Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques

Sombir Singh* *M.Tech. Scholar (CSE) BRCM CET, Bahal, India*
Sunil K. Maakar *Asstt. Prof. in CSE Dept BRCM CET, Bahal, India*
Dr.Sudesh Kumar *Assoc. Prof. in CSE Dept. BRCM CET, Bahal, India*

Abstract— Security is playing a very important and crucial role in the field of network communication system and Internet. Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now a days the advancement in the computational power the DES seems to be weak against the brute force attacks. To improve the security of DES algorithm the transposition technique is added before the DES algorithm to perform its process. By using an Enhanced DES algorithm the security has been improved which is very crucial in the communication and field of Internet. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm.

Keywords— Columnar, Cipher text, Decryption, DES, Encryption, LPT, Plain text, RPT, SCTTMR, Transposition.

I. INTRODUCTION

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of 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 and Message Digest algorithms [10], [14].
For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic Algorithm mode). Algorithm mode is a combination of a series of the basic algorithm and some block cipher and some feedback from previous steps. We compare and analyzed algorithms DES and RSA [8].

II. DATA ENCRYPTION STANDARD

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key length [16].

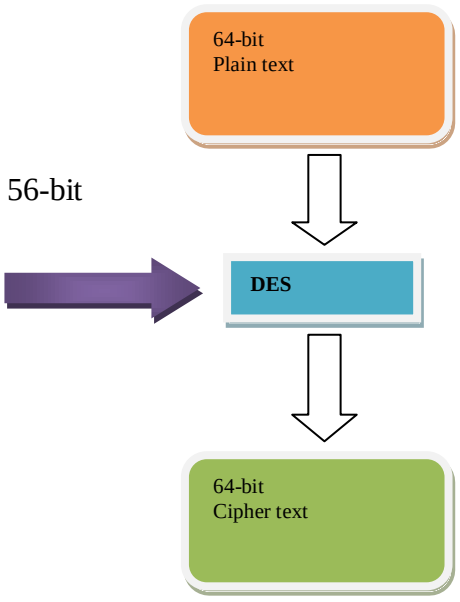

Fig. 1. The conceptual working with DES

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

[1] In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.
[2] The Initial permutation is performed on 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 produced the 32-bit from 48-bit.
e. These 32 bits are permuted using P-Box Permutation.
f. The P-Box output 32 bits are XORed with the LPT 32 bits.
g. The result of the XORed 32 bits are become the RPT and old RPT become the LPT.This process is called as Swapping.
h. Now the RPT again given to the next round and performed the 15 more rounds.
[5] After the completion of 16 rounds the Final Permutation is performed [10][17].

III. DOUBLE DES

It is also called 2DES.It's process is the same as DES but repeated same process 2 times using two keys K1 and K2.First it takes plain text, produced the cipher text using K1 and then take up the cipher text as input, produced another cipher text using K2 shown in fig. 1 .The Decryption Process is shown in fig. 2[10].

