Data Encryption Standard (DES) ALGORITHM

Tophan Kumar Jena

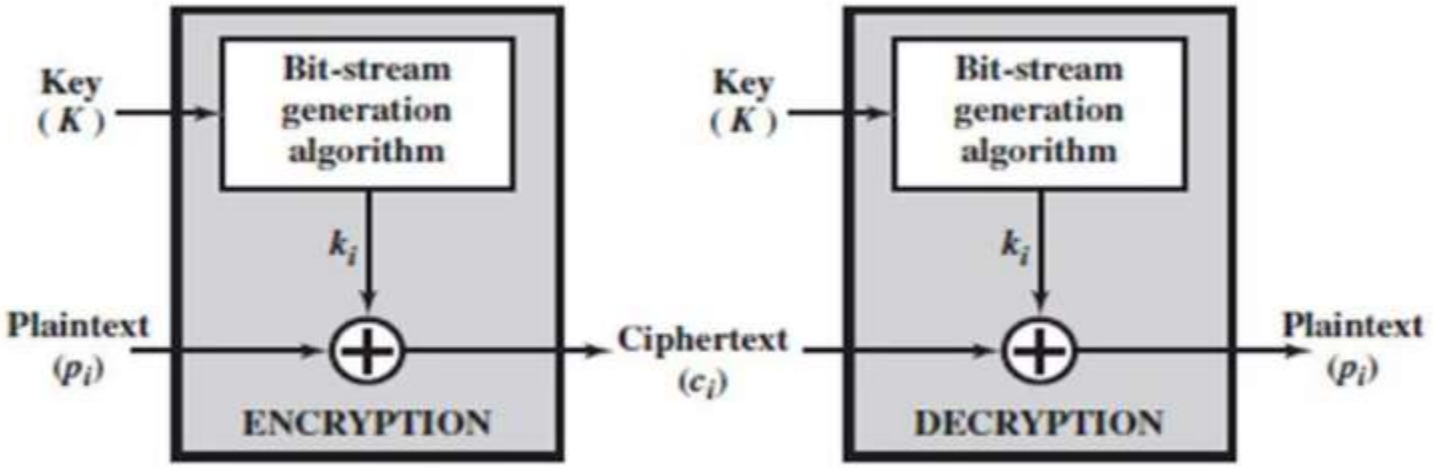
Asst. Professor

Dept.of CSE

Stream Cipher and Block Cipher

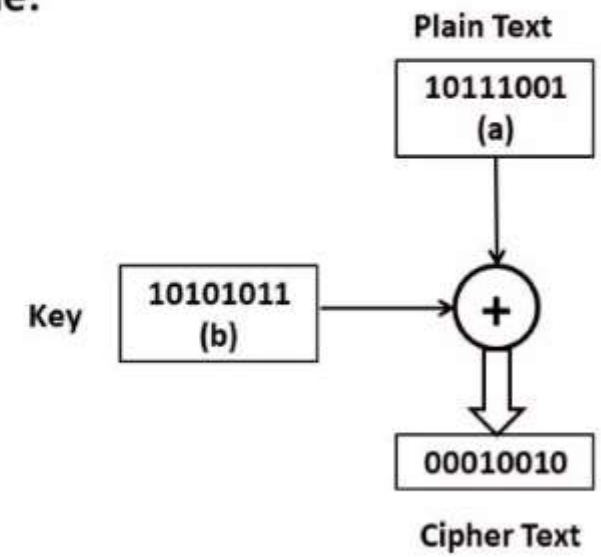
- Stream Cipher: A stream cipher is one that encrypts a digital data stream one bit or one byte at time .
- Example- Vigenere Cipher , Vernam Cipher

