

# Cryptography

## ECE5632 - Spring 2026

### Lecture 4A

**Dr. Farah Raad**



# Lecture Topic

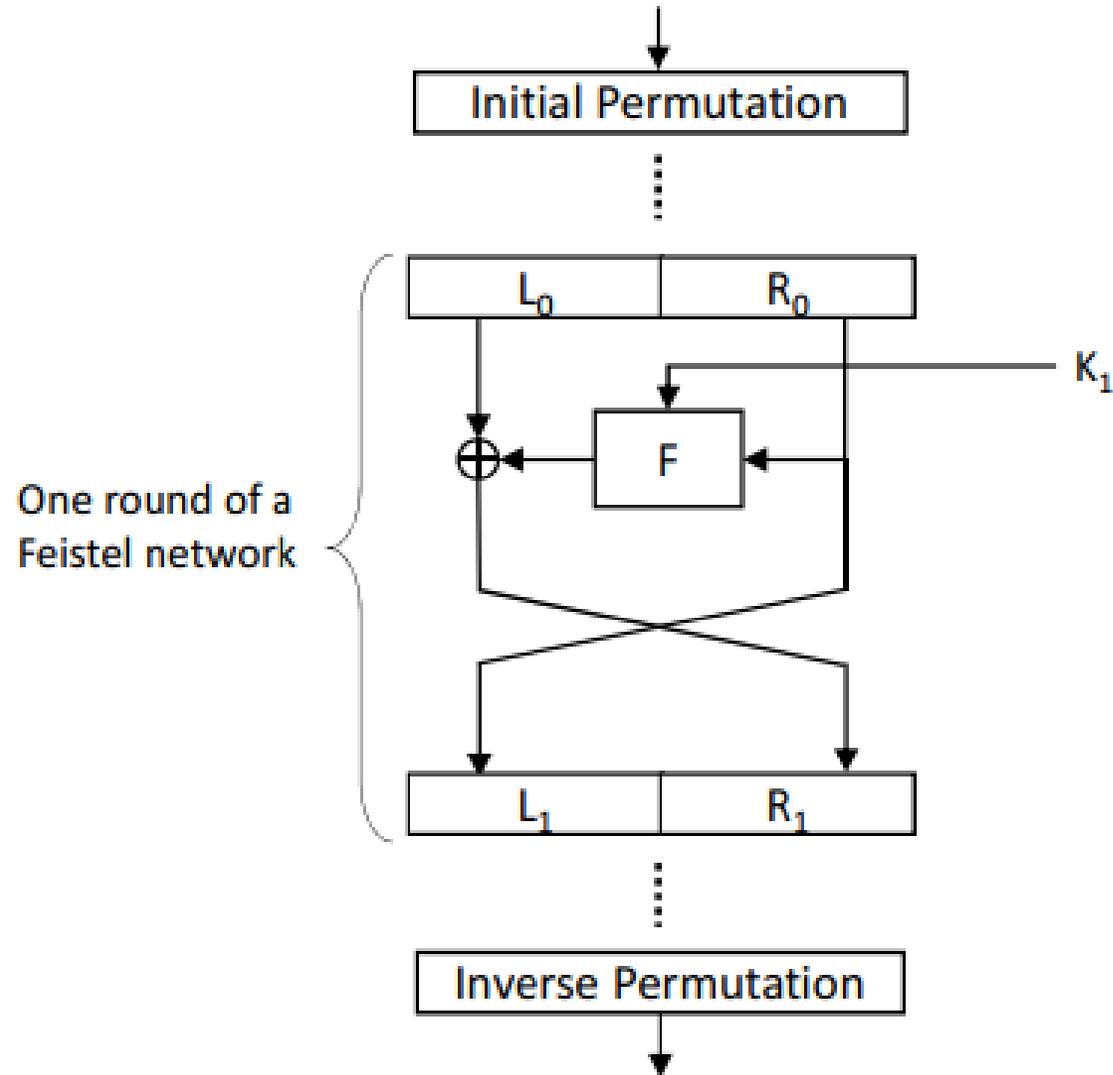
# DES

# Relation between DES and SDES

	SDES	DES
Block size	8 bits	64 bits
Key size	10 bits	56 bits
Sub key size	8 bits	48 bit
Function F	Acts on 4 bits	Acts on 32 bits
S-boxes	2	8
S-box size	4 x 4	4 x 16
rounds	2	16

