Enhancing the Security of Simplified DES Algorithm Using Transposition and Shift Rows

Adeem Akhtar[1] and Muhammad Zia Ullah Baig[2], Waleej haider[3]

[1, 2, 3] MS Computer Science, MAJU, Pakistan

ABSTRACT

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

Keywords: *DES Algorithm, Transposition, Shift Rows, S-DES.*

1. INTRODUCTION

Encryption is the process of encoding the plaintext into a secret code and decryption is the reverse process of decoding the secret code into plaintext.

There are two types of technique used: asymmetric-key or public-key and symmetric-key or secrete-key. Asymmetric-key uses different keys for encryption and decryption. But Symmetric key uses same key for encryption and decryption.

Asymmetric-key cryptography includes RSA, Digital Signature and Message Digest algorithms and symmetric-key cryptography includes S-DES,DES, AES, 3DES, IDEA, Blowfish algorithms etc [1], [2]

2. SIMPLIFIED DATA ENCRYPTION STANDARD

S-DES is a block cipher. It encrypts the data in a block of 8 bit. It produces 8 bit cipher text. The key length is 10 bits.

Initially the key is consisting of 10 bits. The algorithm is shown in below figure1 [3].

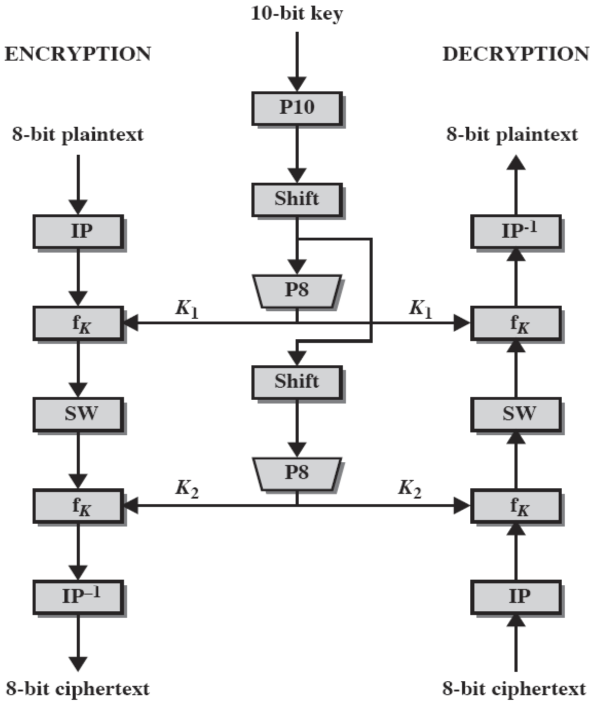


Fig.1. S-DES Algorithm

S-DES algorithm:

8-bit plain text is passed to initial permutation (IP) function. The IP is performed on plain text. The initial permutation produces two halves of permuted block: Left 4-bit and Right 4-bit.

The function fK(L, R) = (L ⊕ F(R, SK), R) Where XOR is the exclusive-OR operation and key is a sub -key. Computation of f(R, key) is done as follows.

1. Apply expansion/permutation E/P=] to input 4-bits.
2. Add the 8-bit key (XOR).
3. Pass the left 4-bits through S-Box S0 and the right 4-bits through S-Box S1.
4. Apply permutation P4 =].

At the end of the algorithm, the inverse permutation is applied; the inverse permutation is done by applying, IP-1 where we have IP-1(IP(X)) =X.

3. 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[4],[1],[2]:

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

1. 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.2. In this figure the plain text is HELLO and the cipher text is HLOEL.

