ISSN 2320 -2610

Volume 6, No.3, May – June 2017

International Journal of Multidisciplinary in Cryptology and Information Security

Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis01632017.pdf

Towards Security Enhancement using Block Cipher Algorithm with Transposition Techniques

Aamir Maqsood[1], Waleej Haider[2]

[1]Mohammad Ali Jinnah University Karachi, Pakistan, aamirmaqsoodlive@gmail.com

Sir Syed University of Engineering & Technology, Karachi, Pakistan, directlyproportional2u@yahoo.com

ABSTRACT

In the age of internet, the security of information sharing has been increased exponentially, the authenticity of the data shared from one node to another is required a complex security mechanism which based on modern cryptography. Simplified DES is a block cipher algorithm which is used to encrypt data block by block using Feistel properties. In this proposed enhancement, the security of previous S-DES algorithm can be improved and strengthened by the use of transposition techniques which will enhance the secrecy of the data to be transmitted. In order to provide the glance of enhanced S-DES, mathematical implementation has been performed.

Key words: S-DES, Rail Fence, Route Transposition, Cryptosystem.

1. INTRODUCTION

The general phenomenon of cryptography is same from the day first; to encrypt a plain text into a cipher text and numerous efforts has been made for creating or increasing the encryption techniques. Although the authentic transmission of data may require some other security facts such as transaction or authentication over wire or wireless networks demands end to end secure connections that needs to be addressed but the strong encryption of a plain text is the key process of the integrity of data. In order to increase the security of Simplified Data Encryption Standard technique [1], the keys generation has been modified by adding Rail fence transposition technique in the process which made the process of key generation more complex and confusing [2].

In the encryption process, route transposition cipher technique has been hybrided and the encryption methodology has been revised which creates the diffusion and complexity in the process of encryption [3]. S-DES, Rail fence and Router transposition are different cryptographic techniques, a combination of these techniques in a single cryptosystem will enhance the security of data being sent.

2. EXISTING S-DES CRYPTOSYSTEM

Existing S-DES cryptosystem is use 8 bit block of plain text as in input and encryption process performs along with two 8 bit sub keys which provide cipher text.

2.1 S-DES SUB KEYS GENERATION

The Simplified Data Encryption Standard existing algorithm takes 10 bits of data block as an input, illustrated in Figure 1, which is subjected to be permuted in Table P10 and then the result is divides in two equal halves. After performing single bit left shift (LS-1) operation on both pairs, the result is subjected to be permuted in Table P8 which creates first sub key (K1) for the encryption algorithm.

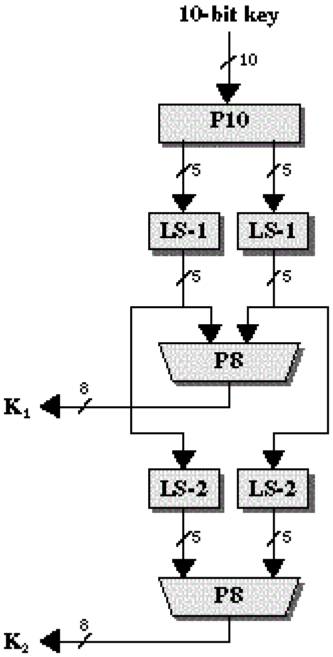

Figure 1: S-DES Key existing Keys generation.

Two bits left shift operation (LS-2) is performed on the result received from first LS-1 and permuted in Table P8 which provides second sub key (K2).

2.2 ENCRYPTION AND DECRYPTION

In the encryption phase, five consecutive operations performed:

1. S-DES takes an 8 bit block of a plain text in initially permuted from IP table.
2. A mangler's function f_k performed.
3. A permutation function that switches the two halves of the data.
4. Again mangler's function f_k which provide permutation and substation function.

The Final permutation table which is inverse of the IP table.