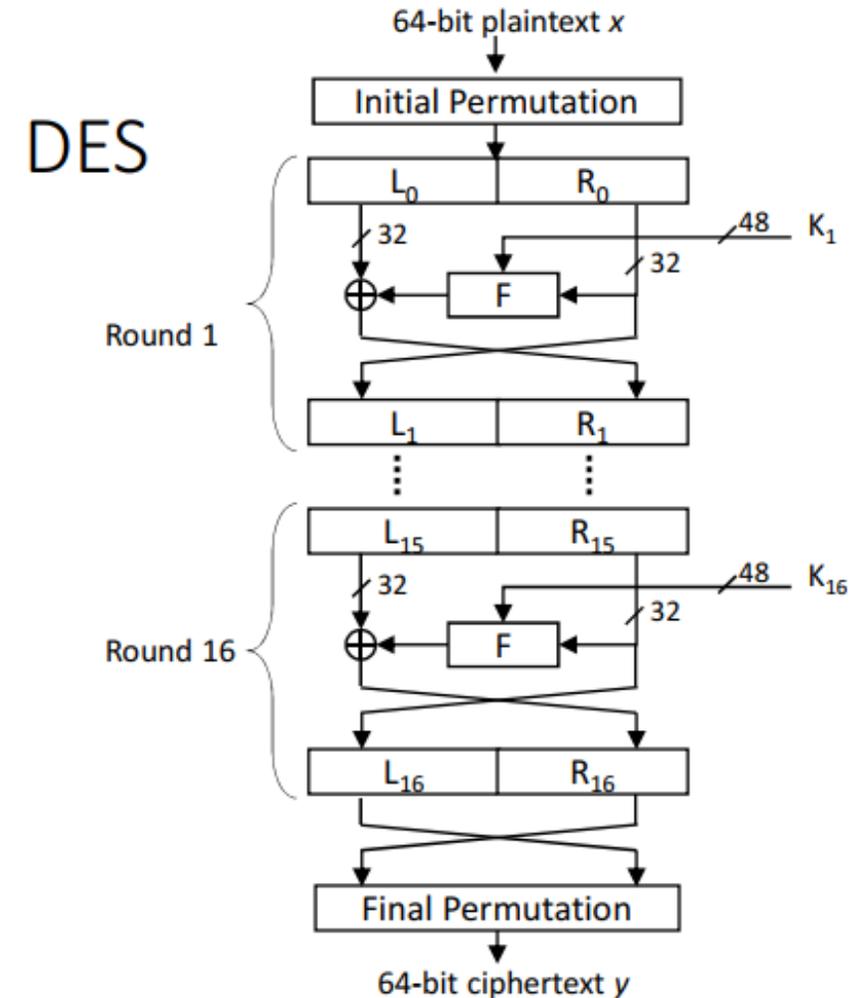
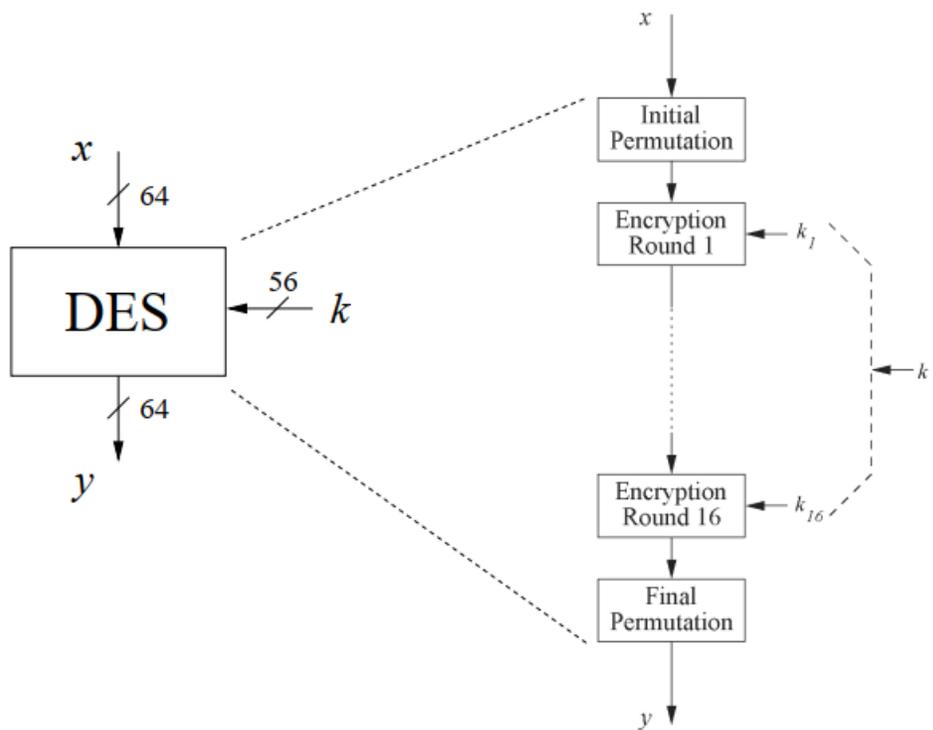


# Feistel Network

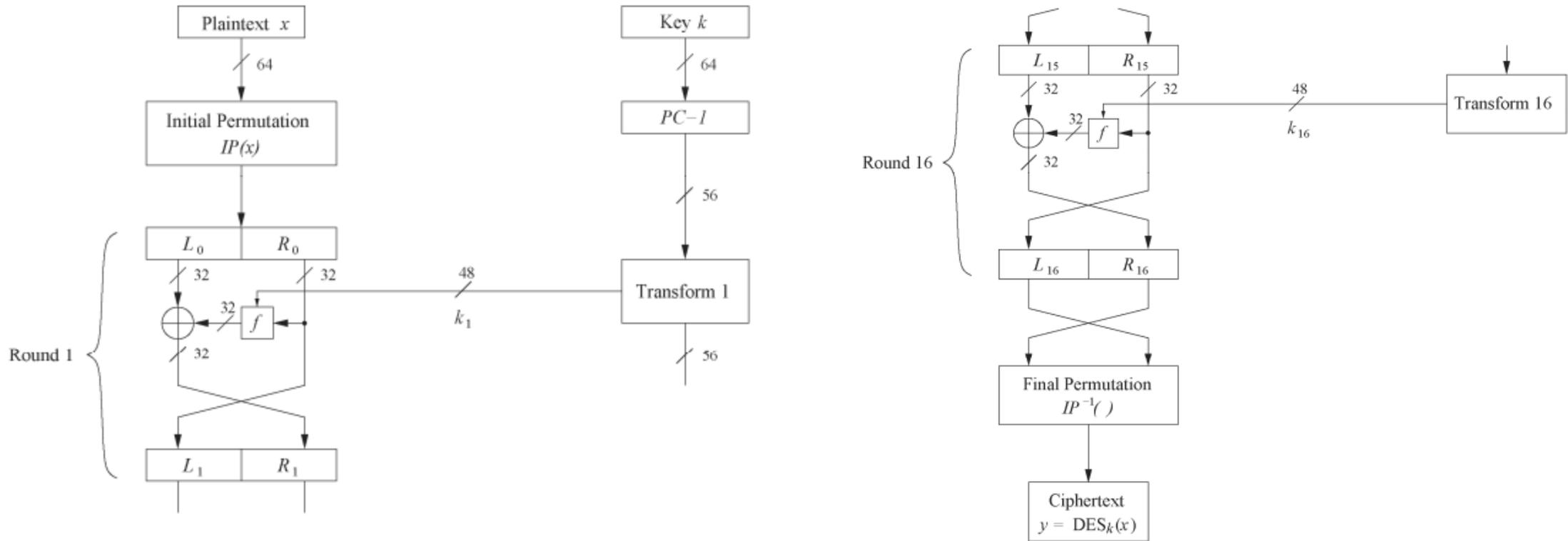


# DES Algorithm

- Encrypts blocks of size 64 bits.
- Uses a key of size 56 bits.
  - Symmetric cipher: uses same key for encryption and decryption
  - Uses 16 rounds which all perform the identical operation
  - Different subkey in each round derived from main key



