International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 289-306
http://dx.doi.org/10.14257/ijsia.2015.9.4.27

A Review and Comparative Analysis of Various Encryption Algorithms

Rajdeep Bhanot[1] and Rahul Hans[2]

[1]*Research scholar, DAV University Jalandhar,*
[2]*Assistant Professor in dept. of CSE, DAV University Jalandhar*
Email:er.rajbhanot@gmail.com
Email: rahulhans@gmail.com

Abstract

Now days, Data security is very challenging issue that touches many areas including computers and communication. Recently, we came across many attacks on cyber security that have played with the confidentiality of the users. These attacks just broke all the security algorithms and affected the confidentiality, authentication, integrity, availability and identification of user data. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. Encryption is the process of converting normal data or plaintext to something incomprehensible or cipher-text by applying mathematical transformations or formulae. These mathematical transformations or formulae used for encryption processes are called algorithms. We have analysed ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA etc. Among them DES, Triple DES, AES, RC5, BLOWFISH, TWOFISH, THREEFISH and IDEA are symmetric key cryptographic algorithms. RSA and ECC are asymmetric key cryptographic algorithms. In this paper, we have analysed various encryption algorithms on the basis of different parameters and compared them to choose the best data encryption algorithm so that we can use it in our future work.

Keywords: *Security, Cryptograph, Algorithm, Key, Cipher, Security attacks, NIST etc.*

1. Introduction

Cryptography algorithm is the technique or some formula that makes data or network secure by providing security. Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The highly use of networking leads to the data exchange over the network while communicating to one and another system. While communication it is very important to encrypt the message so that intruder cannot read the message. Network security is highly based on cryptography [18]. Basically, Cryptography is an art of hiding information by encrypting the message. The art of protecting information (encryption) it into an unreadable format (encrypted text), called cipher text. Only those who

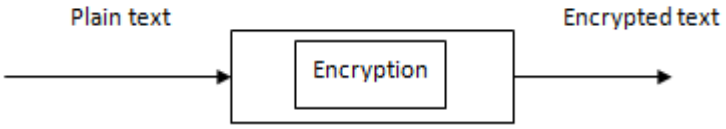

Figure 1. Encryption

ISSN: 1738-9976 IJSIA

possess a secret *key* can de-cipher (*decrypt*) the message into plain text. The system in which first data(*Plain text*) in encrypted at sender side and decrypted into plain text again at receiver end using a unique key or some particular formula is called a Cryptographic system. Encrypted messages can sometimes be broken by cryptanalysis, also called *code-breaking* [26].

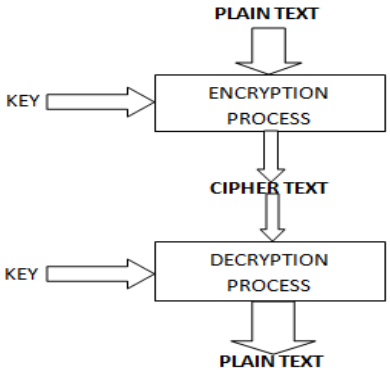

Figure 2. Encryption Process

Although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.
On the basis of the input data, cipher algorithms are classified as *block ciphers*, in which the size of the block is of fixed size for encryption and *stream ciphers* in which a continuous stream is passed for encryption and decryption. Among the algorithms taken under consideration, some of them are block cipher like RSA, DES, AES, Blowfish, Twofish, Threefish etc. and some of them are stream cipher i.e. ECC, RC5 etc.

2. Basic Terminology used in Cryptography

There are some terms which we should know for better understanding of encryption algorithms. This terminology is very important to understand because in every algorithm description, we are going to discuss these common terms:

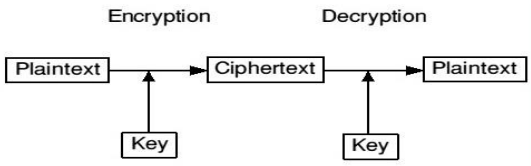

Figure 3. Encryption Terminology

2.1 Plain Text or Normal Text

The original text or message used in communication in called as Plain text.
Example: John sends “Hello” to Perry. Here “Hello” is Plain text or Original message.

2.2 Cipher Text

The plain text is encrypted in un-readable message. This meaningless message is called Cipher Text.

Example: “Hello” message is converted in “-&tt%”. This meaningless message is Cipher Text.

2.3 Encryption

Encryption is a process of converting Plain text into Cipher text. This non-readable message can securely be communicated over the unsecure network. Encryption process is done using encryption algorithm.

2.4 Decryption

Decryption process is the reverse of Encryption process, i.e. Cipher text is converted into plain text using particular encryption algorithm.

2.5 Key

A key is a numeric or Alpha-numeric text (mathematical formula). In encryption process it takes place on Plain text and in decryption process it takes place on cipher text.

2.6 Key Size

Key size is the measure of length of key in bits, used in any algorithm.

2.7 Block Size

Key cipher works on fixed length string of bits. This fix length of string in bits is called Block size. This block size depends upon algorithm.

2.8 Round

Round of encryption means that how much time encryption function is executed in complete encryption process till it gives cipher text as output.

Cryptography systems can be broadly classified into two categories:

- Symmetric encryption algorithms
- Asymmetric encryption algorithms

Symmetric encryption algorithms, that use a single key that both the sender and recipient have. This key is kept secret among sender and receiver so that no intruder can steal the data to be transferred by encrypting it.

Asymmetric encryption algorithm or *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Individuals who practice this field are known as cryptographers.

