Survey on Symmetric Key Cryptography

[1]Animesh Kumar, [2]Deepak Idnani, [3]Kaushal Soni, [4]Nitin Taneja,
[5]Rounak Shrivastava, [6]Prof. Sneha Ambhore
[1,2,3,4,5,6] *Ajeenkya D.Y Patil University, Lohegaon, Pune .*

***Abstract* -** The innovations in communication networks and computation in past years has led to huge amount of data flowing from one place to another. A lot of cryptographic algorithms have been invented and executed to keep the network of communication secure. But with gradually powerful computers progressing out every day, more and more complex systems are being built with reasonable data outlays to maximize security over the channel. So, in this survey paper, we have discussed about some of the symmetric-key cryptosystems: AES, DES, 3DES, IDEA, Blowfish and there features , this survey paper proposes a modified implementation of symmetric algorithm to enhance its security with a minimum computational trade-off.

***Keywords* -** Symmetric key cryptography , DES , 3DES , AES , Blowfish , IDEA

I. INTRODUCTION

In this Symmetric key cryptography we use of one key functions. In the terms of mathematic these functions are used to compute in one direction but it is very difficult to compute this in reverse directions. This is what allows user to publish user public key, which is derived from user private key. It is very difficult to work at backend and determine the private key. A common one key function used today is factoring large prime numbers.To get products it is easy to multiply two prime numbers.In data security cryptography play an important roles. It provides confidentiality and also maintains integrity between authorized users. Confidentiality, data integrity, entity authentication, and data authentication is used for the security purpose in the cryptography by using various mathematical techniques.Combination of key to encrypts the plaintext in cryptographic algorithm.

II. ALGORITHM DESCRIPTION

A. Data Encryption standard (DES) - DES is a symmetric key block cipher in which user use the same key for encryption and decryption. DES is given by NIST (National Institute of Standard Technology).Initially user has 64 – bit plain text as input. Initially user has 64 – bit key out of which 8 – bit used for equality check. User have 64 – bit plain text as input for converting plain text to cipher text and 56 – bit key is passed through the Round Key Generator and produce 48 – bit key for each round. Firstly 64 – bit key passes through the initial permautation after that there are 16 rounds, which mean 16 steps are being executed for converting plain text to cipher text. Each round is Feistel cipher and each round has a 48 – bit key. DES can be applied in CBC, ECB, CFB and OFB modes at the end final permautation is applied on the input plain text produces 64 – bit cipher text. The drawback of this algorithm is that it is not a secure algorithm because it is easy for hackers to attack this algorithm by brute force attack in which the hacker try to break the all possible keys total there are 2^56 keys possible keys.

Data Encryption Standard (DES) is a 16 round Feistel Cipher. It takes a input a 64-bit and 64-bit secret key and DES consist of 3 main platform:

1. Initial Permutation
2. Round Function
3. Final Permutation

Refer Fig1 for the block diagram of DES Algorithm

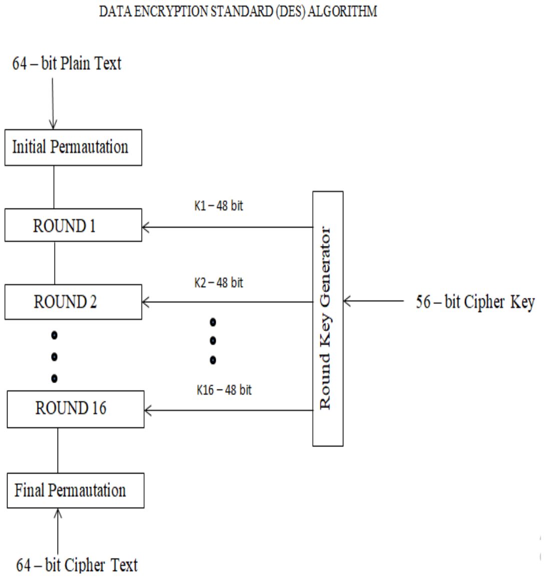


Figure 1 : DES

B. Triple Data Encryption Standard (3DES) - This algorithm also called TDA(Triple Data Algorithm) and applies cipher algorithm for Data Encryption Standard (DES) three times to each data block. The Overall length is 192 bits in Triple Des containing three blocks each block of length 64-bit. The Way for doing encryption in Triple DES is the same as we done in DES, but there is only one change in it that the algorithm is repeated three times, Because of this it is called Triple DES Algorithm. In this algorithm key is divided into three parts i.e. part k1,k2 and k3 respectifully.Now the original text is encrypted with the help of first key which is k1, decrypted with the help of second key i.e. key k2, and finally encrypted again with the third key i.e. key k3. Due to this Triple DES runs three times slower than DES, Also taking about security point of view Triple DES is more secure than DES. Out of 64 bits long the actual key length used in DES is only 56 bits in length. The right- Most bit is called the parity bit in each byte and get ignored.Due to ignoring of the last bits of every byte only seven bits is used and makes the key length of 56 bits.This means that the key length is actually used is of 168 bits. Refer Fig2 for the block diagram of 3DES Algorithm

