Differential Cryptanalysis on S-DES

Keshav Raj[1], Bharti Sharma[1], Neeraj Kumar[2], Dr. Dalveer Kaur[3]

[1]B.Tech. (EC) IV year students, Shobhit University, Meerut
[2]Assist. Prof. Dept. of Electronics, Informatics & Comp. Engg. Shobhit University, Meerut
[3]Assistant Professor, Punjab Technical University, Jalandhar

ABSTRACT

In this paper differential attack on S-DES is carried out. S-DES is the reduced version of DES algorithm. This algorithm operates on 8-bit message block with 10-bit key and DES operates on 64-bit message block with 56-bit key. This paper analyzed the differential attack on S-DES. Differential attack is used to break a cipher by trying each possible key.

Keyword S-DES, encrypt, decrypt, cipher function

1. INTRODUCTION

Security is the main concerns of the organizations participating in the information revolution. Although cyber space has become new arena of information exchange and commerce, it can become a place for new forms of old crimes. Cryptographers are constantly searching for the perfect security system, a system that encrypts quickly but is hard or impossible to break. [1]

1.1 S-DES

S-DES is a reduced version of the DES algorithm. It has similar properties to DES but deals with a much smaller block and key size (operates on 8-bit message blocks with a 10-bit key). It was designed as a test block cipher for learning about modern cryptanalytic techniques such as differential cryptanalysis.

It is a variant of Simplified DES. The same key is used for encryption and decryption. Though, the schedules of addressing the key bits are altered so that the decryption is the reverse of encryption. An input block to be encrypted is subjected to an initial permutation *IP*. Then, it is applied to two rounds of key-dependent computation. Finally, it is applied to a permutation which is the inverse of the initial permutation. [2]

2. DIFFERENTIAL ATTACK ON S-DES

Differential cryptanalysis is a chosen plaintext/ chosen ciphertext attack.[3] In which the attacker is able to select inputs to a cipher and examine the Output. Differential cryptanalysis provides a good understanding of the possible weakness of cipher and techniques to overcome them. Differential cryptanalysis involves the analysis of the effect of the plaintext pair difference on the resulting ciphertext difference.[4]Consider the following basic linear cipher function:

$$C = P \oplus K$$

We take the difference pair of ciphertext with no information about key:

$$C \oplus C' = P \oplus K \oplus P' \oplus K$$

$$C \oplus C' = P \oplus P'$$

The above equation shows us the difference between the plaintext is the same as the difference between ciphertext because of linearity of the function.[4]

	ΔY given ΔX						
X	Y	0	1	2	3	4	5
0000	01	00	10	01	00	11	01
0001	11	00	10	10	11	11	01
0010	00	00	01	01	11	11	10
0011	01	00	01	10	00	11	10

0100	10	00	10	01	00	11	01
0101	00	00	10	10	11	11	01

Table-1: Difference pair table for So

S-DES is not a linear function. Thus, the difference between ciphertext is not equal to difference between plaintext. In S-DES, the difference in a ciphertext pair for a specific difference of a plaintext pair is influenced by the key [5].

2.1. Difference pairs of an s-box

The input difference pairs of an S-Box is denoted as ΔX and output difference pairs of an S-Box is denoted as ΔY.

Where,

$$\Delta X = X' \oplus X''$$

And $$\Delta Y = Y' \oplus Y''$$

X' and X'' are the plaintext and Y' and Y'' are output of difference pair table.

2.2 Difference distribution table

In this table row is represented by ΔX and column by ΔY and the element represents the number of occurrences.

- With the help of this table we can obtained the input and output values from their differences.[5]

We have $\Delta X = 12$ and $\Delta Y = 3$, Number of occurrence = 2. Then input pair is (6,10) & (10,6)

- We can also find the key bits which are involved in S-Box if the input pairs and output difference are known.[5]

Assuming X'=6, X''=10 and the S-Box is So.Then Y'=3 and Y''=0 & ΔY=3.Let the inputs of S-Box X'&X'' are xoring with same key and we will find the output I'&I''.I'=X'$\oplus$K and I''=X''$\oplus$K. because we used the same key so key has no influenced on the input difference value so from the above analysis-$\Delta X = \Delta I = 6 \oplus 10 = 12$

Now from the distribution table we obtained that ΔX=12 and ΔY = 3 have the 2 possible values, so there are two possible value for the key.since ΔI=12 then the possible value I that can satisfy the distribution table is 4 and 8 for these value ΔY must be equal to zero.

K=X $\oplus$ I, the first possible key is obtained from

K=I'$\oplus$ X'=4$\oplus$ 6=2 and K=I'$\oplus$ X''=4$\oplus$ 10=14.

so the obtained keys are 2 and 14.in the same manner,

K=I''$\oplus$ X'=8$\oplus$ 6=14 and K=I''$\oplus$ X''=8$\oplus$ 10=2.

