ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

Analysis of Various Cryptographic Algorithms

Swati Singh, Sudhir Kumar

M.Tech, Department of Computer Science, BBAU Central University, Lucknow, U.P., India
M.Tech, Department of Computer Science, BBAU Central University, Lucknow, U.P., India

ABSTRACT: In this modern era, the exchange of images, audios, videos and text files are done over a wireless communication channel which is known as internet. So the security of these valuable data is more important. For the security of these documents we use a term i.e. called cryptography. Cryptography can be defined as a hiding technique in which the readable format of data gets changed into non- readable format. In our survey paper we discussed about the various cryptographic techniques and also compared these techniques on the basis of their key size, block size, rounds and many more parameters.

KEYWORDS: Cryptography Techniques, DES, 3DES, RSA, AES, BLOWFISH and ELLIPTIC CURVE Cryptography.

I. INTRODUCTION

Cryptography can be defined as an art of hiding the data. By using the cryptography techniques the plain text changes into the cipher text which is non-readable to the unauthorized users. In cryptography we use only two text formats and these are pain text and cipher text. Plain text is a message given by the sender which is readable by everyone on the internet. So for the security of this plain text or message we apply the cryptography on it. The main aim of cryptography is to provide the security of data over the internet. This security can be provided by the encrypting the data into cipher text which is unknown to the intruders.

Purpose of cryptography: The main purpose of cryptography is for the following four parameters-
1. *Authentication*: Authentication is used for the proof of the identities of sender and receiver. We use authentication to define that the origin of the message is identified and known to the receiver.
2. *Integrity*: Integrity is used to define that the content i.e. sent by the sender is same as the content received by the receiver. There is no modifications of alterations are made by the third party vendors.
3. *Confidentiality*: Confidentiality defines that the only sender and intended receiver are allowed to send the content of the message.
4. *Access control:* Access control specifies and controls on who can access the process.

Types of cryptography: Cryptography can be divided into two main parts and these are:-

1. *Symmetric key cryptography*: Symmetric key cryptography can be defined as the part of cryptography in which a single key is used for both encryption and decryption process.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

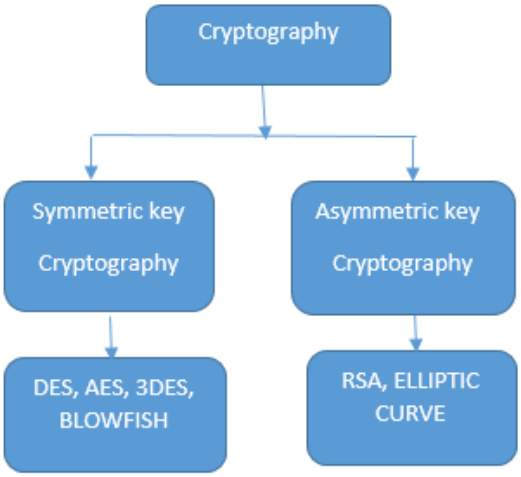

Fig.1. Block diagram of cryptography techniques

2. *Asymmetric key cryptography*: Asymmetric key cryptography can be defined as a part of cryptography in which two keys are used. One key is used for encryption process and another key is used for decryption process.

II. LITERATURE SURVEY

In this modern era the best way to communicate with others is wireless medium which is internet. When we communicate with others then we send our details, confidential files, our other important records with them via this channel. But this channel is also not secured for the communication as there are many unauthorized users who are waiting for this record. They hack this record for their personal use. So, to make our data secure from these vendors we use cryptography techniques which changes our data from readable format to non-readable format before sending it to receiver. There are many algorithms which are used for the security of data.

A. DES Algorithm:

Data encryption standard is the extended version of DES algorithm. As DES is a part of symmetric key cryptography so the only a key will be used here for the both encryption and decryption process. DES is introduced in 1977 and has approved by National Bureau of Standards (NBS) which is now called National Institute of Standards and Technology (NIST). DES takes the 64 bits of input as a plain text and provides the 64 bits of output in the cipher text. It takes 16 rounds of encryption on each 64 bit blocks of data. The key size of this algorithm is 56 bits and the block size is 64 bits. DES algorithm is used in many financial and commercial uses but is not much secured as its key size is not too long to protect the data [2].