# The DES Feistel Network



- Bitwise initial permutation, then 16 rounds
  1. Plaintext is split into 32-bit halves  $L_i$  and  $R_i$
  2.  $R_i$  is fed into the function  $f$ , the output of which is then XORed with  $L_i$
  3. Left and right half are swapped
- L and R swapped again at the end of the cipher, i.e., after round 16 followed by a final permutation
- Advantage: encryption and decryption differ only in key schedule

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

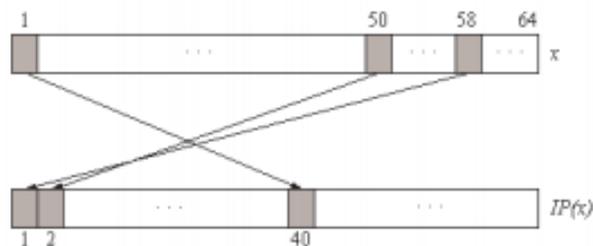


# Initial and Final Permutation

- Bitwise Permutations.
- Inverse operations.
- Described by tables  $IP$  and  $IP^{-1}$ .

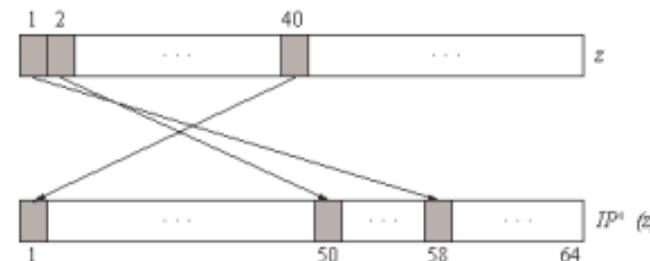
Initial Permutation

$IP$							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



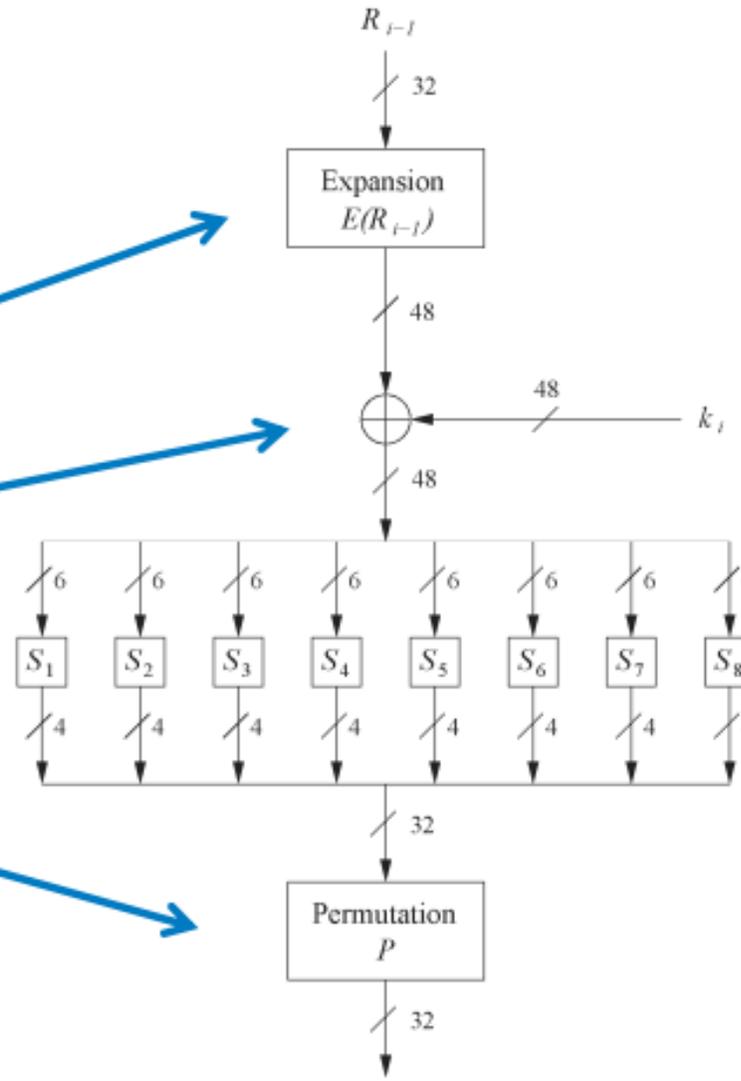
Final Permutation

$IP^{-1}$							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



# The f-Function

- main operation of DES
- $f$ -Function inputs:  
 $R_{i-1}$  and round key  $k_i$
- 4 Steps:
  1. Expansion  $E$
  2. XOR with round key
  3. S-box substitution
  4. Permutation