Stream Cipher



Stream Cipher

- **Example:**

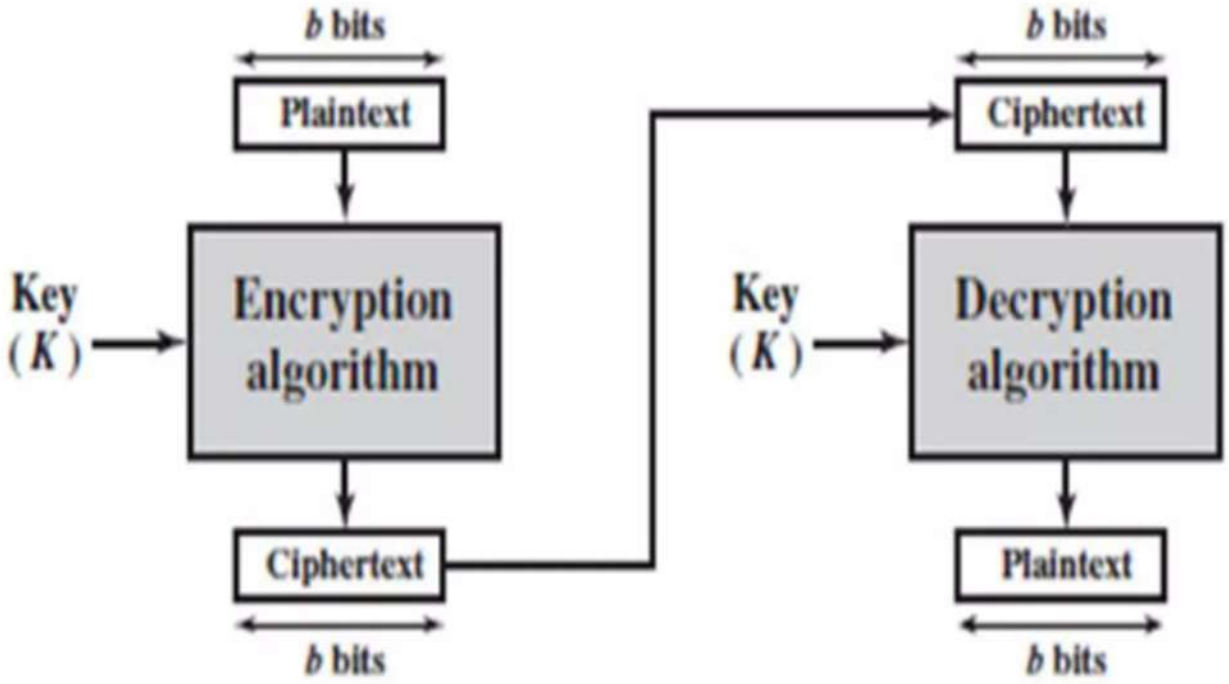


Block Cipher

- Bolck of bytes encrypted at a time .
- A Block cipher is one in which a block of plaintext is treated as a whole and produce a cipher text block of equal length .
- Length of cipher text block is remain same as length of plaintext block .
- Typically a block of size 64 or 128 bit is used

  Example- DES , Triple DES, AES Algorithm

Block Cipher



INTRODUCTION

- DES is a symmetric-key block cipher for encrypting digital data.
- Developed by IBM in early 1970s.
- It was a modified form of the project called Lucifer by Horst Feistel.
- The cipher was first published by NIST in 1973.
- It was finally published in FIPS in 1977.

