International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 2, February 2016

ISSN: 2394-4404

Improved Key Generation Algorithm In Data Encryption Standard (DES)

Deepika Rani Bansal

M.Tech Student,
Department Of Computer Science & Engineering,
Apex Institute Of Engineering & Technology,
Jaipur, India

Preeti Thakur

Professor,
Department Of Computer Science & Engineering,
Apex Institute Of Engineering & Technology,
Jaipur, India

Abstract: ***At present security is the major issue for confidential information. Information transmitted over network must be protected from attacks of intruders. Using encryption we can protect our important information from malicious users. Encryption is the method transforming information into format which is hard to understand. There are several algorithms for encryption with their benefits, security level and performance.***

Among these encryption algorithms DES (Data Encryption Standard) is also an encryption technique. It is simple and fast. It is based on hardware. Goal of designing an encryption algorithm is to provide better security and performance from attackers. DES has also security constraints. Here, a new method is introduced for key generation using two array of random numbers, of size eight. Using this method problems of weak and semi weak key can be resolved completely. In this improved key generation method security is enhanced because of random numbers array without compromising the performance.

Keywords: Encryption, security, performance, information;

I. INTRODUCTION

When we talk about security it is necessary that we know cryptography[1]. Today it is must to secure sensitive data transmitted over network or kept in storage from attackers[2].

Cryptography is a technique that provides mathematical steps to secure data [3]. Encryption word is attached with cryptography[4]. Encryption converts our sensitive data to unreadable form. Doing this we may be sure that no one can understand our data even it is leaked somehow. The form of data which is unreadable is called cipher text. Decryption is opposite to encryption. It converts unreadable data to readable data. Using encryption and decryption only intended parties can see the message.

According to [5] there are two types of cryptography:

- ✓ *Classical cryptography:* uses substitution and permutation to encrypt the message.
- ✓ *Modern cryptography:* uses various methods to encrypt the message.

Cryptography has following goals [6]:

- ✓ CONFIDENTIALITY: It is related to secrecy of message.
- ✓ INTEGRITY- Only authorized parties can alter the message not others.
- ✓ AUTHENTICATION*:* only those parties whose identification is checked and found correct can only access the data.
- ✓ NON-REPUDIATION*:* This service prevents the parties from denying their previous commitments.

As in [3] there are two types of cryptographic protocols:

- ✓ *SYMMETRIC KEY:* Same key is shared by both sender and receiver.
- ✓ *ASYMMETRIC KEY:* Sender and receiver have different keys, called public and private keys.

II. DATA ENCRYPTION STANDARD

In the context of symmetric cryptography DES (Data Encryption Standard) is widely used[2]. DES was developed by team of IBM in 1974[7]. It is published in United States National Bureau Of Standards in 1977[8].DES is a block cipher , it takes 64 bits size block of data and encrypt it into

ISSN: 2394-4404

equal size cipher text . DES is based on XOR operation and left shift rotation. Along these operations permutation and substitution are also used. DES has three phase:

- ✓ *KEY GENERATION:* There is 64 bit key from which 16, 48 bits keys are derived . These keys are derived using key generation algorithm. 64 bits key is gone through a parity drop table , where parity bit of the characters is discarded and permutation is done. Now it becomes 56 bits key , it is divided into two halves (C_0,D_0) C_0 and D_0 are left shifted separately . Shifting for round 1,2,9 and 16 is one bits and two bits for rest. After shifting C_0 and D_0 becomes C_1 and D_1 . These C_1 and D_1 are concatenated into C_1D_1 and then Permutation choice 2 is applied which yields 48 bits round key. This key is key1. For second round C_1 and D_1 are shifted then concatenated and permuted yielding key2 and C_2 and D_2. This process will be continued till round 16. At the end of round 16 we have 16, 48 bits keys. Which will be used later in encryption .

