Data Encryption Standard Algorithm (DES) for Secure Data Transmission

Nirmaljeet Kaur
Research scholar
BGIET,Sangrur,India

Sukhman Sodhi
Assistant Professor
BGIET,Sangrur,India

ABSTRACT
Cryptography is a technique for secure data communication. Encryption is the process of encoding messages in such a way that only authorized parties can read it. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. DES algorithm is a 64 bit block cipher with key of 56 bits. In this paper we will discuss the DES technique for secure data transmission while maintaining the authenticity and integrity of the message. In this, message is encrypted before the data transmission process starts. The encryption and decryption of data is done by using the data encryption standard algorithm [1].

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
Cryptography, symmetric key, asymmetric key, DES algorithm

1. INTRODUCTION
Data Security is the main aspect of secure data transmission over unreliable network. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. For the security purpose there is a concept of cryptography. Cryptography provides the security to the data by hiding the data from unauthorized user. It provides a security by giving a concept of encryption and decryption. The process of encoding the plaintext into cipher text is called Encryption and reverse of decoding cipher text to plaintext is called Decryption. This can be done by two techniques i.e by symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography uses the same key for encryption and decryption. But the Asymmetric key cryptography uses one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature etc[4].

2. DATA ENCRIPTION STANDARD ALGORITHM
DES is a block cipher; it encrypts the data in a block of 64 bits. The key length is 56 bits, initially the key consists of 64 bits. The bit positions 8, 16, 24, 32,40,48,56, 64 are discarded from the key length [1].

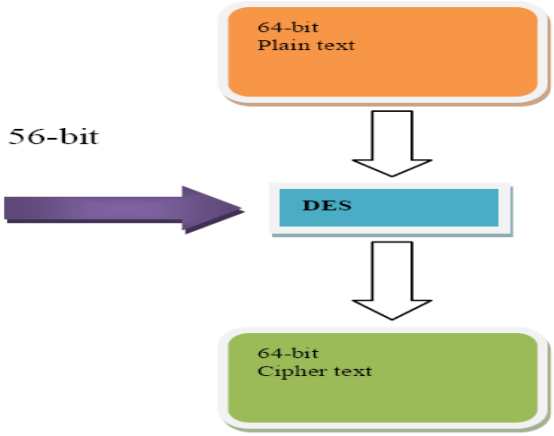

Fig 1: Working of DES

DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which is called as a Round Algorithm:-

1. In the first step, the initial 64-bit plain text block is handed over to the Initial Permutation (IP) function.
2. The Initial permutation is performed on the plain text.
3. The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).
4. Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key:

a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.

b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.

c. Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step.

d. Using the S-box substitution 32-bits are produced from 48-bits.

e. These 32 bits are permuted using P-Box Permutation.

f. The output of P-Box is XORed with the LPT which is of 32 bits.

g. The result of the XORed (32 bits) becomes the RPT and old RPT become the LPT.This process is called as Swapping.

2.1 Double DES

Two DES is same as DES but in this some processes are repeated two times using two keys i.e. K1 and K2.First the K1 key is applied on the plain text and it is converted into the cipher text and then K2 key is applied to produce the resultant cipher text.

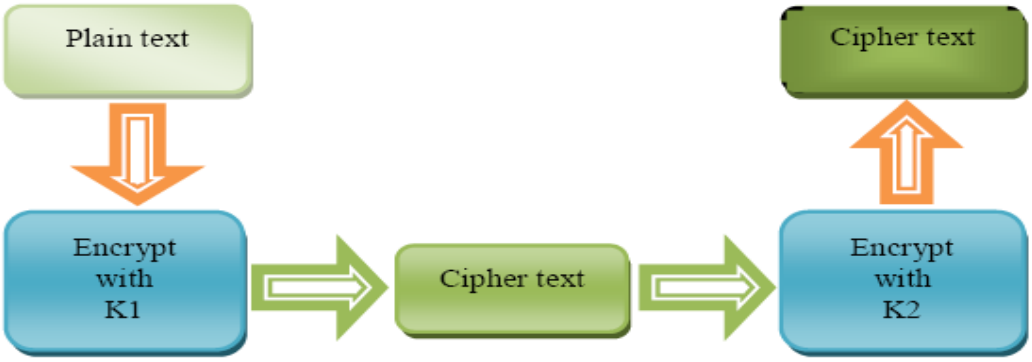

Fig 2: Encryption process using two keys K1 and K2

2.2 Triple DES

Triple DES is DES three times, In 3 DES the plain text block P is first encrypted with a key K1, then encrypted with second key K2, and finally with third key K3, where K1, K2 and K3 are different from each other.

