International Journal of Computer Science and Software Engineering (IJCSSE), Volume 6, Issue 7, July 2017
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 152-154

# A Modified Simplified Data Encryption Standard Algorithm

**Syed Naveel Habib[1], Rizwan Awan[2] and Waleej Haider[3]**

[1, 2, 3] Graduate Research Student, Department of Computer Science, Mohammad Ali Jinnah University, Karachi, Pakistan

0333-3585180

[1]naveelsyed@yahoo.com, [2]rizwan.awan1990@gmail.com, [3]directlyproportional2u@yahoo.com

**ABSTRACT**

Encryption is the process to safe confidential data to transmit over insecure channel. Data is not secure because of attackers and intruders. Simplified DES is insecure algorithm because of its 8 bits static keys. We propose the modification in simplified Des algorithm to secure data. We use random number generation keys to make more secure the S-DES algorithm.

Keywords: *S-DES, Encryption, Decryption, Cryptography, Random Number, Security.*

## 1. INTRODUCTION

In this paper we are modifying simplified data encryption standard S-DES. We will define main module of S-DES which are given below.

The process in which to convert plain text to cipher text is called encryption and process which involve to convert cipher text to plain text is called decryption. We can encrypt or decrypt any data through two techniques.

- Symmetric key algorithm
- Asymmetric key algorithm

In the process of symmetric key algorithm sender and receiver does not required different key they share same key but in asymmetric key algorithm two different keys are used one for encryption and another for decryption. We have symmetric key algorithm like S-DES, DES, 3-DES, AES, blowfish etc. and asymmetric key algorithm like RSA.

### 1.1 Simplified data encryption standard

#### 1.1.1 Key Generation for S-DES

In this algorithm we provide 10 bits data to perform permutation. After permutation we divide the resultant 10 bits into two halves. Two groups of 5 bits pass through the two LS-1 module as shown in figure 1. Output of both LS-1 module will become the input of permutation of 8 bits table and LS-2 modules. 8 bits output of permutation table will be the first 8 bits key of S-DES. Output of both LS-1 module will become the input of permutation of 8 bits table. After the permutation we get 2nd key of 8 bits.

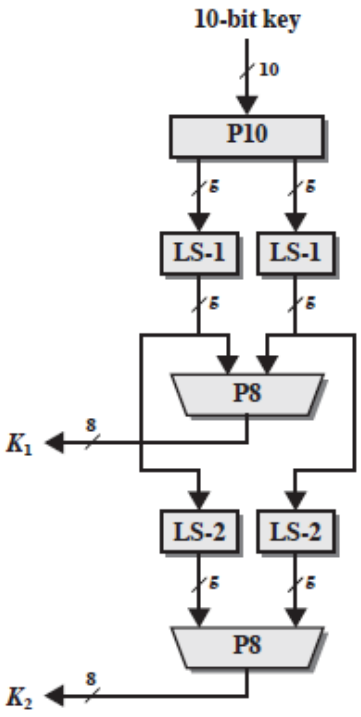


*Fig. 1. Key generation process*

#### 1.1.2. S-DES Algorithm

S-DES algorithm is divide into two module. A Switch function is used to do iteration in algorithm. Algorithm starts with 8 bits of plain text passing through initial permutation table. Then algorithm will perform function fk which include substitution and permutation operation with the help of 8 bits key-1. Then algorithm will perform switch and then perform function fk again with 8 bits key-2. After fk data passing through the inverse

initial permutation table. Finally we get 8 bits cipher text from 8 bits of plain text.