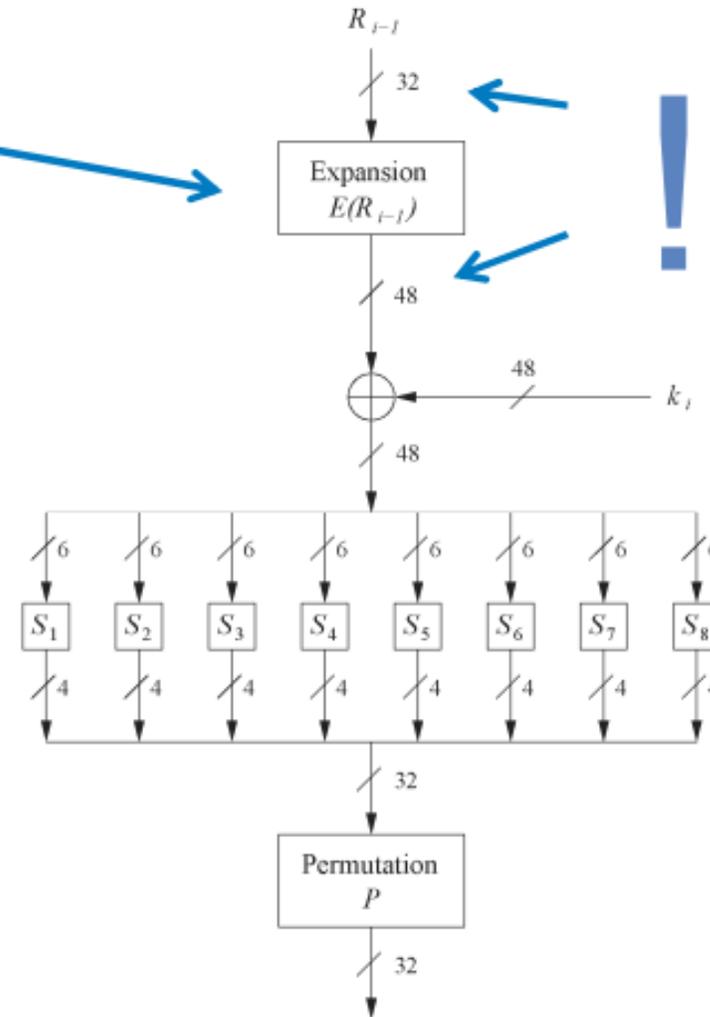
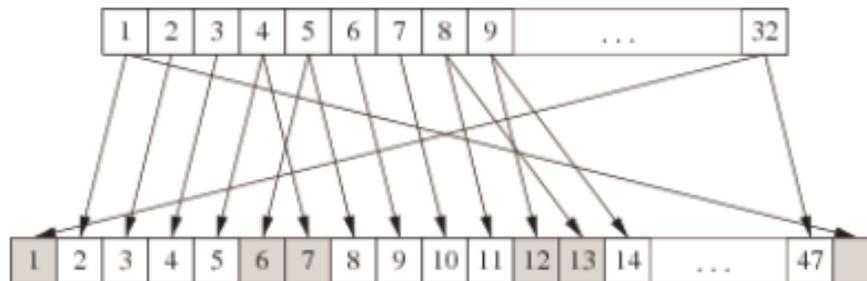


# The Expansion Function E

## 1. Expansion E

- main purpose:  
increases diffusion

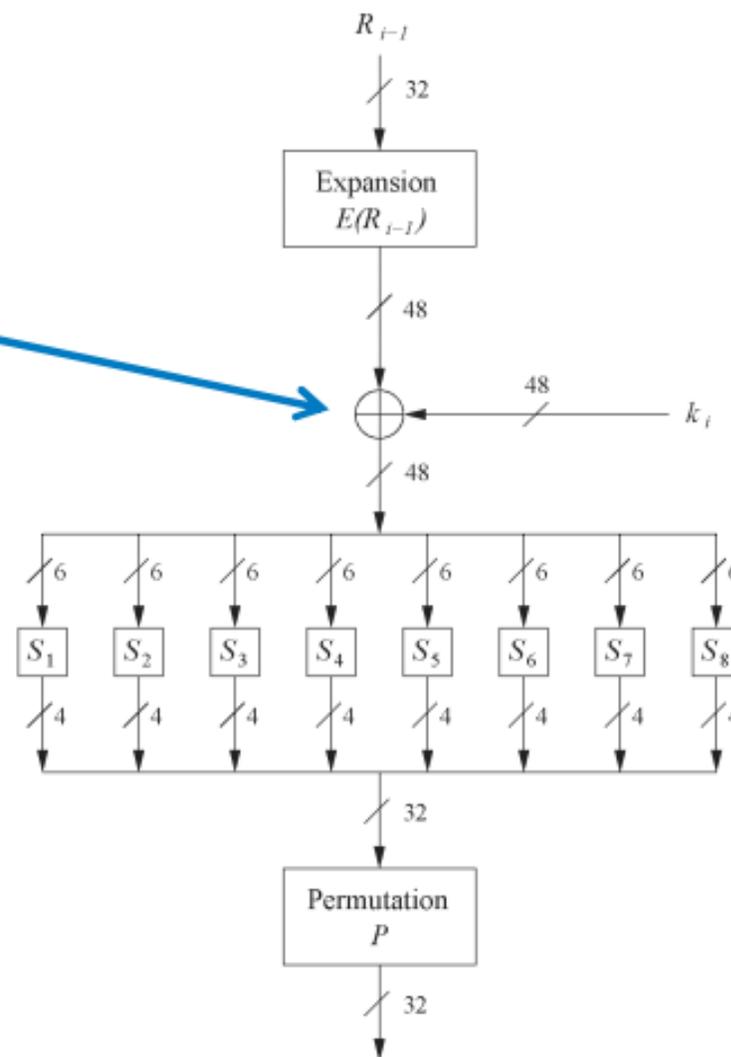
$E$	
32	1 2 3 4 5
4	5 6 7 8 9
8	9 10 11 12 13
12	13 14 15 16 17
16	17 18 19 20 21
20	21 22 23 24 25
24	25 26 27 28 29
28	29 30 31 32 1



# Add Round Key

## 2. XOR Round Key

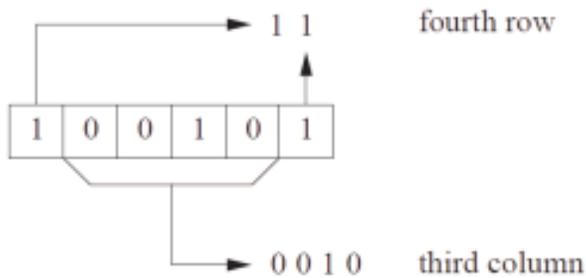
- Bitwise XOR of the round key and the output of the expansion function  $E$
- Round keys are derived from the main key in the DES keyschedule (in a few slides)