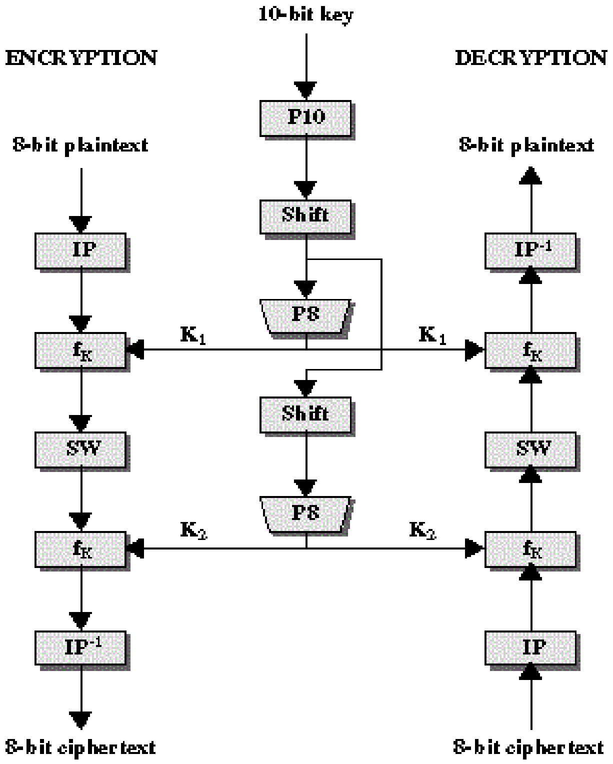

Figure 2: Encryption and Decryption of S-DES.

In the decryption phase, the whole process is performing in reverse altogether in order to get 8 bit plain text block from cipher text.

3. Literature Review

The importance of the cryptography is proved by the numerous activities done by the researchers in recent years as the security of information sharing has been increased exponentially and the need of authenticity and integrity is required a complex security mechanism, the techniques in block ciphers vary from substitution, transposition to the product of both. In a very useful technique of transposition is the Rail fence cipher technique, which is used to encrypt plain text data into a cipher text by writing it in a zigzag patter in more than one line, the pattern is generally known as Rail fence due to its resemblance with a Rail fence [2].

For instance a plain text P="PAKISTAN" on a two rail fence will provides us Cipher text as shown in Figure 3.

P		K		S		A	
	A		I		T		N

Figure 3: Rail Fence Transposition

Writing the first line followed by second line generate a cipher using rail fence and C="PKSAAITN".

Another technique is the route transposition cipher technique, which is used to encrypt plain text into Cipher text by writing it in a grid of dimensions and then the generate the cipher text in a pattern according to the key which are generally spiral inward, start form the top and clock and anti-clock wise reading [3].

For instance a plain text P= "PAKISTAN IS IN ASIA" subject to place in 4x4 grid illustrated in Figure 4.

P	S	I	A
A	T	S	S
K	A	I	I
I	N	N	A

Figure 4: Route Transposition

To generate the cipher text, the pattern of readings will be started from the bottom the first column into a clock wise position which provides us Cipher:

C= "IKAPSIASIANNATSI".

Enhancement of security in Data Encryption Standard algorithm has been done by applying Ceaser block cipher algorithm in order to diffuse the cipher generated from DES [4]. In another modification, Fusion of Blowfish algorithm has been applied with DES [5]. Modification in S-DES has been done by generating Sub keys using 2*1 Matrix, the technique is known as Bunch Matrix Technique, for Encryption: C = [cij] = [eij × pij] mod 256 where eij is refers to encryption matrix and for Decryption: P = [pij] = [dij × cij] mod 256 where dij is refers to a decryption matrix [6].

4. Proposed Security Enhanced S-DES

To enhance the security by adding more Feistel properties such as confusion and diffusion, the security enhancement is proposed, the sub keys generation of S-DES process has been customized illustrated in Figure 5.

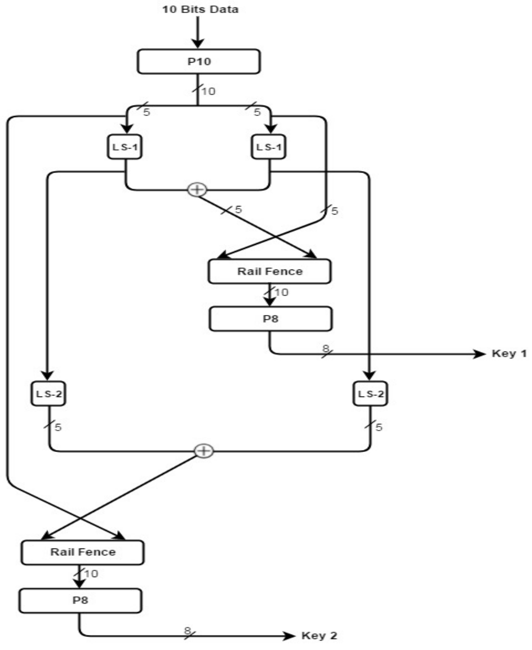

Figure 5: Enhanced S-DES Sub Keys generation

The steps have been performed for the sub keys generations are:

4.1 First Sub Key Generation

Take a 10 bit block Input data, Input has been permuted from table P10, Result has been split into two halves, Single bit left shift (LS-1) operation has been performed on both halves, Both Halves merged together via XOR operation and the 5 bits result generated, 5 bits generated result merged with the right side of 5 bit split from step no. 3 activity, Rail fence technique applied, The result of Rail Fence technique has been subjected to be permuted from table P8 which provides a first sub key (K1) illustrated in Figure 5.

4.2 Second Sub Key Generation

Take an earlier results of both LS-1 operations and Double bits left shift (LS-2) operation has been performed, merged together via XOR operation and the 5 bits result generated, 5 bits generated result merged with the left side of 5 bit split from the step no. 3 activity, Rail fence technique applied, The result of Rail Fence technique has been subjected to be permuted from table P8 which provides a second sub key (K2) illustrated in Figure 5.

4.3 Modified S-DES

Modification has been performed on S-DES algorithm in order to enhance the security, in this proposed system, Initially 8 bit plain text block is subjected to be permuted from table IP, the result split into two halves and the right side half has been subject to E/P table, merged with first 8 bits sub key (K1) and route cipher technique applied

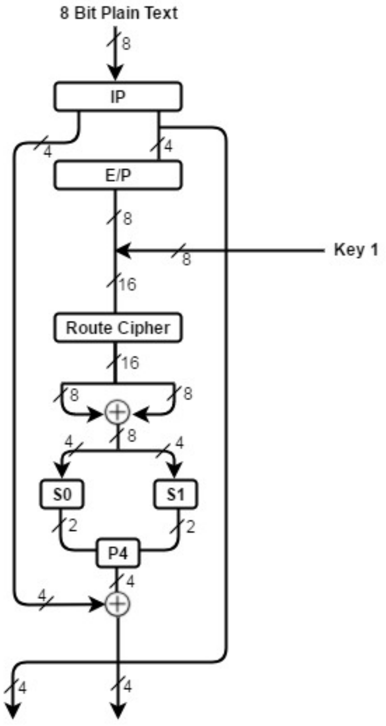

Figure 6: First Part of Modified S-DES

The 16 bits result split into two halves and XOR operations applied, the 8 bit result of XOR operation has been split into two halves and Matrix S0 and S1 applied in order to get 2 bits pair; the result of matrix operations, both pairs has been permuted from Table P4 and XOR operations applied on the result of 4 bits along with the left half of the result of table IP in the initial permutation; illustrated in Figure 6. The result has been subject to E/P table, merged with first 8 bits sub key (K2) and route cipher technique applied.

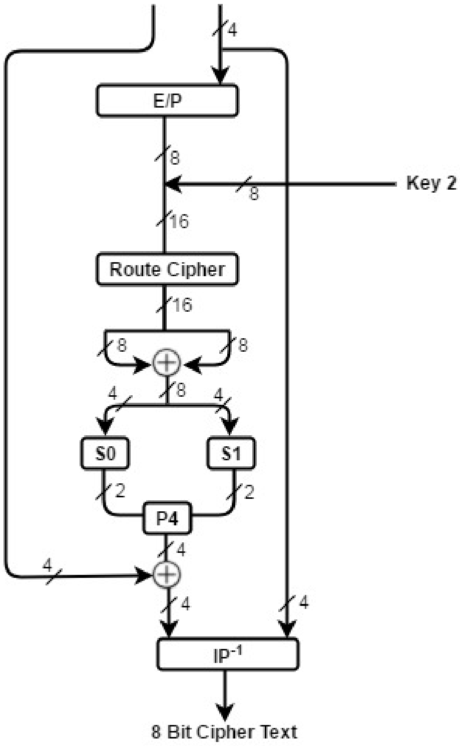

Figure 7: Second Part of Modified S-DES

The 16 bits result split into two halves and XOR operations applied, the 8 bit result of XOR operation has been split into two halves and Matrix S0 and S1 applied in order to get 2 bits pair; the result of matrix operations, both pairs has been permuted from Table P4 and XOR operations applied on the result of 4 bits along with the right half of the result of table IP in the initial permutation, the 4 bits result has been permuted from the Inverse permutation table IP-1 along with the 4 bits result of first P4 permutation and get the 8 bit block Cipher text; illustrated in Figure 7.