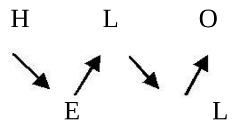
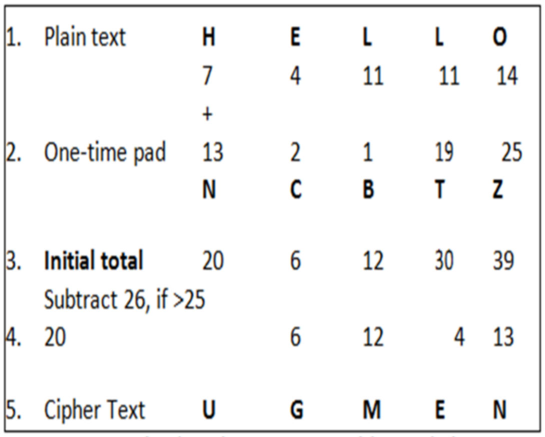


Fig. 2. Rail Fence Technique

2. 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. 3. 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. Cipher text produced by using Simple Columnar Transposition Technique with multiple rounds is much more complex to crack as compare to the basic technique.

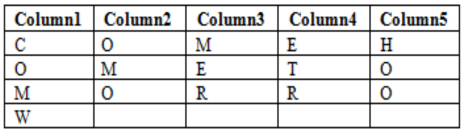


1. Plain text	H	E	L	L	O
	7	4	11	11	14
	+				
2. One-time pad	13	2	1	19	25
	N	C	B	T	Z
3. **Initial total**	20	6	12	30	39
Subtract 26, if >25					
4. 20		6	12	4	13
5. Cipher Text	U	G	M	E	N

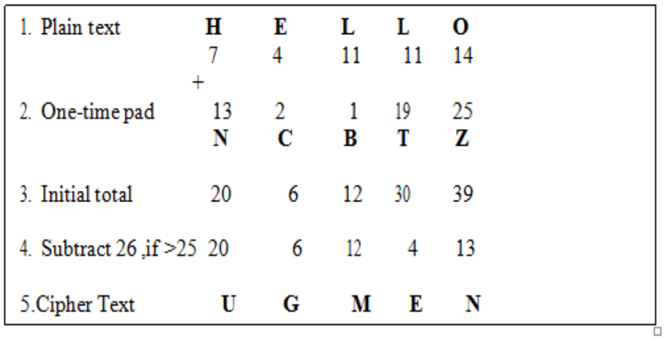
Fig. 3. Simple Columnar Transposition Technique

3. 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. 4. 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 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-time pad	13	2	1	19	25
	N	C	B	T	Z
3. Initial 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. 4. The Vernam Cipher (One-Time Pad)

4. 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.

4. SHIFT ROWS STAGE

This stage (known as ShiftRows) is shown in figure 5. This is a simple permutation
an nothing more. It works as follow:

- The first row of state is not altered.
- The second row is shifted with ‘1’ bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.

For decryption process, Inverse Shift row is used. It works as follows:

- The first row of state is not altered.
- The second row is shifted 2 bytes to the left in a circular manner.
- The third row is shifted with ‘1’ bytes to the left in a circular manner.

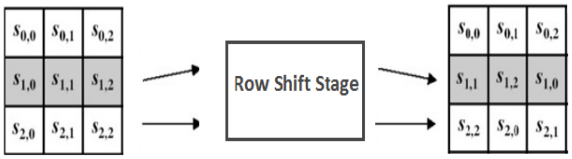

$s_{0,0}$ $s_{0,1}$ $s_{0,2}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$
Row Shift Stage
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$
$s_{1,1}$ $s_{1,2}$ $s_{1,0}$
$s_{2,2}$ $s_{2,0}$ $s_{2,1}$

Fig. 5. Shift Rows stage.

5. 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 S-DES is a very powerful algorithm but these machines may be broken S-DES security. In order to deliver S-DES algorithm; there must be a most control security mechanism of transposition cryptographic technique is added on it.. The S-DES algorithm has 8-bit key which is not so powerful against the Brute force attack. To improve the key strength the S-DES transposition technique and shift row stage cryptography is powerful scheme and can be implemented before to precede the S-DES algorithm.