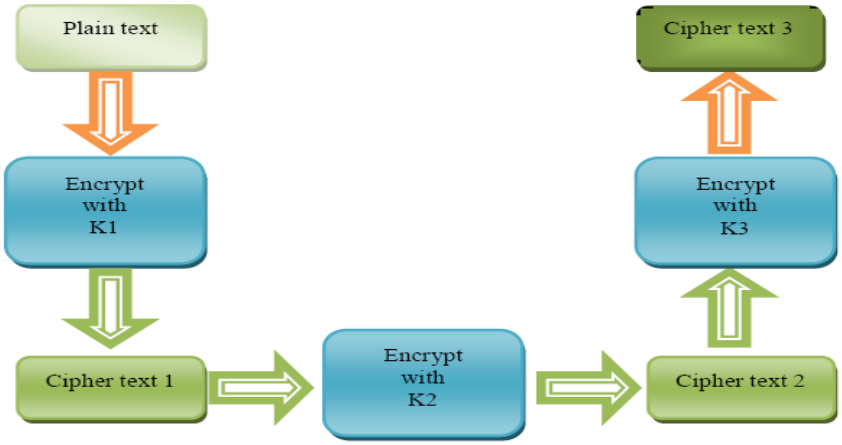

Fig 3: Encryption process in Triple DES with three keys K1 , K2 and K3.

3. KEY GENERATION PHASE

The system requires input key (64 bits). This will be converted to binary value and then 56 bit key is produced. 1 bit is placed at every even place and 0 is placed at every odd place of 56 bit block [11].

1) Divide the result into two halves (28 bit each) (C0 and D0)

2) To obtain C1 and D1, perform left shift to the previous results.

3) Find the value of K1 where K1= C1 || D1. The pipes (||) indicate concatenation.

4) Concatenate C1 and D1 to achieve 56 bit block and use this as input to the next round to obtain C2 and D2, C3 and D3 and so on .

5) In the 56 bit block, every even bit is substituted with 1 and every odd position is substituted with 0 bit

