

Improvement of S-DES Technique by use of Key Bunch Matrix and Randomizers

Arghya Ray
Final year-Department of CSE
SRM University
Vadapalani Campus
Chennai - 600026,
Tamil Nadu, India.

Santhoshi Bhat
Pre-Final year-Department of CSE
SRM University
Vadapalani Campus
Chennai - 600026,
Tamil Nadu, India.

ABSTRACT

In this modern age information sharing and transfer has increased exponentially. The information shared is vulnerable to unauthorised access and inception. Cryptography is used to provide secrecy in message transmission. The Simplified Data Encryption Standard or in short S-DES algorithm is used to encrypt messages to form secret text. The previously used S-DES technique can be strengthened by use of randomised key generation techniques which will strengthen the secrecy of the message to be transferred.

General Terms

Key Bunch Matrix; S-DES.

Keywords:

Information Security; Information hiding; Information Security; Key-Bunch Matrix; S-DES.

1. INTRODUCTION

Classical methods of cryptography encrypt plain text to generate cipher text. However, the transmission of cipher text may easily arouse attackers' suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to increase the strength of encryption through S-DES technique[1], the key generation in S-DES[2] is made randomized by use of randomizing algorithms and a key bunch matrix[3]. Thus the message sent is more secure.

2. EXISTING SYSTEM

S-DES and Key Bunch Matrix are two separate cryptosystems. A combination of these two cryptosystems as one single cryptosystem will enhance the security of the message being sent.

Simplified DES (S-DES)

The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext. The encryption algorithm involves five functions: an initial permutation (IP); a complex mangler's function labeled f_K , which involves both permutation and substitution operations and depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function f_K again; and finally a permutation function that is the inverse of the initial

permutation (IP^{-1}). The function f_K takes two 8-bit keys which are obtained from the original 10-bit key.

The S-DES algorithm flow is shown in below figure1. The encryption and decryption processes are almost the operations in reverse order except the stages IP and IP^{-1} . The plaintext entered should be of 8 bits long while the key should be 10 bits long.

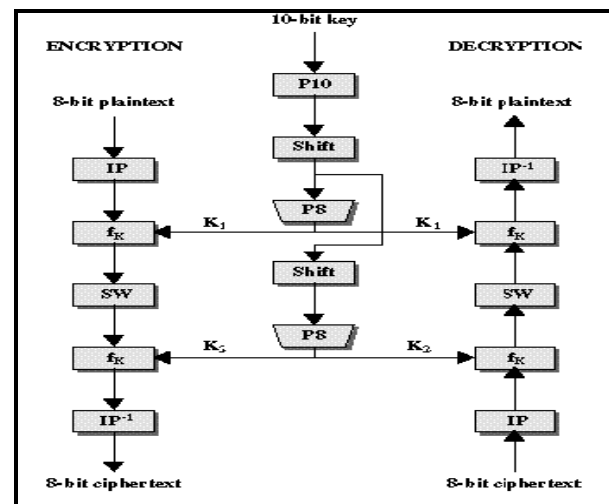


Fig1. S-DES Encryption and Decryption

The 10-bit key is first subjected to a permutation (P10) and then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first sub key (K1). The output of the shift operation again feeds into another shift and (P8) to produce the 2nd sub key (K2).

Key Bunch Matrix

The Key Bunch Matrix is a $n \times n$ matrix consisting of values of key elements. We have

$P = [p_{ij}]$: Plain Text

$C = [c_{ij}]$: Cipher Text

K = Key Generated

$E = [e_{ij}]$: Encryption Matrix

$D = [d_{ij}]$: Decryption Matrix

The operation of the Key Bunch Matrix is explained in Figure2. Here, the plain text is taken as input and using an equation a key is randomly generated. This key is multiplied

with the number equivalent of the plain text and the cipher text is got.



Fig2. Key Bunch Matrix operation

The relation is expressed as :

$$(e_{ij} \times d_{ij}) \bmod 256 = 1$$

$$\text{Encryption : } C = [c_{ij}] = [e_{ij} \times p_{ij}] \bmod 256.$$

$$\text{Decryption : } P = [p_{ij}] = [d_{ij} \times c_{ij}] \bmod 256.$$

These two cryptosystems works well individually but their strength can be increased by combination of them.

3. PROPOSED SYSTEM

To cope with the drawbacks of the existing system a new cryptosystem is proposed where the key generation of the S-DES process is made randomized by the help of Key-Bunch Matrix.

In Fig 3 the original message entered by the user is encrypted by the S-DES Encryption which uses the key generated randomly from the Key Bunch Martix algorithm, thus getting the cipher text as output from the first stage of the proposed cryptosystem.

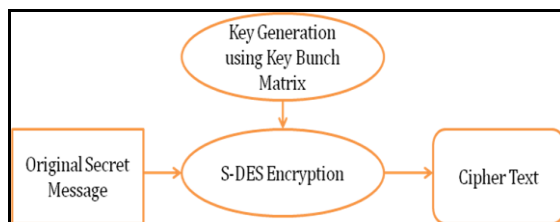


Fig3. Key Generation and Cryptography Process

This cryptosystem will enhance the working of S-DES encryption as now the user need not enter the 10 bit key. The keys will be generated automatically based on the equation given for Key Bunch matrix. This will not only make the algorithm more secure but also will be more convenient.

