How S-DES Works

Febiana Hanani, Indri Rahmayuni, Ahmad Fikri A.

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11053@students.if.itb.ac.id,
If11007@students.if.itb.ac.id,If11045@students.if.itb.ac.id

Abstract

Data Encryption Standard (DES) is one of the most widely used symmetric key cryptography algorithm. Therefore, the susceptibility of DES to different kind of attacks has been a concern since the algorithm was first made public. The problem has escalated to the point that Electronic Frontier Foundation has now built a DES cracking machine, at a cost of less than 250,000 USD, that can find the right key in about three days. Of course, the cryptanalytic technique used to find this key might seem overwhelming for us as students to learn. Hence, we need a simpler version of DES in order to learn about these cryptanalytic techniques, S-DES is the answer. S-DES is simpler version of DES that operates on 8-bit message blocks and 10-bits key. This paper discuss about S-DES design, how S-DES works, and different kind of attacks on S-DES.

Keywords : S-DES, attack.

1. Introduction

S-DES is a simpler version of the DES algorithm. S-DES operates on 8-bit message blocks and 10-bits key. It was designed as a test block cipher for learning about modern cryptanalytic techniques such as linear cryptanalysis, differential cryptanalysis, and linear-differential cryptanalysis. The same key is used for encryption and decryption. With its 10-bits key, comparing to 56-bits key used by DES, S-DES is much more vulnerable to an attack. Different kind of attacks that have been proven successful to reveal S-DES key or subset of key are brute force attack, chosen plain text attack, chosen cipher text attack, and known plain text attack.

2. S-DES

S-DES operates on 8-bit message blocks and 10-bits key. It consists of three steps: initial permutation, two rounds key-dependent computation, and inverse of initial permutation.

The 10-bit key is used to generate two different blocks of 8-bit sub keys. The first block is used in the first round of key-dependent permutation and the second block is used in the second round. First, the 10-bit key is subject to an initial permutation, Permuted Choice 1 which is determined by table PC-1, to generate two 5-bit blocks named A_0 and B_0.

Table 1 PC-1

9	7	3	8	0
2	6	5	1	4

There are two rows in the table. The first row determines the bits of A_0 and the second row determines the bits of B_0. Thus, the bits of A_0 are bits 9, 7, 3, 8, 0 of 10-bit key and the bits of B_0 are bits 2, 6, 5, 1, 4 of 10-bit key. Second, a single left shift is performed on A_0 and B_0 yielding A_1 and B_1. Third, B_1 is concatenated to A_1 and then subjected to the second permutation, Permuted Choice 2 which is determined by table PC-2, to form the first block of 8-bit sub keys named K_1.

Table 2 PC-2

3	1	7	5	0	6	4	2

Thus, the bits of K_1 are bits 3, 1, 7, 5, 0, 6, 4, and 2 of bits of A_1B_1. Fourth, a two left shifts is performed on A_1 and B_1 yielding A_2 and B_2. Fifth, B_2 is concatenated to A_2 and then subjected to the second permutation, Permuted Choice 2, to form the second block of 8-bit sub keys named K_2.

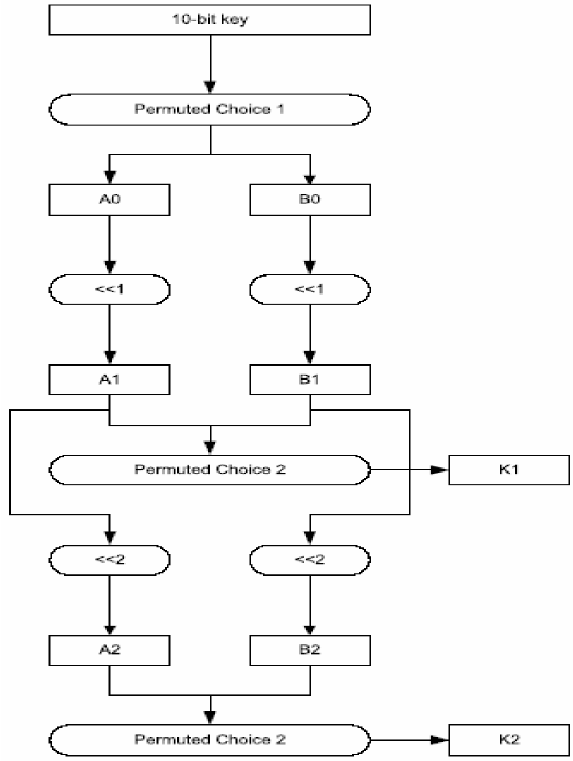

Figure 1 S-DES Key Generation

The encryption procedure can be summarized as:

$$C = E(P, K) = IP^{-1}(\rho_2(\rho_1(IP(P))))$$

where,

C : cipher text
P : plain text
K : 10-bit key
IP : initial permutation
IP^{-1} : inverse of initial permutation
ρ_1 : first round of key dependent computation
ρ_2 : second round of key dependent computation

First, the 8-bit message block is subjected to an initial permutation, IP, which is determined by table IP, to generate two 4-bit blocks named L_0 and R_0.

Table 3 IP

7	6	4	0
2	5	1	3

There are two rows in the table. The first row determines the bits of L_0 and the second row determines the bits of R_0. Thus, the bits of L_0 are bits 7, 6, 4, 0 of 8-bit message block and the bits of R_0 are bits 2, 5, 1, 3 of 8-bit message block. Second, L_0 and R_0 are subjected to first round of key dependent computation yielding L_1 and R_1, which can be summarized as follows:

$$\mathbf{L_1 = R_0}$$
$$\mathbf{R_1 = L_0 \oplus f(R_0, K_1)}$$

where,

f : key dependent cipher function (will be explained bellow)

Third, L_1 and R_1 are subjected to second round of key dependent computation yielding L_2 and R_2, which can be summarized as follows:

$$\mathbf{L_2 = R_1}$$
$$\mathbf{R_2 = L_1 \oplus f(R_1, K_2)}$$

Fourth, R_2 is concatenated to L_2 and then subjected to the second permutation, IP^{-1} which is inverse of initial permutation. The result of this last step is ciphered 8-bit message block corresponding to the input.

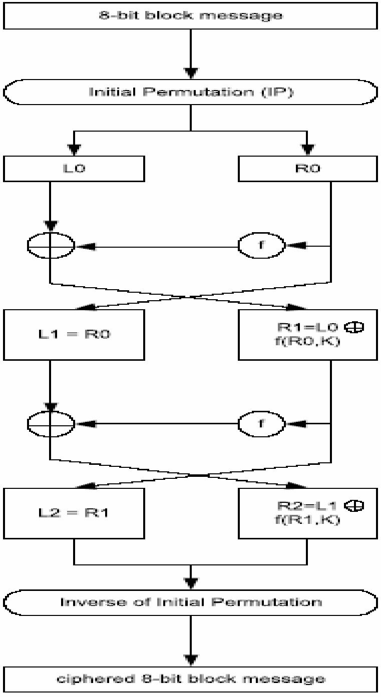

Figure 2 S-DES Encryption Procedure

The first step of key dependent cipher function, f, is to pass the 4-bit block input to function E. E is a function which takes 4-bit block input and yields a 8-bit block as output according to table:

Table 4 E

3	0	1	2	1	2	3	0

The 8-bit block then XORed with the 8-bit sub key, K_1 for first round and K_2 for second round. The result of this XORing operation is then split into two 4-bit blocks, the first four bits from the most significant bit being C_0 and the remaining bits being C_1. C_0 and C_1 are then applied to S_0 and S_1 respectively. S_0 and S_1 are S-Boxes which take in a 4-bit input and yield a 2-bit output.

Table 5 S_0

1	0	2	3
3	1	0	2
2	0	3	1
1	3	2	0

Table 6 S_1

0	3	1	2
3	2	0	1
1	0	3	2
2	1	3	0

An example of how to get output using S_0 and 1001 as input is as follows: we take the first bit and the last bit of 1001 and then used this result to represent a number in base 2, in which we get 3 (11 equals to 3 in base 2). 3 is the row number we are looking for. Then we take the middle two bits of 1001 and then, same as above, used this result to represent a number in base 2, in which we get 0 (00 equals to 0 in base 2). 0 is the column number we are looking for. The element of 3rd row and 0th column is 1, which in binary is written as 01. Hence, using 1001 as input, we get 01 as the output. The output of S_0 and S_1 are concatenated and then subjected to a permutation, P, which is determined by table P. The result of this last step becomes the result of key-dependent cipher function f.

