

Chapter 7

Block Cipher Operation Part 1





Learning Objectives

- After studying this chapter, you should be able to:
 - **Analyze the security of multiple encryption schemes.**
 - **Explain the meet-in-the-middle attack.**
 - **Compare and contrast ECB, CBC, CFB, OFB, and CTR modes of operation.**



DES Weaknesses

- During the last few years critics have found some weaknesses in DES.
- Weaknesses in Cipher Design
 1. **Weaknesses in S-boxes**
 2. **Weaknesses in P-boxes**
 3. **Weaknesses in Key**



Weaknesses of S-Boxes

- Two specific chosen inputs to S-box array may create same output.
- It is possible to obtain same output in single round by changing bits in only three neighboring S-boxes*.
- In S-box 4 last three output bits can be derived in same way as first output bit by complementing some input bits*.

	<i>0</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	<i>12</i>	<i>13</i>	<i>14</i>	<i>15</i>
<i>0</i>	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
<i>1</i>	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
<i>2</i>	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
<i>3</i>	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-Box 1

*** Homework. Find an example of the weakness.**



Weaknesses of P-Boxes

- It is not clear what is the purpose of Initial and Final Permutations
- In Expansion P Box 1st and 4th bit of every 4 bit series is repeated

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01



Weaknesses of Keys

- Let us try the first weak key to encrypt a block two times.
- After two encryptions with the same key the original plaintext block is created. Note that we have used the encryption algorithm two times, not one encryption followed by another decryption.

Key: 0x0101010101010101

Plaintext: 0x1234567887654321

Ciphertext: 0x814FE938589154F7

Key: 0x0101010101010101

Plaintext: 0x814FE938589154F7

Ciphertext: 0x1234567887654321

Weak keys

<i>Keys before parities drop (64 bits)</i>	<i>Actual key (56 bits)</i>
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFFF

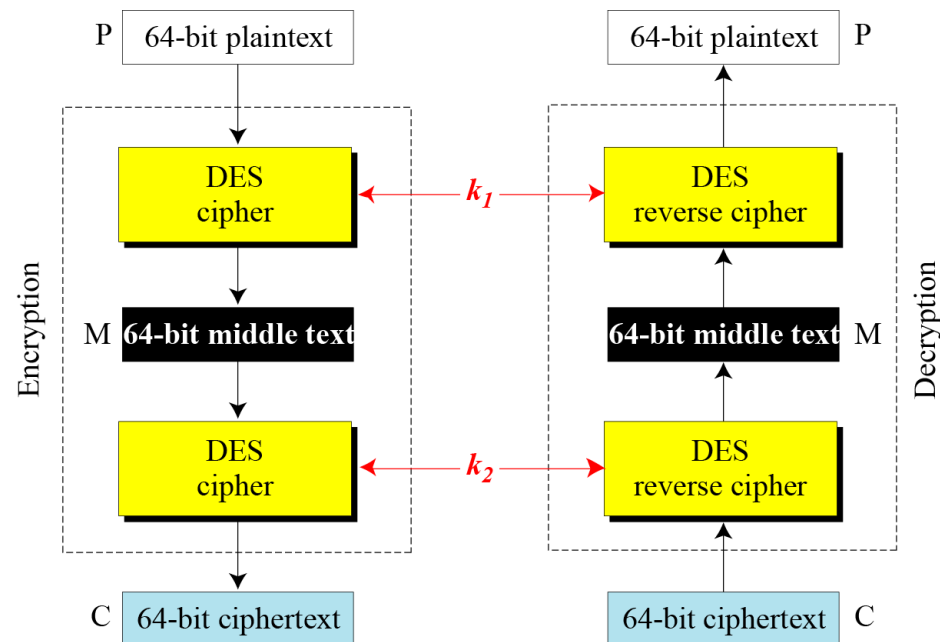


Multiple DES

- The major criticism of DES regards its key length.
- Clearly, a replacement for DES was needed!
 - **theoretical attacks that can break it**
 - **exhaustive key search attacks are possible**
- Fortunately DES is not a group.
 - **This means that we can use double or triple DES to increase the key size.**
 1. Double DES- 2 rounds of DES
 2. Triple DES- 3 rounds of DES