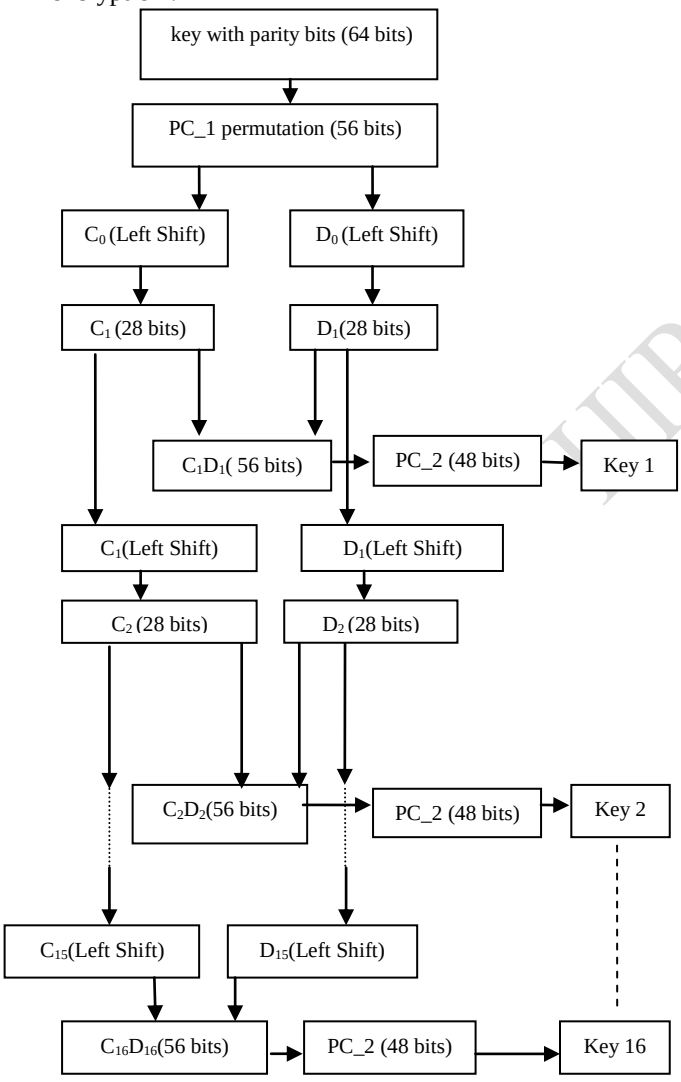

Figure 1: Key generation process

✓ *ENCRYPTION :* There are sixteen rounds of encryption. Sixteen keys(k1.....k16) are used in sixteen round(R1.....R16) respectively.

Encryption is performed on block of 64 bits[9]. After initial permutation this is divided into two halves L_0 and R_0, each of 32 bits. After that encryption is performed in following phases:

- *EXPANSION:* R is expanded 32 bits to 48 bits in every round.
- *XOR:* Expanded R and the key is XORed, yielding 48 bits.
- *SUBSTITUTION:* There are eight substitution boxes (s1,s2,....s8)[6]. Each box has four rows and sixteen columns. XORed 48 bits are divided into eight groups of six digits. Each group is passed through s-box(s1,s2,...s8). Every substitution box is like a matrix with rows and columns, first and last digits of a six bits group denote row of s-box and middle four bits denote column. After substitution we get four bits from each s-box, thus from eight s-boxes, 32 bits output comes.