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

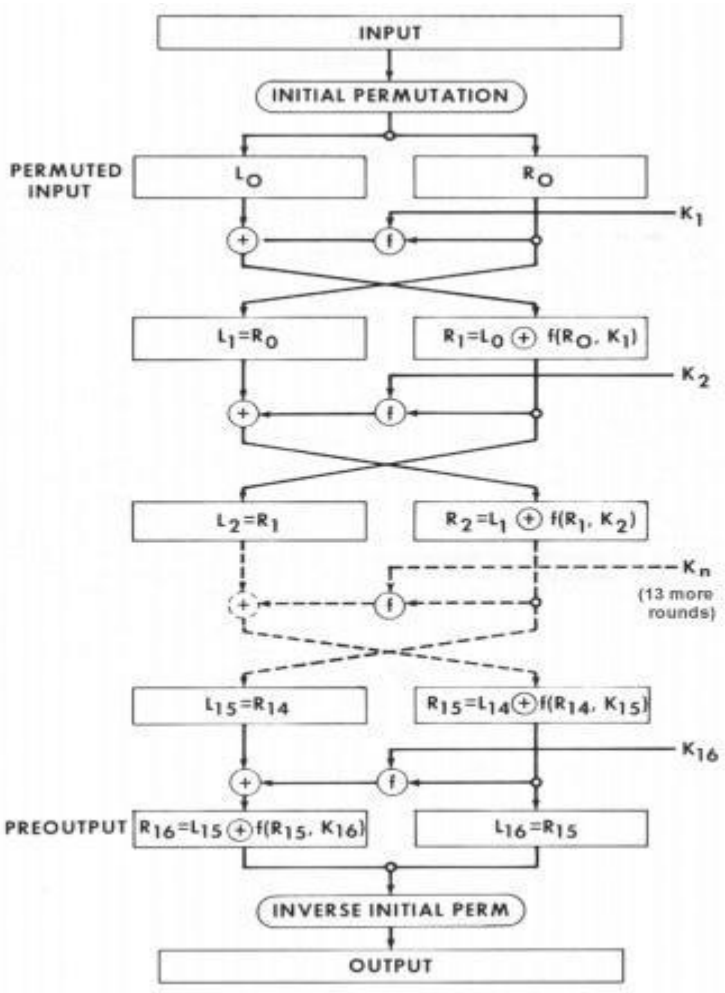

Fig.2. DES Algorithm

B. AES Algorithm:

AES algorithm was developed by Joan Daemen and Vincent Rijmen in 2001 which are two Belgian cryptographers. As we use these algorithms for the security purposes but AES algorithm is also used for its better speed also. We can also say that AES is a successor of DES algorithm. AES algorithm [4] is also recommended by the NIST. The block size of AES algorithm is 128 bits and the rounds (10, 12, 14…) used in it depends on its key size. A single key is used in AES algorithm for both encryption and decryption process. The encryption made in AES is fast and reliable. The key lengths of the AES algorithm are 128, 192 and 256 i.e. sufficient to protect classified information. There is also a drawback of AES algorithm and which is its performance. Sometimes it becomes so much complex.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

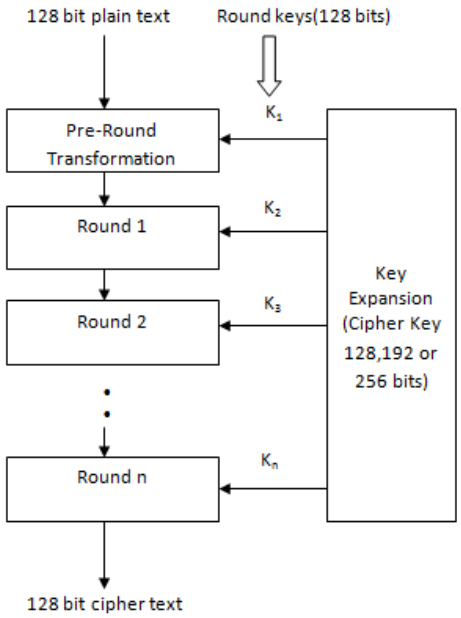

Fig.3. AES Algorithm

C. 3DES Algorithm:

3DES algorithm is introduced by IBM in 1978 to overcome the problems of DES algorithm. So we can say that 3DES is the successor of DES algorithm [2]. The key size used in 3DES algorithm is three times bigger than the key size used in DES algorithm which is 168 bits (3*56 bits) and the rounds used to complete a one encryption process are 48 (3*16) which are also three times larger in comparison with the DES algorithm. In the 3DES algorithm to complete the encryption and decryption process we use three keys. Suppose if we have three keys named K1, K2 and K3 then initially key K1 will be used for the encryption process and then key K2 will be used for decryption process and finally key K3 will be used for the encryption process. The two times encryption process over the data makes it stronger and difficult to break. The block size used in 3DES algorithm is 64 bits.