Double DES

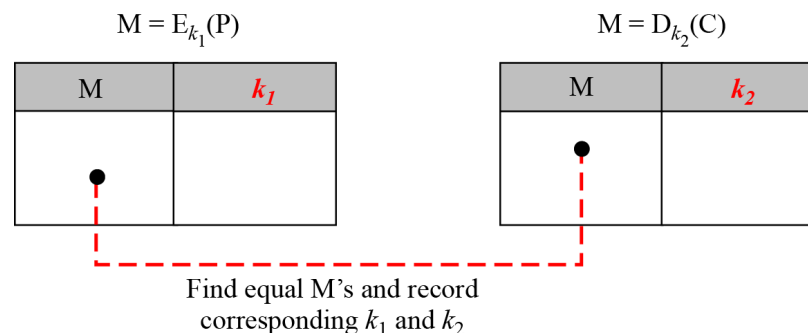
- Apply DES twice to encrypts on each block
 - Each application with a different key → requires 2 keys
 - $C = E_{K2}(E_{K1}(P))$
- Issues:
 - **Reduction to single key**
 - a single key that is equivalent to using 2 keys
 - not likely but proved as impossible in 1992.
 - **Meet-in-the-middle attack**
 - more serious;
 - first described by Diffie in 1977



Double DES- Cont.

- MITM Attack

- Works whenever use a cipher twice
- Since $X = E_{K_1}(P) = D_{K_2}(C)$
- Attack by encrypting P with all keys and store the results
- Then decrypt C with keys and match X value
 - It is a known plaintext attack (i.e. known pair (P,C) , and attempts to find by trial-and-error a value X in the “middle” of the double-DES encryption of this pair. Chances of this are much better at $O(2^{56})$ than exhaustive search at $O(2^{112})$.



Triple DES

- Triple DES → use 3 encryptions
 - would seem to need 3 distinct keys
 - but can use 2 keys

