International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 7-14
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

A REVIEW AND COMPARISON OF VARIOUS BLOCK CIPHER AND STREAM CIPHER ALGORITHMS

Amaan Anwar
Department of Computer Science & Engineering
Jamia Hamdard, New Delhi, India

Abstract— **These days, Data security is extremely testing issue that touches numerous ranges including PCs and correspondence. As of late, we went over numerous attacks on digital security that have played with the secrecy of the clients. These attacks simply broke all the security algorithms and influenced the authentication, confidentiality, availability, integrity and identification of user data. Cryptography is one such approach to ensure that authentication, confidentiality, availability, integrity and identification of user data can be kept up and security and protection of data can be given to the client. Encryption is the way toward changing over ordinary data or plaintext to something vast or figure message by applying scientific changes or formulae. These scientific changes or formulae utilized for encryption procedures are called algorithms. I have investigated eight data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, RC5 and IDEA and so forth. In which DES, Triple DES, AES, RC5, BLOWFISH and IDEA are symmetric key algorithms. RSA and ECC are asymmetric key cryptographic algorithms. In this paper, I have examined different encryption algorithms on the premise of various parameters and contrasted them with pick the best data encryption algorithm with the goal that we can utilize it in our future work.**

I. INTRODUCTION

Cryptography algorithm is the strategy or some equation that makes data or network secure by giving security. Cryptography is the study of contriving strategies that permit data to be sent in a protected form in a manner that the main individual ready to recover this data is the expected beneficiary. The exceptionally utilization of networking prompts to the data trade over the network while conveying to one and another network. While correspondence it is vital to encrypt the message with the goal that intruder can't read the message. Network security is based on cryptography. Essentially, Cryptography is an art of concealing data by encryptimg the message. The specialty of ensuring data (encryption) it into an unreadable format (encrypted text), called cipher text. Just the individuals who have a secret key can de-cipher (decrypt) the message into plain text. The network in which first data(Plain text) in encrypted at sender side and decrypted into plain text again at receiver end utilizing a unique key or some specific equation is known as a Cryptographic network. Encrypted messages can once in a while be broken by cryptanalysis, additionally called code-breaking.

In Modern cryptography procedures are for all intents and purposes unbreakable. As the Internet and different types of electronic correspondence turn out to be more predominant, electronic security is turning out to be progressively essential. Cryptography is utilized to ensure email messages, credit card data, and corporate information. A standout amongst the most famous cryptography systems utilized on the Internet is Pretty Good Privacy since it's viable and free.

On the premise of the input data, cipher algorithm are delegated block cipher, in which the measure of the block is fixed for encryption and stream cipher in which a continous stream is passed for encryption and decryption. Among the calculations thought about, some of them are block cipher like RSA, DES, AES, Blowfish, Twofish, Threefish and so forth and some of them are stream cipher i.e. ECC, RC5 and so forth.

II. OUTLINE OF VARIOUS ALGORITHMS

In this segment I will talk about different cryptographic algorithms to be investigated for their execution assessment. To begin the analysis of algorithm firstly we ought to know that what is Algorithm really. "An algorithm is a grouping of unambiguous directions for taking care of an issue", i.e., for acquiring a required yield for any true blue contribution to a limited measure of time. I am taking eight encryption algorithms those are DES, Triple DES, RSA, AES, ECC, BLOWFISH, RC5, IDEA and so on.

1. Rivest-Shamir-Adleman (RSA)

The RSA (Rivest-Shamir-Adleman) algorithm is the most vital public key cryptonetwork. It is best known and generally utilized public key. It utilizes extensive numbers like 1,024 bits in size. It has one round of encryption only. It is asymmetric block cipher. RSA is a algorithm utilized by todays computer to encrypt/decrypt messages. RSA is an asymmetric cryptographic algorithm. Asymmetric implies that there are two distinctive keys are utilized as a part of encryption and decryption process.

This is additionally called public key cryptography, since one of them can be shared with everybody and another key must be kept private. It depends on the calculating issue. RSA remains for Ron Rivest, Adi Shamir and Leonard Adleman, who created and openly portrayed it in 1978. Anybody can utilize public key for encryption of a message, however with right now distributed strategies, if public key is sufficiently large, as it were somebody with learning of the prime factorization can possibly decrypt the message. The RSA algorithm can be utilized for both digital signature and public key encryption.
RSA Algorithm:-,

1. select p and q
2.calculate n = p * q
3. calculate φ(n) = (p - 1) * (q - 1)
4. select e s.t(such that) 1 < e < φ(n) and e and n are co-prime.
5. calculate d s.t (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)

Consequently, by taking above algorithm the plain content in encrypted form (cipher text) and then decrypted from cipher to plain text.