Block diagram of the algorithm is given below

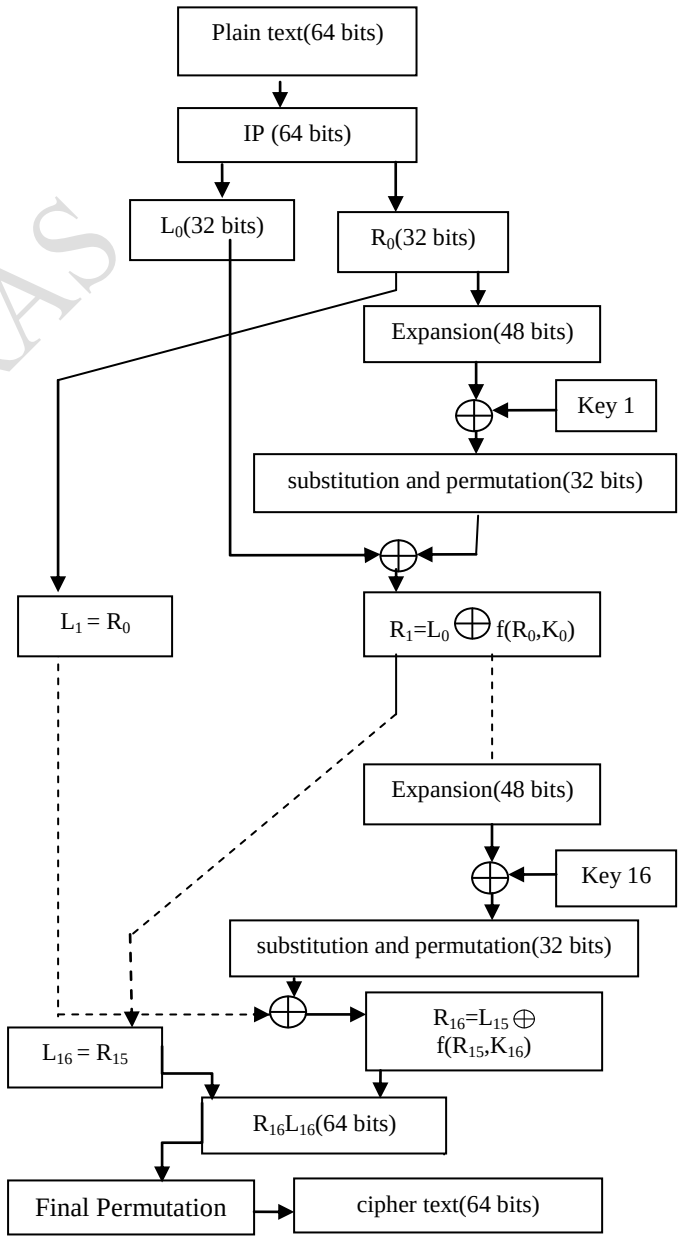

Figure 2: Encryption Process

ISSN: 2394-4404

- *PERMUTATION:* 32 bits are permuted according to a given array of permuted choice 2.

After permutation 32 bits are XORed with L. Result is become Right side (R) for next round, while old R side becomes new Left side(L). This process is repeated for sixteen rounds using the keys (k1....k16). After round 16, R_{16} and L_{16} are concatenated and then final permutation is done. Now result is 64 bits cipher text.

✓ *DECRYPTION:* Decryption is reverse process of encryption[5]. Initial permutation is done on 64 bits cipher text. Then it is divided into two halves each of 32 bits (L_{16},R_{16}). Now same process of encryption is repeated from round 1 to round 16, using the key 1 to key 16. In decryption process keys are used in reverse order means key 16 will be used in round 1, key 15 in round 2, key 14 in round 3 and so on. Block diagram for decryption is given in figure 3.