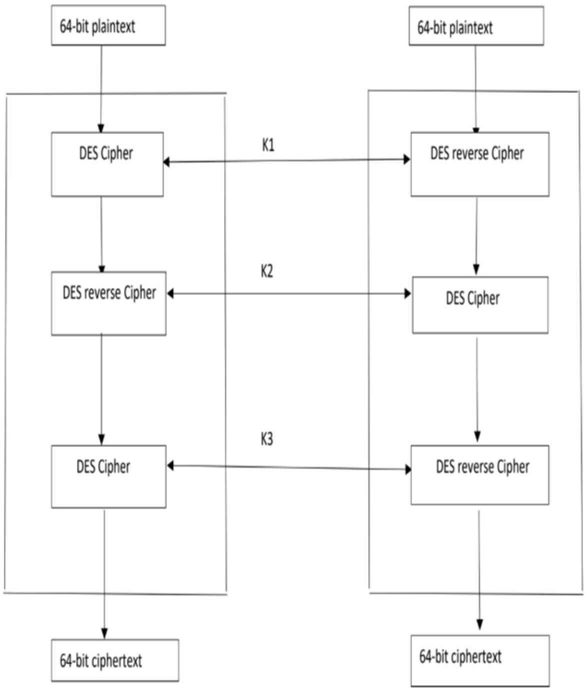


Figure 2: Triple Data Encryption Standard

C. IDEA - IDEA is fast and fairly secure and is strong to both differential and linear analysis. In public domain, it is one of the secure block ciphers, which is based on substitution-permutation concept . IDEA uses six 16-bit subkeys and half round uses four, a total of 52 of 8.5 rounds. IDEA under certain hypothesis is having a strong resistance against cryptanalysis. It uses multiple group operations, which increases the strength against most of the attacks. The 128-bit key size makes it one of the strong security algorithms. There is no weakness related to linear or algebraic attacks which have been reported yet .

Operation Idea operates on 64-bit block using a 128-bit key and it has 8 identical transformations and an output transformation. In this algorithm the processes for encryption and decryption are similar.

Key Schedule - The key is selected from the first 8 sub-keys, First round of k1 is being the lower 16 bit; further groups of 8 key are generated by rotating the main key left 25 bits between each group of 8 bits. That is circulate less than once per round, on an average of total 6 rotation.

Refer Fig3 for the block diagram of IDEA Algorithm

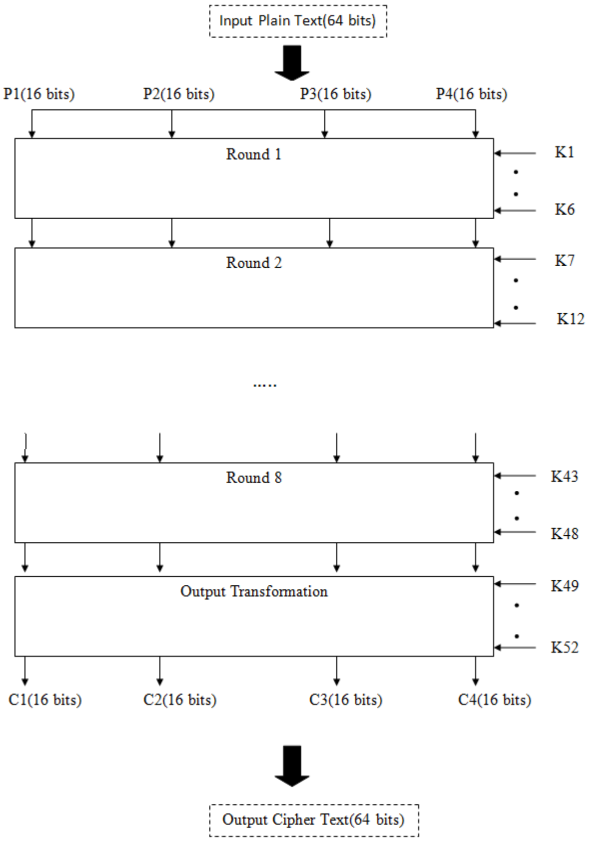


Figure 3: IDEA

D. Blow Fish - Blowfish is a symmetric key cipher, developed in 1993 by Mr. Bruce Schneier and combined in many cipher blocks and encryption products. Blowfish provides a good encryption rate in software and no effectual cryptanalysis of it has been enact to date. However, the Advanced Encryption Standard (AES) now receives more concern, and Schneier approves Twofish for modern applications.