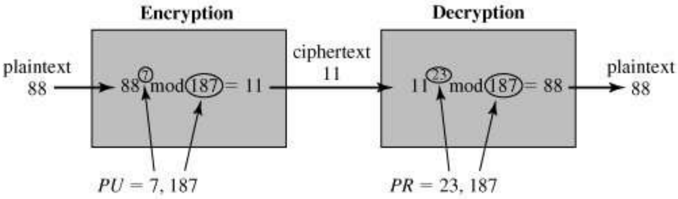

Fig: **RSA Algorithm Example**

In RSA cryptographic algorithm the primary drawback is its encryption speed. It expends plenty of time for data encryption. Really this is drawback of asymmetric key algorithms. It gives great level of security however it is slow for encrypting documents. Another risk in this algorithm is fake key inclusion at decryption level so the mystery key ought to be private and right to accomplish the encryption in fruitful way.

2. International Data Encryption algorithm(IDEA)

IDEA (International Data Encryption algorithm) is a block encryption algo composed by Xuejia Lai and James L and it was initially depicted in 1991.The unique algorithm experienced couple of alterations lastly it got named as International Data Encryption Algorithm (IDEA).
IDEA is a block cipher that works with 64 bit input (plain text and cipher text) blocks and it is controlled by 128 bit key. This algorithm deals with 64-bit plain text and cipher text block (at a movement). For encryption reason, the 64-bit plain text is separated into four 16 bits sub-blocks. In our examination, we mean these four pieces as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits).

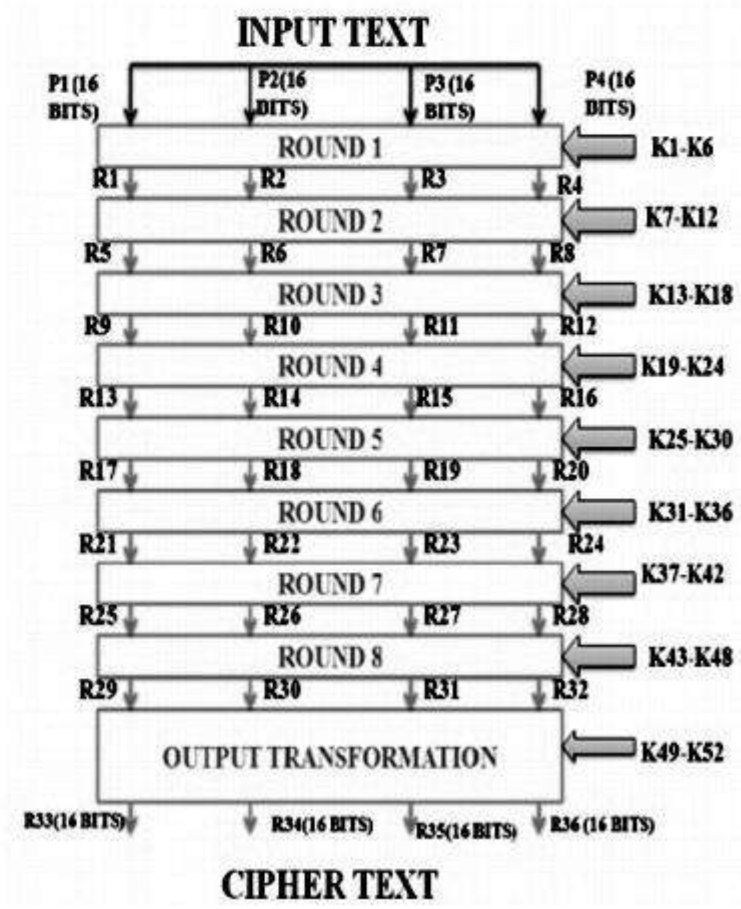

Fig: IDEA algorithm

Each of these blocks experiences 8 rounds and one output transformation phase. In all of these eight rounda, a few (logical and arithmetic) operations are performed. All through the eight rounds, similar successions of operations are rehashed.
In the last stage output transformation phase, we perform just arithmetic operations. Toward the start of the encryption procedure, the 64 bit plain text is isolated in four equivalent size blocks and prepared for round1 input. The yield of round1 is the input of round2. Essentially, the yield of round2 is the input of round3, etc. At last, the yield of round8 is the input for output transformation, whose yield is the resultant 64 bit cipher text [lets take C_1 (16bits), C_2 (16 bits), C_3 (16 bits) and

