International Journal of Advance Research in Science and Engineering
Volume No 06, Special Issue No. (02), September 2017, ICITTESE-17
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SURVEY PAPER ON CRYPTOGRAPHY

Harpreet Kaur, Vaishali Verma, Jaya Mishra

[1,2,3] *Computer Science &Engineering, Columbia Institute of Engineering & Technology, (India)*

ABSTRACT

In today's generation, each & every person uses the facility of internet. But, this may cause several problems related to our data confidentiality, integrity & authentication. People need to be sure that their internet communication is kept confidential. When they shop online; they need to be sure that the vendors are authentic. When they send their transactions request to their banks, they want to be certain that the integrity of the message is preserved.

To be secured, information needs to be hidden from unauthorized access, protected from unauthorized change, and available to an authorized entity when it is needed. Network security uses the concept of cryptography to encrypt & decrypt the important message. In this survey, we see the different algorithms of cryptography and analyze the best algorithm which provide high efficiency and encrypt the message in such a way which will not be understand by the intruders (hackers).

Keyword: - Encryption, AES, DES, 3DES, Blowfish.

I. INTRODUCTION

Nowadays**,** a lot of applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions takes place through wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability, also known as CIA triad [1].

Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on Cryptography (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack [2]. Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into cipher text (scrambled message after encryption). Many encryption algorithms are widely available and used in information security like AES, DES, 3DES etc.

II. LITERATURE SURVEY

Some of the concepts used in cryptography are as follows:

1.1 Cryptography

- Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text. It is understood by the sender, the recipient and also by anyone who gets an access to that message.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.
- Encryption: The process of encoding plain text messages into cipher text messages is called encryption.
- Decryption: The reverse process of transforming cipher text messages back to plain text is called as decryption.
- Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

2.2 Types of Cryptography

- Secret Key Cryptography:- When the same key is used for both encryption and decryption, DES, Triple DES, AES, RC5 and etc., may be the examples of such encryption, then that mechanism is known as secret key cryptography.

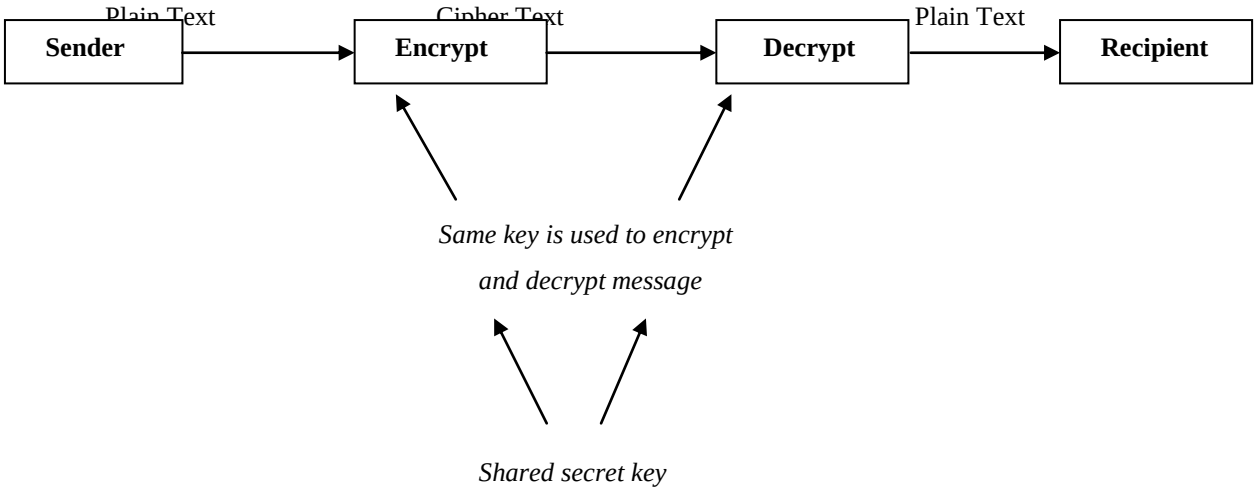

Fig:- 2 Secret Key Cryptography

- Public Key Cryptography:- When two different keys are used, that is one key for encryption and another key for decryption, RSA, Elliptic Curve and etc., may be the examples of such encryption, then that mechanism is known as public key cryptography.