Schneier developed Blowfish as a general-purpose algorithm, proposed as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were registered, delayed by patents or were commercial or government secrets. Schneier has declared that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is with this placed in the public domain and can be openly used by anyone.

Refer Fig4 for the block diagram of Blowfish Algorithm

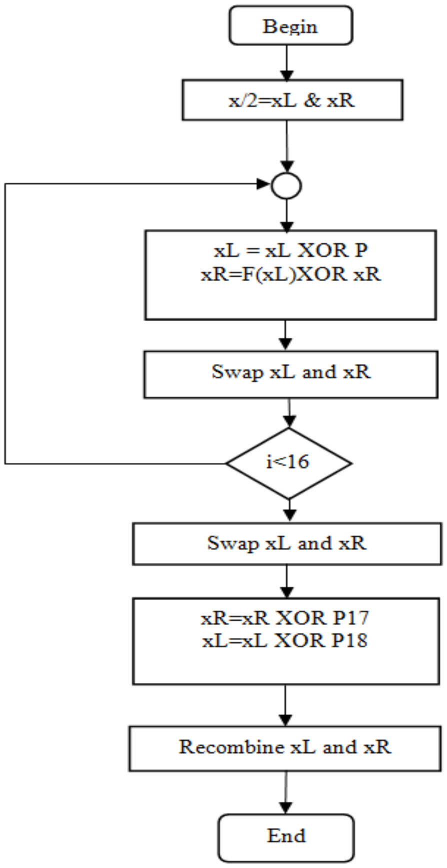


Figure 4: Blowfish

Algorithm - The F-function divides the 32bit input into four 8th bit quarters and uses the four equal parts as feed into the Sboxes. Sboxes accept 8bit input and generate 32bit output. The outputs are added modulo 2^{32} and XOR to generate the resultant 32bit output. On 16 completed round, again use the left swap, and XOR Left with K of 18 and R with K of 17. Decryption is almost the same as that of the encryption, except that P of 1, P of 2, …, P of 18 are used in the backward manner. This is that not so apparent because xor is changeable and integrative. A mutual wrong perception is to use opposite manner of encryption as in the place of decryption algorithm.

Blowfish's key schedule starts by starting the P array and also the Sboxes with numerals generated from the hexadecimal digits of , which contains none of the expected patterns. The protected key is now, byte to byte, repeating the key only if it is necessary, XOR it with all of the P entries in manner of one after other. A 64bit all the zero blocks are been encrypted with the algo it approaches. The generated ciphertext replace P_1 and P_2. The exact similar ciphertext then encrypted once more with the all new subkeys, and the all new ciphertext then takes place of P_3 and P_4. This continues, renew the whole P array and all of the entries of the Sboxes. In all, the Blowfish algorithm will be able to run for 521 times to give all new subkeys - about 4kilobytes of data being is processed.

E. Advance Encryption Standard (AES) - AES symmetric block cipher Feistel structure that means it uses the similar key for both encrypt and decrypt AES algorithm accepts a plain text of 128 bits and a choice of three 128, 192, 256 key length permuted with variable 10, 12, and 14 rounds. The variable nature of Rijndael provides it with a great security, and the key size up to 256 gives it a resistance to the future attacks.

AES algorithm is the most popular and widely used. According to survey it is said that AES algorithm is faster than 3DES Algorithm .

There was need in improvement in DES as its key sixe is too small . With increase in computing power , Triple DES was invented to overcome vulnerability against exhaustive key search attack but it was found slow.

The features of AES are as follows –

- block cipher
- 128-bit data has 10 rounds , 192 bits has 12 rounds , 256-bit has 14 rounds
- Secure than Triple-DES
- Provide full specification and design details .