DES overview

64-bit plaintext

64-bit plaintext

Encryption

DES
cipher

56-bit key

DES
reverse cipher

Decryption

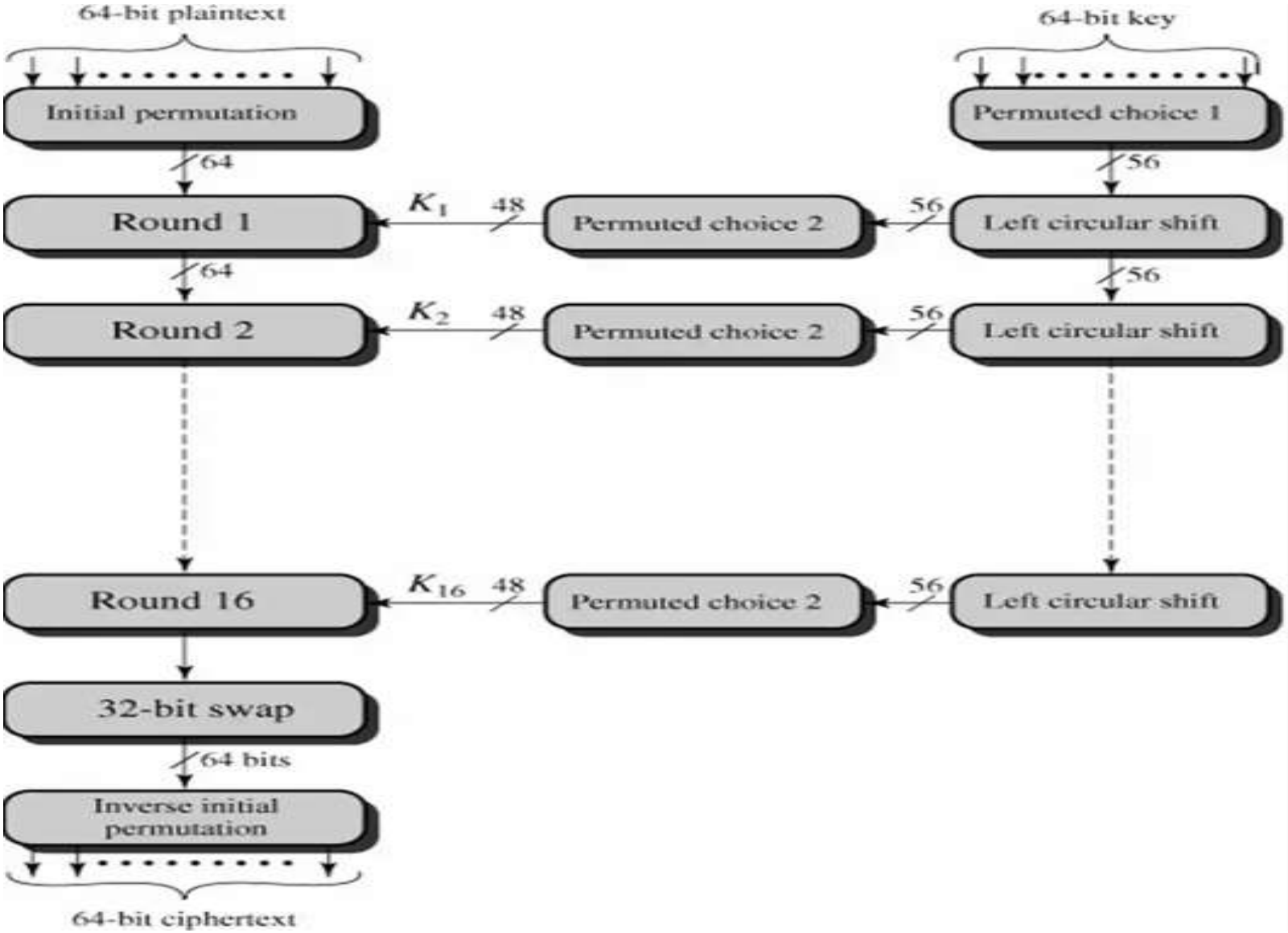
64-bit ciphertext

64-bit ciphertext

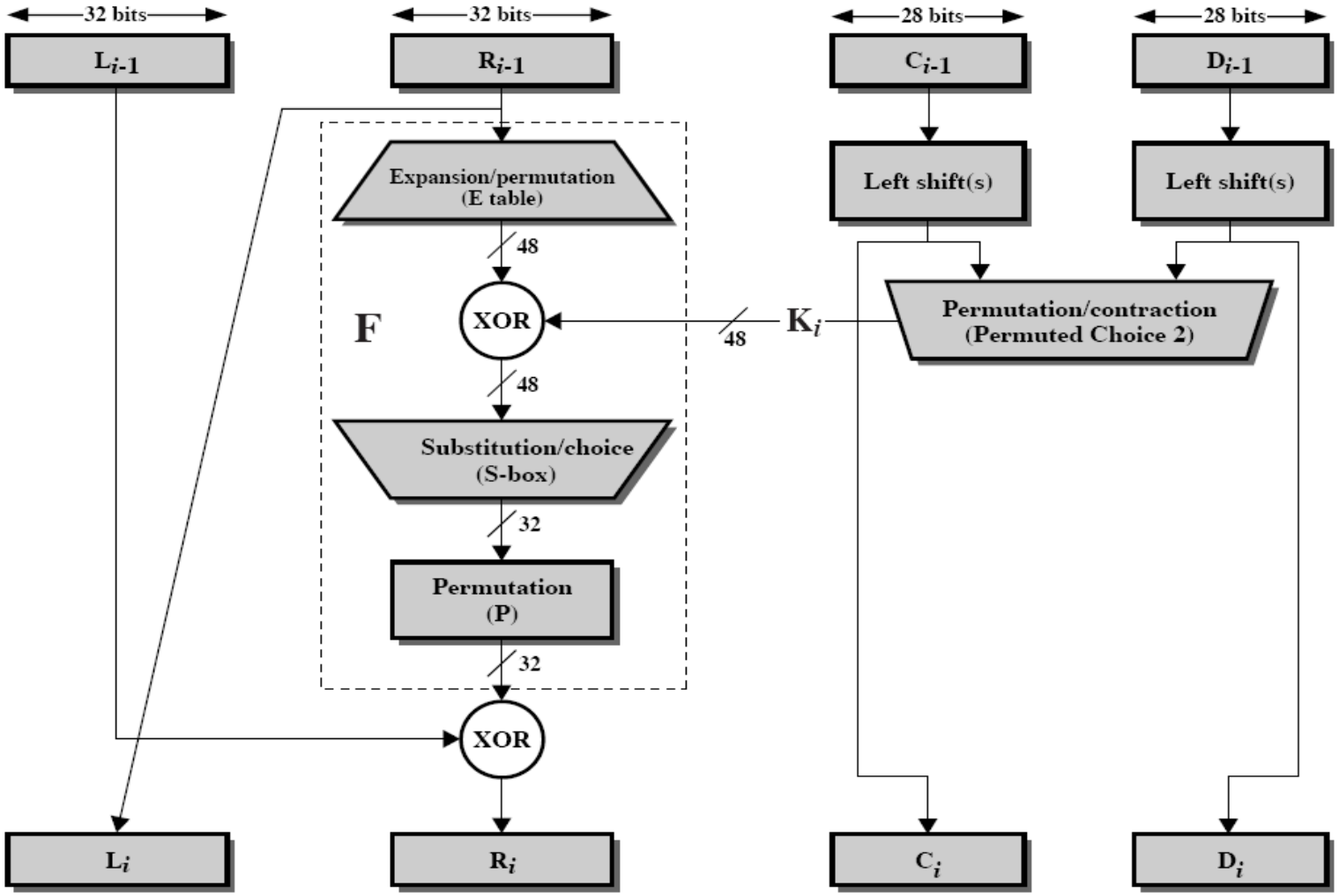
DES *Basics*

- It takes plain text of size 64-bits & produces Ciphertext of size 64-bits.
- But it has a cipher key of size 56-bits.
- Number of subkeys : 16
- Subkey size: 48 bit
- Building blocks of DES
  - P-Box
  - S-Box
  - XOR
  - Sixteen Feistel rounds