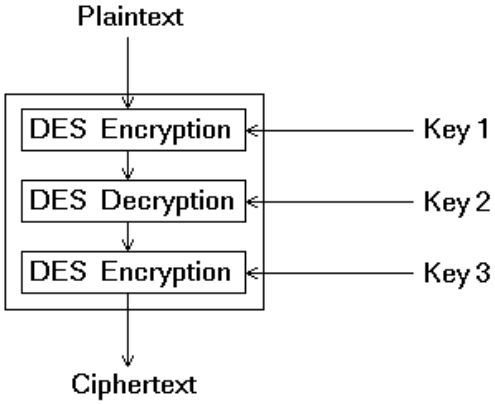

Fig.4. 3DES Algorithm

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

D. Blowfish Algorithm:

Blowfish is an example of symmetric key cryptography which uses only a single key foe both the encryption process and decryption process. It converts the plain text into the symmetric cipher text using a single key. Blowfish is introduced by Bruce Schneier in 1993. After its introduction, it is used for many large number of cipher suits and also for encryption method. The key size used in blowfish algorithm [1] is 32-448 bits and the block size is 64 bits. The structure of blowfish is a fiestel network. The rounds used by blowfish to complete a complete round of encryption are 16 rounds. The blowfish algorithm consist of two sub parts which are-

4.1 key expansion part

4.2 data encryption part.

As the block size of blowfish algorithm is 64 bits (as opposed to e.g. AES's 128 bit block size) make it vulnerable to birthday attack particularly in context with HTTPs.

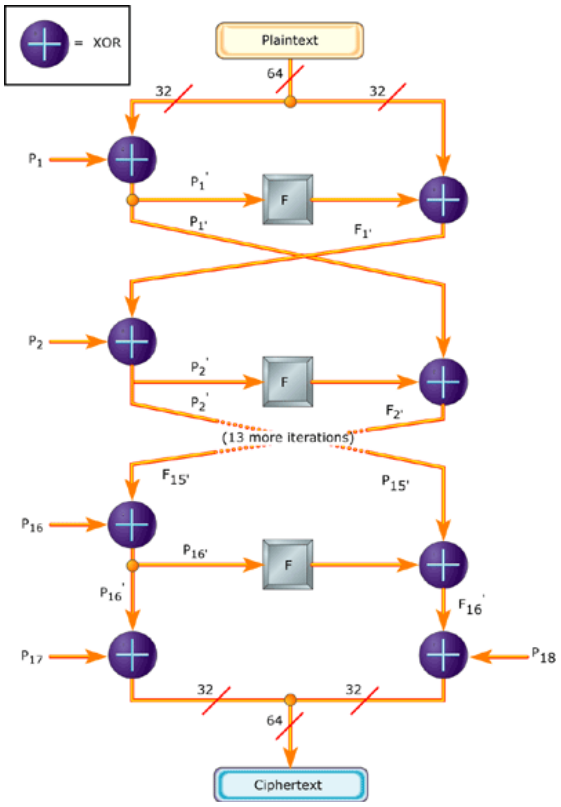

Fig.4. Blowfish Algorithm

E. RSA Algorithm: 1978. As RSA is an example of asymmetric key cryptography so two keys will be used here. One key will be used for encryption process and other must be used for decryption process. The key size used in RSA algorithm is 1024 bits which is enough to secure the data which will be sent over the communication channel. Due to its long key size it provides the better security but it also has a disadvantage which is its performance. The performance of RSA algorithm gets decrease because it takes too much time for encryption process. The RSA algorithm can be defined as-

1. Choose p and q
2. Compute n = p * q
3. Compute φ (n) = (p - 1) * (q - 1)

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

4. Choose e such that 1 < e < φ (n) and e and n are co-prime.
5. Compute a value for d such that (d * e) % φ (n) = 1.
6. Public key is (e, n)
7. Private Key is (d, n)
8. For encryption C=me (mod n) and decryption m =cd (mod n)

RSA algorithm is used for the public key cryptography where one key is known to everyone and other must be kept serious. RSA algorithm is developed by Rivest, Shamir &Adlemanin

Hence, by following above algorithm the plain text in encrypted form or cipher text and then decrypted from cipher text to plain text.