C_4 (16 bits)]. As IDEA is a symmetric key algo, it utilizes a similar key for encryption/decryption. The decrypting procedure is the same as the encryption procedure aside from that the sub keys are inferred utilizing an alternate algorithm. The measure of the cipher key is 128bits. In the whole encryption we utilize add up to 52 keys (round1 to round8 and output transformation phase), created from a 128 piece cipher key. In each round (round1 to round8) we utilize six sub keys. Every sub-key comprises of 16bits and the output transformation utilizes 4 sub-keys.

3. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was found in 1985 by Victor Miller from IBM and Neil Koblitz from University of Washington as an option for executing public key cryptography. This ECC (Elliptic Curve Cryptography) is Built on algebric structures of elliptic curves over limited fields i.e. Elliptic curve theory. ECC Create Faster, Smaller and more proficient keys when contrasted with other encryption algorithm. In this, encryption is done in elliptic curve equation form. ECC is that much productive that it can yield a level of security with 164 bit key that other network require a 1,024 bit key to accomplish that security level i.e.it offers the greatest security with smaller bit sizes that is the reason it expends less power and thus, Elliptic curve cryptography is useful for battery reinforcement moreover. The utilization of elliptic curve in cryptography was recommended autonomously by Neal Koblitz and Victor S. Miller in 1985.. Fundamentally, an elliptic curve is a plane curve over a limited field.
Which comprises of the point values fulfilling the condition,
y2 = x3+Ax+B,
Where a and b are the constant point values.
In the encryption procedure of Elliptic curve cryptography, we have numerous choices to utilize ECC cryptography yet we will talk about easiest way.
As per this encryption procedure,
1. The sender should first encode any message M as a point on the elliptic curve Pm.
2. The user should first encode any message M as a point on the elliptic curve Pm.
3. Select appropriate curve and point G as in D-H.
4. Every user picks private key nA<n and processes open key PA=nAG
5. For encryption:
Pm : Cm={kG, Pm+kPb}, where k is a random number
6. For decryption decrypt Cm process:
Pm+kPb–nB(kG) = Pm+k(nBG)–nB(kG) = Pm

These days, it is basically utilized as a part of the resource constrained environments, for example, mobile network and ad-hoc wireless network. The primary preferred standpoint of ECC uses short key length which prompts to quick encryption speed and less power utilization. For instance, a 160 bit ECC encryption key size give the same level of security as 1024-bit RSA encryption key and it perform 15 times quicker relying on the platform on which it is implemented. The shortcoming of ECC is that it increases the size of encrypted text and second shortcoming is that ECC is reliant on exceptionally complex equations which prompt to rise the complexity of encryption algorithm.

4. RC5

RC5 is a symmetric key block cipher. It is developed by Ronald Rivest in 1994. RC("Rivest Cipher") or it is likewise called "Ron's Code". AES (Advanced Encryption Standard) is straightforwardly in view of RC5. It utilizes key sizes 0 to 2040 bits however recommended count is 128 bits. RC5 utilizes block sizes of 32, 64 or 128 bits yet 64 bits are proposed. It's fiestel-like network. It has 1 to 255 encryption rounds yet 12 rounds are recommended initially. It is appropriate for software/hardware implementation, since it utilizes just those operations which are accessible in typical microprocessor.