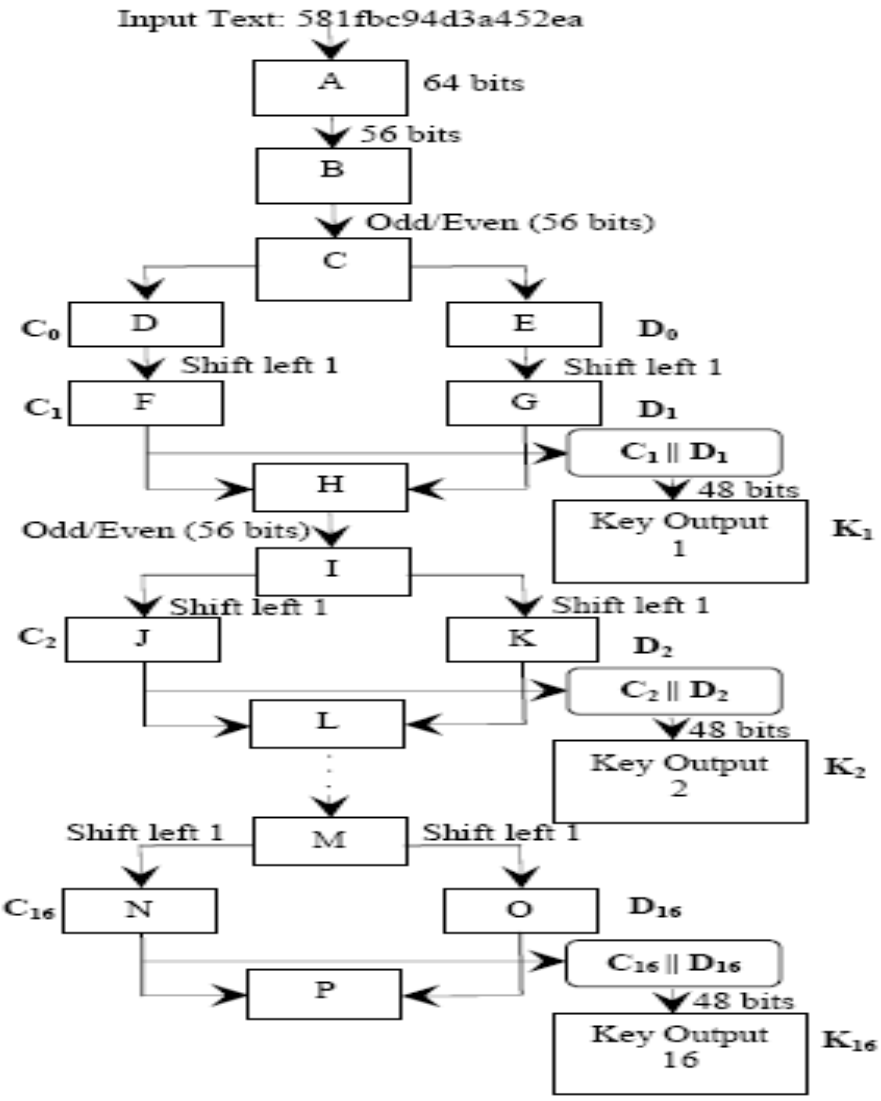

Fig 4: Key generation process

4. DATA ENCRYPTION

In data encryption phase first the initial permutation of the plain text is generated .The result of permutation is spited into two halves, L0, (left) and R0 (right). Each half is of 32 bits in length [5].

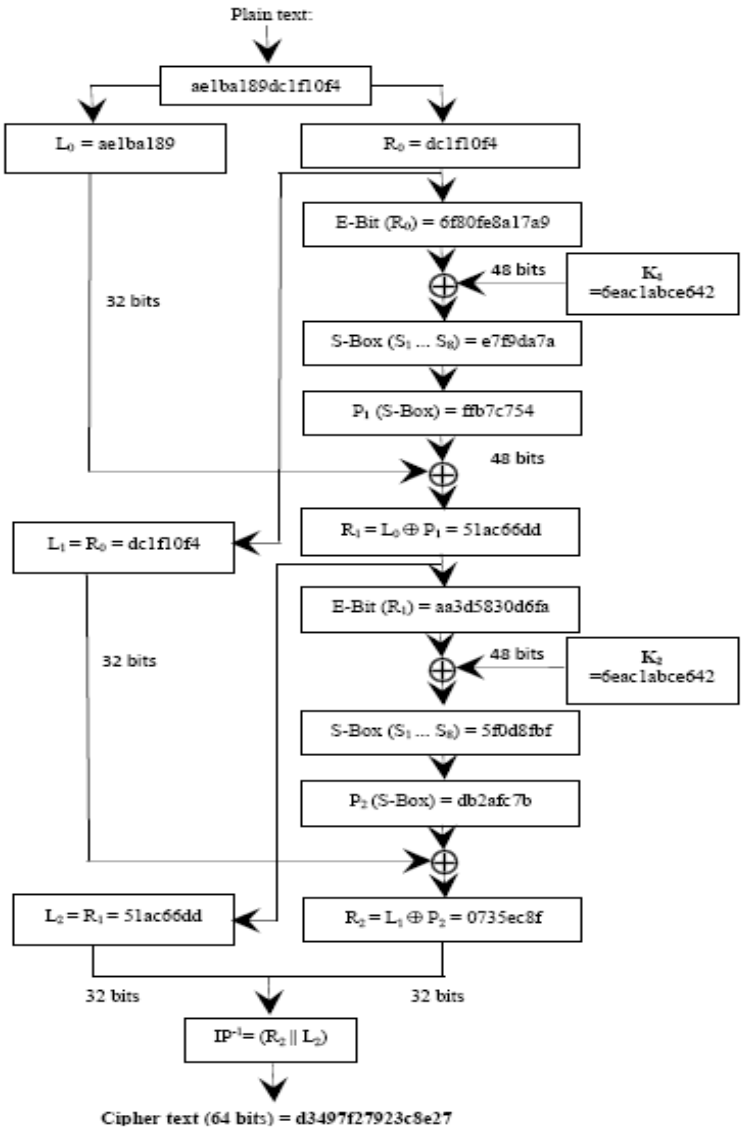

Fig 5: DES Encryption

5. DES DECRYPTION

During the first round of the decryption process, the cipher text is divided into two halves, L2, (left) and R2 (right) .