Asymmetric encryption provides more security as compared to symmetric key encryption but in case of encryption speed, symmetric encryption is on lead.

3. Main Objectives of Cryptography

Encryption or Cryptography have some goals that needs to be fulfilled for user benefit. Modern cryptography concerns itself with the following four objectives:

3.1 Confidentiality

The information cannot be understood by anyone for whom it was unintended.

3.2 Integrity

The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3.3 Non-repudiation

The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

3.4 Authentication

The sender and receiver can confirm each other's identity and the origin/destination of the information.

3.5 Access Control

Only authorised users can access the data. This is done to avoid unauthorized user access.

A plain text is encrypted using an algorithm called "encryption algorithm". A cipher text is decrypted using an algorithm called "decryption algorithm". A key is used at the time of encryption and decryption process. The security level of cryptography is determined by the key space or key length (size of key).

4. Overview of Various Algorithms

In this section we will discuss about various cryptographic algorithms to be analysed for their performance evaluation. To start the algorithm analysis firstly we should know that what is Algorithm actually. "An algorithm is a sequence of unambiguous instructions for solving a problem", i.e., for obtaining a required output for any legitimate input in a finite amount of time. We are taking twelve encryption algorithms under consideration those are DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5, IDEA etc.

4.1 DES (Data Encryption Standard)

It was developed in the early 1975 at IBM labs by Horst Fiestel. The DES was approved by the NBS (*National Bureau of Standards*, now called *NIST -National Institute of Standards and Technology*) in 1978. The DES was standardized by the *ANSI* (*American National Standard Institute*) under the name of *ANSI X3.92*, better known as *DEA* (*Data Encryption Algorithm*). The DES was once a predominant symmetric-key algorithm for the encryption of electronic data. But now it is an outdated symmetric key data encryption method. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. Data encryption standard works on a particular principle. Data encryption standard is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity)[25]. Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 2^{56} or 72,057,594,037,927,936, attempts to find the correct key [20].

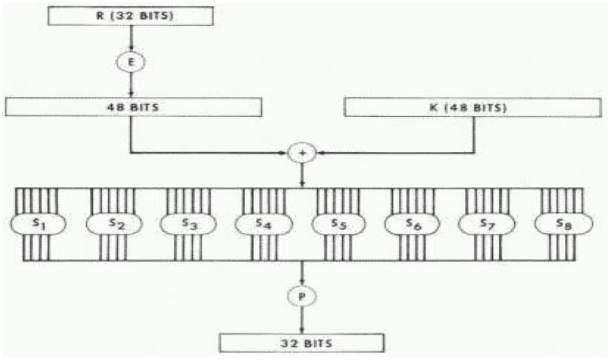

Figure 4. Function F of DES

Above is the structure of function F of DES algorithm. The block of the message is divided into two halves. The right half is expanded from 32 to 48 bits using another fixed table. The result is combined with the sub-key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half. Many security experts felt the 56-bit key length was inadequate even before DES was adopted as a standard. Even so, DES remained a trusted and widely used encryption algorithm through the mid-1990s[26]. However, in 1998, a computer built by the Electronic Frontier Foundation (EFF) decrypted a DES-encoded message in 56 hours. By harnessing the power of thousands of networked computers, the following year EFF cut the decryption time to 22 hours. Data Encryption Standard can also be used for single user encryption like storing some data in hard disk.

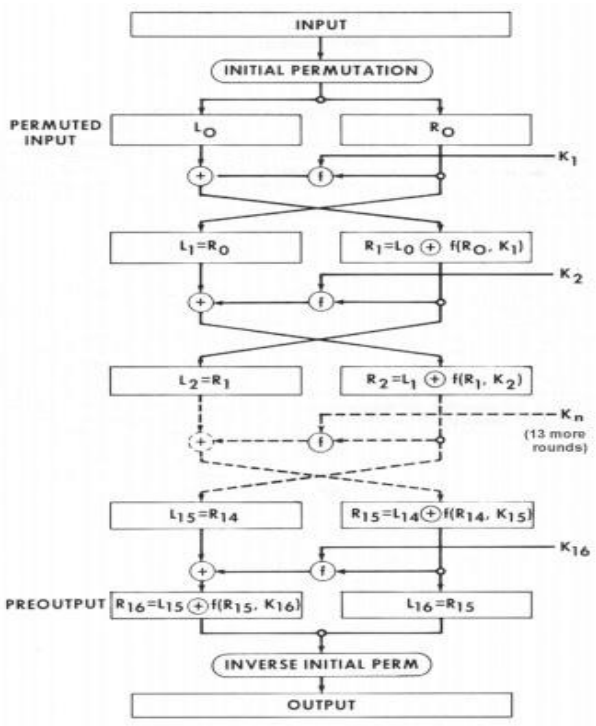

Figure 5. DES Encryption Procedure

In its encryption process, DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. In all rounds, encryption is done using function F. DES have three modes of operation: ECB (Electronic Code Book), CBC(Cipher Block Chaining), CFB(Cipher Feedback) and OFB(Output Feedback)[20]. Encryption strength is directly tied to key size, and 56-bit key lengths have become too small relative to the processing power of modern computers. So, NIST felt the need of new and more secure data encryption algorithm in the field. The Data Encryption Standard was officially withdrawn in May 2005.

There is no strong limitation found rather than its small key size which offers less security. The only successful attack on DES is Brute force attack. It's another weak point is its encryption speed which is very slow.