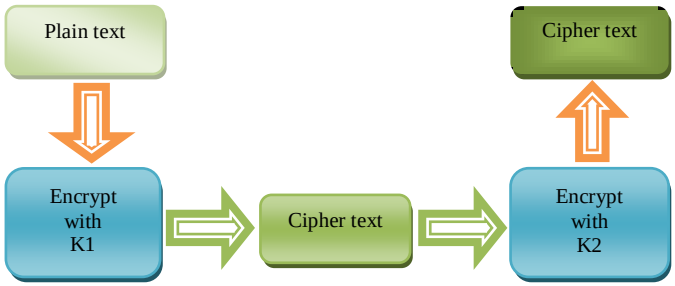

Fig. 2. Encraption process using two keys K1 and K2

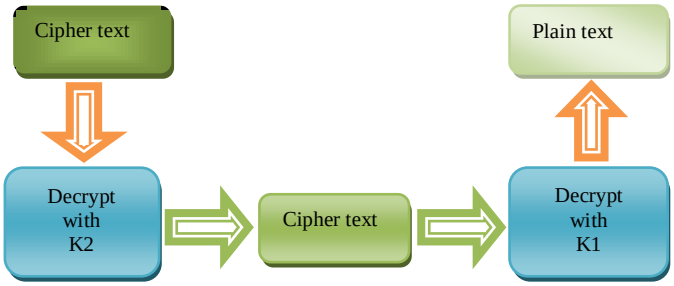

Fig. 3. Decraption process using two keys K1 and K2

IV. TRIPLE DES

Triple DES is DES -three times. It comes in two flavours: One that uses three keys, and other that uses two keys. The Idea of 3-DES is shown in to the fig.4. 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. To decrypt the cipher text C and obtain the plain text, we need to perform the operation P= DK3 (DK2 (DK1(C))). But in Triple DES with two keys the algorithms works as follows:

[1] Encryption the plain text with key K1. Thus, we have EK1 (p).
[2] Decrypt the output of step1 above with key K2. Thus, we have DK2 (EK1 (P)).
[3] Finally, encrypt the output of step 2 again with key K1.Thus, we have EK1 (DK2 (EK1 (P))).
The idea of 3-DES with two keys are shown in fig. 5.

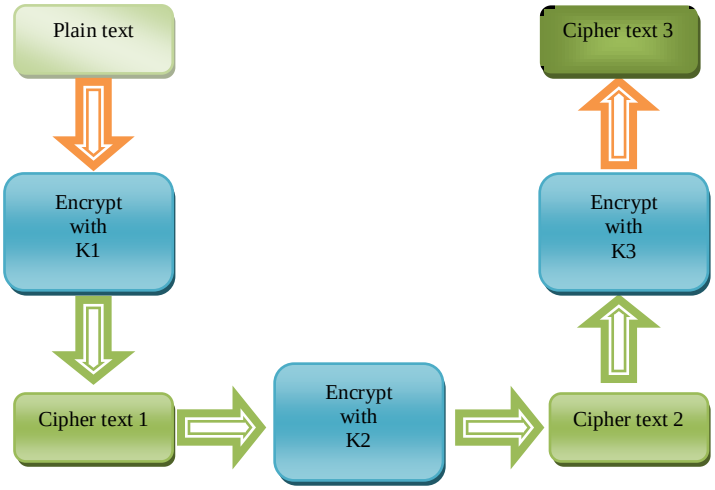

Fig. 4. Encryption process Triple DES with three keys K1, K2 and K

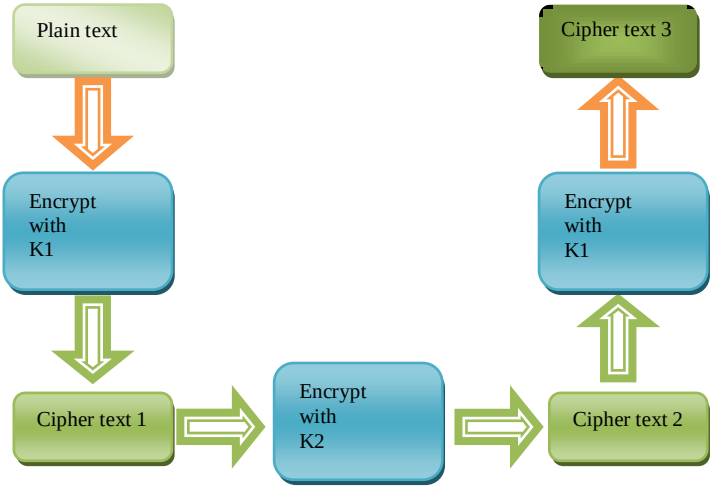

Fig. 5. Decryption process Triple DES with two keys K1 and K2

V. THE TRANSPOSITION TECHNIQUE

The transposition technique does not replace the one alphabet with another like the substitution technique but perform the permutation on the plain text to convert it into cipher text. The various transposition techniques are used to perform the operation given below[6],[10],[14]:

A. Rail Fence Technique
B. Simple Columnar Transposition Technique
C. Vernam Cipher (One-Time Pad)
D. Book Cipher/Running Key Cipher

A. RAIL FENCE TECHNIQUE

The Rail Fence Technique is simplest transposition technique. This technique involves writing plain text as a sequence of diagnosis and reading it row-by-row to produce the cipher text. An example is shown below in fig.6. In this figure the plain text is HELLO and the cipher text is HLOEL.