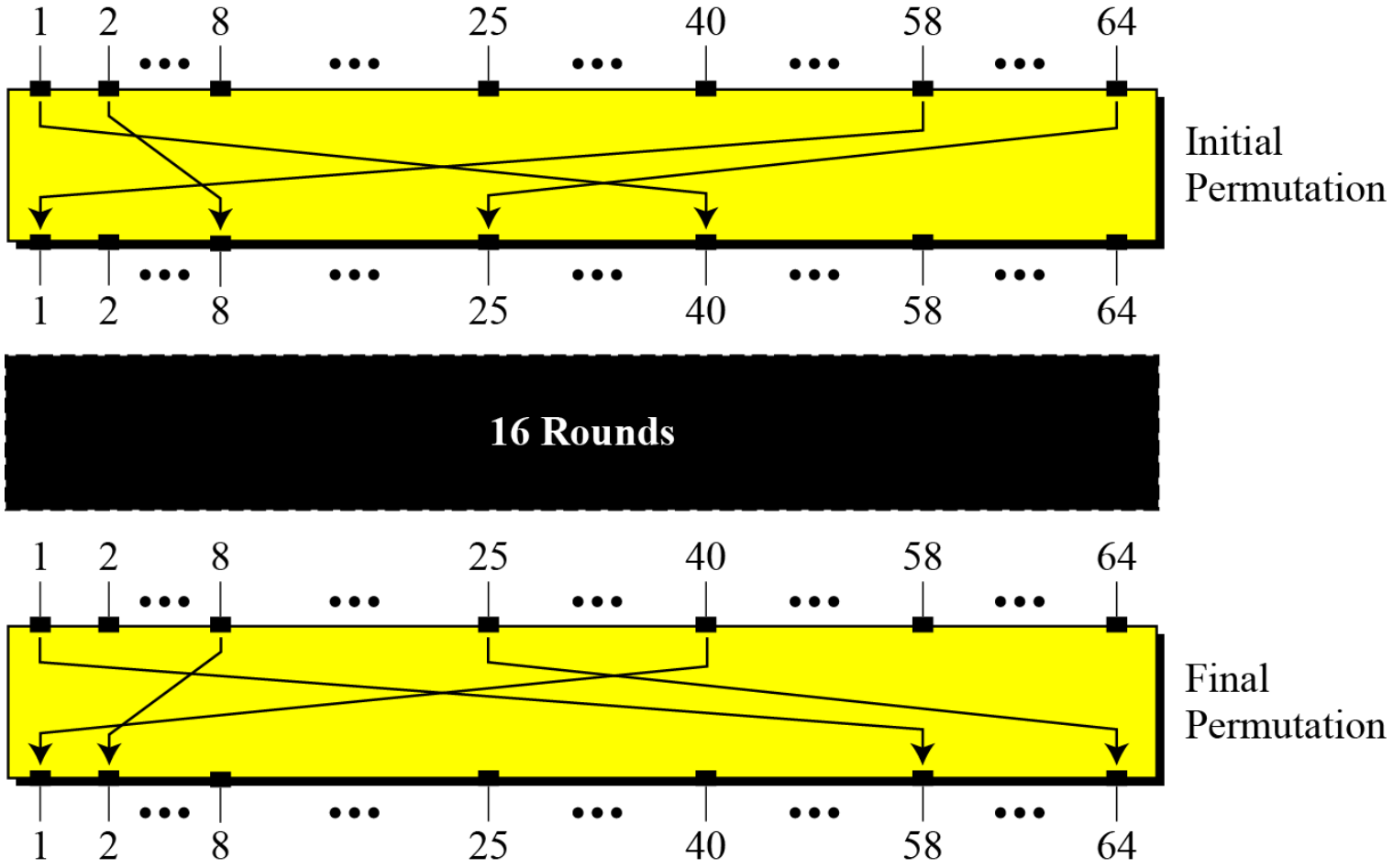
DES ENCRYPTION ALGORITHM



ROUND FUNCTION



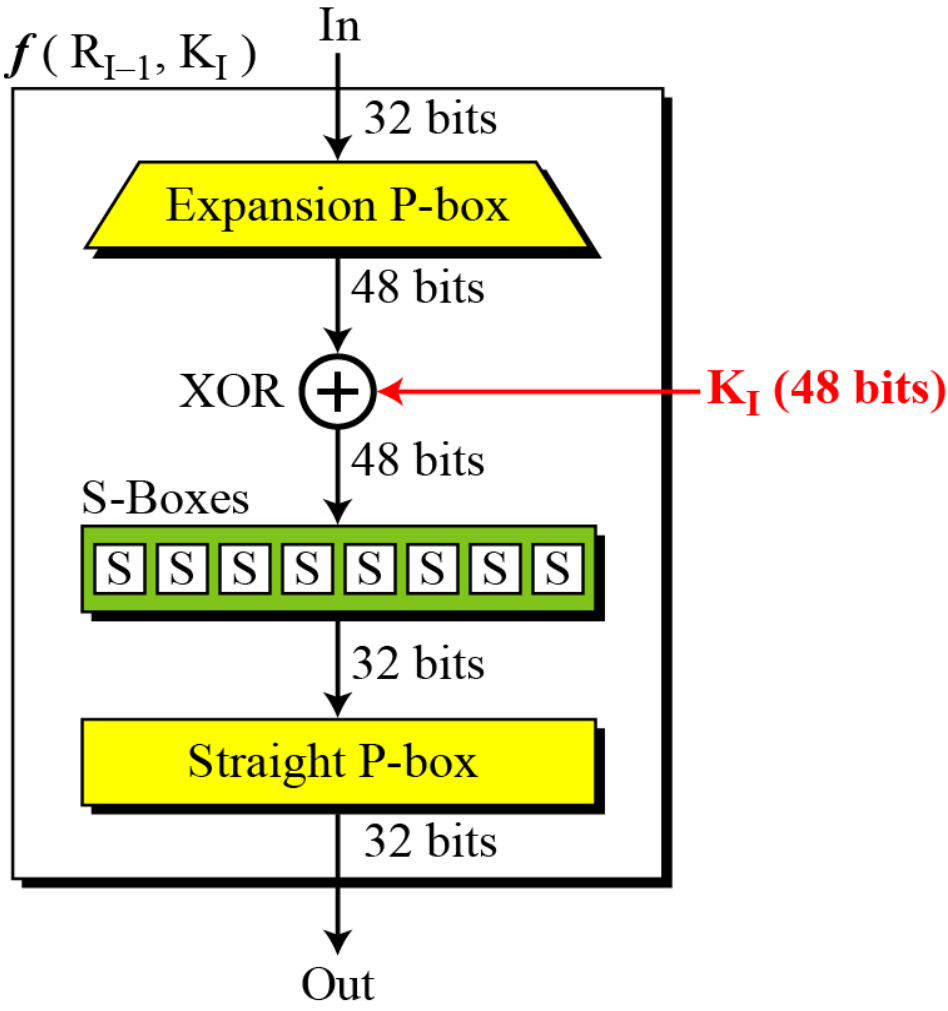
Initial and Final Permutation



Initial and Final permutation

Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

- The heart of DES is the DES function.
- The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output