	Output difference ΔY			
Input Difference ΔX	0	1	2	3
0	16	0	0	0
1	0	8	4	4
2	0	4	12	0
3	4	4	0	8
4	0	4	0	12
5	4	4	8	0
6	0	8	4	4
7	8	0	4	4
8	2	2	10	2
9	4	4	0	8
10	10	2	2	2
11	0	8	4	4
12	2	10	2	2
13	8	0	4	4
14	2	2	2	10
15	4	4	8	0

Table-2: Difference distribution table for So

2.3 Differential characteristics

With the help of differential characteristics we find the subkey, k'' used in the last round. We create a differential characteristic using the following difference pair.[6]

ΔX= 12, ΔY=3

E = [3 0 1 2 1 2 3 0]

ΔUi = 10010110

Using figure 1 we obtained ΔVi

ΔVi = 01100100

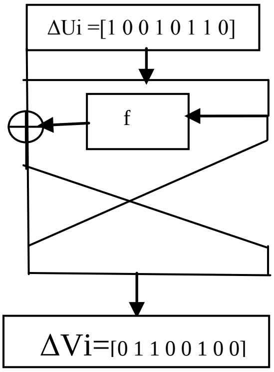

Figure – 1: differential characteristics

3. IMPLEMENTATION OF DIFFERENTIAL ATTACK

3.1 Implementation steps

Step followed in differential cryptanalysis as follows

1. The plaintext is encrypt with unknown key.
2. Now for finding the ΔI encrypt the plaintext with assumed key.
3. Find the value of I’ & I’’ using difference pair table, For that value ΔY=0.
4. Now xoring the plaintexts with I’ & I’’ and get possible values of keys K_1 and K_2.
5. Decrypt the ciphertext using K_1. If Plaintext is matched then encryption is cracked. Otherwise use K_2.

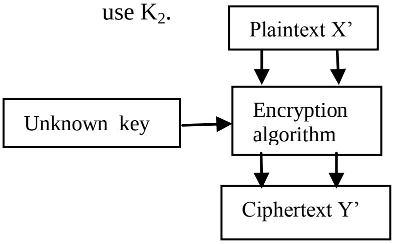

Figure – 2: Generation of ciphertext using unknown key

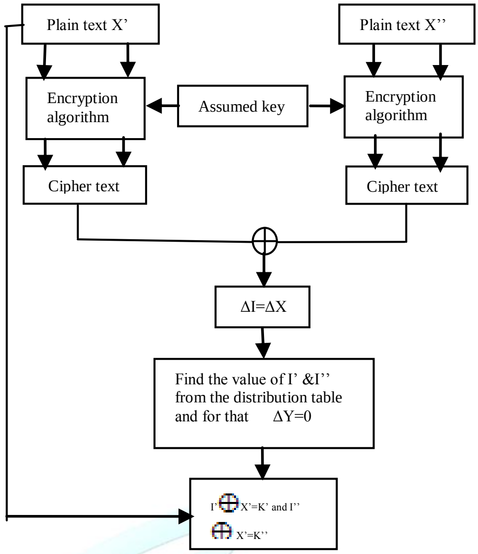

Figure – 3: Generation of I’ & I’’ using assumed key

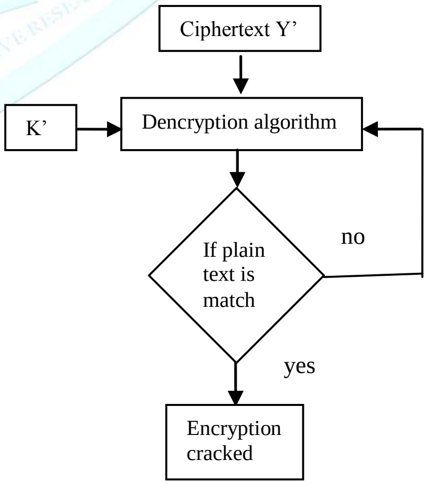

Figure – 4: Evaluation of actual key

4. RESULT

This section shows that the result obtained by running the differential attack on S-DES in C.

Round 1 input differential characteristics, ΔUi=96

Round 1 output differential characteristics, ∆Vi=64

Expansion E= [3 0 1 2 1 2 3 0]

S-Box input	Possible keys	Actual key
00000100 00001000	00000010 00001110	00000010
00000111 00001101	00000101 00001111	00000101
00000010 00001010	00000010 00001010	00001010

I. When S – Box input are 4 & 8, possible key 2 & 14 are applied on S-Box & ciphertext is cracked by key 2 then key 2 is actual key.

II. When S – Box input are 7 & 13, possible key 5 & 15 are applied on S-Box & ciphertext is cracked by key 5 then key 5 is actual key.

III. When S – Box input are 2 & 10, possible key 2 & 10 are applied on S-Box & ciphertext is cracked by key 10 then key 10 is actual key.

5. CONCLUSION

The represented result shows that the differential attack found 8 bit of the subkey of the last round. These sub key bits are the actual 8 bits of the S-DES 10 bit key, 2 bit are still missing i.e. found by matching of 2^2 possibilities.

REFERENCES

1. A framework for security analysis of mobile wireless networks, Theoretical Computer Science, In Press, Accepted Manuscript, Available online 5 September 2006, Sebastian Nanz and Chris Hankin.
2. Edward Schaefer, 1996, A Simplified Data Encryption Standard Algorithm, Cryptologia 96 .
3. Eli Biham and Adi Shamir, 1993, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, Berlin, Germany.
4. Fauza Mirzan, 2000, Block ciphers and Cryptanalysis, Department of Mathematics, Royal Holloway University of London.
5. Eli Biham and Adi Shamir , 1990, Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology—CRYPTO’90. Springer-Verlag.2-21.
6. Howard M. Heys, 2000, A tutorial on Linear and Differential Cryptanalysis, Memorial University of Newfoundland, Canada.
7. Jaon Daemen, Vincent Rijmen, 2000,AES Proposal: Rijndael, http://csrc.nist.gov/encryption/aes/ Last Visited:7th February 2001.
8. Henning Schulzrinne, 2000, Network Security: Secret Key Cryptograph, Columbia University, New York.
9. Joe Kilian and Philip Rogaway, 1995, A Fast Method for the Cryptanalysis of Subsitution Ciphers, Dragoer, Denmark.