6. THE PROPOSED WORK

The proposed structure has first to process the Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR) and then the output comes from SCTTMR will gain undergone Shift Rows Stage. The plain text message is first converted into the cipher text by using Simple Columnar Transposition Technique and Shift Row Stage 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 and Shift Rows 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 Shift row is then converted into a bit form because the S-DES algorithm applies its process on bit level as usual. Then the S-DES has performed its work same as original S-DES. The Enhanced S-DES algorithm encryption scheme is shown in fig. 6.The Enhanced S-DES algorithm decryption scheme is shown in fig. 7

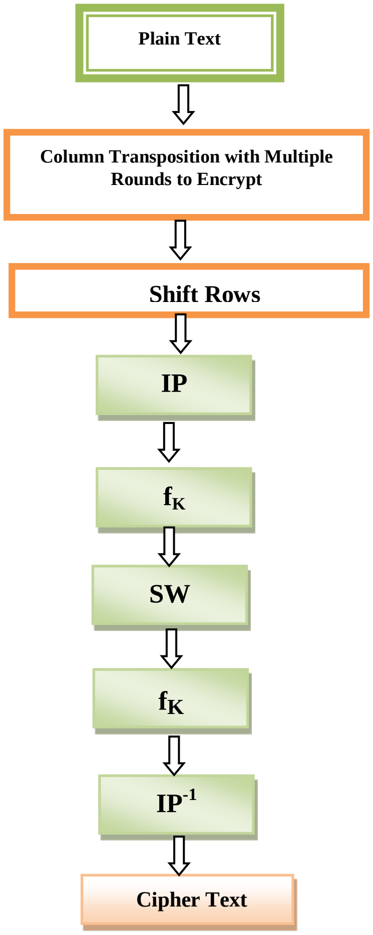


Fig. 6. Encryption with Enhanced S-DES

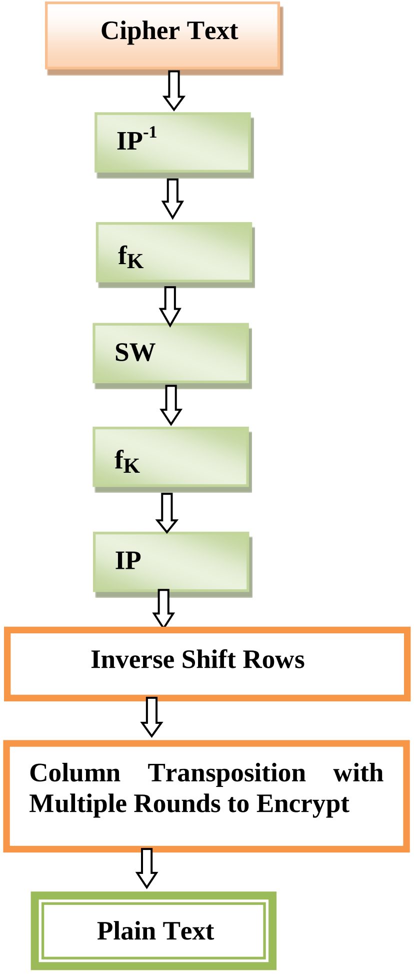
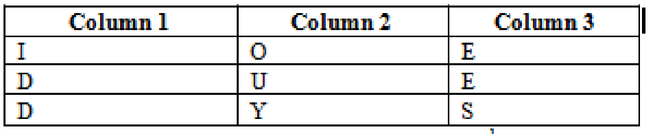


Fig. 7. Decryption with Enhanced S-DES

To test the Enhanced DES algorithm, we have to take the input plain text “DID YOU SEE” 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.8.

Column 1	Column 2	Column 3
D	I	D
Y	O	U
S	E	E

Fig. 8. Simple Columnar Transposition Technique 1st round to encrypt



Column 1	Column 2	Column 3
I	O	E
D	U	E
D	Y	S

Fig. 9. 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 “IOEDUEDYS”. 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 “OUYEESIDD”. The produced cipher text is then again taken in to row shift as shown in fig 10

Column 1	Column 2	Column 3
O	U	Y
E	S	E
D	I	D

Fig. 10. Shift Row Stage

The input text for S-DES is “OUYESEDID” and produced the final cipher text in Hexadecimal (CF4A218C4C8C7C827C), using the key (0010010111).The process is shown in Fig. 11.