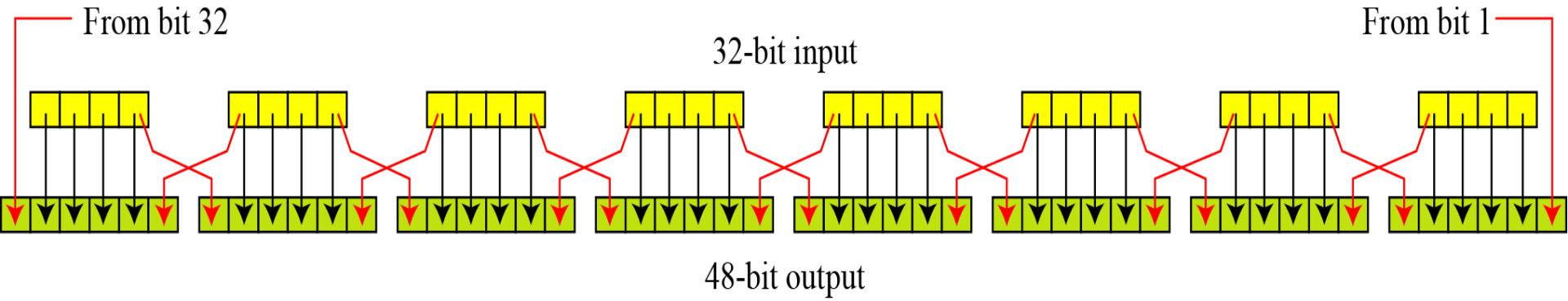


Expansion of P-Box

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

Expansion P-box

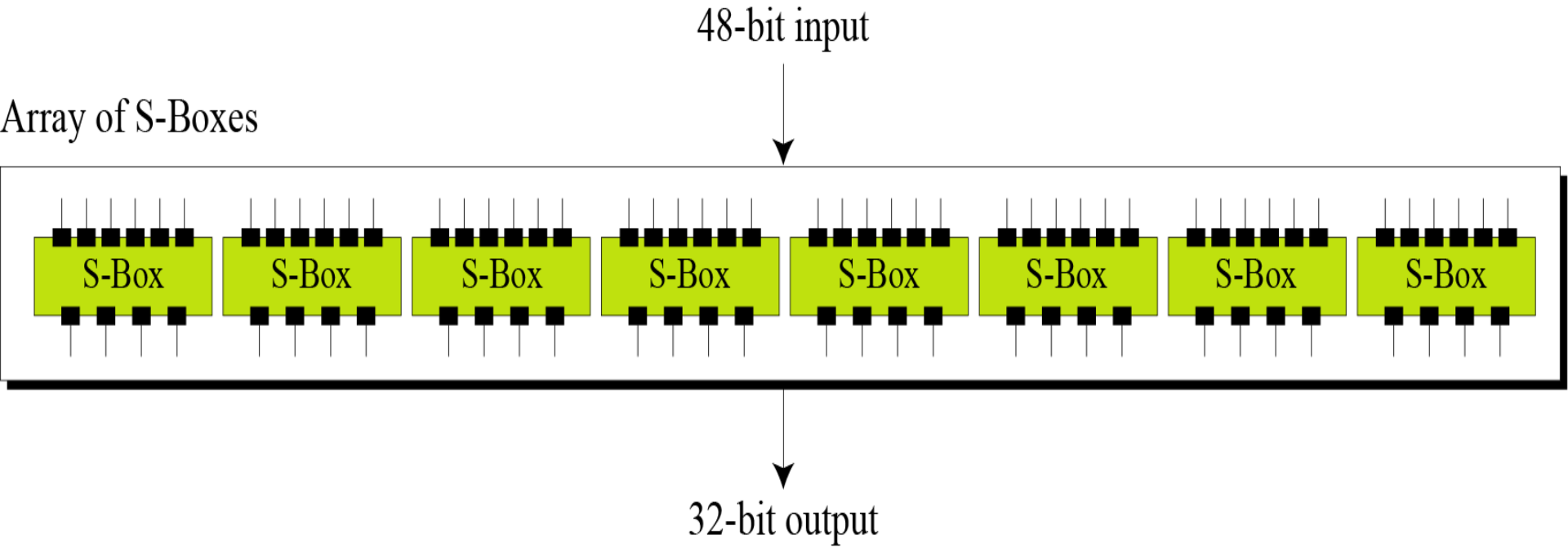
- *Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.*



- After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.
- Note that both the right section and the key are 48-bits in length.
- Also note that the round key is used only in this operation.

S-Boxes

- S-box provides the substitution function i.e. each 6-bit input block is replaced by a 4-bit output block from the S-box.



S-Box(Contd…)

- ***Following Table shows the contents for S-box 1.***
- ***Refer textbook for the rest of the boxes .***

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

Example-The input to S-box 1 is 100011. What is the output?

- Solution
- If we write the first and the sixth bits together, we get 11 in binary, which is 3 in decimal.
- The remaining bits are 0001 in binary, which is 1 in decimal.
- Now, check the value in row 3 & column 1 in S-box 1.
- The result is 12 in decimal, which in binary is 1100.
- So the input 100011 yields the output 1100.

Key Generation

- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

- Parity Drop: It is a compression transposition step.It drops the parity bit (bit 8, 16, 24, 32,…, 64) from the 64-bit key and permutes the rest of the bits according tothe following table

Parity-bit drop table

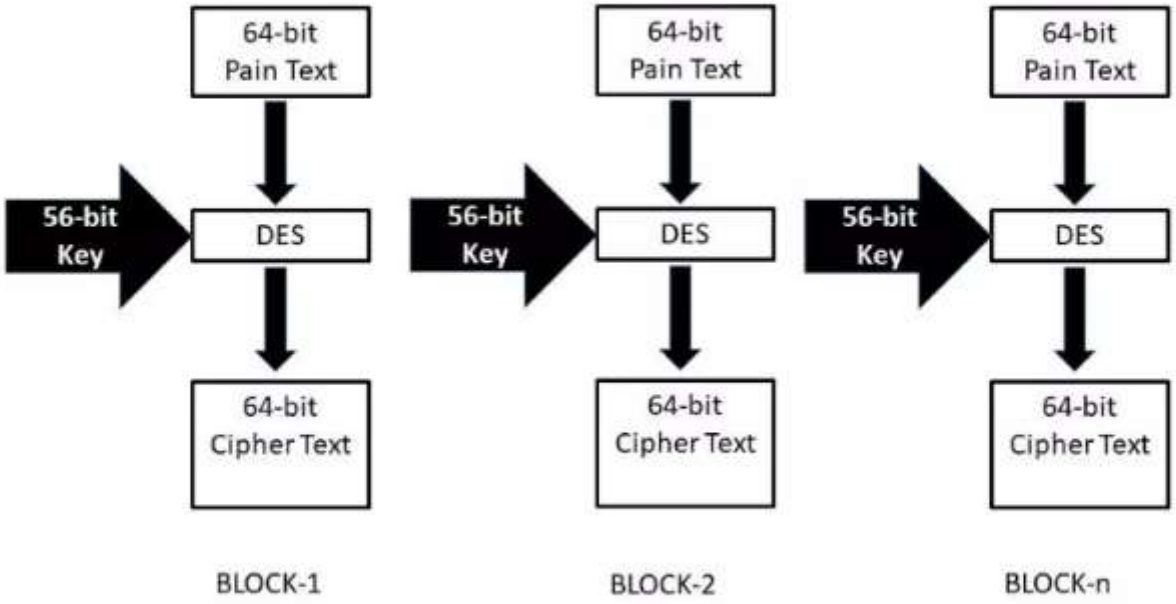
57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

- The 56-bit key is now divided into two 28-bit parts.
- Then each part is left shifted(circularly) by either one or two bits in each round as shown in the table.

Number of bits shifts

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

How DES Works



Application of DES

- Secure File/Data transfer
- Electronic Funds Transfer
- Encrypted Storage Data
- Secure communications

Strength of DES

- Key length 56 bits ie 2^{56}keys .
- Brute-force attack take more than thousand of years .