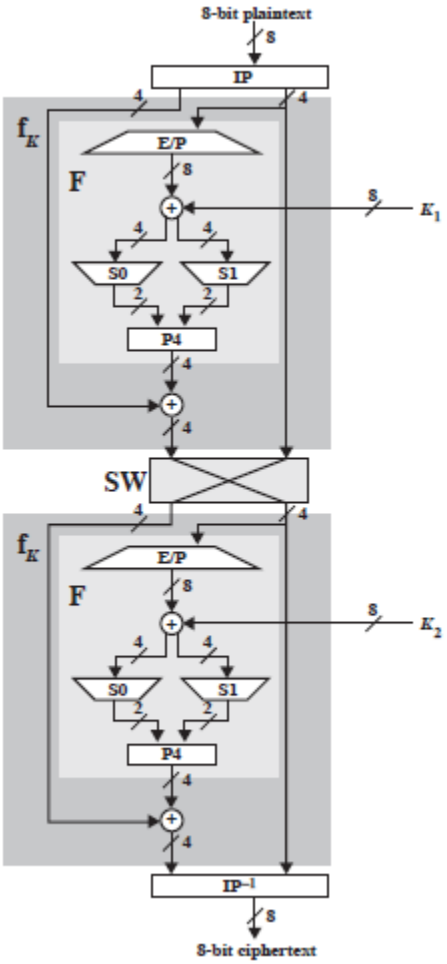


*Fig. 2. Simplified DES Encryption Process*

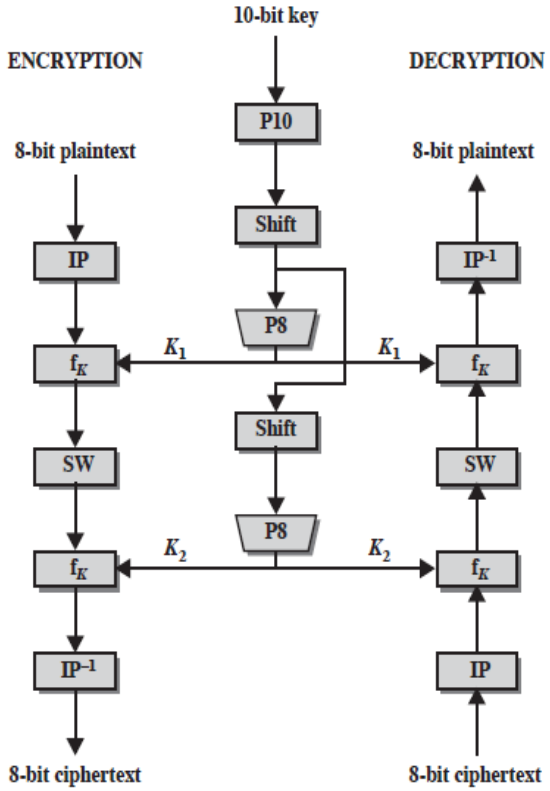


*Fig. 3. Simplified DES scheme*

## 2. METHODOLOGY

In this paper we modified S-DES key generation process through pseudo random number key generation (PRNKG). PRNKG use system current time as a seed and perform function with passphrase to generate 16 bits of Key. This 16 bits of Key is very difficult to guess by attacker. After generating of 16 bits key we divide the key into two halves of 8bits of Key-1 and Key-2 as shown in figure 4.

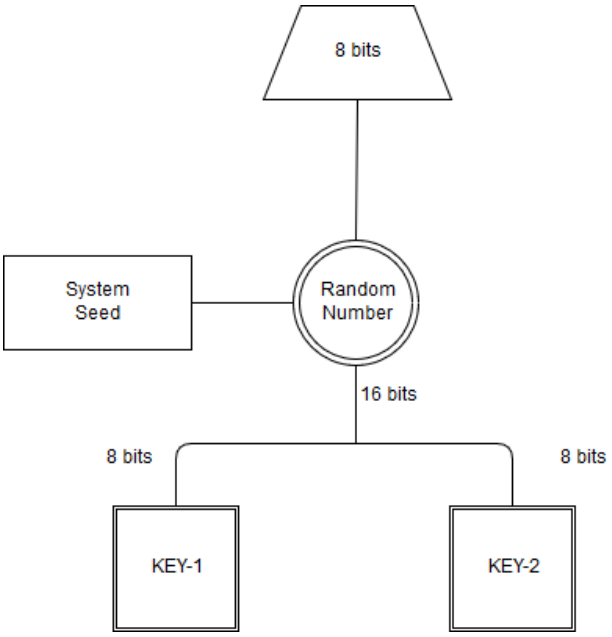


*Fig. 4. Random Key Generator*

## 3. LITERATURE REVIEW

There are many new research has been done in last few year a lot of changing and Modification in SDES. Here are some research which help to find out some problem and techniques.

G.Suman & Ch. Krishna [1] in this paper the researcher improve the security of S-DES Algorithm and they added some substitution techniques in S-DES algorithm to perform the process.

Clark [2] using different optimization techniques and some important analysis done in research.

Vilmalathithan [3] use genetic algorithms to break a SDES.

Grag [4] use memetic algorithms and genetic algorithms to break a SDES.

## 4. CONCLUSION

In these days security is playing a very vital role in communication. When we communicate with another person we threat regarding security in paper we find out solution to make more secure S-DES algorithm. In this paper we propose random key generation to make attacker difficult to guess.

## REFERENCES

[1] Alallayah, Khaled M., et al. "Applying neural networks for simplified data encryption standard (SDES) cipher system cryptanalysis." Int. Arab J. Inf. Technol. 9.2 (2012): 163-169.

[2] Schaefer, Edward F. "A simplified data encryption standard algorithm." Cryptologia 20.1 (1996): 77-84.

[3] Yang, Bo, Kaijie Wu, and Ramesh Karri. "Scan based side channel attack on dedicated hardware implementations of data encryption standard." Test Conference, 2004. Proceedings. ITC 2004. International. IEEE, 2004.

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

[5] Garg, Poonam. "Genetic algorithm attack on simplified data encryption standard algorithm." Special Issue: Advances in Computer Science and Engineering 23 (2006): 139-174.