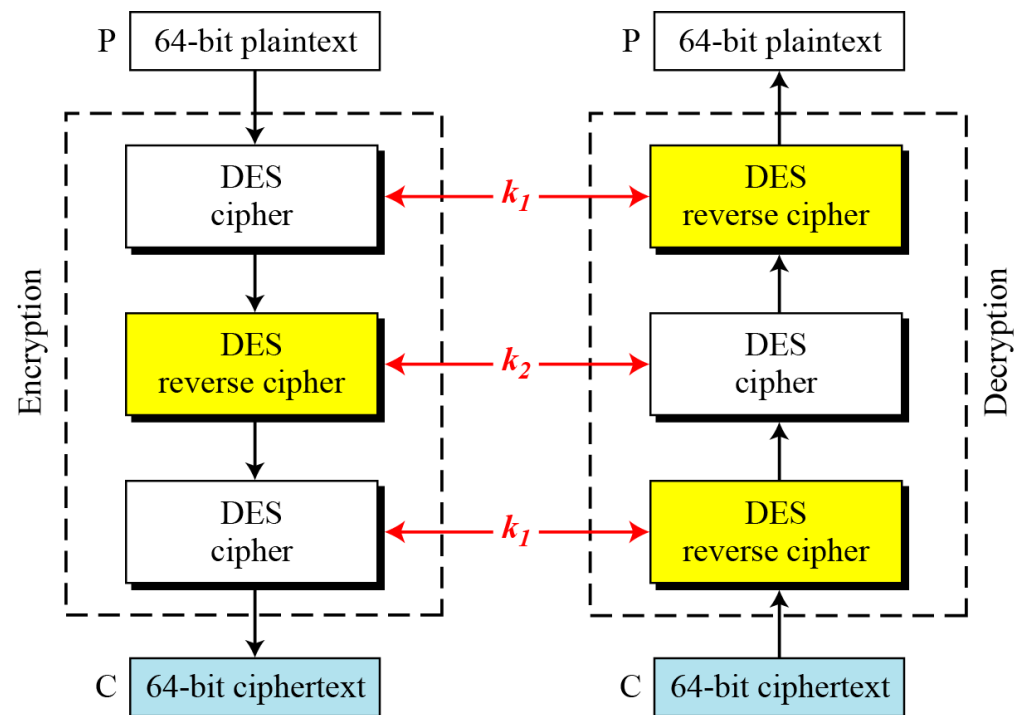
$$C = E_{K_1} (D_{K_2} (E_{K_1} (P)))$$

- **What if $K_1=K_2$?**

The possibility of known-plaintext attacks on triple DES with two keys has enticed some applications to use triple DES with three keys.

Triple DES with three keys is used by many applications such as PGP

- *no current known practical attacks*
- *several proposed impractical attacks might become basis of future attacks*





Triple DES- Cont.

- The design of DES was revealed by IBM in 1994.
- Many tests on DES have proved that it satisfies some of the required criteria as claimed.
- S-Boxes
 - The design provides confusion and diffusion of bits from each round to the next.
- P-Boxes
 - Between two rows of S-boxes (in two subsequent rounds), there are one straight P-box (32 to 32) and one expansion P-box (32 to 48). These two P-boxes together provide diffusion of bits



S-box Design Criteria

1. The entries of each row are permutations of values between 0 and 15.
2. S-boxes are nonlinear. No output of any S-Box is too close to a linear function of the input bits.
3. If two inputs to an S-box differ in one bit, the output bits differ in at least two bits.
4. If two inputs to an S-box differ only in two middle bits (bits 3 and 4), the output must differ in at least two bits.
 - **$S(x)$ and $S(x \oplus 001100)$ must differ in at least two bits where x is the input and $S(x)$ is the output.**



S-box Design Criteria- Cont.

5. If two inputs to an S-box differ in the first two bits (bits 1 and 2) and are the same in the last two bits (5 and 6), the two outputs must be different.
 - $S(x) \neq S(x \oplus 11bc00)$, in which **b** and **c** are arbitrary bits.
6. There are only 32 6-bit input-word pairs (x_i and x_j), in which $x_i \oplus x_j \neq (000000)_2$. These 32 input pairs create 32 4-bit output-word pairs. If we create the difference between the 32 output pairs, $d = y_i \oplus y_j$, no more than 8 of these d 's should be the same.
7. A criterion similar to # 6 is applied to three S-boxes.
8. In any S-box, if a single input bit is held constant (0 or 1) and the other bits are changed randomly, the differences between the number of 0s and 1s are minimized.



P-box Design Criteria

1. Each S-box input comes from the output of a different S-box (in the previous round).
2. No input to a given S-box comes from the output from the same box (in the previous round).
3. The four outputs from each S-box go to six different S-boxes (in the next round).
4. No two output bits from an S-box go to the same S-box (in the next round).




P-box Design Criteria- Cont.

5. For each S-box, two output bits go to the first or last two bits of an S-box in the next round. The other two output bits go to the middle bits of an S-box in the next round.
6. If an output bit from S_j goes to one of the middle bits in S_k (in the next round), then an output bit from S_k cannot go to the middle bit of S_j . If we let $j = k$, this implies that none of the middle bits of an S-box can go to one of the middle bits of the same S-box in the next round.



Summary

- 
- DES Weaknesses
 - S-boxes
 - P-boxes
 - Key
 - Double DES a.k.a. 2DES
 - Triple DES a.k.a. 3DES
 - 2 keys
 - 3 keys
 - Design Criteria
 - S-Box
 - P-Box

Any Question???