Complete illustration of modified S-DES algorithm is below:

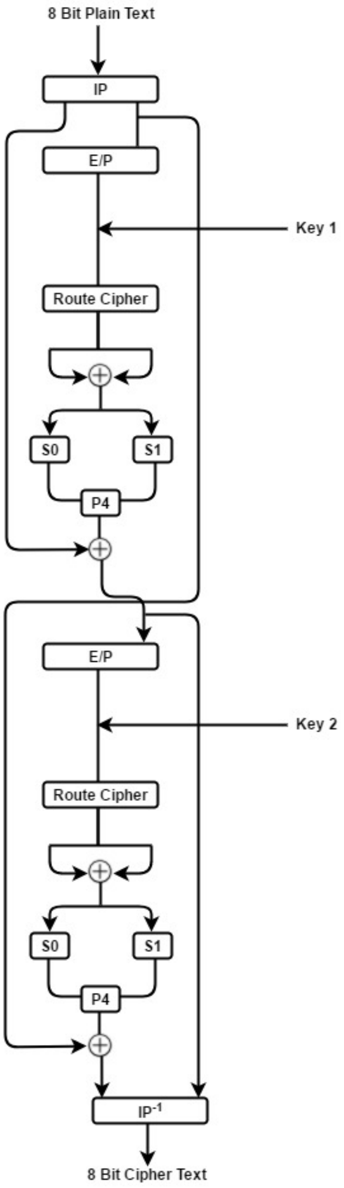

Figure 8: Modified S-DES

5. Mathematical Implementation

To demonstrate the proposed enhanced Simplified Data Encryption Standard, mathematical implementation has been performed step by step.

5.1 Sub Keys Generation

Step 1:
In the initial phase, 10 bit data has been taken for the purpose of sub keys generation.
D=1011001101
Permutation Table P10:

Positions	3	5	2	7	4	10	1	9	8	6
Data	1	0	0	1	1	1	1	0	1	0

Step 2:
Split the result of Step 1 into two halves.

Left Half	1	0	0	1	1
Right Half	1	1	0	1	0

Single bit left shift applied on both halves.

LS-1 on Left Half	0	0	1	1	1
LS-1 on Right Half	1	0	1	0	1

XOR applied on both halves and result = 10010

Step 3:
The result of Step 3 (10010) has been merged with the right half of initial permutation result which has been performed in Step 1 (11010) and Rail Fence transposition technique has been applied.
1101010010

1		0		0		0		1	
	1		1		1		0		0

The result of Rail Fence Transposition is:
1000111100

Step 4:
The Rail fence transposition result has been permuted from table P8 to and generated first sub key K1.
Permutation Table P8:

Positions	6	3	7	4	8	5	10	9
Data	1	0	1	0	1	1	0	0

Sub Key K1= 10101100

Step 5:
In order to generate Second Sub Key (K2), apply double bits left shit operation on the result of LS-1 in Step No. 2.

LS-1 on Left Half	0	0	1	1	1
LS-1 on Right Half	1	0	1	0	1

LS-2 applied:

LS-2 on Left LS-1	1	1	1	0	0
LS-2 on Right LS-1	1	0	1	1	0

XOR applied on both halves and result = 01010

Step 6:
The result of Step 5 (01010) has been merged with the left half of initial permutation result which has been performed in Step 1 (10011) and Rail Fence transposition technique has been

applied.

0101010011

0	1	1	1
1	1	0	1
1	0	1	0
1	1	0	0

0	0	0	0	1
1	1	1	0	1

The result of Rail Fence Transposition is:
0000111101

Step 7:
The Rail fence transposition result has been permuted from table P8 to and generated second sub key K2.
Permutation Table P8:

Positions	6	3	7	4	8	5	10	9
Data	1	0	1	0	1	1	1	0

Sub Key K2= 10101110

5.2 Modified S-DES Cipher

Step 1:
In initial phase of modified S-DES, 8 bit plain text block has been permuted from IP table.
P=10111001
Permutation Table P10:

Positions	2	6	3	1	4	8	5	7
Data	0	0	1	1	1	1	1	0

Step 2:
Split the result of Step 1 into two halves.