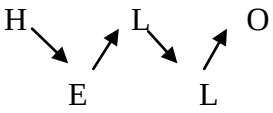

Fig. 6. Rail Fence Technique

B. SIMPLE COLUMNAR TRANSPOSITION TECHNIQUE

The Simple Columnar Transposition Technique is the variation of the Rail Fence Technique. This technique simply arranges the plain text as a sequence of rows of the rectangle that are read in column randomly. Example of this

technique is shown in the fig. 7. The plain text is COME HOME TOMORROW and the cipher text is OMOETRHOOMERCOMW if we choose the column order 2, 4, 5,3,1. The Simple Columnar Transposition Technique is also used multiple rounds to provide a tight security. Ciphertext produced by using Simple Columnar Transposition Technique with multiple rounds is much more complex to crack as compare to the basic technique.

1. Plain text	**H**	**E**	**L**	**L**	**O**
	7	4	11	11	14
	+				
2. One-timep pad	13	2	1	19	25
	N	**C**	**B**	**T**	**Z**
3. Intial total	20	6	12	30	39
4. Subtract 26, if >25	20	6	12	4	13
5. Cipher Text	**U**	**G**	**M**	**E**	**N**

Fig. 7. Simple Columnar Transposition Technique

C. VERNAM CIPHER (ONE-TIME PAD)

The Vernam Cipher, also called one-time pad, is also implemented using a random set of non repeating characters as the input cipher text. The Vernam Cipher is used one-time pad, which is discarded after a single use, and therefore suitable only for short messages. Example of Vernam Cipher is shown in fig. 8. The plain text is HELLO is converted into UGMEN cipher text by applying one-time pad NCBTZ. The Vernam Cipher was first implemented at AT&T with the help of the a device called Vernam machine.

Column1	Column2	Column3	Column4	Column5
C	O	M	E	H
O	M	E	T	O
M	O	R	R	O
W				

1. Plain text	**H**	**E**	**L**	**L**	**O**
	7	4	11	11	14
	+				
2. One-timep pad	13	2	1	19	25
	N	**C**	**B**	**T**	**Z**
3. Intial total	20	6	12	30	39
4. Subtract 26 ,if >25	20	6	12	4	13
5.Cipher Text	**U**	**G**	**M**	**E**	**N**

Fig. 8. The Vernam Cipher(One-Time Pad)

D. BOOK CIPHER/RUNNING KEY CIPHER

The idea used in Book Cipher, also called Running Key Cipher is quite simple, and is similar in principle to the Vernam Cipher. For producing the cipher text, some portion of text from a book is used, which serve the purpose of the one time pad.

VI. DESIGN CONCEPT

In present days, the parallel processor and advanced computer machines are discovered which can perform the computation and calculation at very high speed. The DES is a very powerful algorithm but these machines may be broken DES security. So to provide the most power to DES algorithm security the transposition cryptographic technique is added to DES algorithm. The DES algorithm has 56-bit key which is not so powerful against the Brute force attack. To improve the key strength the DES transposition technique cryptography is powerful scheme and can be implemented before to precede the DES algorithm.

VII. THE PROPOSED WORK

The proposed scheme has first to process the Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR). The plain text message is first converted into the cipher text by using Simple Columnar Transposition Technique .The various rounds of SCTTMR may depend upon the security to provide the message. If the more security is needed then added more rounds of the SCTTMR scheme and if the normal security then uses minimum 1 or 2 rounds. The input to the SCTTMR is a plain text message and the output is ciphered text message. To apply this scheme we required the matrix or table to perform the encryption process and column number which provide the security key.

The output from SCTTMR is then converted into a bit form because the DES algorithm applies its process on bit level as usual. Then the DES has performed its work same as original DES. The Enhanced DES algorithm encryption scheme is shown in fig. 9.The Enhanced DES algorithm decryption scheme is shown in fig. 10.