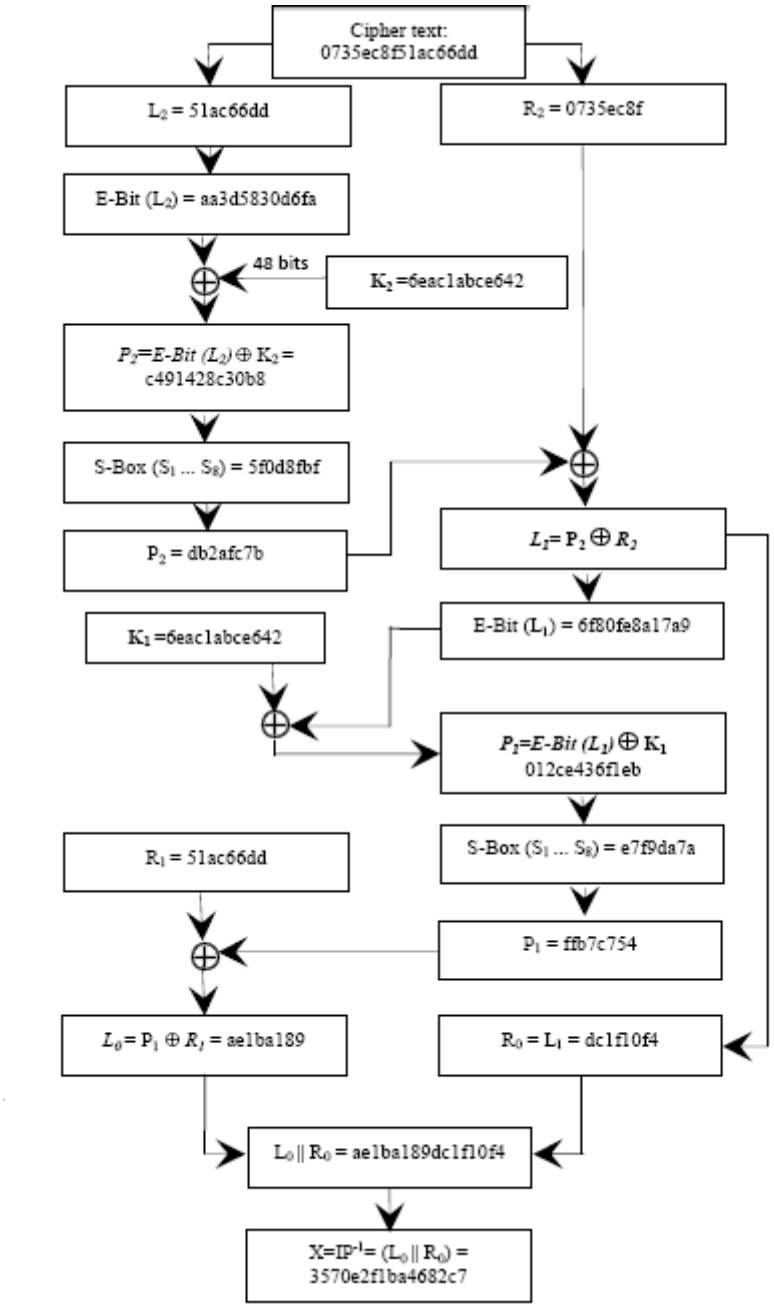

Fig 6: DES Decryption

6. RESULTS

6.1 Key generation

Key generation is a process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/ decrypted. The figure shows that the system requires input key (64 bits). This will be converted to binary value and then 56 bit key is produce.