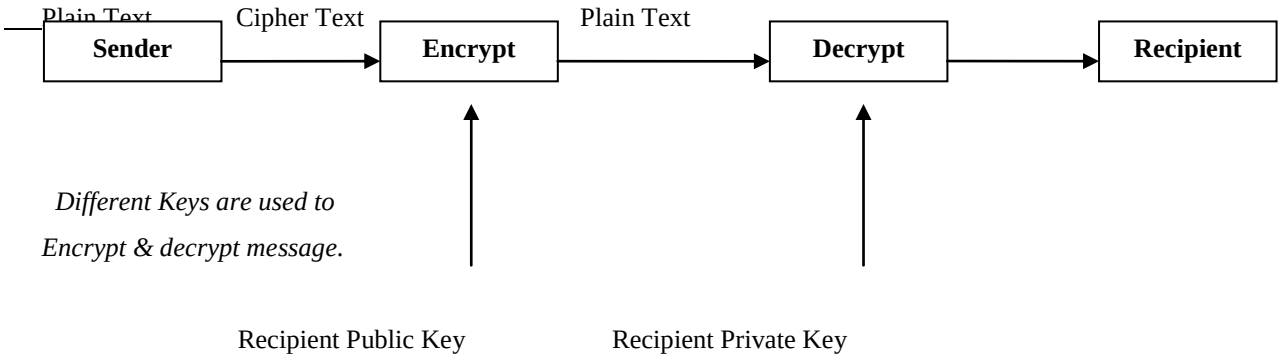

Fig: - 2 Public Key Cryptography

International Journal of Advance Research in Science and Engineering
Volume No 06, Special Issue No. (02), September 2017, ICITTESE-17
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

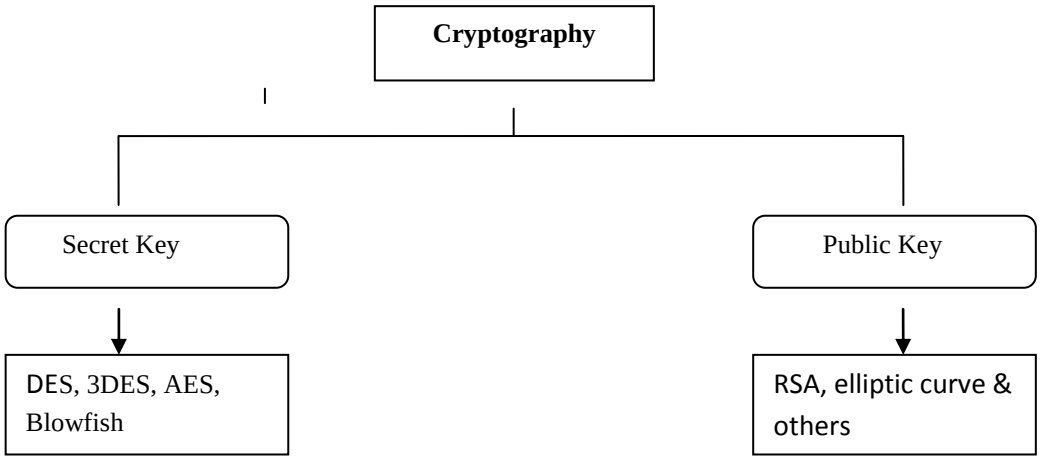

Fig 3:- Classification of cryptography

III. RELATED WORKS

3.1 DES (Data Standard Encryption)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key.

DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm as described by Davis R. [4] takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. In the case of DES, each block size is 64 bits. DES also uses a key of 56 bits to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt the message. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa).

The Broad level steps in DES are as follows [3]:

1. In the first step, the 64-bit plain text message is handed over to an Initial permutation (IP) function.
2. The initial permutation is performed on plain text.
3. The IP produces two halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now, each of LPT and RPT go through 16 rounds of encryption process.
5. In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
6. The result of this process produces 64-bit cipher text

