES for the wide range of applications [2]. It 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 [3]. AES algorithm: first substitute bytes, the shift the rows, then mixes column and finally add the round key.

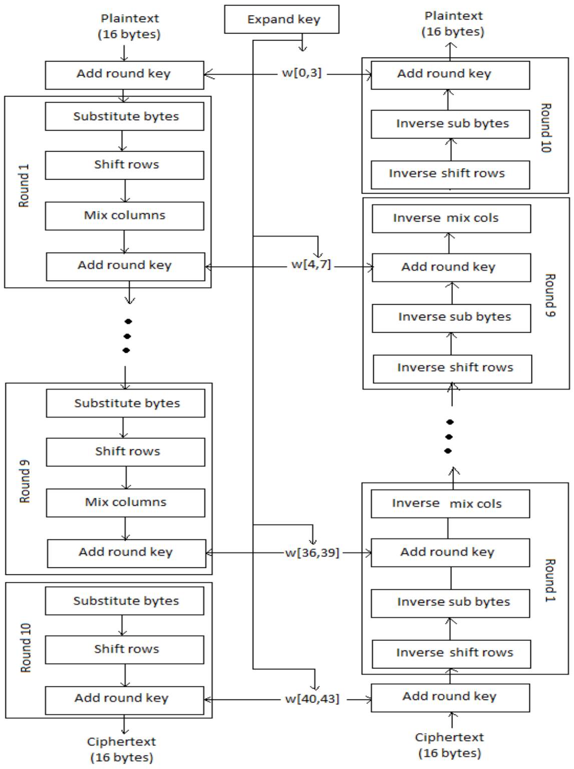

Fig. 3 AES Overview

D. *Blowfish –*

Blowfish was designed in 1993 by Bruce Schneier, as a fast alternative to existing encryption algorithms. Blowfish is a symmetric block cipher that can be effectively used for encryption. It takes a variable-length key from 32 bits to 448 bits, making it ideal for securing data [4]**.** Blowfish 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-key arrays totaling 4168 bytes. Data encryption occurs via a 16 round network. Each round consists of a key dependent permutation, and a key and data dependent substitution. All operations are XORs and additions on 32-bit word. The only additional operations are four indexed array data lookups per round [5].

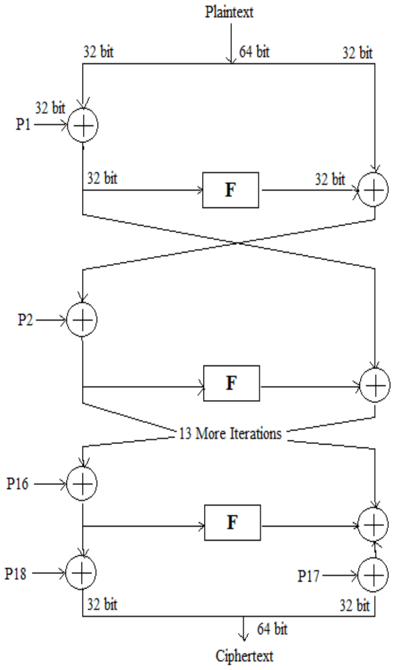

Fig. 4 Blowfish Architecture

III. COMPARISON OF DIFFERENT ALGORITHMS

The comparison of different symmetric key cryptographic algorithms DES, 3DES, AES and Blowfish is given in the following table.

TABLE I COMPARISON OF DIFFERENT SYMMETRIC CRYPTOGRAPHIC ALGORITHM

ALGORITHM METHOD	DES	3DES	AES	BLOWFISH
Year	1977	1978	1998	1993
Developed by	IBM	IBM	Joan Daemen, Vincent Rijmen.	Bruce Schneier.
Structure	Balanced Feistal Network.	Feistal Network.	Substitution & Permutation network.	Feistal Network.
Key Size (bits)	56 bits	112 bits, 168 bits	128 bits, 192 bits, 256 bits.	Variable key length, 32-448 bits.
Block Size (bits)	64	64	128	64
No. of Rounds	16	48	9	16
Efficiency	Slow	Relatively slow in software.	Efficient in both Software and Hardware.	Highly efficient in Software.
Vulnerabilities	Brute Force Attacks, Linear and Differential Cryptanalysis.	Some theoretical attacks.	Side Channel Attack.	Not prone to attacks.
Cipher Type	Block Cipher	Block Cipher	Block Cipher	Block Cipher
Speed	Fast	Moderate	Fast	Very Fast
Memory Usage	High	Very High	Medium	Very Low

IV. CONCLUSION

In this paper, Cryptography concept has been explained, mainly the cryptography techniques are of two types: Symmetric and Asymmetric. Symmetric algorithm[10-11] uses same key for performing the encryption and decryption while asymmetric algorithm uses different keys for performing encryption and decryption. The Symmetric and Asymmetric key algorithms both are highly efficient for securing the data over any communication medium. In this paper we have done the comparison between various symmetric algorithm such as DES, 3DES, AES, Blowfish and after the comparison we have concluded that AES is the best among algorithm DES, 3DES for various parameters like speed, efficiency, memory usage. In terms of security also AES is the best among the other three algorithms. Blowfish is though little bit fast but is weaker than the AES, so AES is the best among all the Symmetric key algorithms.

ACKNOWLEDGEMENT

The authors are grateful to Mrs. Sumitra Samal Assistant professor Department of Computer Science and Engineering, Shri Shankaracharya Institute of Proffessional Management and Technology (SSIPMT), Raipur for time to time guidance.

REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, “COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHM”, International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012.

[2] Shaify Kansal, Meenakshi Mittal, “Performance Evaluation of various Symmetric Encryption Algorithms”, International Conference on Parallel, Distributed and Grid Computing 2014.

[3] Vishal R. Pancholi, Dr Bhadresh P. Patel, “Cryptography: Comparative Studies of Different Symmetric Algorithms”, International Journal of Technology and Science, Vol. VI, Issue I, 2015 pp 4-7.

[4] Jawahar Thakur, Nagesh Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 1, Issue 2, December 2011.

[5] Tingyuan Nie, Chuanwang Song, Xulong Zhi, “Performance Evaluation of DES and Blowfish Algorithm”, IEEE.

[6] Pushpendra Verma, Dr Jayant Shekhar, Preety, Amit Asthana, “A Survey for Performance Analysis Various Cryptography Techniques Digital Contents”, International Journal of Computer Science and Mobile Computing, ISSN 2320-038X, Vol. 4, Issue 1, January 2015, pg 522-531.

[7] E.Thambiraja, G.Ramesh, Dr R.Umarani, “A Survey on Various Most Common Encryption Technique”, International Journal of Advance Research in Computer Science and Software Engineering, ISSN 2277 128X, Vol. 2, Issue 7, July 2012.

[8] Dr Jyotiprakash Patra “An LSB Method Of Image Steganographic Techniques” Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 5, Issue 4, (Part -5) April 2015, pp.62-65

[9] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader, Mohie Mohamed Hadhoud, ”Performance Evaluation of Symmetric Encryption Algorithms”, International Journal of Computer Science and Network Security, Vol. 8 No. 12, December 2008.

[10] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Dr Goutam Sanyal, “A Comparative Survey of Symmetric and Assymetric Key Cryptography”, 2014 International Conference on Electronics, Communication and Computational Engineering.

[11] Monika Agrawal, Pradeep Mishra, “A Comparative Survey on Symmetric Key Encryption Techniques”, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882