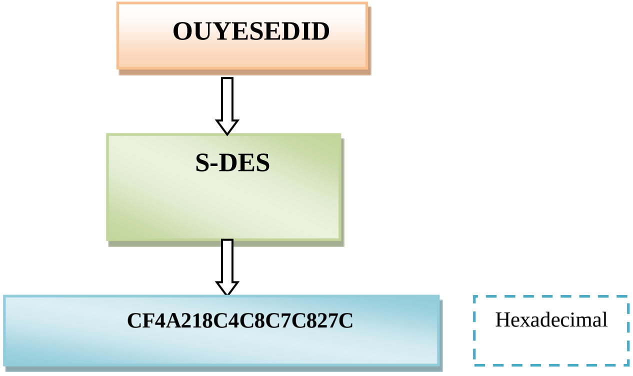


Fig. 11. Encryption with Enhanced DES

Now the opposite to the encryption process, we have performed the decryption process. We take the output cipher text from S-DES (CF4A218C4C8C7C827C), key (0010010111) and apply the decryption process as normally using S-DES. The complete process of decryption is shown in fig.12.

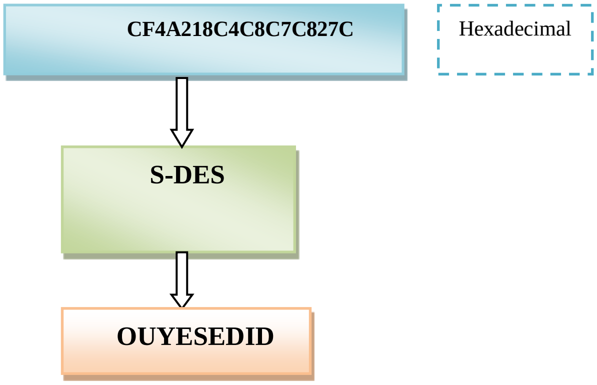
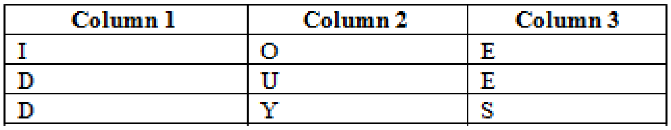


Fig. 12. Decryption with Enhanced S-DES

The decrypted output of the S-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 13, fig.14 and fig.15.

Column 1	Column 2	Column 3
O	U	Y
E	E	S
I	D	D

Fig. 13. Inverse Row Shift technique



Column 1	Column 2	Column 3
I	O	E
D	U	E
D	Y	S

Fig. 14. Simple Columnar Transposition Technique 2nd round to decrypt

Column 1	Column 2	Column 3
D	I	D
Y	O	U
S	E	E

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

The final output from the Simple Columnar Transposition Technique is the plain text DID YOU SEE.

7. CONCLUSIONS

In today's time, the security is playing a very significant and influential 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 S-DES implementation has some flaws, to overcome the most of flaw the Enhanced S-DES algorithm is designed. The Designed system improved the security power of original S-DES. The only weakness of Enhanced S-DES is additional computation is required but nowadays, computer have parallel and high speed computation power so the drawback of the Enhanced S-DES algorithm is neglected because our main aim is to enhance the security of a system. By using the Enhanced S-DES algorithm the security is very constricted and nearly impossible to crack and break the Enhanced S-DES algorithm.

ACKNOWLEDGMENT

We would like to articulate our deep gratitude to Assistant Professor. Waleej Haider who has always been our motivation for carrying out the research paper work.

REFERENCES

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

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

[3] Lavkush Sharma , Bhupendra Kumar Pathak & Ramgopal Sharma Breaking of Simplified Data Encryption Standard Using Genetic Algorithm.

[4] 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.