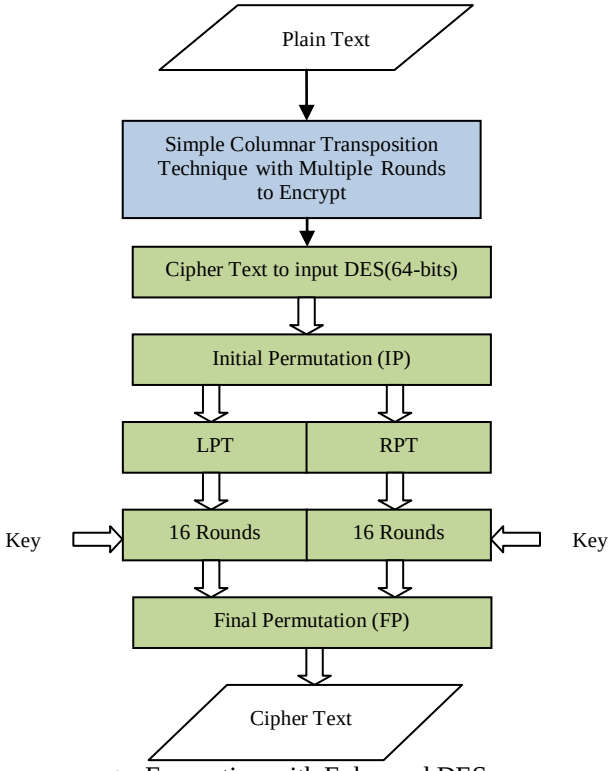

Fig. 9. Encryption with Enhanced DES

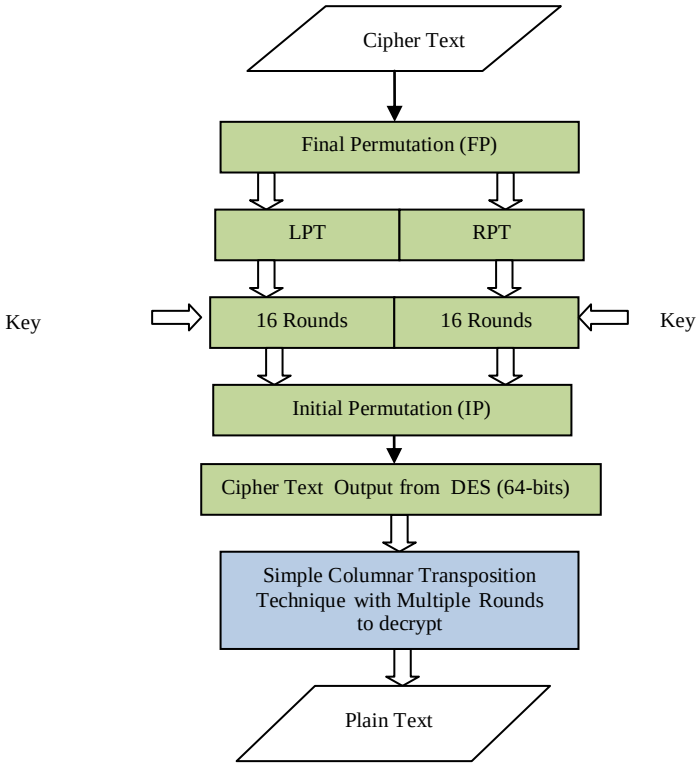

Fig. 10. Decryption with Enhanced DES

VIII. THE RESULT AND DISCUSSION

To test the Enhanced DES algorithm, we have to take the input plain text "HOW ARE YOU" and then apply the Enhanced DES algorithm. The Simple Columnar Transposition scheme is implemented first, to encrypt the plain text which is shown in fig.11.