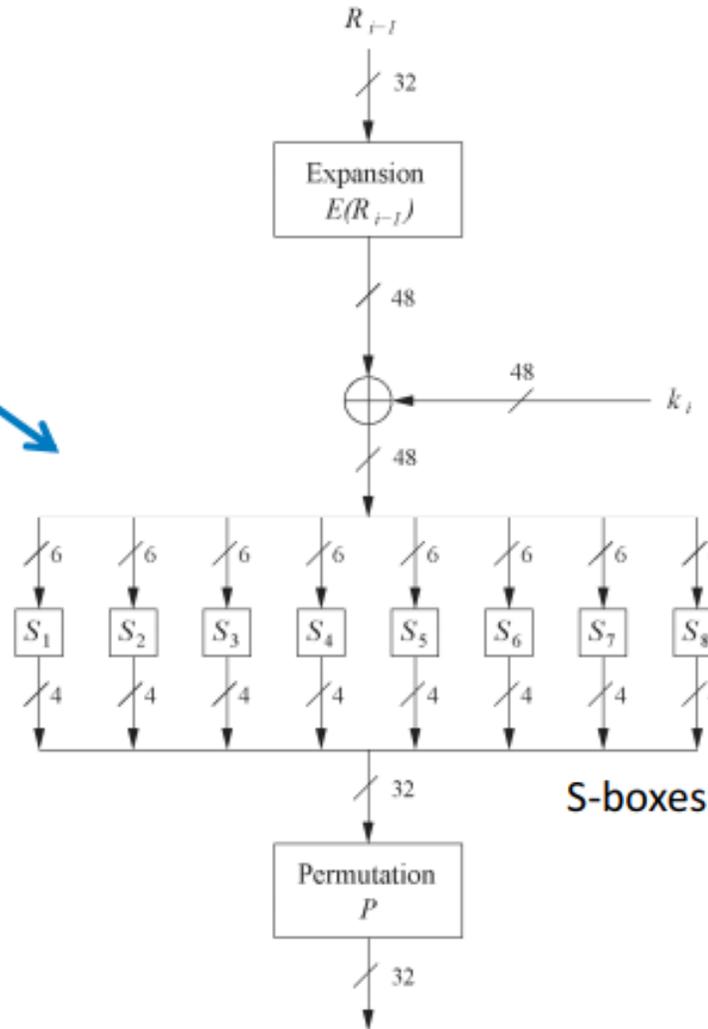
# The DES S-Boxes

## 3. S-Box substitution

- Eight substitution tables.
- 6 bits of input, 4 bits of output.
- Non-linear and resistant to differential cryptanalysis.
- Crucial element for DES security!
- Find all S-Box tables and S-Box design criteria in *Understanding Cryptography* Chapter 3.



$S_1$	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	01	10	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



S-boxes add nonlinearity to the cipher:

$$\text{i.e., } S(a) \oplus S(b) \neq S(a \oplus b).$$

Nonlinearity prevents attackers from express the DES i/p and o/p with a system of linear equations where the key bits are the unknowns.

# The DES S-Boxes

S-box  $S_1$

$S_1$	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	01	10	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

S-box  $S_2$

$S_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S-box  $S_3$

$S_3$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

S-box  $S_4$

$S_4$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

S-box  $S_5$

$S_5$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

S-box  $S_6$

$S_6$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

S-box  $S_7$

$S_7$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

S-box  $S_8$

$S_8$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
3	02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