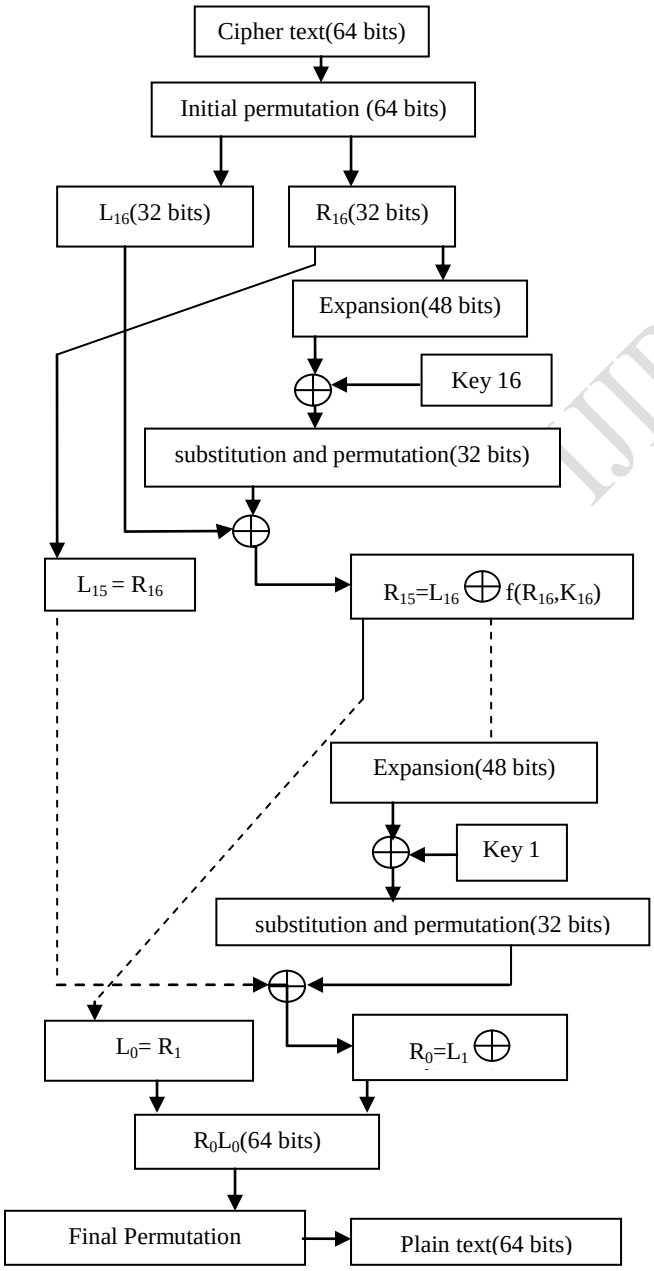

Figure 3: Decryption Process

At the end of sixteen rounds R_0, L_0 is concatenated and final permutation is done. Result is our 64 bits plain text.

Like other encryption algorithms DES is also prone to attacks.

There are following possible attacks on DES[2]:

- *BRUTE FORCE*: In this attack every possible combinations of 2^{55} are tried to find the plain text. Machine is used for this purpose.
- *DIFFERENTIAL CRYPTANALYSIS:* In differential cryptanalysis it is assumed that plain text is already known and only 48 bits keys are remaining to find. There are 2^{47} combinations.
- *LINEAR CRYPTANALYSIS*: This works like differential cryptanalysis but has only 2^{43} combinations.

DES has problems of weak and semi weak keys. Sometimes two keys generated by DES are same or palindrome of each other. These keys are called weak keys[6].

1F1F 1F1F 0E0E 0E0E	FEFE FEFE FEFE FEFE
1F1F 1F1F 1F1F 1F1F	0101 0101 0101 0101

Table 1: Weak Keys

In below table pairs of semi weak keys are shown. One of the keys in a pair would encrypt the message and second will decrypt it back. Keys are opposite to each other [6].

01E0 01E0 01F1 01F1	E001 E001 F101 F101
E0FE E0FE F1FEF1FE	FEE0 FEE0 FEF1 FEF1

Table 2: Semi Weak Keys

III. LITERATURE REVIEW

In [5] DES is improved using random number generator. Here message is divided into 64 bits blocks and different keys are generated using 56 bits master key. Keys generation is done using random number generator. Keys generated from 56 bits master are also 56 bits. For every block of message bits different key will be used. In this approach although security is enhanced but time taken to finish the process will be long enough.

Authors in [12] changed the XOR operation in DES. They replaced the two state key (0,1) from 4 state key (0,1,2,3) . XOR operation is replaced by new operation which uses two 4 states keys. This method provides security but increase complexity.

In [2] authors give a new method of key generation in DES. They used odd even substitution method for key generation. Odd even substitution is applied on 56 bits key at every step.

In [9] authors give a change to existing DES by using two keys , left key and right key . They used method of Blowfish algorithm to generate the keys. This algorithm is called fused DES_BLOW. However security is enhanced due to use of double key but complexity is also increased.