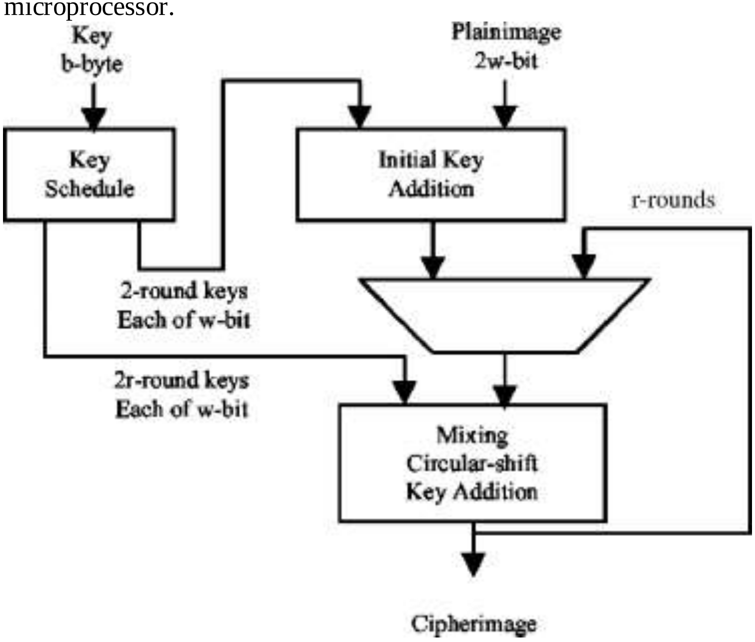

Fig: **RC5 Encryption Procedure**

Above Figure is demonstrating the fundamental working method of RC5 encryption algorithm. The RC5 encryption algorithm is a block cipher that proselytes plain text data blocks of 16, 32, and 64 bits into cipher text(block) of a similar length. The algorithm is sorted out as an arrangement of iterations called rounds r that takes values. RC5 works with two 32 bit registers A which contains the initial input text(plain text) and B contains the output cipher at the Encryption end. To start with we place plain text into the registers A and B then encryption/decryption are applied on it. In encryption strategy, Input text is kept in two 32 bit input

registers A and B where number encryption round are 2r+2 and round keys will be
S[0, 1, 2,… .2r+1].
Output stored in A and B.

```
Steps: A = A + S[0] and B = B + S[20]
for i = 1 to r
do{
A = $((A \oplus B) <<< B) + S[2i]$
B = $((B \oplus A) <<< A) + S[2i+ 1]$
}
```

After this procedure the data is encrypted and kept in registers A and B called cipher text.
For decryption process, Cipher text is paced in registers A and B.

```
Steps: for i = r back to 1
do{
B = $((B - S[2i + 1]) >>>A) \oplus A$
A = $((A - S[2i]) >>> B) \oplus B$
}
B = B – S[20] and A = A - S[0]
```

After this we will get the estimation of A and B.
This algorithm reverses operations on registers A and B.

5. Blowfish

Blowfish was created by Sir Bruce Schneier in 1993. It is fundamentally a symmetric block cipher having variable length key from 32 bits to 448 bits. It works on block size 64 bits. It is a 16-round Feistel cipher and uses huge key dependent S-Boxes. Every S-box contains 32 bits of data.

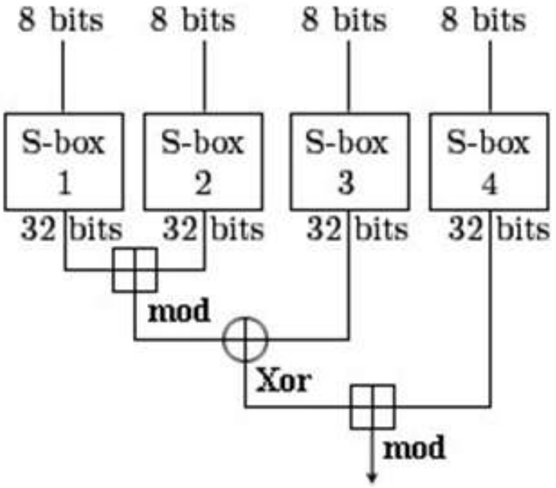

Fig: Blowfish Function F

Above Diagram demonstrates the Blowfish's F-function. The function divide the 32 bit input to four 8-bit quarters, and uses the quarters as input to S-boxes. The yields are then added with (Mod) modulo 232 and XORed to deliver the last 32-bit yield i.e. encrypted data. For Decryption at another end a similar procedure happens, however in turn around order.