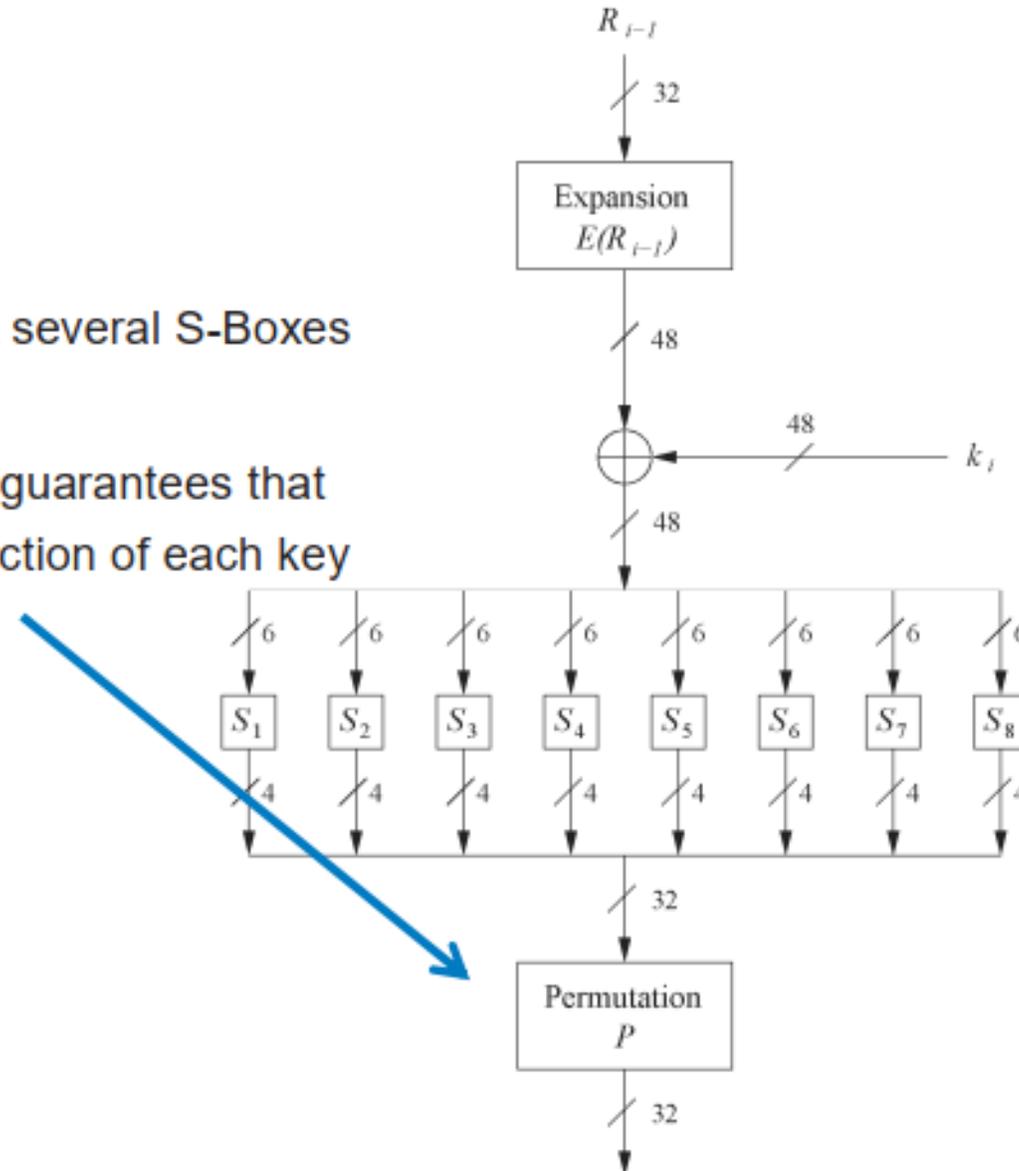


# The Permutation P

## 4. Permutation P

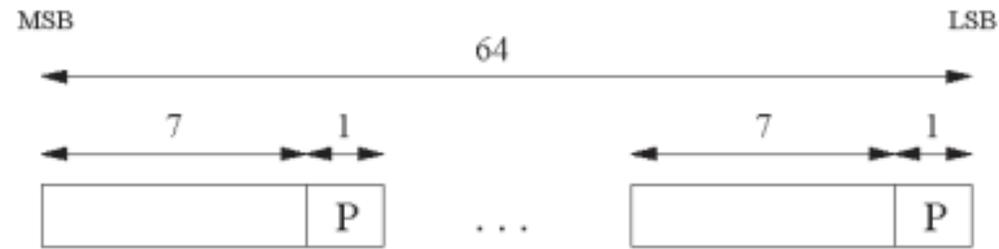
- Bitwise permutation.
- Introduces diffusion.
- Output bits of one S-Box effect several S-Boxes in next round
- Diffusion by E, S-Boxes and P guarantees that after Round 5 every bit is a function of each key bit and each plaintext bit.

$P$							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25



# Key Schedule

- Derives 16 round keys (or *subkeys*)  $k_i$  of 48 bits each from the original 56 bit key.
- The input key size of the DES is 64 bit. **56 bit key** and 8 bit parity:



P = parity bit

- **Parity bits are removed** in a first **permuted choice  $PC-1$** :  
(note that the bits 8, 16, 24, 32, 40, 48, 56 and 64 are not used at all)

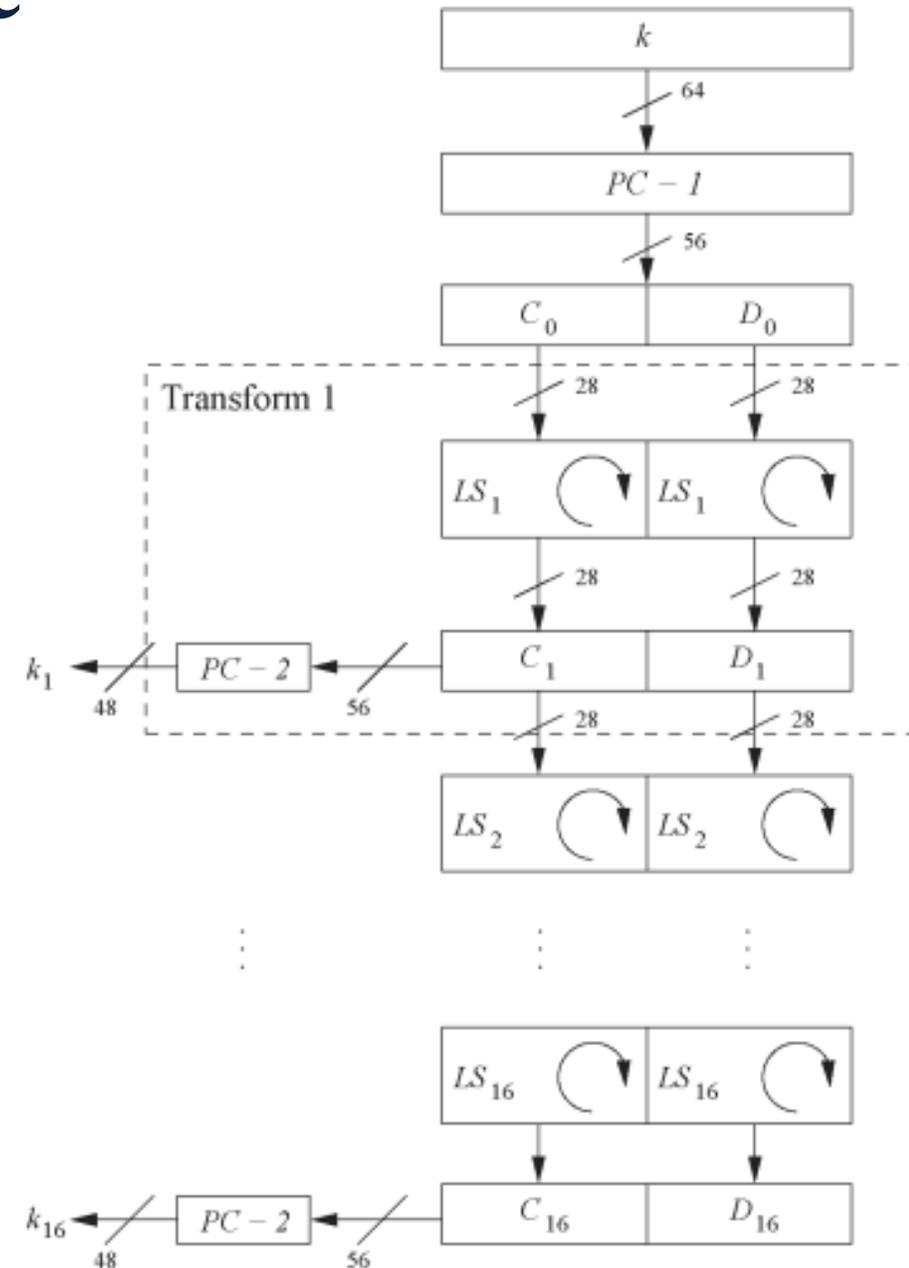
$PC - 1$							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