Refer Fig5 for the block diagram of AES Algorithm

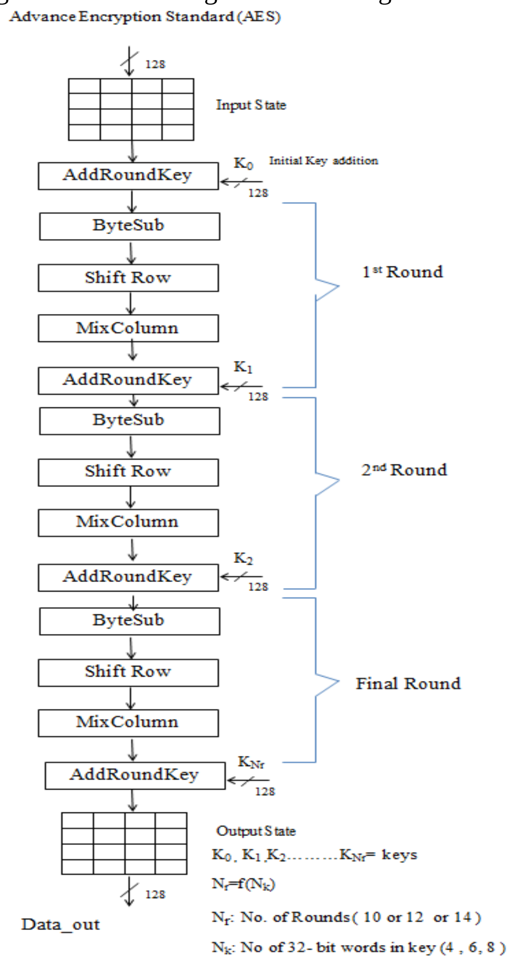
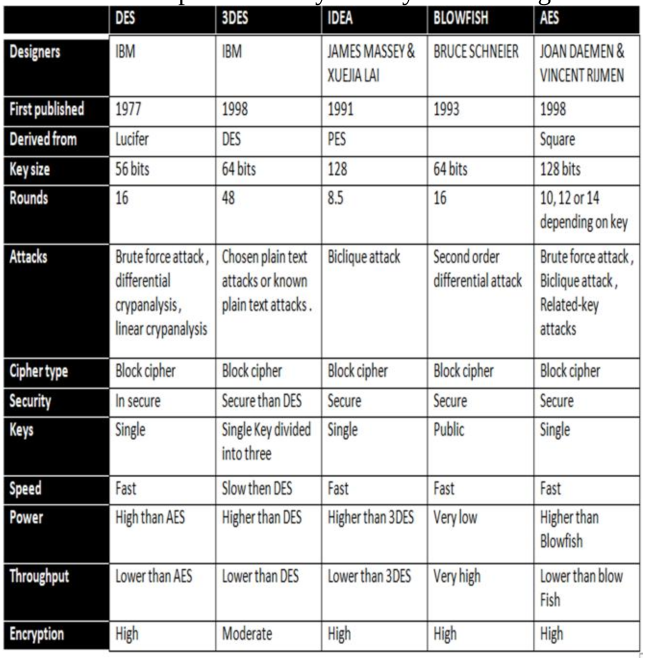


Figure 5: Advance Encryption Standard

III. COMPARATIVE ANALYSIS

Refer Table 1 for the comparative analysis of the symmetric algorithm

Table 1: Comparative analysis of symmetric Algorithm



	DES	3DES	IDEA	BLOWFISH	AES
Designers	IBM	IBM	JAMES MASSEY & XUEJIA LAI	BRUCE SCHNEIER	JOAN DAEMEN & VINCENT RIJMEN
First published	1977	1998	1991	1993	1998
Derived from	Lucifer	DES	PES		Square
Key size	56 bits	64 bits	128	64 bits	128 bits
Rounds	16	48	8.5	16	10, 12 or 14 depending on key
Attacks	Brute force attack , differential crypanalysis , linear crypanalysis	Chosen plain text attacks or known plain text attacks .	Biclique attack	Second order differential attack	Brute force attack , Biclique attack , Related-key attacks
Cipher type	Block cipher	Block cipher	Block cipher	Block cipher	Block cipher
Security	In secure	Secure than DES	Secure	Secure	Secure
Keys	Single	Single Key divided into three	Single	Public	Single
Speed	Fast	Slow then DES	Fast	Fast	Fast
Power	High than AES	Higher than DES	Higher than 3DES	Very low	Higher than Blowfish
Throughput	Lower than AES	Lower than DES	Lower than 3DES	Very high	Lower than blow Fish
Encryption	High	Moderate	High	High	High

IV. CONCLUSION AND FUTURE WORK

From the studies which user have surveyed considering security, such as DES , 3DES , Blowfish , IDEA , AES . The memory necessity of symmetric algorithm is lesser the asymmetric encryption algorithm and asymmetric algorithm runs slower than symmetric key algorithm also , symmetric key encryption provides more security than asymmetric key encryption.

V. REFERENCES

[1]. International Journal of Science Technology Management and Research Volume 3, Issue 6, June 2018 ISSN: 2456-0006

[2]. International Journal of Science Technology Management and Research

[3]. Volume 3, Issue 8, May 2018 ISSN (online): 2456-0006

[4]. Soft Computing: Theories and Applications pp 261-271 Part of the Advances in Intelligent *Systems* and Computing book series (AISC, volume 742)

[5]. Information Systems Design and Intelligent Applications pp 299-313 Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 862)

[6]. IEEE Proceedings 38th Annual Symposium on Foundations of Computer Science Print ISBN**:** 0-8186-8197-7 Print ISSN: 0272-5428 INSPEC Accession Number: 5816571

[7]. Introduction to Symmetric Cryptography María Naya-Plasencia HAL Id: hal-01953897 https://hal.inria.fr/hal-01953897 Submitted on 13 Dec 2018