4. ENCRYPTION

The encryption process starts with the user being asked to enter the message. This message is then encrypted using the S-DES technique where the key is generated randomly by the help of the Key Bunch Matrix generation technique.

4.1 Mathematical Explanation

Input:

Plaintext: HI

Unique Key: 5

Here this unique key is used like a password. This unique key should be same during both encryption and decryption process, else decryption wont take place.

After the randomized operation is completed, the key bunch matrix formed is 46 and 139. Since there are two letters in the entered cipher text, hence the matrix formed is 2*1. These are used during the encryption and decryption operations using S-DES.

The two characters are extracted one by one and converted to its binary equivalent which is entered as input to the S-DES process. This input goes through all the five steps in S-DES through the use of the keys generated in Key Bunch Matrix and thus forms the secret message. The secret message formed is 0013 and 0032.

5. DECRYPTION

The decryption process starts with the user entering the unique key. If this key matches, the decryption process will continue.

5.1 Mathematical Explanation

Input:

Unique Key: 5

Cipher text: 000500020046013900130032

The cipher text consists of the unique key, the length of the plaintext, the randomized keys used during the S-DES operation, and the encrypted message.

All parts are extracted one by one. Initially the first four bits are extracted and checked to check whether the unique key matches or not. If these keys match, then the decryption process continues. Next the randomized keys are extracted and decrypted to get the keys used during encryption process. These keys are used during the decryption process of the cipher text.

6. IMPLEMENTATION

To demonstrate the proposed system we use Java platform and BlueJ version 1.3.5 as the software. The number of lines used in coding for developing the cryptosystem is 1128.

Figure 4 shows the encryption process in BlueJ. The entered plaintext is “HI” and the unique key is 5. This plaintext is encrypted by the use of the modified S-DES and we get the cipher text as “000500020046013900130032” which is transmitted to the receiver. This cipher text contains the unique key, the randomized keys and also the hidden message.

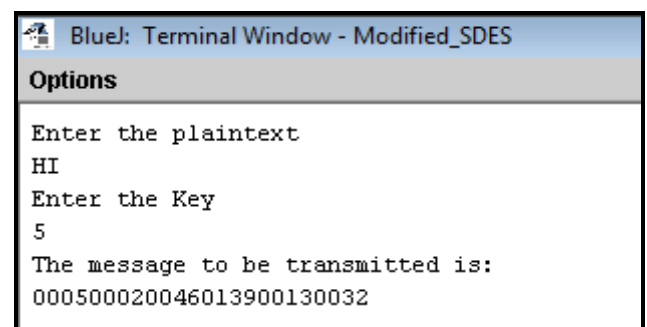
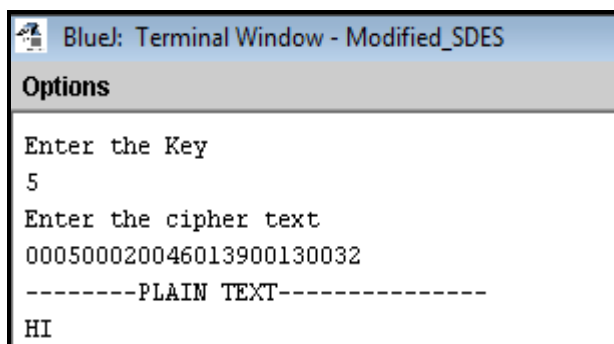


Fig4. Encryption Process

Figure 5 shows the decryption process in BlueJ. The received message is “000500020046013900130032”. The user is also made to enter the unique key.

If this unique key matches, the decryption process is continued. The encrypted randomized keys are extracted and decrypted to get the keys for the S-DES process. The S-DES decryption process is performed to get the original plaintext back.



```
Blue: Terminal Window - Modified_SDES
Options
Enter the Key
5
Enter the cipher text
000500020046013900130032
-----PLAIN TEXT-----
HI
```

Fig5. Decryption Process

Thus, the cryptosystem works successfully and is explained with the example. The main advantage of this cryptosystem is the use of randomized keys through the use of key bunch matrix.

7. FUTURE RESEARCH

The future work can be the use of public and private keys to strengthen the security. The use of hashing and other algorithms as a combination with this new cryptosystem can also strengthen the message being sent.

The use of hash functions will also enable the message being sent more securely.

8. CONCLUSION

The S-DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output. It can be enhanced by use of randomized keys and the key bunch matrix. The cryptosystem is explained by the help of an example and it worked successfully.

9. ACKNOWLEDGEMENTS

We are greatly thankful to Mr. V.U.K Sastry for presenting such a wonderful idea of sending secret messages through the Key Bunch Matrix algorithm. His idea is the backbone of our proposed cryptosystem which will help in transfer of secret messages more securely by enhancing the working of the S-DES Cryptosystem.

10. REFERENCES

- [1] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.
- [2] Data Encryption Standard (DES) ".National Bureau of Standards (US).Federal Information Processing Standards Publication National Technical Information Service. Springfield VA. April 1997
- [3] V.U.K. Sastry and K. Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix", IJCA(0975-8887)