4.2 3DES (Triple Data Encryption Standard)

In cryptography techniques, Triple Data Encryption Standard (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block. Triple-DES is also proposed by IBM in 1978 as a substitute to DES. So, 3DES is simply the DES symmetric encryption algorithm, used three times on the same data. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text[14].

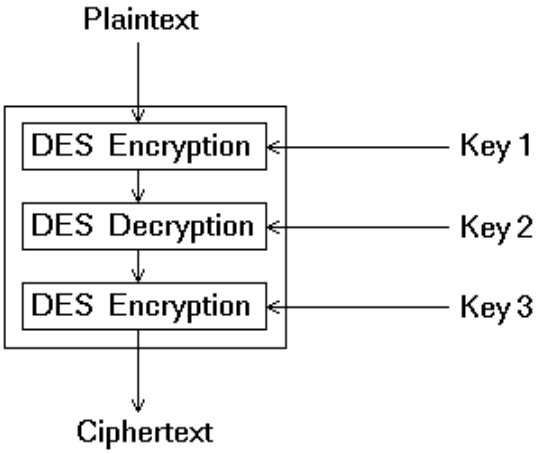

Figure 6. 3DES Structure

In this, same data is encrypted two times more using DES. Hence, this makes the encryption stronger and more difficult to break. Triple DES is basically a Block cipher which uses 48 rounds (Three tim es the DES) in its computation, and has a key length of 168 bits. 3-DES also uses the Block size of 64 bits for encryption[14]. There are following modes:

4.2.1 DES-EDE3 : Encrypt, Decrypt and Encrypt with 3 unique keys as mentioned above (Key1, Key2, Key3).

4.2.2 DES-EEE3 : A block of data is encrypted, and encrypted again with a different key and finally encrypted once more with another key, using a total of 3 unique keys.

4.2.3 DES-EDE2 : Here we only use two keys, in which the first and last encryption is done using exactly the same key.

4.2.4 DES-EEE2 : Finally this also uses two keys, the first and last encryption is done using the same key.

3DES is a trick to reuse DES encryption algorithm but with three distinct keys. 3DES is believed to be secure up to at least 2^{112} security, but it is slow, especially in software computations [18]. 3-DES also provides adequate security. That's why users needed the successor of 3-DES.

The main advantage of Triple DES is that it is three times secure (as it is combination or three DES algorithms with different keys at each level) than DES that's why it is preferred over simple DES encryption algorithm. It provide adequate security to the data but it is not the best because it consumes lot of time and its encryption speed also less than DES encryption algorithm.

4.3 RSA (Rivest-Shamir-Adleman Algorithm)

The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is best known and widely used public key scheme. It uses large integers like 1,024 bits in size. It has only one round of encryption. It is asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process[8].

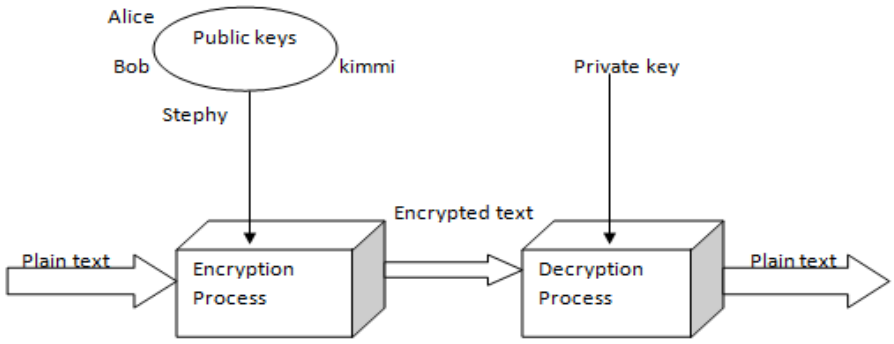

Figure 7. RSA Algorithm (Asymmetric Key Cryptography)

This is also called public key cryptography, because one of them can be shared with everyone and another key must be kept private. It is based on the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who developed and publicly described it in 1978 [18]. A user of RSA creates and then publishes the product of two large prime numbers (P*Q), along with an auxiliary value (I), as their public key. The prime factors (P*Q) must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Following algorithm is used in RSA,

1. Choose p and q
2. Compute n = p * q
3. Compute $\varphi(n) = (p - 1) * (q - 1)$
4. Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime.
5. Compute a value for d such that $(d * e) \% \varphi(n) = 1$.
6. Public key is (e, n)
7. Private key is (d, n)
8. For encryption $C=m^e \pmod n$ and decryption $m = c^d \pmod n$

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

In RSA cryptographic algorithm the main disadvantage is its encryption speed. It consumes lot of time to encrypt data. Actually this is disadvantage of asymmetric key algorithms because the use of two asymmetric keys. It provides good level of security but it is slow for encrypting files. Another threat in this algorithm is fake key insertion at decryption level so the secret key should be private and correct to achieve the encryption in successful manner.

4.4 AES (Advanced Encryption Standard)

In 1997, the National Institute of Standards and Technology (NIST) announced an initiative to choose a successor to DES; in 2001, it selected the Advanced Encryption Standard as a replacement to DES and 3DES. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys[21].