Authors in [10] give the idea of using DES three times with three different keys. This enhanced algorithm is called Triple DES. It became popular from 1978.Security is enhanced due to use of three keys. Problem with this is forty eight rounds for encryption of 64 bits, which is too much time consuming and makes the algorithm slower.

Authors in [11] has used different method of permutation called Simple Columnar Transposition Technique , they arranged plain text in columns to make it cipher text .This columnar transposition rounds may be one , two or three according to required security.

IV. IMPROVED DES

In improved DES key generation part is improved. Encryption and decryption are as usual. In key generation algorithm we have used two arrays of size eight. One is Left Random Array and another is Right Random Array. In these arrays eight values will be filled by a Random number generator, these values are between 0 to 27.

IMPLEMENTATION: Key generation algorithm is implemented in visual c# programming language, software tool is Microsoft Visual Studio 2010, operating system used is windows 10, processor is core i7, with 2.20 GHz frequency. RAM of the system is 8 GB.

Procedure of key generation using random number generator is following:

i. ***Key generation Procedure*** - We have 64 bits key . After using parity drop table we have 56 bits key . This 56 bits key is divided into two halves C_0 and D_0 . Now using left random array , values in C_0 , at positions given in random array is flipped .

Suppose the first value of left random array is 25 then 25th bit of C_0 is checked if it is zero then it is converted into one or vice versa. Using this eight positions of C_0 are flipped. Now same procedure is repeated for D_0 with right random array, yielding C_1 and D_1.

After this, left shift is done of C_1 and D_1. Number of left shift for each round are as before in old DES. When left shift is completed C_1 and D_1 are concatenated and permuted choice 2 is applied which gives us 48 bits key. This is our first key.

Procedure for other rounds (2,3,....16) is same . For each round left and right array will be used.

At the end of round 16 we get our 16th key. Block diagram is given in Figure 4.

Example: Suppose we have 16 digits hexadecimal key K=0123456789ABCDEF and two left and right random arrays given below:

RIGHT RANDOM ARRAY

9	2	3	21	25	15	11	11

LEFT RANDOM ARRAY

0	26	5	4	13	4	12	25

Using the random key generation algorithm sixteen keys are generated. Step by step procedure for key generation is given in TABLE III.

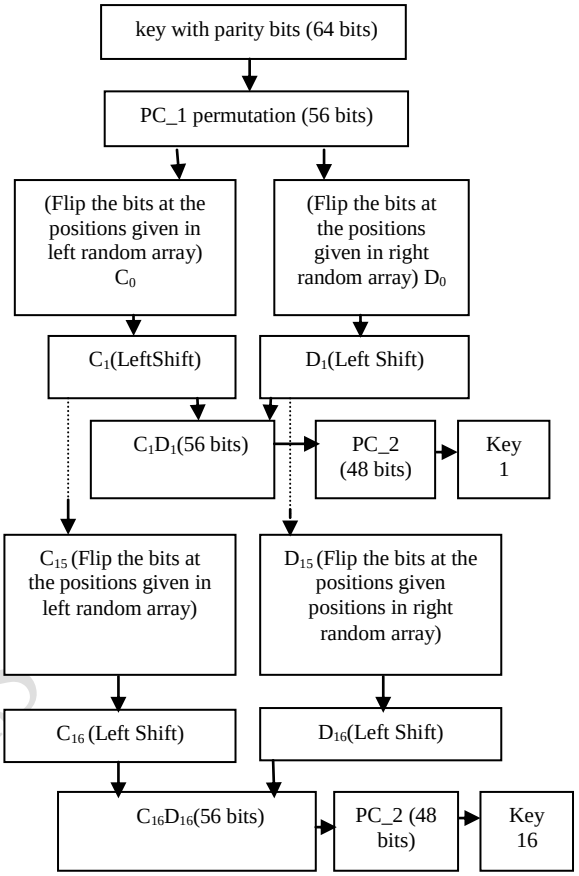

Figure 4: Random key generation process

Operation	Result
K=0123456789ABCDEF Bit conversion(64 bits)	0001001000110100010100111001111000 1001000010101011110011011111101111
Apply permutation choice_1(56 bits)	11110000011001100101010100000011 01001011100001101110100001111
Divide the permuted key into two halves (28 bits)	C_0=11110000110011001010100001 D_0=10100101110001101110100011111
(round 1) Flip the bits of C_0 at the positions given in left random array. (28 bits)	C_1=11000000100011011011100101
Flip the bits of D_0 at the positions given in right random array. (28 bits)	D_1=00100001110010101110100011001