DES Decryption

- Decryption uses the same algorithm as encryption,except that the application of subkeys is reversed.
- The initial and final permutations are reversed

Double DES

Double DES

- In this approach, we use two instances of DES ciphers for encryption and two instances of reverse ciphers for decryption.
- Each instances use a different key.
  - The size of the key is doubled.
- There are issues of reduction to single stage.
- However, double DES is vulnerable to meet-in-the-middle attack.

Double DES

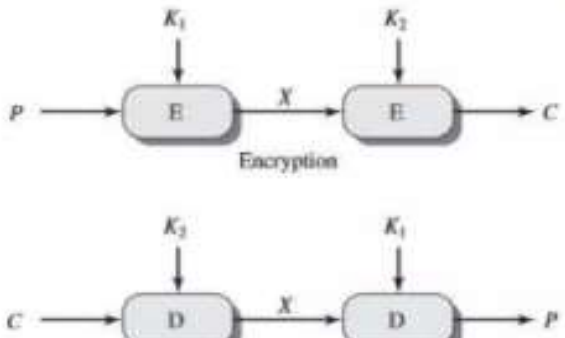
Double DES

- Given a plaintext P and two encryption keys K_1 and K_2, a cipher text can be generated as,

$$C = E(K_2, E(K_1, P))$$

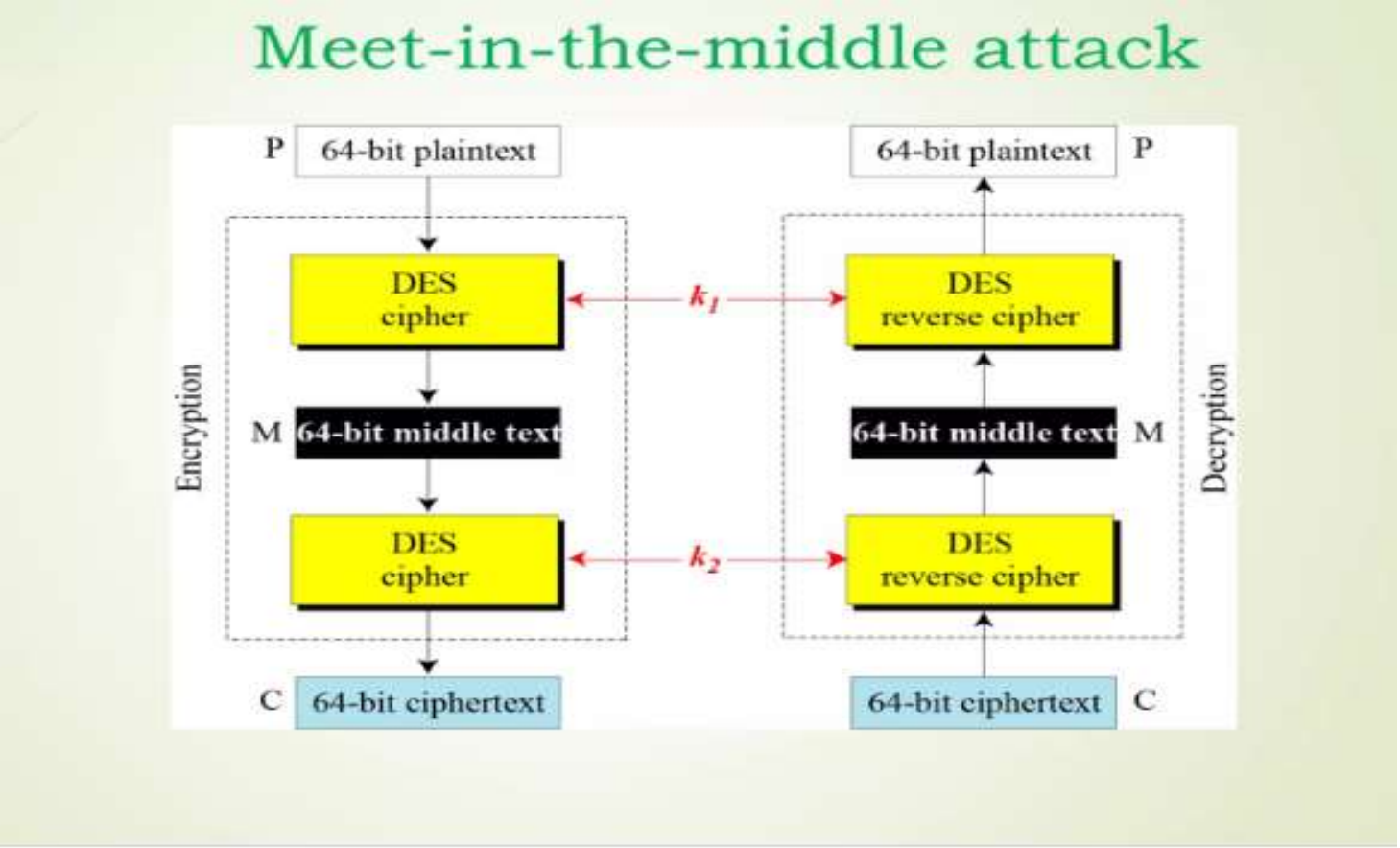
- Decryption requires that the keys be applied in reverse order,