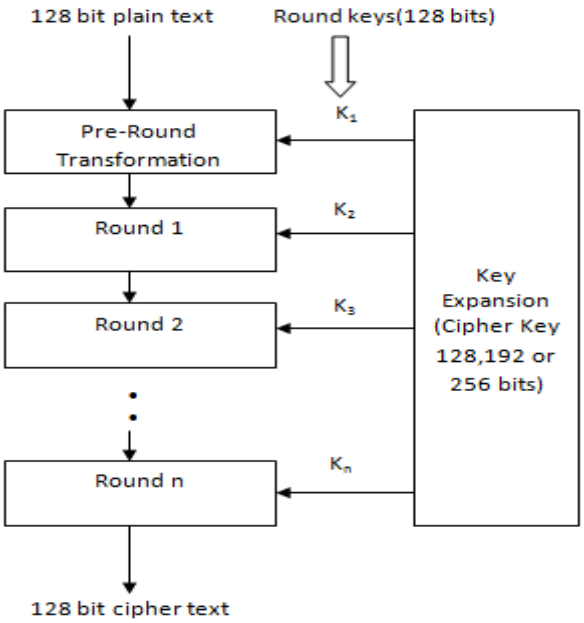

Figure 8. AES Algorithm

In each case, all other rounds are identical, except for the last round.

Each round in encryption process further follows some steps to complete each round till n. Each round possess four rounds i.e. Substitute byte, Shift rows, Mix Column and Add round key.

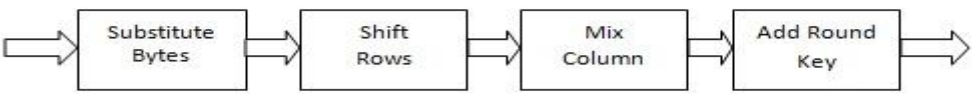

Figure 9. AES Round Steps

Substitution round: In this step, Sub-Bytes are byte-by-byte substituted during the forward encryption process.

Shift Rows: In this, shifting the rows of the state array during the forward process(S-Box process)

Mix Column: Mix Columns for mixing up of the bytes in each column separately during the forward process.

Add Round Key: In this step, round key is added to the output of the previous step during the forward process. This step differs from others because of key size difference.

In AES encryption process, it uses different round keys. These keys are applied along with other mathematical operations on an array of data. This data is present in blocks of particular size. This array is called state array. This encryption process includes following process:

1. First derive the different round keys from cipher key.
2. Initialize the state array with block data or plaintext.
3. Start with initial state array by adding round key.
4. Perform the process of state manipulation in nine rounds.
5. After tenth round of manipulation, we will get the final output as cipher text.

By following above process we get the final encrypted text or cipher text.

4.5 ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller from IBM and Neil Koblitz from University of Washington as an alternative mechanism for implementing public-key cryptography. This ECC (Elliptic Curve Cryptography) is Based on algebraic structures of elliptic curves over finite fields i.e. Elliptic curve theory. ECC Create Faster, Smaller and more efficient keys as compared to other encryption algorithm. In this, encryption is done in elliptic curve equation (used in mathematics) form. ECC is that much efficient that it can yield a level of security with 164 bit key that other system require a 1,024-bit key to achieve that security level i.e.it offers the maximum security with smaller bit sizes that is why it consumes less power[25] and hence, Elliptic curve cryptography is good for battery backup also. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. Basically, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers).

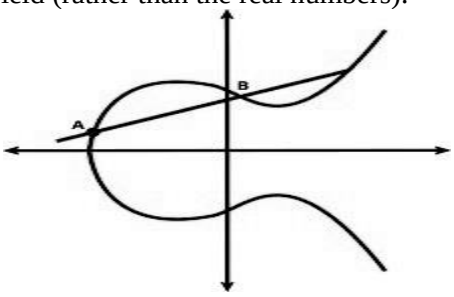

Figure 10. Elliptic Curve Representation

Which consists of the point values satisfying the equation,

$$y^2 = x^3+Ax+B,$$

Where a and b are the constent point values.

In the encryption process of Elliptic curve cryptography, we have many options to use ECC cryptography but we will discuss simplest way.

According to this encryption technique,

1. The sender must first encode any message M as a point on the elliptic curve P_m.
2. The user must first encode any message M as a point on the elliptic curve P_m.
3. Select suitable curve & point G as in D-H.

4. Each user chooses private key $n_A<n$ and computes public key $P_A=n_AG$
5. For encryption encrypt:
   $P_m : C_m=\{kG, P_m+kP_b\}$, where k is a random number
6. For decryption decrypt C_m compute:
   $P_m+kP_b–n_B(kG) = P_m+k(n_BG)–n_B(kG) = P_m$

Nowadays, it is mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks. The main advantage of ECC uses short key length which leads to fast encryption speed and less power consumption. For example, a 160 bit ECC encryption key size provide the same level of security as 1024-bit RSA encryption key and it perform 15 times faster depending upon the platform on which it is implemented.

The disadvantage of ECC is that it increases the size of encrypted text and second disadvantage is that ECC is dependent on very complex equations which lead to increase the complexity of encryption algorithm.

4.6 Blowfish

Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round Feistel cipher and uses large key dependent S-Boxes. Each S-box contains 32 bits of data.

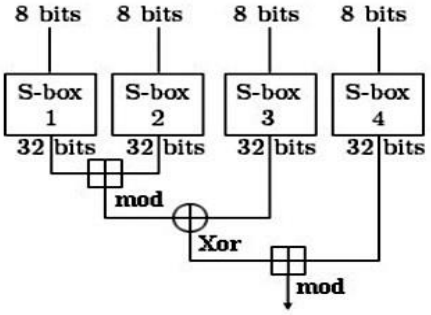

Figure 11. Blowfish Function F.