Column 1	Column 2	Column 3
H	O	W
A	R	E
Y	O	U

Fig. 11. Simple Columnar Transposition Technique 1st round to encrypt

Column 1	Column 2	Column 3
O	R	O
W	E	U
H	A	Y

Fig. 12. Simple Columnar Transposition Technique 2nd round to encrypt

The random column number is 2, 3, 1 is taken in the 1st round and the output of the 1st round is ciphered text "OROWEUHAY". Now apply the round 2nd which have been taken the output of 1st round as an input and used the same random number to produce the cipher text which is as "REAOUYOWH". The input text for DES is "REAOUYOWH" and produced the final cipher text in Hexadecimal (D7926AE97F7889099767729885CE54BC),using the key in Hexadecimal (133457799BBCDFF).The process is shown in Fig. 13.

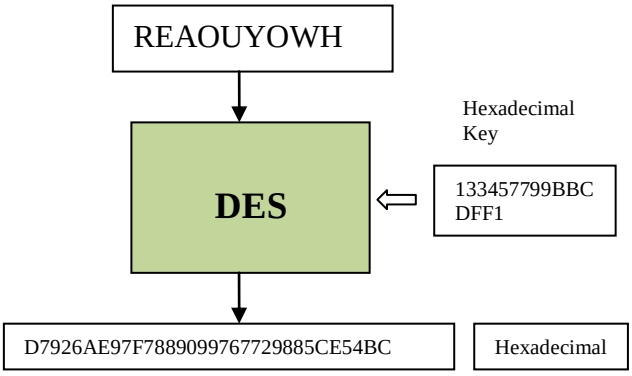

Fig. 13. Encryption with Enhanced DES

Now the opposite to the encryption process, we have performed the decryption process. We take the output cipher text from DES (D7926AE97F7889099767729885CE54BC), key (133457799BBCDFF) and apply the decryption process as normally using DES. The complete process of decryption is shown in fig.14.

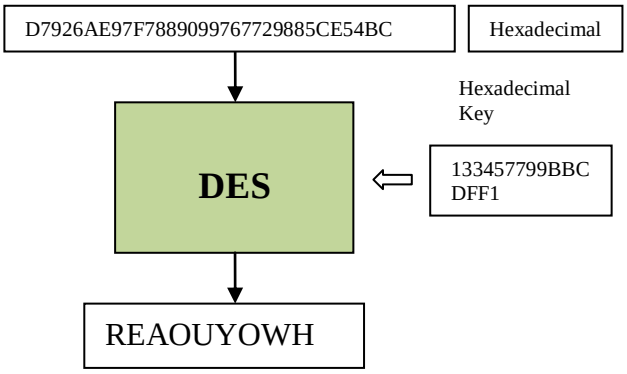

Fig. 14. Decryption with Enhanced DES

The decrypted output of the DES algorithm is taken and the Simple Columnar Transposition Decryption Technique is applied to get the plain text .The complete decryption is shown in fig.15 and fig.16.

Column 1	Column 2	Column 3
O	R	O
W	E	U
H	A	Y

Fig. 15. Simple Columnar Transposition Technique 2nd round to decrypt

Column 1	Column 2	Column 3
H	O	W
A	R	E
Y	O	U

Fig. 16. Simple Columnar Transposition Technique 2nd round to decrypt

The final output from the Simple Columnar Transposition Technique is the plain text HOW ARE YOU.

IX. PROPERTIES OF THE ENHANCED DES

The Enhanced DES has the following advantages over simple DES:

a. The security of the algorithm is increased. The Simple Columnar Transposition Technique with multiple rounds is used before DES and the round can be increased and decreased according to need.
b. The Brute Force attack is weak against the Enhanced DES because the intruder required breaking the DES and Simple Columnar Approach both. He required extra time to hack the algorithm.
c. If the intruder is success to hack the key of DES in any way then he required the random number of the columnar approach to reach the plain text.

The Enhanced DES has the following disadvantages over simple DES:

a. The main disadvantage of using this approach is the extra computation is required to perform the operation. But this is not so crucial because our main aim is to provide tighter security.
b. The second disadvantage is to generate the random number of columns and to send it on the network. This is also not so hard at today's time because the speed of machines is very high.