Left Half	0	0	1	1
Right Half	1	1	1	0

Step 3:
The Right 4 bits subjected to be permuted from Table E/P.

Positions	4	1	2	3	2	3	4	1
Data	0	1	1	1	1	1	0	1

The result merges with first Sub Key K1.

E/P result	K1 result
01111101	10101100

0111110110101100

Step 4:
Route transposition technique applied on the result of step 3. To generate the cipher text, the pattern of readings will be started from the bottom the first column into a clock wise position which provides us Cipher:
1110111100010101

Step 5:
Split the result of Step 4 into two halves of eight bits.

XOR operation applied on both halves and result = 11111010

Step 6:
Split the result into two halves and Matrix S0 and S1 applied

Left Half	1	1	1	0	1	1	1	1
Right Half	0	0	0	1	0	1	0	1

in order to get 2 bits pair results.

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \quad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \quad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

S0=10
S1=00

Step 7:
Result of Step 6 has been merged and subjected to be permuted from P4.
Permutation Table P4:

Positions	2	4	3	1
Data	0	0	0	1

The XOR operation applied on the result of table P4 (0001) and the left half of initial permutation from the step 2 (0011).
0010

Step 8:
The Right 4 bits subjected to be permuted from Table E/P.

Positions	4	1	2	3	2	3	4	1
Data	0	0	0	1	0	1	0	0

The result merge with second Sub Key K2.

E/P result	K1 result
00010100	10101110

0001010010101110

Step 9:
Route transposition technique applied on the result of step 8.

0	0	1	1
0	1	0	1
0	0	1	1
1	0	0	0

To generate the cipher text, the pattern of readings will be started from the bottom the first column into a clock wise position which provides us Cipher:
1000011110000101

Step 10:
Split the result of Step 4 into two halves of eight bits.

Left Half	1	0	0	0	0	1	1	1
Right Half	1	0	0	0	0	1	0	1

XOR operation applied on both halves and result = 00000010

Step 11:
Split the result into two halves and Matrix S0 and S1 applied in order to get 2 bits pair results.
S0=01
S1=01

Step 12:
Result of Step 11 has been merged and subjected to be permuted from P4.
Permutation Table P4:

Positions	2	4	3	1
Data	1	1	0	0

The XOR operation applied on the result of table P4 (1100) and the right half of initial permutation from the step 2 (1110).
0010

Step 13:
The result of Step 12 (0010) and Step 7 (0010) has been subjected to be permuted from inverse of initial permutation Table IP-1
Permutation Table IP-1:

Positions	4	1	3	5	7	2	8	6
Data	0	0	1	0	1	0	0	0

The Cipher is: 00101000

6. CONCLUSIONS

The S-DES encryption algorithm takes an Input of 8 bits block of plain text with two sub keys and the whole operation encrypt the plain text into a cipher text, the S-DES security has been enhanced by adding the functionality of the Transposition cipher techniques which increased the complexity of the algorithm, created more confusion and diffusion property and the proposed modification expected to be helpful for the learning purpose as well.
The proposed modified S-DES cryptosystem has been mathematically explained in steps by the help of an example and the execution results proof the security enhancement in the algorithm.

REFERENCES

1 William Stallings, **Cryptography and Network Security: Principles and practices**, Fifth Edition, ISBN 10: 0-13-609704-9, ISBN 13: 978-0-13-609704-4

2 Laurie Burton, **Secret Codes with Rail Fence Cipher Method**, Western Oregon University, www.wou.edu

3 Weber, Ralph E. **Masked Dispatches: Cryptograms and Cryptology in American History**, *1775-1900*. Ft. George G. Meade, MD: Center of Military History, National Security Agency, 1993.

4 Yashwant kuma, **Enhancing the Security of Data Using DES Algorithm along with Substitution Technique**, IJECS ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016, Page No. 18395-18398

5 Alaa H. AL-Hamami, **A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique**, WCSIT ISSN: 2221-0741 Vol. 1, No. 3, 88-91, 2011

6 Arghya Ray, **Improvement of S-DES Technique by use of Key Bunch Matrix and Randomizers**, IJCA (0975 – 8887) Volume 70– No.13, May 2013