Till now, no assault has been discovered fruitful against Blowfish encryption algorithm.
Blowfish is a variable key length algorithm and it have 64-bit block cipher. The algorithm comprise of two sub parts, one is key extension part and second data encryption part. Data encryption is finished by finishing 16 rounds fiestel network. Each round comprise of key reliant permutation in P-Box and key/data reliant substitution in S-Box.
Algorithm comprises of S-Box and P-Box.
The P-array comprises of 18 sub-keys of 32-bit.
P1, P2,...,P18.
There are four 32-bit S-boxes in which 256 entries in each:
$S_1[0]$, $S_1[20]$,..., $S_1[255]$; $S_2[0]$, $S_2[20]$,..,, $S_2[255]$; $S_3[0]$, $S_3[20]$,..., $S_3[255]$; $S_4[0]$, $S_4[20]$,..,,$S_4[255]$.
For encryption following method is carried out,

```
* Divide x into two 32-bit parts:
 (xL) and (xR)
 For i = 1 to 16:
 xL = xL XOR Pi
 xR = F(xL) XOR xR
 then Swap xL and xR
 Next i
then Swap xL and xR  =>or Undo the last swap.
 xR = xR XOR P17
 xL = xL XOR P18
 then Recombine xL and xR.
*Divide xL into four eight-bit quarters: a, b, c, and d
F(xL) = ((S1,a + S2,b $mod_{232}$) XOR S3,c) + S4,d $mod_{232}$
```

Decryption is precisely the same as encryption in reverse order.
Blowfish gives a decent encryption rate in software. It is much quicker than DES and IDEA. In numerous encryption experiment the Blowfish encryption algorithm is pronounced best in security level it offers and speed of encryption, which is superior to the majority of the encryption algorithm accessible.

6. Data Encryption Standard (DES)

It was produced in the mid 1975 at IBM labs by Horst Fiestel. The DES was endorsed by the NBS (National Bureau of Standards, now called NIST - National Institute of Standards and Technology) in 1978. The DES was institutionalized by the ANSI (American National Standard Institute) under the name of ANSI X3.92, also known as DEA (Data Encryption Algorithm). The DES was previously a prevalent symmetric-key algorithm for the encryption of data. In any case, now it is an obsolete symmetric key data encryption technique. DES utilizes 56 bits key for encryption/decryption. It finishes the 16 rounds of encryption on each 64 bits data blocks.

Data encryption standard deals with a specific guideline. Data encryption standard is a symmetric encryption framework that utilizations 64-bit pieces, 8 bits (one octet) of which are utilized for parity checks (to confirm the key's integrity). Each of the key's parity bits (1 each
8 bits) is utilized to check one of the key's octets by odd parity, that is, each of the parity bits
is acclimated to have an odd number of '1's in the octet it has a place with. The key in this way has a genuine valuable length of 56 3bits, which implies that exclusive 56 bits are really utilized as a part of the algorithm. So it would take a most extreme of (2)^56 or 72,057,594,037,927,936, attempts to locate the right key.

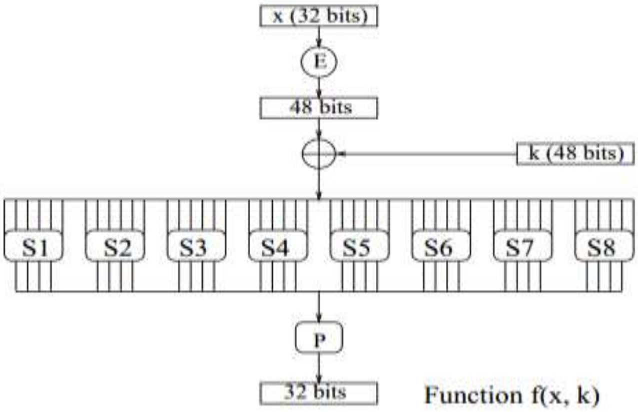

Fig: **Function F of DES**

The structure of function F of DES algorithm. The block of the message is isolated into two parts. The right half is extended from 32 to 48 bits utilizing another fixed table. The outcome is consolidated with the sub-key for that round utilizing the XOR operation. Utilizing the S-boxes the 48 coming about bits are then changed again to 32 bits, which are accordingly permutated again utilizing yet another fixed table. This at this point completely rearranged right half is currently joined with the left half utilizing the XOR operation. In the next round, this combination is utilized as the new left half. Numerous security specialists felt the
56-bit key length was insufficient even before DES was received as a standard. All things considered, DES remained a trusted and broadly utilized encryption algorithm through the mid-
1990s. Be that as it may, in 1998, a PC worked by the Electronic Frontier Foundation (EFF) decoded a DES-encoded message in 56 hours. By using many networked pc, the next year EFF cut the decoding time to 22 hours. Data Encryption Standard can likewise be utilized for single client encryption like putting some data in hdd.