Now left shift the C_1 and D_1 by one bit. (28 bits)	C_1=10000001000110110 10111001011 D_1=01000011100101011 10100010010
Concatenate C_1, D_1 into C_1 D_1 and apply Permutation Choice_2.(48 bits)	K1=00001001101000100 110111001010 111010110000011010 0
(round 2) Flip the bits of C_1 at the positions given in left random array. (28 bits)	C_2=10110001010110100 10110001111
Flip the bits of D_1 at the positions given in right random array. (28 bits)	D_2=11000111100110011 10100010100
Now left shift the C_2 and D_2 by one bit. (28 bits)	C_2= 01100010101101001011 00011111 D_2= 10001111001100111010 00101001
Concatenate C_2, D_2 into C_2 D_2 and apply Permutation Choice_2.(48 bits)	K2=11110011000001101 0011101000 010011110101111000110
Repeat the above procedure for round (3,4,.....16) yielding 16 keys each of 48 bits . Rotations for round 1,2,9,16 is one bit and 2 bits for others.	

Table 3: Random Key Generation Procedure

Keys generated from above procedure are given in figure 5.

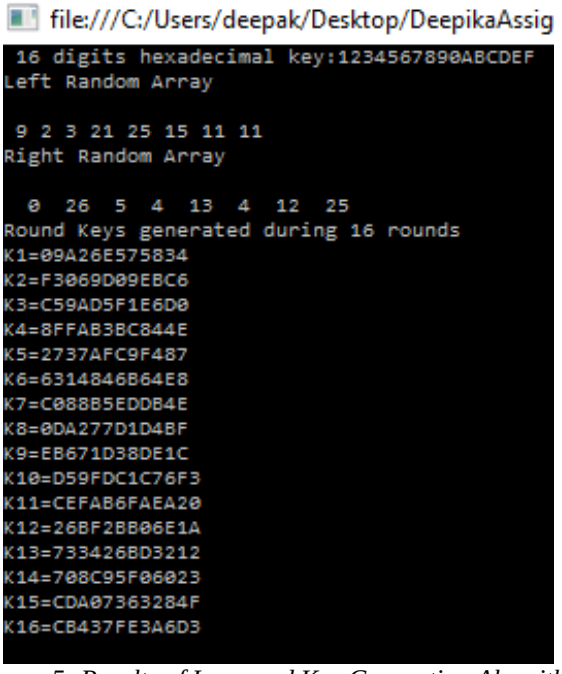

Figure 5: Results of Improved Key Generation Algorithm

✓ *ENCRYPTION PROCESS:* Method of encryption is the same as in old DES . Plain text is divided into 64 bits blocks[6]. Each block goes through 16 rounds of encryption at the end of 16th round we get cipher text . Encryption process is explained before in this paper . Here we encrypt the text using above 16 keys in figure 5 . Encryption process for given example is given in TABLE IV.

Hexadecimal code is used for Cipher text and keys.