$$P = D(K_1, D(K_2, C))$$



(a) Double encryption

Meet-in-the-middle attack



Meet-in-the-middle attack

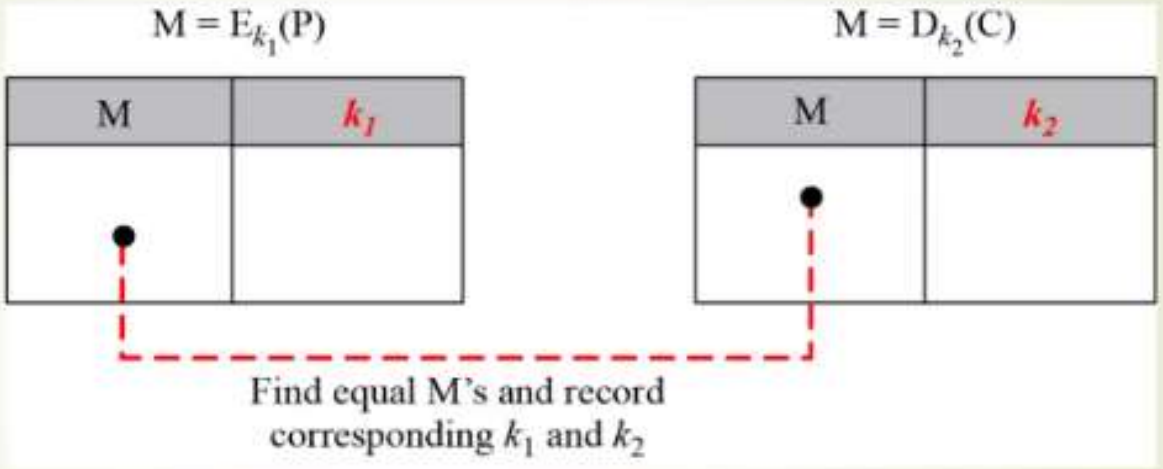
Meet-in-the-middle attack

- The middle text, the text created by the first encryption or the first decryption, M, should be same

$$M = E_{K1}(P) \qquad M = D_{K2}(C)$$

- Encrypt P using all possible values of K_1 and records all values obtained for M.
- Decrypt C using all possible values of K_2 and records all values obtained for M.
- Create two tables sorted by M values.
- Now compares the values for M until we finds those pairs of K_1 & K_2 for which the value of M is same in both tables.

Meet-in-the-middle attack

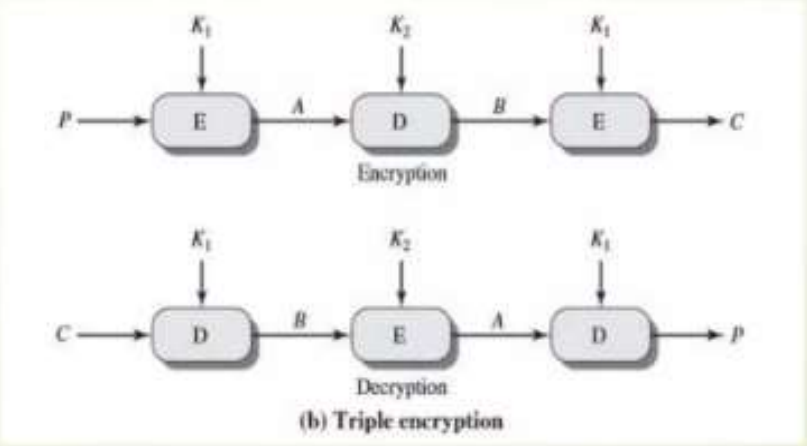


- Instead of using 2^{112} key search tests, we have to use 2^{56} key search tests two times.
- Moving from a Single DES to Double DES, we have to increased the strength from 2^{56} to 2^{57}.

Triple DES with 2-key

Triple DES with 2-key

- Use three stages of DES for encryption and decryption.
- The 1st, 3rd stage use K_1 key and 2nd stage use K_2 key.
- To make triple DES compatible with single DES, the middle stage uses decryption in the encryption side and encryption in the decryption side.
- It's much stronger than double DES.



(b) Triple encryption

Triple DES with 2-key

- The function follows an encrypt-decrypt-encrypt (EDE) sequence.

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, C)))$$

- By the use of triple DES with 2-key encryption, it raises the cost of meet-in-the-middle attack to 2^{112}.
- It has the drawback of requiring a key length of $56 \times 3 = 168$bits which may be somewhat unwieldy.

Triple DES with 3-key

Triple DES with 3-key

- Although the attacks just described appear impractical, anyone using two-key 3DES may feel some concern.
- Thus, many researches now feel that 3-key 3DES is the preferred alternative.
- Use three stages of DES for encryption and decryption with three different keys.
- 3-key 3DES has an effective key length of 168 bits and is defined as,

$$C = E(K_3, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_3, C)))$$

Triple DES with 3-key