Above Diagram shows the Blowfish's F- function. The function splits the 32 bit input into four 8-bit quarters, and uses the quarters as input to S-boxes. The outputs are added (Mod) modulo 2^{32} and XORed to produce the final 32-bit output i.e. encrypted data. For Decryption at another end the same process takes place, but in reverse order[21].

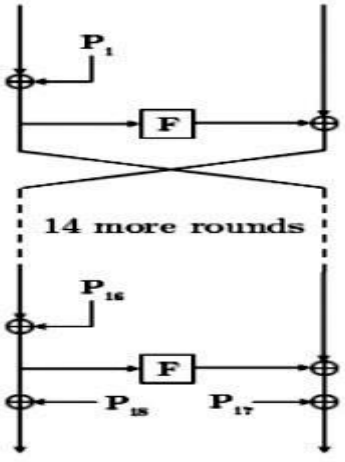

Figure 12. Blowfish Procedure

Till now, no attack has been found successful against Blowfish encryption algorithm.

Blowfish is a variable key length algorithm and it is having 64-bit block cipher. The algorithm consist of two sub parts, one is key expansion part and second data encryption part. Data encryption is done by completing 16 rounds fiestel network. Each round consist of key dependent permutation in P-Box and key/data dependent substitution in S-Box[4].

Algorithm consists of S-Box and P-Box.

The P-array consists of 18 sub-keys of 32-bit.

P1, P2,...,P18.

There are four 32-bit S-boxes with 256 entries each:

S1[0], S1[20],..., S1[255];
S2[0], S2[20],..,, S2[255];
S3[0], S3[20],..., S3[255];
S4[0], S4[20],..,, S4[255].

For encryption following procedure is followed,

Divide x into two 32-bit halves:

(xL) and (xR)

For i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

Next i

Swap xL and xR (or Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR.

Divide xL into four eight-bit quarters: a, b, c, and d

$F(xL) = ((S1,a + S2,b \bmod 2^{32}) \text{ XOR } S3,c) + S4,d \bmod 2^{32}$

Decryption is exactly the same as encryption but reverse process is followed.

Blowfish provides a good encryption rate in software. It is much faster than DES and IDEA. In many encryption simulation experiments the Blowfish encryption algorithm is declared best because of security level that is offers and speed of encryption, which is better than the most of the encryption algorithm available.

4.7 Twofish

Twofish is also a symmetric block cipher having fiestel structure. It is also developed and explained by bruce schneier in 1998. Twofish also uses block ciphering like Blowfish. It is efficient for software that runs in smaller processor (smart cards) and embedding in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Twofish is license-free, un-patented and freely available for use. In twofish encryption it uses key sizes of 128, 192 and 256 bits. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm.

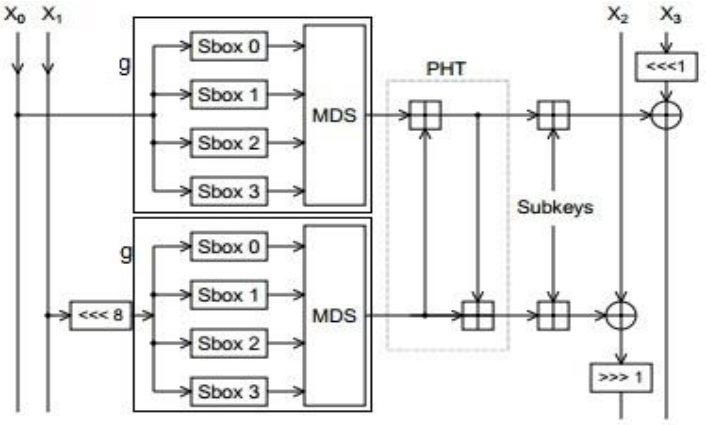

Figure 13. Round Function of Twofish

Above figure shows the Round function working of Twofish. This round function encrypts the data. This round function repeatedly encrypts the data 16 times and then gives final cipher text after 16th round [26].

In above figure,

1. X_0 and X_1 on the left the inputs to the g functions after the rotation by 8 bits of one of them.
2. The g function consists of 4 byte key-dependent S-boxes followed by a linear mixing step

(MDS matrix).

3. The results of the two g functions are combined using a PHT (Pseudo-Hadamard Transform).
4. After that two keywords are added. One right among them is rotated by 1 bit and then both of these keywords are XORed into the result on the left.
5. For next round, right and left halves swapped.

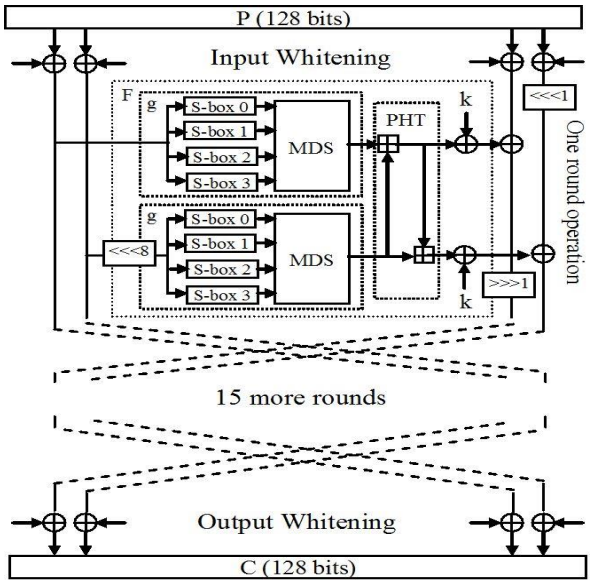

Figure 14. Twofish Procedure

6. After 16 rounds of encryption the last swap is reversed and four keywords are XORed with another four keywords to produce the final encrypted text or cipher text.