Hex string: 4141414144444444 Equivalent binary string (64bits):0100000101000001010000 0101000001010001000100010001000100010001000100		
Round	Encrypted Hex Code	Key
1	00000000500640CB	09A26E575834
2	500640CB198BD081	F3069D09EBC6
3	198BD081EA877A92	C59AD5F1E6D0
4	EA877A9201C9D115	8FFAB3BC844E
5	01C9D115D283BE43	2737AFC9F487
6	D283BE434BF9DDF6	6314846B64E8
7	4BF9DDF65C40D1DF	C088B5EDDB4E
8	5C40D1DF0C1044AC	0DA277D1D4BF
9	0C1044AC642094DE	EB671D38DE1C
10	642094DE29ED765C	D59FDC1C76F3
11	29ED765CA7612BF9	CEFAB6FAEA20
12	A7612BF96F91F034	26BF2BB06E1A
13	6F91F034159E61A4	733426BD3212
14	159E61A442CE77FE	708C95F06023
15	42CE77FE3ABA0050	CDA07363284F
	3ABA00509A9B0115	CB437FE3A6D3

16		
Cipher Text: 15F001F0F3A00270		

Table 5: Encryption In Every Round

- ✓ *DECRYPTION:* Decryption process will be same as discussed in previous section . Round Keys are used in reverse order (k16,k15,.....k1).

V. CONCLUSION

Algorithm being used for encryption should be able to secure data and fast enough. DES is fast and popular but needs some improvements regarding its security. In this paper we have tried to improve key generation method of DES, using two random arrays of size eight. Randomness improve the security of algorithm. Every time when this improved key generation algorithm is run, different random arrays will be generated. Now attacker needs 56 bits key as well as two random arrays to generate sixteen keys .Although it is very difficult to find key and arrays yet Any how he knows both key and random arrays, values of random arrays will be changed at that time.

In future work, random arrays for each round may be different, means 32 random arrays for 16 rounds. Two random arrays for each round. Size of array can be enlarged to make it difficult to find.

ACKNOWLEDGMENT

I want to give my sincere thanks to Ms. Preeti Thakur, for her guidance throughout my research. Her deep knowledge and diligence helped me a lot.

I also thanks my family and friends for their kind support. Thanks to everyone who helped me directly or indirectly.

REFERENCES

[1] Tanenbaum, Andrew S., and Maarten Van Steen. *Distributed systems*. Prentice-Hall, 2007.pp-389-396

[2] Sison, Ariel M., et al. "Implementation of Improved DES Algorithm in Securing Smart Card Data." *Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity*. Springer Berlin Heidelberg, 2012. 252-263. Rabah, Kefa. "Theory and implementation of data encryption standard: A review." *Information Technology Journal* 4.4 (2005): 307-325.

[3] Shah Kruti, R., and Bhavika Gambhava. "New Approach of Data Encryption Standard Algorithm." In *strings*, vol. 1, p. B8. 2012.

[4] Singh, Ramveer, Awakash Mishra, and D. B. Ojha. "An Instinctive Approach for Secure Communication–Enhanced Data Encryption Standard (EHDES)."*International journal of computer science and Information technology* 1.4 (2010): 264-267.

[5] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone.*Handbook of applied cryptography*. CRC press, 1996.

[6] Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." *IBM journal of research and development* 38.3 (1994): 243-250.

[7] Anchugam, K., and M. Tamilselvi. "New Data Encryption Standard Algorithm." *International Journal of Computer Science and Network Security (IJCSNS)* 13.4 (2013): 106.

[8] Mahajan, Prerna, and Abhishek Sachdeva. "A study of Encryption algorithms AES, DES and RSA for security." *Global Journal of Computer Science and Technology* 13.15 (2013).

[9] Al-Hamami, A., M. Al-Hamami, and S. Hashem. "A proposed modified data encryption standard algorithm by using fusing data technique." *World of Computer Science and Information Technology Journal* 1.3 (2011): 88-91.

[10] Barker, William Curt. *Recommendation for the triple data encryption algorithm (TDEA) block cipher*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2004.

[11] Singh, Sombir, Sunil K. Maakar, and Dr Sudesh Kumar. "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques."*International Journal of Advanced Research in Computer Science and Software Engineering, ISSN* 2277 (2013): 464-465.

[12] Patel, Payal, Kruti Shah, and Khushbu Shah. "ENHANCEMENT OF DES ALGORITHM WITH MULTI STATE LOGIC." International Journal of Research in Computer Science 4.3 (2014): 13.