Table 7 P

1	0	3	2

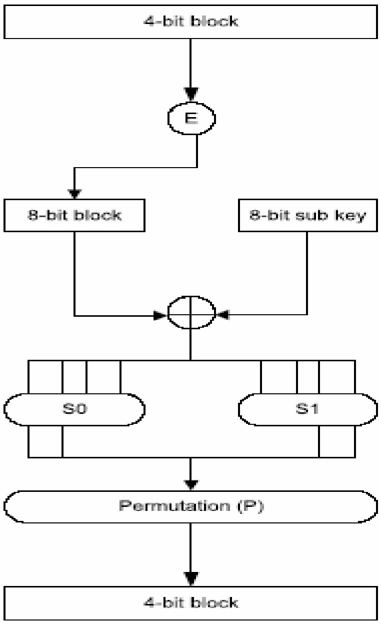

Figure 3 S-DES Key Dependent Cipher Function

The decryption procedure is the same as the encryption procedure, but the sub keys are applied in the reverse order. K_2 is used in the first round and K_1 is used in the second round.

$$\mathbf{P = D (C, K) = IP^{-1} (\rho_2 (\rho_1 (IP (C))))}$$

3. Attack On S-DES

It is feasible to attack S-DES using **brute force attack** since it only has a key size of 10 bits. In order to perform this kind of attack, we need to have a plain text-cipher text pair in which we search the key space until the appropriate plain text encrypted with the guessed key yields the cipher text.

Differential cryptanalysis is a chosen plain text/chosen cipher text attack. **Chosen plain text attack** is a scenario in which the attacker has the ability to chose plain text and to view their corresponding cipher text. **Chosen cipher text attack** is a scenario in which the attacker has ability to choose cipher text and to view their corresponding plain text. Differential cryptanalysis involves the analysis of the effect of the plain text pair difference on the resulting cipher text difference. In S-DES, the difference in a cipher text pair for a specific difference of a plain text pair is influenced by the key. By utilizing this fact, we can reveal information about the key 1).

Linear cryptanalysis is a known plain text attack. **Known plain text attack** is a scenario in which the attacker has access to the pairs (Pi, Ci), i = 1, . . .N of known plain texts and their corresponding cipher texts. Linear cryptanalysis is based on the fact that there are high probability of occurrences of linear expressions consisting the plain text bits, cipher text bits, and key bits. The goal is to find the linear expression which holds with the highest linear probability bias. A linear expression consisting the plain text bits, cipher text bits, and key bits with a high linear probability bias means that the cipher used is not sufficiently random. Using the linear expression with the highest linear probability bias obtained, we can reveal information about the key 5).

4. Conclusion

In this paper, we have shown the design issue of S-DES and how it works in enciphering and deciphering message. With 10-bits key, different kind of attacks have been done successfully on S-DES. These including brute force attack, chosen plain text attack, chosen cipher text attack, and known plain text attack. Having this kind of characteristic, we can use S-DES as a first step in learning about cryptanalytic technique. Furthermore, this technique can also be used to attack more complicated cryptography algorithm, in this case it will be DES.

References

[1] E.Biham and A.Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[2] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research*, Wiretap Politics, & Chip Design, O'Reilly and Associates, 1998.

[3] J.Killian and P.Rogaway, *How to Protect DES Against Exhaustive Key Search*, Advances in Cryptology-CRYPTO '96, Lecture Notes in Computer Science, Springer-Verlag, 1996.

[4] K.S.Ooi and Brain Chin Vito, *Cryptanalysis of S-DES*, University of Sheffield Centre, Taylor's College, 2002.

[5] M.Matsui, *Linear Cryptanalysis Method for DES cipher,* EUROCRYPT,1994.