Above figure represents the overall working process of Blowfish encryption algorithm. Twofish contains total 16 rounds of data encryption and we get the final 128 bit cipher text after completing 16 rounds of encryption [12]. Twofish encryption algorithm also provides good level of security but it lacks in encryption speed as compared to blowfish.

4.8 Threefish

Threefish is a symmetric key block cipher designed by bruce schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir bellare, jesse walker. It was first published in year 2008. Threefish block cipher is directly related to Blowfish and Twofish. Threefish algorithm is tweakable block cipher. Tweakable block cipher take three inputs, a key, a tweak and block of massage. A unique tweak value is used to encrypt every block of massage. The tweak value is 128 bits for all block sizes. Threefish encryption uses three type of keys 256 bits, 512 bits or 1024 bits. In Threefish, the key size is equal to the block size. It means it uses three block sizes i.e. 256, 512 or 1024 bits. It applies encryption in 72 rounds generally, but in case of 1024 bit block size its encryption rounds are 72. Threefish uses no S-BOX or other table lookups in order to avoid timing attacks[21].

Three fish encryption algorithm uses following round function.

In this encryption process following steps are followed,

1. Threefish uses $N_r/4 +1$ different round keys.
2. To calculate these keys the original key words,
   $K_0 , K_1 \ldots, K_{Nw-1}$ are appended.
   The tweak words t_0, t_1 are appended with an additional tweak word too.
   $$t_2=t_0 \oplus t_1$$
   $$k_{Nw}= C_{240} \oplus k_0 \oplus k_1, \ldots\ldots \oplus k_{Nw-1}$$
3. The round keywords $k_{s,I}$ are defined like,
   $$K_{s,I} = \begin{cases} k_{(s+i) \bmod (Nw+1)} & i= 0,\ldots,N_w-4 \\ k_{(s+i) \bmod (Nw+1)} + t_{s \bmod 3} & i=N_w-3 \\ k_{(s+1) \bmod (Nw+1)} + t_{s \bmod 3} & i=N_w-2 \\ k_{(s+1) \bmod (Nw+1)} + s & i= N_w-1 \end{cases}$$
4. Mix function takes a tuple of words (X_0,X_1) and returns another tuple of words (Y_0,Y_1)
5. The function , $Y_0= X_0+X_1 \bmod 2^{64}$
   $$Y_1= (Y_1 <<< R_{(d \bmod 8),J}) \oplus Y_0$$
6. $R_{d,j}$ is a fixed set of rotation constant.
7. If d mod 4==0 then the round key $K_{d/4}$ is added to words.
8. Then, the mix function is used to consecutive words.

Threefish-256 and Threefish-512 apply this round 72 times. Threefish-1024 applies this round 80 times.

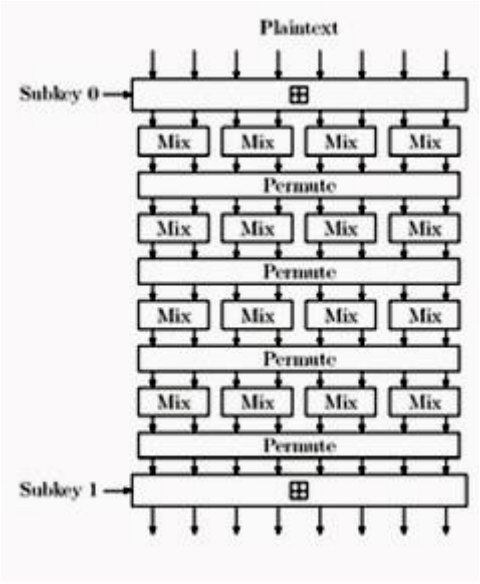

Figure 15. Threefish-1024 Block cipher round

Above figure representing Threefish-1024 one round of encryption having plain text block and sub-key with tweak value. It is using four blocks of 256 bits each. For this case the 80 rounds of encryption are done.

4.9 RC5

RC5 is a symmetric-key block cipher. It is designed by Ronald Rivest in 1994. RC stands for "Rivest Cipher" or it is also called "Ron's Code". AES (Advanced Encryption Standard) is directly based on RC5. It uses key sizes 0 to 2040 bits but suggested count is 128 bits. RC5 uses block sizes of 32, 64 or 128 bits but 64 bits are suggested. It is fiestel-like network [16]. It has 1 to 255 encryption rounds but 12 rounds are suggested originally. It is suitable for hardware and software implementation, because it uses only those operations which are available in typical microprocessor [19].

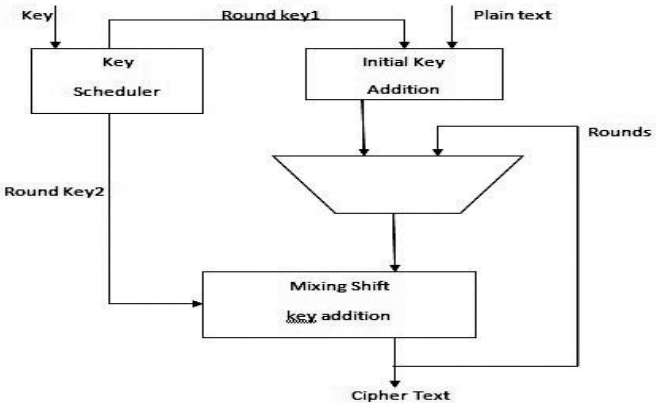

Figure 16. RC5 Encryption Procedure

Above Figure is showing the basic working procedure of RC5 encryption algorithm. The RC5 encryption algorithm is a block cipher that converts plain text data blocks of 16, 32, and 64 bits into cipher text blocks of the same length. The algorithm is organized as a set of iterations called rounds r that takes values. RC5 works with two 32 bit registers A and B which contains the initial input text or plain text as well as the output cipher at the

end of encryption. First we load plain text into the registers A and B then encryption and decryption functions are applied on it[23].