# Key Schedule

- Split key into 28-bit halves  $C_0$  and  $D_0$ .
- In rounds  $i = 1, 2, 9, 16$ , the two halves are each rotated left by **one bit**.
- In **all other rounds** where the two halves are each rotated left by **two bits**.
- In each round  $i$  permuted choice **PC-2** selects a permuted subset of 48 bits of  $C_i$  and  $D_i$  as round key  $k_i$ , i.e. **each  $k_i$  is a permutation of  $k$ !**

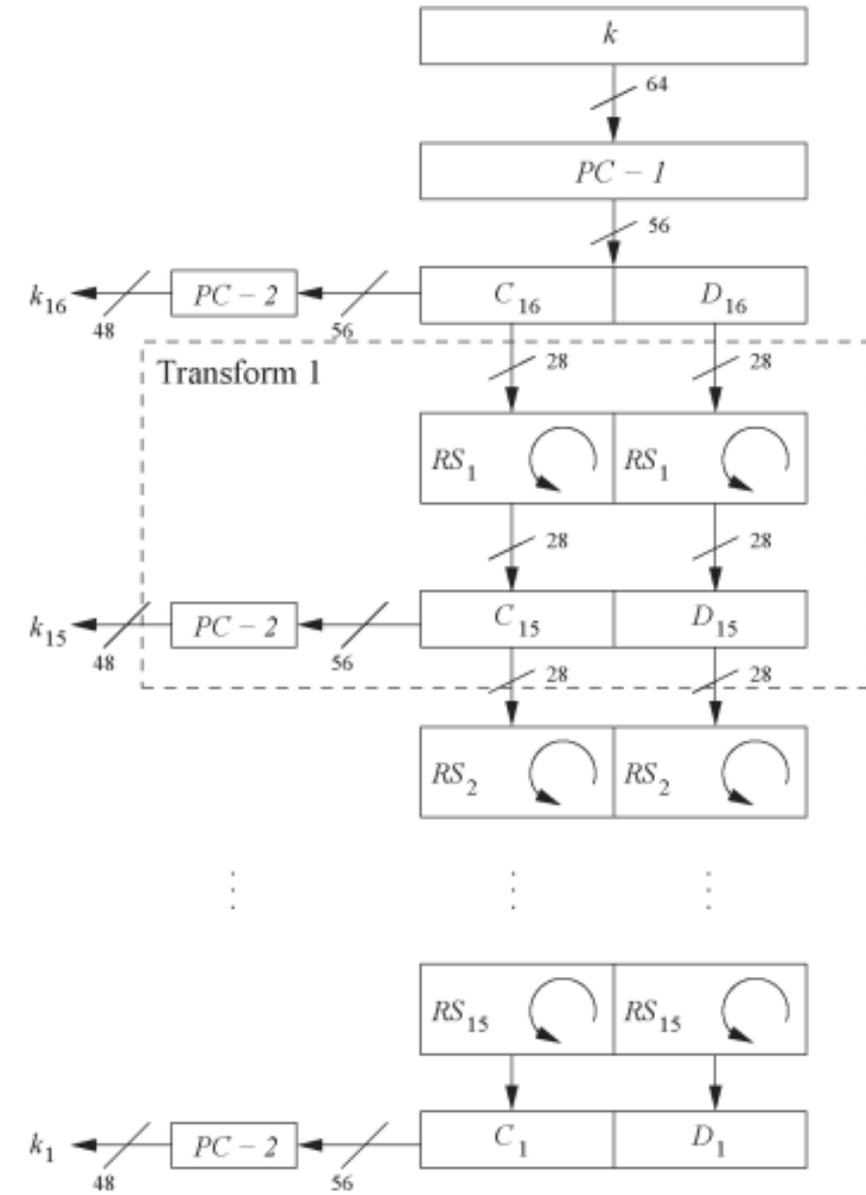
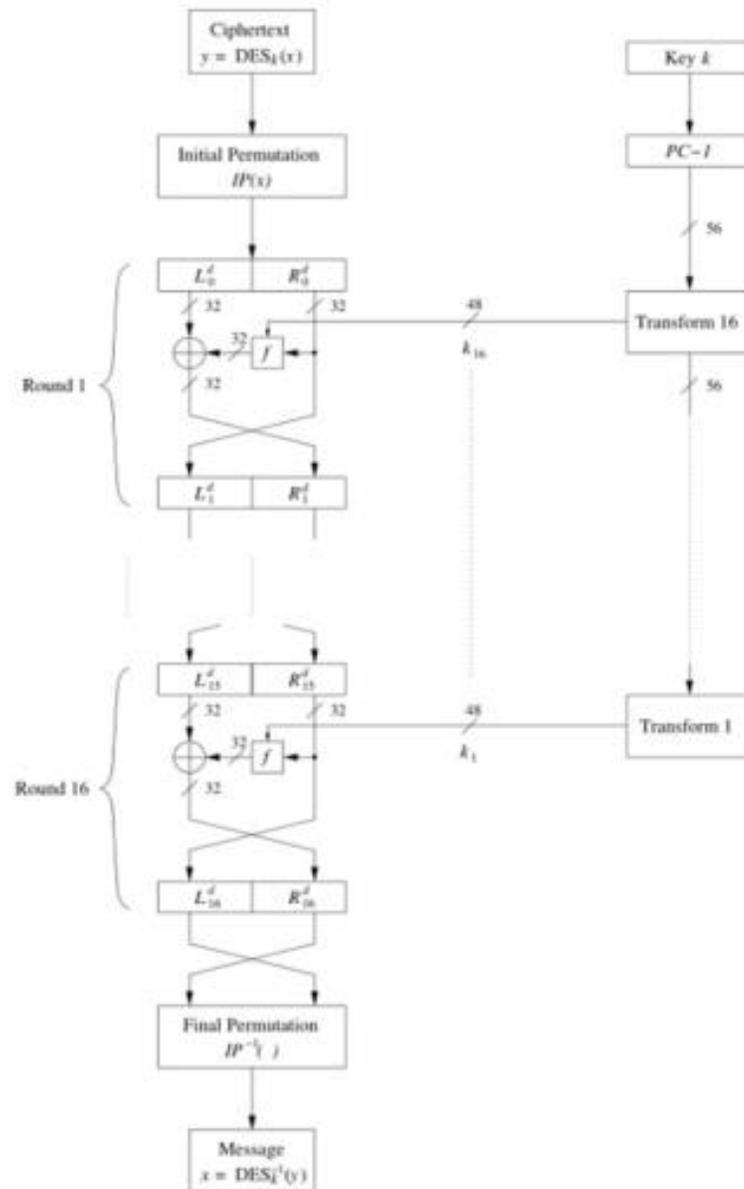
PC-2							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