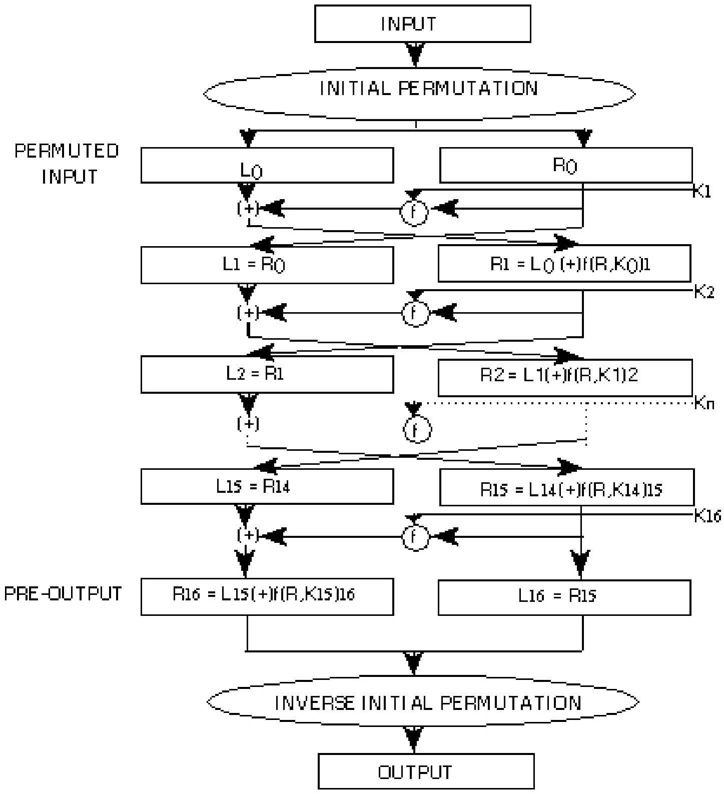

Fig: **DES Encryption Procedure**

In its encryption procedure, DES utilizes 56 bits key for encryption/decryption. It finishes the 16 rounds of encryption on each 64 bits data blocks. In all rounds, encryption is done utilizing function F. DES have three methods of operation: ECB (Electronic Code Book), CBC (Block cipher Chaining), CFB(Cipher Feedback) and OFB(Output Feedback). Encryption quality is specifically attached to key size, and 56-bit key lengths have turned out to be too little in respect to the power of current computers. In this way, NIST felt the need of new and more secure data encryption algorithm in the field. The Data Encryption Standard was authoritatively pulled back in May 2005. There is no solid confinement discovered as opposed to its little key size which offers less security. The main fruitful attack on DES is Brute Force. It's another powerless point
is its encryption speed which is low.

7. Triple Data Encryption Standard (3DES)

In cryptography methods, Triple Data Encryption Standard (3DES) is the basic name for the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to every block of data. Triple-DES is likewise proposed by IBM in 1978 as a substitute to DES. In this way, 3DES is just the DES symmetric encryption algorithm, utilized three times on the same data. Three DES is likewise called as T-DES. It utilizes the straightforward DES encryption algorithm three times to upgrade the security of text which is encrypted.

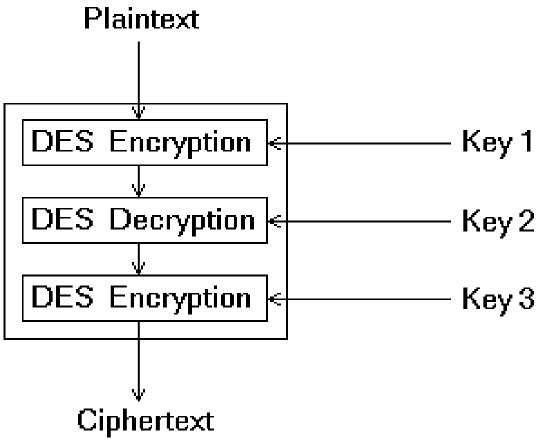

Fig: **3DES Structure**

In this, same data is encrypted 2X more utilizing DES. Consequently, this makes the encryption more stronger and more hard to break. Triple DES is essentially a block cipher which utilizes 48 rounds (Three times the DES) in its algorithm, and has a key length of 168 bits. 3-DES additionally utilizes the Block size of 64 bits for encryption. And the modes are :

- **DES-EDE3** : Encrypt, Decrypt and Encrypt with 3 one of a kind keys as said above (Key1, Key2, Key3).
- **DES-EEE3** : A data block is encrypted, and encrypted again with an alternate key lastly encrypted yet again with another key, utilizing a sum of 3 special keys.
- **DES-EDE2** : Here we just utilize two keys, in which the first and last encryption is
done utilizing the very same key.
- **DES-EEE2** : this also utilizes two keys, the first and last encryption is carried out utilizing a same key.