F. Elliptic Curve Cryptography:

Elliptic Curve Cryptography (ECC) was introduced by Victor Miller from IBM and Neil Koblitz in 1985. It is one of the alternative mechanisms for implementing the public key cryptography. This ECC (Elliptic Curve Cryptography) is Based on algebraic structures of elliptic curves over finite fields i.e. elliptic curve theory [5]. The more Faster, Smaller and more efficient keys are created by ECC in comparison with other encryption algorithm. The key size used in elliptic curve cryptography is 168 bit which is efficient to protect the data and also consumes less power. A good battery backup is provided by the elliptic curve cryptography.

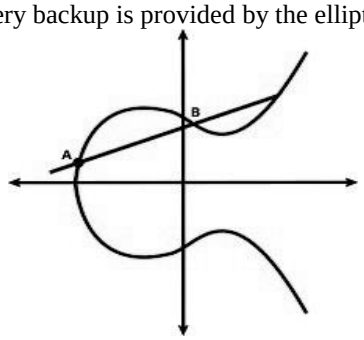

Fig.5. Elliptic Curve Representation

III. COMPARISON OF VARIOUS TECHNIQUES

In our paper we Stimulation Speed, Trojan horse, Hardware & Software Implementation and Ciphering & Deciphering Algorithm. So, the comparison can be given as-made a comparative study of various cryptographic algorithms in two parts. We compared symmetric algorithm in one part and asymmetric algorithm in another part. We made this comparison on the basis of various factors which are its Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds,

1. Developed in:

RSA	1978
DES	1977
AES	2000
3DES	1978
BLOWFISH	1993
ECC	1985

2. Key size:

RSA	1024 bits
DES	56 bits
AES	128, 192, 256 bits
3DES	168 bits
BLOWFISH	32-448 bits
ECC	168 bits

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

3. Block size:

RSA	Min 512 bits
DES	64 bits
AES	128 bits
3DES	64 bits
BLOWFISH	64 bits
ECC	64 bits

4. Ciphering and Deciphering keys:

RSA	Asymmetric
DES	Symmetric
AES	Symmetric
3DES	Symmetric
BLOWFISH	Symmetric
ECC	Asymmetric

5. Scalability:

RSA	Not Scalable
DES	Scalable
AES	Not Scalable
3DES	Not Scalable
BLOWFISH	Scalable
ECC	Scalable

6.Algorithm type:

RSA	Different
DES	Same
AES	Same
3DES	Same
BLOWFISH	Same
ECC	Different

7. Encryption and Decryption

RSA	Slower
DES	Moderate
AES	Faster
3DES	Slower
BLOWFISH	Faster
ECC	Faster

8. Power Consumption:

RSA	High
DES	Low
AES	Low
3DES	Low
BLOWFISH	Low
ECC	Low

9. Security:

RSA	Least Secure
DES	Not Secured Enough
AES	Excellent Secured
3DES	Excellent Secured
BLOWFISH	Least Secured
ECC	Average Secured

10. Inherent Vulnerabilities:

RSA	Brute Forced and Oracle attack
DES	Brute Forced, Linear and differential Cryptanalysis attack
AES	Brute Force Attack
3DES	Meet-in-the-middle-attack
BLOWFISH	Birthday Attack
ECC	Brute Force Attack

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 3 , March 2018

11. Rounds:

RSA	1
DES	16
AES	10/12/14
3DES	48
BLOWFISH	16
ECC	16

IV. CONCUSION:

As we know that the cryptography techniques are used for the security of data. These techniques are used for the encryption and decryption process over the data. In our survey paper we discussed about so many security techniques like DES. 3DES, AES, RSA, BLOWFISH and ECC. We made a comparison among these techniques on the basis of various factors like their key size, block size, inherent vulnerabilities etc. After making comparison among them we come to an end that 3DES algorithm is best for the security of data because it uses three keys to encrypt and decrypt the data. The key size used by 3DES is much strong to break. So in future we can use this algorithm for the better security of data.

REFERENCES

[1]. Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, "A Study of New Trends in Blowfish Algorithm", International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.
[2].Nirmaljeet Kaur, SukhmanSodhi,"Data Encryption Standard Algorithm (DES) for Secure Data Transmission", International Conference on Advances in Emerging Technology (ICAET 2016).
[3]. E.Meena, Dr. G. Ravi, "Secure Protocol for Jamming Attacks and Time-Delayed Broadcast in Wireless Communications ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 2, Issue 4, ISSN : 2456-3307.
[4]. B.Janapriya, " Video Steganography Schema based on AES Algorithm and 2D Compressive Sensing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 2, Issue 2, ISSN : 2456-3307.
[5]. RajdeepBhanot and Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications (IJSA), Vol. 9, No . 4 (2015), pp. 289-306.