X. CONCLUSIONS

In todays time,the security is playing a very important and powerful role in the field of networking, Internet and various communication system .The electronic communication system is used in banking, reservation system and marketing which required a very tight security system. The original DES implementation has some weaknesses, to overcome the most of weakness the Enhanced DES algorithm is designed. The Designed system improved the security power of original DES. The only drawback of Enhanced DES is extra computation is needed but the todays computer have parallel and high speed computation power so the drawback of the Enhanced DES algorithm is neglected because our main aim is to enhance the security of a system. By using the Enhanced DES algorithm the security is very tight and approximately impossible to crack and break the Enhanced DES algorithm.

ACKNOWLEDGMENT

I would like to articulate our deep gratitude to my thesis guide Asst. Prof. Sunil Maaker who has always been my motivation for carrying out the paperwork. I express my deep sense of gratitude to Dr. Sudesh Kumar, Professor and Head of Computer Science and Engineering Department of BRCM College of Engineering and Technology, Bahal, Haryana for providing the necessary facilities during the research and encouragement from time to time. Special thanks to the institute, BRCM College of Engineering and Technology, for giving me such a nice opportunity to work in the great environment. Thanks to my friend and colleague who have been a source of inspiration and motivation that helped me during my dissertation period. And to all other people who directly or indirectly supported and help me to fulfill my task. Finally, I heartily appreciate my family members for their motivation, love and support in my goal.

REFERENCES

[1] M. E. Hellman,"DES will be totally insecure within ten years" lEEE Spectrum, Vo1.16, N0.7, pp32-39, July 1979.
[2] Alani, M.M.," A DES96 - improved DES security ", 7th International Multi-Conference on Systems, Signals and Devices, Amman , 27-30 June 2010.
[3] Seung-Jo Han , Heang-Soo Oh , Jongan Park," IEEE 4th International Symposium on Spread Spectrum Techniques and Application Proceedings ", 22-25 Sep 1996.
[4] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.
[5] Shah Kruti R., Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[6] Govind Prasad Arya, Aayushi Nautiyal, Ashish Pant, Shiv Singh, Tishi Handa,"A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations",The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.
[7] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices", College of Computer Science, Northeastern University, Boston, MA 02115, USA.
[8] Adi Shamir Ronald Rivest and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystem", Communications of the ACM, 21:120–126, 1978.

[9] Kofahi, N.A. Turki Al-Somni Khalid Al-Zamil,"Performance evaluation of three encryption/decryption algorithms.Circuits and Systems", 2003. MWSCAS '03. Proceedings of the 46th IEEE International Midwest Symposium on, 2:790–793, 27-30 December 2003.

[10] William Stallings, " Cryptography and Network Security Principles and Practices", Prentice Hall, November 16, 2005.

[11] A. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[12] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010. Technologies, pp. 84-89, 2006.Bn

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

[14] Atul Kahte, "Cryptography and Network Security",Tata Mcgraw Hill, 2007.

[15] Shasi Mehlrotra seth, Rajan Mishra,"Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011.

[16] Wuling Ren, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication",Second International Conference on Modeling", Simulation and Visualization Methods (WMSVM), 2010.

[17] Sung-Jo Han, Heang-Soo Oh, Jongan Park, "The improved Data Encryption Standard (DES) Algorithm",Department of Electronic Engineering, Chosun University. South Korea.1996 IEEE.

[18] Charels Connell, "An Analysis of New DES: A Modified Version of DES", Locust Street Burlington, USA, Boston MA 02215 USA.

[19] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg, "An Innovative Approach to Enhance the Security of Data Encryption Scheme. International Journal of Computer Theory and Engineering", Vol. 2, No. 3, June, 2010.

[20] Subbarao V. Wunnava, "Data Encryption Performance and Evaluation Schemes", Florida International University, Miami, FL Ernest0 Rassi; Florida Intemational University, Miami, FL 0-7803-7252- 2/02/$10.00 0 2002 IEEE Proceedings IEEE Southeastcon 2002.

[21] D. Coppersmith, "The Data Encryption Standard (DES) and Its strength Against attacks", IBM J. RES. Develop. VOL.38 NO.3 MAY 1994.

[22] Gaurav Shrivastava, "Analysis Improved Cryptosystem Using DES with RSA" VSRD-IJCSIT, Vol. 1 (7), 465-470, 2011.