In encryption procedure, Input text stored in two 32 bit input registers A and B where number of rounds for encryption are 2r+2 and round keys will be S[0,1,2,….2r+1].

Output text will be stored in A and B.

Procedure: A = A + S[0] and B = B + S[20]

for i = 1 to r

do{

A = ((A ⊕ B) <<< B) + S[2i]

B = ((B ⊕ A) <<< A) + S[2i+ 1]

}

After this process the data is encrypted and stored in registers A and B called cipher text.

For decryption process, Cipher text is loaded in registers A and B.

Procedure: for i = r back to 1

do{

B = ((B - S[2i + 1]) >>>A) ⊕ A

A = ((A - S[2i]) >>> B) ⊕ B

}

B = B – S[20] and A = A - S[0]

After this we will get the value of A and B.

This algorithm does reverse operations on registers A and B.

4.10 IDEA (International Data Encryption Algorithm)

IDEA (International Data Encryption algorithm) is a block encryption algorithm designed by Xuejia Lai and James L and it was first described in 1991.The original algorithm went through few modifications and finally it got named as International Data Encryption Algorithm (IDEA)[11].

IDEA is a Block cipher that operates with 64 bit plain text and cipher text blocks and is controlled by 128 bit key. This algorithm works on 64-bit plain text and cipher text block (at one time). For encryption purpose, the 64- bit plain text is divided into four 16 bits sub-blocks. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits).

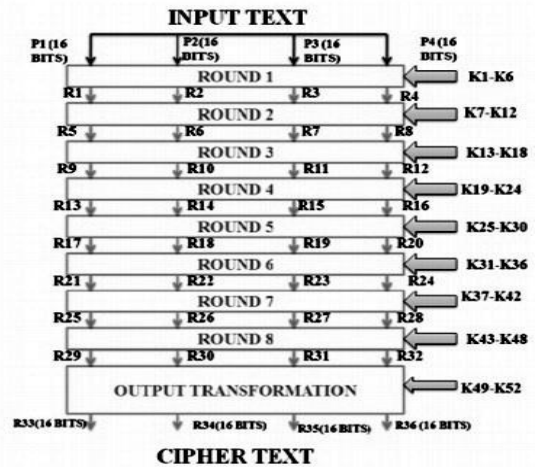

Figure 17. IDEA Encryption Process

Each of these blocks goes through 8 rounds and one output transformation phase. In each of these eight rounds, some (arithmetic and logical) operations are performed. Throughout the eight rounds, the same sequences of operations are repeated. In the last

phase, output transformation phase, we perform only arithmetic operations. At the beginning of the encryption process, the 64 bit plain text is divided in four equal size blocks and ready for round1 input. The output of round1 is the input of round2. Similarly, the output of round2 is the input of round3, and so on. Finally, the output of round8 is the input for output transformation, whose output is the resultant 64 bit cipher text [assumed as C1 (16bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)]. As the IDEA is a symmetric key algorithm, it uses the same key for encryption and for decryption. The decryption process is the same as the encryption process except that the sub keys are derived using a different algorithm[7]. The size of the cipher key is 128bits. In the entire encryption process we use total 52 keys (round1 to round8 and output transformation phase), generated from a 128 bit cipher key. In each round (round1 to round8) we use six sub keys. Each sub-key consists of 16bits and the output transformation uses 4 sub-keys.

5. Comparative Table

Table 1. Comparison of Various Algorithms on the basis of Different Parameters

PARAMETERS	DES	3DES	AES	RSA	BLOWFISH
DEVELOPMENT	In early 1970 by IBM and Published in 1977.	IBM in 1978.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
KEY LENGTH (Bits)	64 (56 usable)	168,112	128,192, 256	Key length depends on no. of bits in the module	Variable key length i.e. 32 – 448
ROUNDS	16	48	10,12,14	1	16
BLOCK SIZE (Bits)	64	64	18	Variable block size	64
ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attack	Key recovery attack, Side channel attack	Brute force attack, timing attack	No attack is found to be successful against blowfish.
LEVEL OF SECURITY	Adequate security	Adequate security	Excellent security	Good level of security	Highly secure
ENCRYPTION SPEED	Very slow	Very slow	Faster	Average	Very fast

Table 2. Comparison of Various Algorithms on the Basis of Different Parameters

PARAMETERS	TWOFISH	THREEFISH	RC5	ECC	IDEA
DEVELOPMENT	Bruce Schneier in 1998	Bruce schneier, Niels Ferguson, Stefan Lucks in 2008	Ron rivest in 1994	Victor Miller from IBM and Neil Koblitz in 1985	Xuejia Lai and James in 1991
KEY LENGTH (Bits)	128, 192, 256	256,512, 1024	0 to 2040 bits key size(128 suggested)	Smaller but effective key	128
ROUNDS	16	For 256,512 key = 72 For 1024 key = 80	1 to 255(64 suggested)	1	8
BLOCK SIZE (Bits)	128	256,512 and 1024	34 , 64, 128(64 suggested)	Stream size is variable	64
ATTACK FOUND	Differential attack, Related key attack	Improved Related-Key Boomerang Attack	Co-relation attack, Timing attack	Doubling attack	Linear attack
LEVEL OF	Secure	Secure	Secure	Highly secure	Secure