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

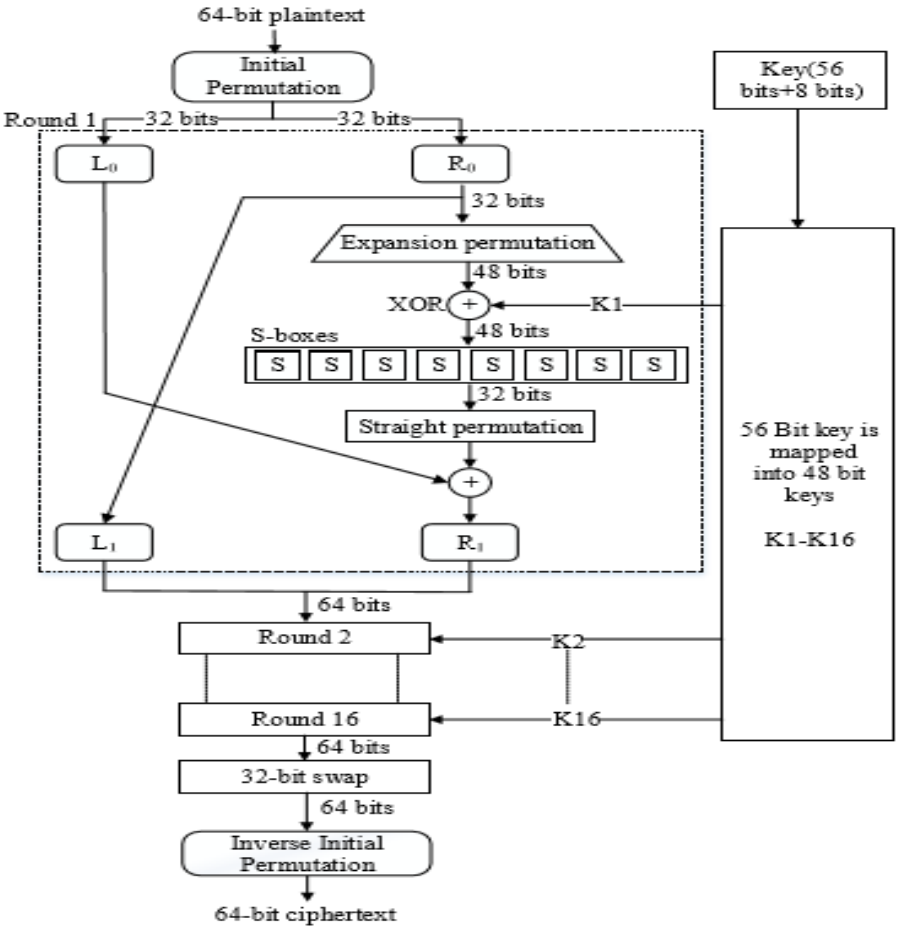

Fig:-4 General Description of DES

3.2 3DES (Triple DES)

Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt-Encrypt (EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message, t.

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (1)$$

Where C (t) is cipher text produced from plain text t, Ek1 is the encryption method using key k1 Dk2 is the decryption method using key K2 Ek3 is the encryption method using key k3 another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (2)$$

TDES algorithm with three keys requires 2^{168} possible combinations and with two keys requires 2^{112} combinations. It is practically not possible to try such a huge combination so TDES is a strongest encryption

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

algorithm. The disadvantage of this algorithm it is too time consuming.

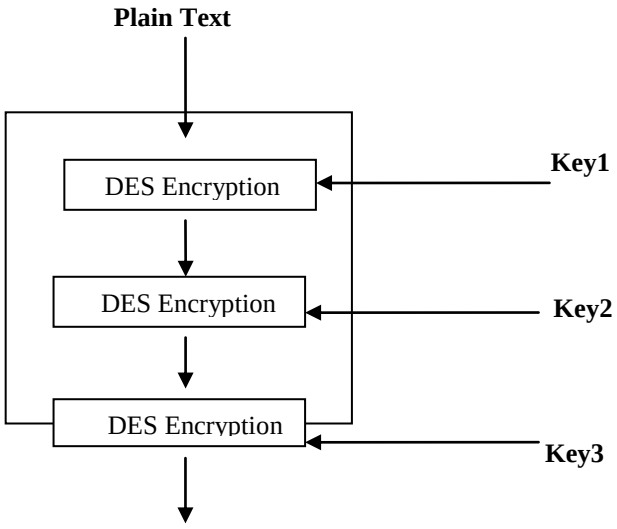

Fig:-4 Encryption in 3DES

3.3 AES (Advanced Encryption Standard)

The AES cipher [6] is almost identical to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. This algorithm is a symmetric-key algorithm, means that the same key is used for both encryption and decryption of the data. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128bit key is 10.

Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an entire block per iteration, e.g., in DES, 64/2 = 32 bits are encrypted in one round. AES, on the other hand, encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds.

AES Encryption [3]:

The encryption process in AES involves following steps:

(i) Do the one-time initialization process:

(a) Expand the 16-byte key to get the actual Key Block to be used.

(b) Do one time initialization of the 16-byte plain text block (called State).

(c) XOR the state with the key block

(ii) For each round do the following:

(a) Apply S-Box to each of the plain text bytes.

(b) Rotate row k of the plain text block (i.e. state) by k bytes.