3DES is a trap to reuse DES encryption algorithm however with three different keys. 3DES
is accepted to be secure up to no less than (2)^112 security, however it is slow, particularly in computing software. 3-DES likewise gives sufficient security. That is the reason clients required the successor of 3-DES.
The fundamental preferred standpoint of Triple DES is that it is three times secure (as it is blend of three DES algorithms with various keys at every level) than DES that is the reason it is favored over basic DES encryption algorithm. It give satisfactory security to the data yet, it is not the best since it devours part of time and its encryption speed additionally less than DES encryption algorithm.

8. Advanced Encryption Standard(AES)

In 1997, the National Institute of Standards and Technology (NIST) declared an activity to pick a successor to DES; in 2001, it choose the Advanced Encryption Standard as a substitution to DES and 3DES. AES (Advanced Encryption standard) is created by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher utilized by the U.S. government to secure ordered data and is executed in hardware and software all through the world for delicate data encryption. AES is really, three block ciphers, AES-128, AES-192 and AES-256. Every cipher encrypt/decrypt data in block of 128 bits utilizing cryptographic keys of 128 bits, 192 bits and 256 bits, separately. In AES there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

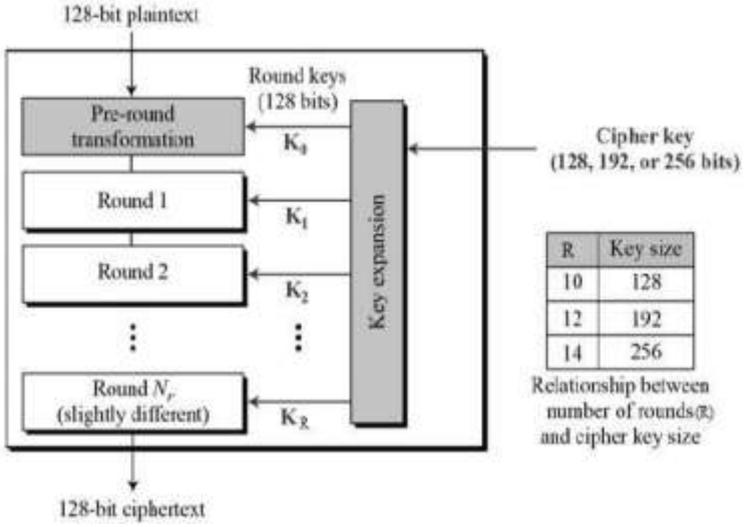

fig: **AES Algorithm**

For every situation, every single round are indistinguishable, with the exception of the last round.
Each round in encryption follows certain steps to complete round till n. Each round have four rounds i.e. Shift rows, Substitute byte Add round key and Mix Column.

Substitution round: In this progression, Sub-Bytes are byte-by-byte substituted amid the process of forward encryption.
Shift Rows: In this, moving the rows of the state array amid the forward process(S-Box)
Mix Column: Mix Columns for stirring up of the bytes in every column independently amid the forward process.

Add Round Key: In this progression, round key is added to the yield of the previous step during the forward process. This progression contrasts from others bcoz of key size variation. In AES process of encryption, it utilizes diverse round keys. These keys are connected alongside other arithmetic operations on a set of data. This data is available in block of specific size. This is known as state array. This encryption procedure incorporates taking after process:

1. Initially determine the diverse round keys from cipher key.
2. Instate the state array with data block or plaintext.
3. Begin with starting state array by including round key.
4. Perform the process of state manipulation in nine rounds.
5. After tenth round of manipulation, we will get the final yield as cipher(text).

By taking after above process we get the final encrypted text(cipher text).