SECURITY					
ENCRYPTION SPEED	Fast	Fast	Slow	Very Fast	Fast

6. Conclusions

In this paper, we have analysed various encryption algorithms. We have found that each algorithm has its own benefits according to different parameters. From the work completed in this paper it is observed that that the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption that will lead to more heat dissipation. So, it is not advisable to use short data sequence and key lengths. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. From above analysis we have found that ECC and Blowfish, these two encryption algorithms are leading with the security level that they provide and faster encryption speed. ECC is having some attacks on it but on Blowfish, no attack is successful yet. So, from this review and analysis we have shortlisted ECC and Blowfish encryption algorithm. These two encryption algorithms are more secure and fast to work with and in future, there is wide scope of improvement in these both encryption algorithms.

References

[1] D. Hakerson, A. Menezes and S. Vanston, “Guide to Elliptic Curve Cryptography”, Springer, **(2004)**; Verlag, NY.
[2] M. Kumar and E. G. Dharma, “A comparative analysis of symmetric key encryption algorithm”, IJARCET, vol. 3, no. 2, **(2014)**.
[3] I. Landge, T. Bharmal and P. Narwankar, “Encryption and decryption of data using two fish algorithm”, World Journal of Science and Technology, vol. 2, no. 3, **(2012)**, pp. 157-161.
[4] J. W. Cornwell, “Blowfish Survey”, Department of Computer Science, Columbus State University, Columbus.
[5] E. Biham and A. shamir, "A differential cryptoanalysis of data encryption stamdard", Springer-verlag, **(1993)**.
[6] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, [online] Available at: http://www.schneier.com/paper-blowfishfse.html.
[7] S. Basuin, “International data encryption algorithm (idea) – a typical illustration”, Journal of global research in computer science (JGRCS), vol. 2, no 7, **(2011)**.
[8] A. Kakkar and M. L Singh, “Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network”, Published in International Journal of engg, and technology(IJET), vol. 2, no. 1, **(2012)**.
[9] J. Daemen, R. Govaerts and J. Vandewalle, “Weak Keys for IDEA”, Springer-Verlag, **(1998)**.
[10] M. Abutaha, M. Farajallah, R. Tahboub and M. Odeh, “Survey Paper: Cryptography Is the Science of Information Security”, published in International Journal of Computer Science and Security (IJCSS), vol. 5, no. 3, **(2011)**.
[11] M. Thaduri, S. Yoo and R. Gaede, “ An Efficient Implementation of IDEA encryption algorithm using VHDL”, Elsevier, **(2004)**.
[12] L. Singh and R. K. Bharti, "Comparative perfomance analysis of cyptographic algorithms", International journal of advanced research in computer science and software engineering (IJARCSSE), vol. 3, no. 11, **(2013)**.
[13] G. C. Kessler, “An Overview of Cryptography”, http://www.garykessler.net/library/crypto.html, **(2006)**.
[14] W. Stallings, "Cryptography and Network Security: Principles and Practice", **(1999)**, Prentice-Hall, New Jersey.
[15] R. L. Rivest, “The RC5 Encryption Algorithm”, MIT laboratory for C.S, Cambridge.
[16] K. Abdullah, “Research Commons at the University of Waikato”, http://waikato.researchgateway.ac.nz/.
[17] W. Diffiee and M. Hellman, “New Directions in Cryptography”, IEEE Transaction Information Theory IT-22, **(1976)**, pp. 644-654.
[18] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e, **(2005)**.

[19] R. L. Rivest, "The RC5 Encryption Algorithm", Proceedings of the Second International Workshop on Fast Software Encryption (FSE), **(1994)**.
[20] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal Research Develop., vol. 38, no. 3, **(1994)**, pp. 243 -250.
[21] J. V. Shanta, "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management", vol. 15, no. 4, **(2012)**, pp.43-49.
[22] A. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and Communication Technologies , **(2006)**, pp. 84-89.
[23] R. L. Rivest, "RC5 Encryption Algorithm", Dr Dobbs Journal, vol. 226, **(1995)**, pp. 146-148.
[24] R. Davis, "The data encryption standard in perspective", Communications Society Magazine, IEEE, **(2003)**, pp. 5 – 9.
[25] Y. F. Huang, "Algorihtm for elliptic curve diffie-Hellman key exchange based on DNA title self assembly", Proceedings of 46th IEEE Theories and Applications, **(2008)**.
[26] N. Islam, M. H. Mia, M. F. I. Chowdhury and M. A. Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, **(2008)**.

Authors

Rajdeep Bhanot, he is a Research Scholar, Computer Science & Engineering Department from DAV University Jalandhar, Punjab (INDIA). B.tech. Professional with specialization in Information Technology from DAV Institute of Engg. & Technology (PTU) Jalandhar, Punjab (INDIA). Attended national level seminar on modern Cryptography techniques organised by PTU Jalandhar.

Rahul Hans, he is working as assistant professor in the Department of computer Science and Engineering at DAV University, Jalandhar Punjab (INDIA). He has done his M.tech in Computer Science and Engineering from Guru Nanak Dev University, Amritsar (INDIA). His research areas include Networking, Operating systems, Distributed computing, Mobile agents. He has various research publications in various international conferences and journal and also presented several papers in various national and international conferences.