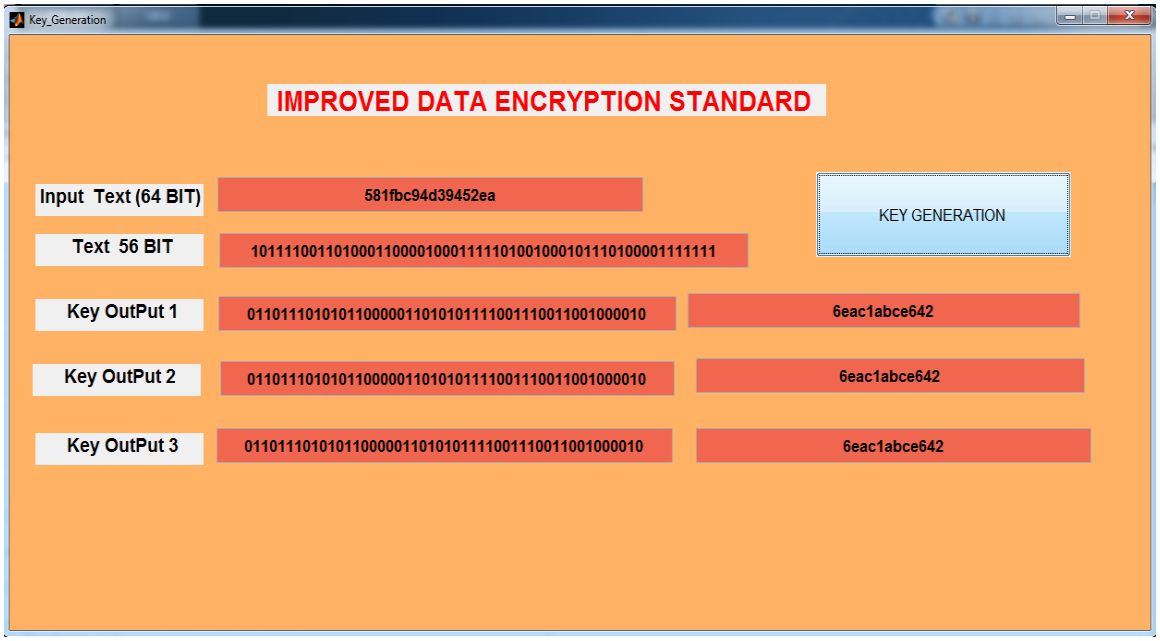

Fig 7: Key generation

6.2 Encryption

The figure shows that Initial permutation of the plain text is generated .The result of permutation is split into two halves, L(left) and R(right) blocks. Each half is 32 bits in length. Final encrypted text is of 64 bits.

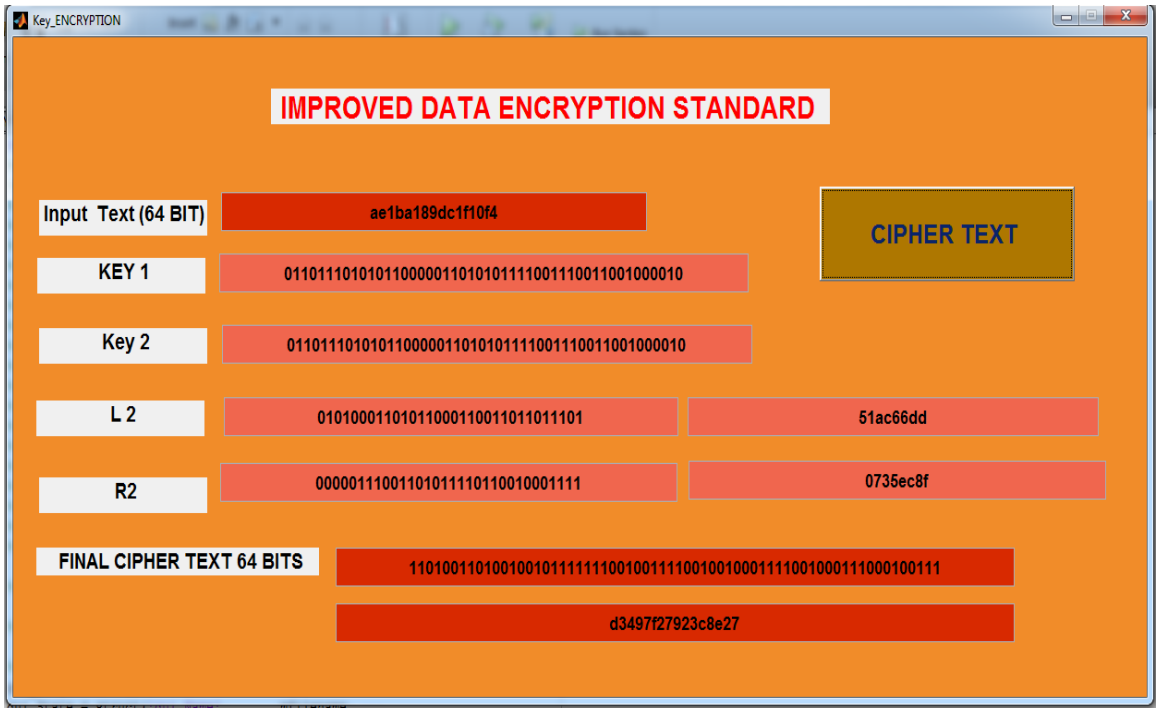

Fig 8: Encryption Process

6.3 Decryption

The figure shows that during the first round of the decryption process, the cipher text is divided into two halves, L(left) and R(right) blocks. Finally the original text is achieved.