(c) Perform mix columns operation. (d) XOR the state with the key block.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

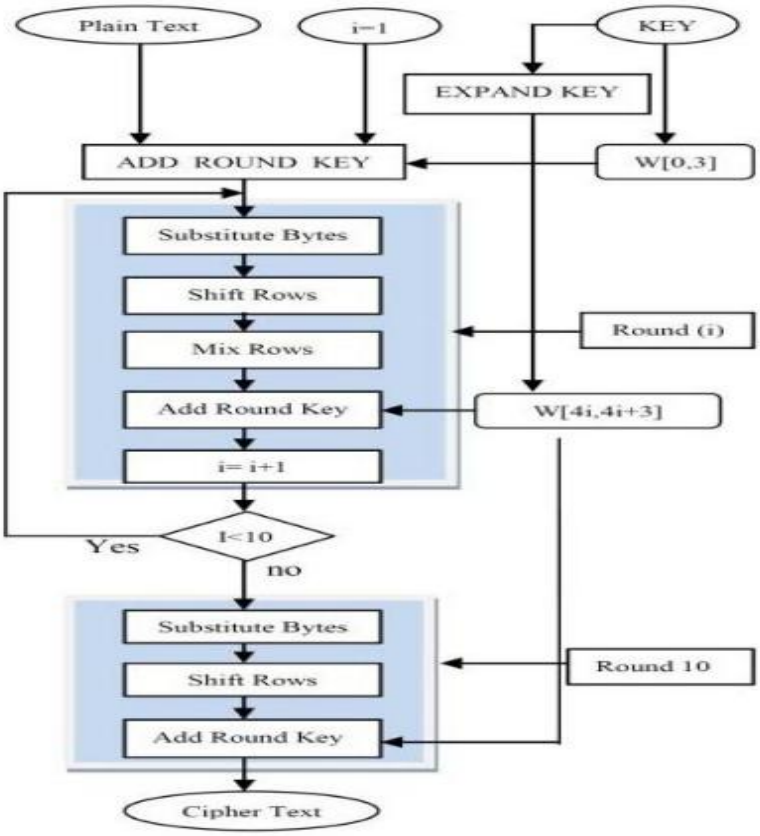

Fig 5:- Advanced Encryption Standard Process

3.4 Blowfish

Blowfish [5] is one of the most common public domain encryption algorithms provided by Bruce Schneier - one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. The Blowfish algorithm was first introduced in 1993.

Operation of Blowfish:

Blowfish encrypts 64-bit block cipher with variable length key. It contains two parts

- **Subkey Generation:** This process converts the key upto 448 bits long to Subkey to total 4168 bits.
- **Data Encryption:** This process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation and key- and data dependent substitution. Blowfish suits the applications where the key remain constant for a long time (e.g. communication link encryption) but not where the key changes frequently (e.g. packet switching).

VI. COMPARATIVE STUDY OF SECURITY ALGORITHM

Table1 shows the comparison between various security algorithms. After seeing the data in the comparison table we found that AES is more efficient, fast and secure algorithms among the others.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Table1. Comparison of Various Security Algorithms

Factors	DES	3DES	AES	Blowfish
Created By	IBM in 1975	IBM in 1978	Vincent Rijimen,Joan Daemen in 2001	Bruce Schneier in 1993
Round(s)	16	48	10, 12, 14	16
Key Length	56	168 or112	128,192 or 256	Variable length key (448-4168 bit)
Block Size	64	64	128	64

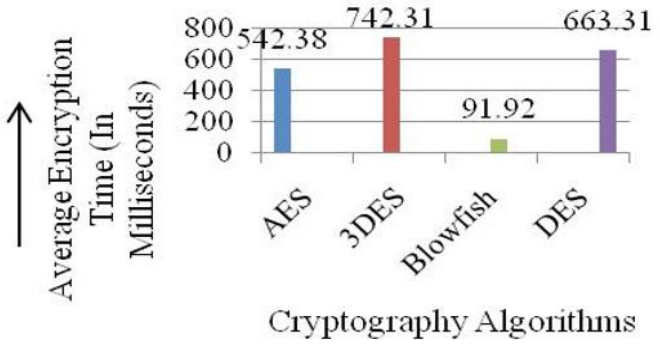

Fig:-6 Encryption Time of Each Algorithm (in ms)

V. CONCLUSION

In the world of internet, information is transmitted in a digital form. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used.

In this paper we are surveyed about various security algorithms. And after studying & analyzing the algorithms we conclude that among these algorithms AES is the more efficient algorithm. In future we can use these algorithms in such a way that it will provide more security in data storage & transmission.

REFERENCES

1. Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.
2. Behrouz A Forouzan, “Data Communications and networking”, McGraw-Hill, 4th Edition.
3. Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Companies, 2008.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

4. Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.
5. Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
6. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.