III. COMPARISON CHART

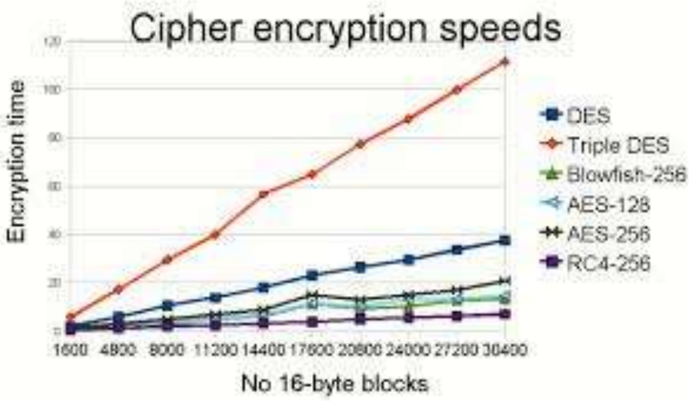

Chart: encryption speed of various algorithm

IV. COMPARATIVE TABLE

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

Parameters- → Algorithms ↓	DEVELOPMENT	LEVEL OF SECURITY	ROUNDS	KEY LENGTH (Bits)	BLOCK SIZE (Bits)	ENCRYPTION SPEED	ATTACKS FOUND
RSA	Ron Rivest, Shamir & Leonard Adleman in 1978	Good level of security	1	Key length depends on no. of bits in the module	Variable block size	Average	Brute force attack, timing attack
IDEA	Xuejia Lai and James in 1991	Secure	8	128	64	Fast	Linear attack
ECC	Victor Miller from IBM and Neil Koblitz in 1985	Highly secure	1	Smaller but effective key	Stream size is variable	Very Fast	Doubling attack
RC5	Ron rivest in 1994	Secure	1 to 255(64 suggested)	0 to 2040 bits key size(128 suggested)	34 , 64, 128(64 suggested)	Slow	Co-relation attack, Timing attack
BLOWFISH	Bruce Schneier in 1993	Highly secure	16	Variable key length i.e. 32 – 448	64	Very fast	No attack is found to be successful against blowfish.
DES	In early 1970 by IBM and Published in 1977.	Adequate security	16	64 (56 usable)	64	Very slow	Exclusive Key search, Linear cryptanalysis, Differential analysis
3DES	IBM in 1978.	Adequate security	48	168,112	64	Very slow	Related Key attack
AES	Vincent Rijmen, Joan Daeman in 2001	Excellent security	10,12,14	128,192, 256	18	Faster	Key recovery attack, Side channel attack

V. CONCLUSION

In this paper, I have examined different encryption algorithms. I have found that every algorithm has its own advantages as indicated by various parameters. From the work finished in this paper it is noticed that, that the strength of each encryption algorithm relies on the number of bits used in a key, kind of cryptography, key management, number of keys,. Longer the key length and data length more will be the power utilization that will prompt to more heat dissipation. Along these lines, it is not fitting to utilize short data sequence and key lengths. All the keys are based upon the mathematical properties and their strength degrade with respect to time. The keys having more number of bits requires more algorithm time which basically shows that the network takes more time for data encryption. From above study we have found that ECC and Blowfish, these two encryption algorithms are driving with the security level that they give quicker encryption speed. ECC is having a few assaults on it however on Blowfish, no assault is fruitful yet. Thus, from this review and comparison I have shortlisted ECC and Blowfish encryption algorithm. These two encryption algorithms are more secure and quick to work with and in future, there is wide extent of change in these both encryption algorithms.

VI. REFERENCE

[1] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”

[2] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e, **(2005)**.

[3] E. Biham and A. shamir, "A differential crypto analysis of data encryption standard", Springer-verlag, **(1993)**.

[4] W. Stallings, "Cryptography and Network Security: Principles and Practice", **(1999)**, Prentice-Hall, New Jersey.

[5] R. L. Rivest, “The RC5 Encryption Algorithm”, Proceedings of the Second International Workshop on Fast Software
Encryption (FSE), **(1994)**.

[6] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal Research Develop., vol. 38, no. 3, **(1994)**, pp. 243 -250.

[7] 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.

[8] M. Kumar and E. G. Dharma, “A comparative analysis of symmetric key encryption algorithm”, IJARCET, vol. 3, no. 2, **(2014)**.

[9] J. Daemen, R. Govaerts and J. Vandewalle, “Weak Keys for IDEA”, Springer-Verlag, **(1998)**.

[10] G. C. Kessler, “An Overview of Cryptography”, http://www.garykessler.net/library/crypto.html, **(2006)**.

[11] A. Nadeem, “A performance comparison of data encryption algorithms”, IEEE data and Communication Technologies , **(2006)**, pp. 84-89.

[12] W. Diffiee and M. Hellman, “New Directions in Cryptography”, IEEE Transaction Data Theory IT-22, **(1976)**, pp. 644-654.