- Note:** The total number of rotations:  
 $4 \times 1 + 12 \times 2 = 28 \Rightarrow D_0 = D_{16}$  and  $C_0 = C_{16}$ !



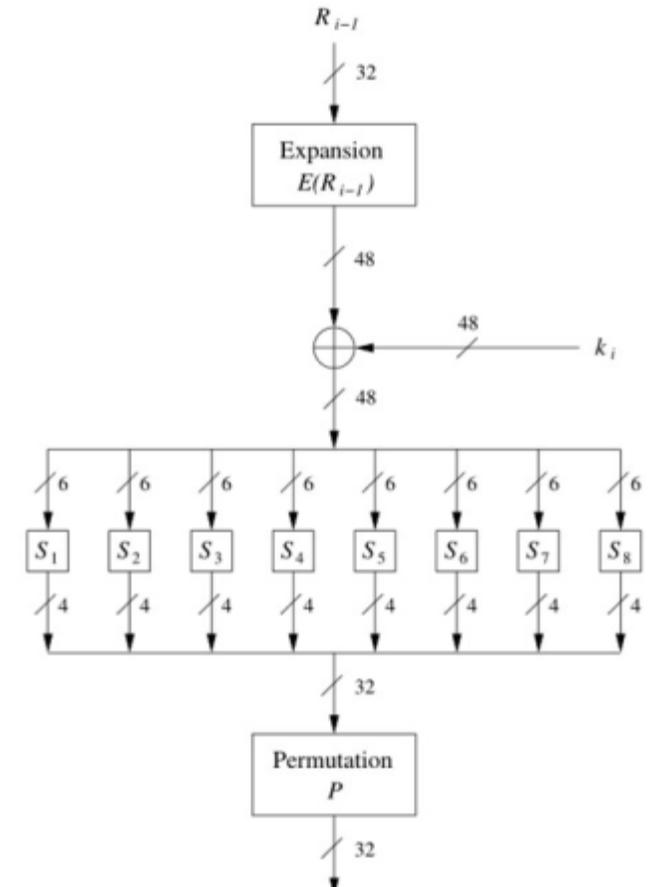
# Decryption

Same function as encryption.  
Only key schedule is reversed.



# Avalanche Effect

- The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.



# Security of DES

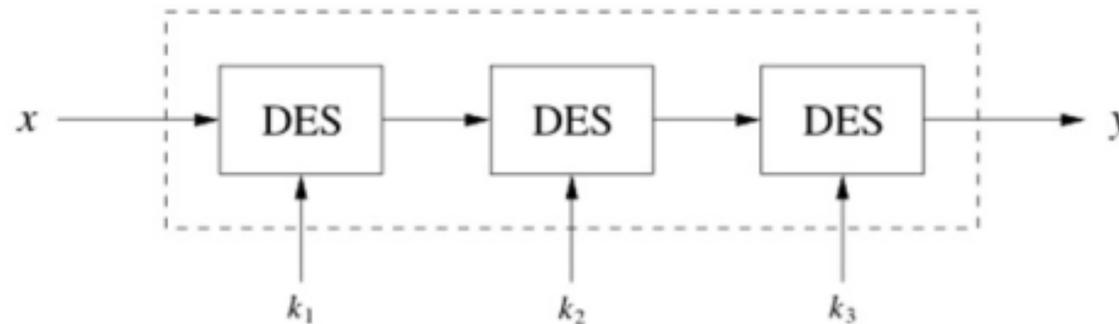
- **After proposal of DES two major criticisms arose:**
  1. Key space is too small (256 keys)
  2. S-box design criteria have been kept secret: Are there any hidden analytical attacks (*backdoors*).
- **Analytical attacks:**
  - Differential cryptanalysis and linear cryptanalysis attacks against DES were proposed only in theory.
- **Brute-force attacks:**
  - Can be easily broken in practice by brute-force attacks, given a special-purpose key-search machine.
  - Examples of actual special-purpose key-search machines include; Deep Crack, and COPACOBANA.



# Triple DES (TDES / 3DES)

- Triple encryption using DES is often used in practice to extend the effective key length of DES to 112.
- **Advantage:**
  - ✓ choosing  $k_1=k_2=k_3$  performs single DES encryption.
  - ✓ No practical attack known today.
  - ✓ Used in many legacy applications, i.e., in banking systems.

$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$





# Thank You!

**See You next Lectures!!**  
**Any Question?**

**THE FIRST BRITISH HIGHER EDUCATION IN EGYPT**

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt

**Tel:** +202383711146 **Fax:** +20238371543 **Postal code:** 12451

**Email:** [info@msa.eun.eg](mailto:info@msa.eun.eg) **Hotline:** 16672 **Website:** [www.msa.edu.eg](http://www.msa.edu.eg)