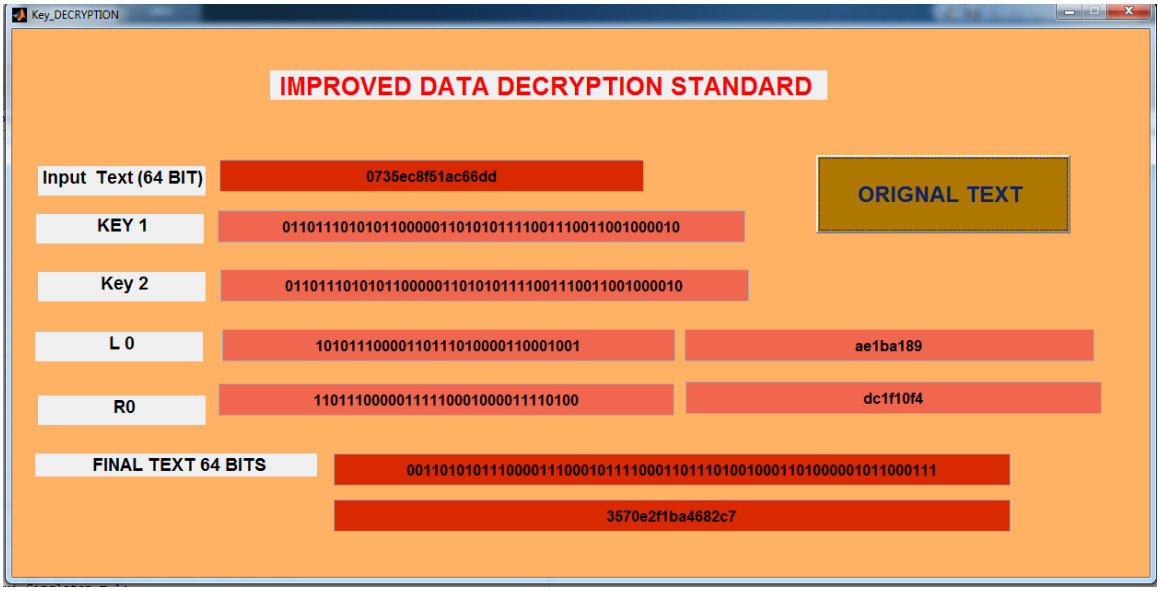

Fig 9: Decryption Process

7. CONCLUSION AND FUTURE SCOPE

As we are moving towards the society where automated information resources are very much in use , it is very important to provide a secure mechanism for data transmission. DES is now considered to be an insecure technique of encryption for some applications like banking system. There are some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new level of security to it. In future we can modify this algorithm by modifying the function implementation ,S- box design and replacing the old XOR by new operation .

8. REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.

[2] Dr. Mohammed M. Alani ― "Improved DES Security"‖, International Multi-Conference On System, Signals and Devices, 2010.

[3] Dhanraj, C.Nandini, and Mohd Tajuddin ― "An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard" ,International Journal of Research And Review in Computer Science,August 2011

[4] Behrouz A. Forouzan." Cryptography and Network Security". Tata McGraw-Hill, 2007.

[5] Goyal Shivangi, (2012), "A Survey on the Applications of Cryptography" International Journal of Science and Technology Volume 1 No. 3.

[6] Kumar aman, Jakhar Sudesh & Makkar Sunil, (2012), "Comparative Analysis between DES and RSA Algorithm's" International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, vol 2.

[7] A.Nath, S.Ghosh, M.A.Mallik, (2010), "Symmetric key cryptography using random key generator" Proceedings of International conference, Vol-2, P-239-244.

[8] P.Saveetha & S.Arumugam, (2012), "Study On Improvement In RSA Algorithm And Its Implementation", International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3.

[9] Shasi Mehlrotra Seth, Rajan Mishra, (2011), "Comparative Analysis of Encryption Algorithms for Data-Communication", IJCST Vol. 2.

[10] Diaasalama, Abdul kader, MohiyHadhoud, (2011), "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, vol 2, no.1.

[11] K. Rabah(2005), "Theory and implementation of data encryption standard: A review", Information Technology Journal, 4: 307-325.