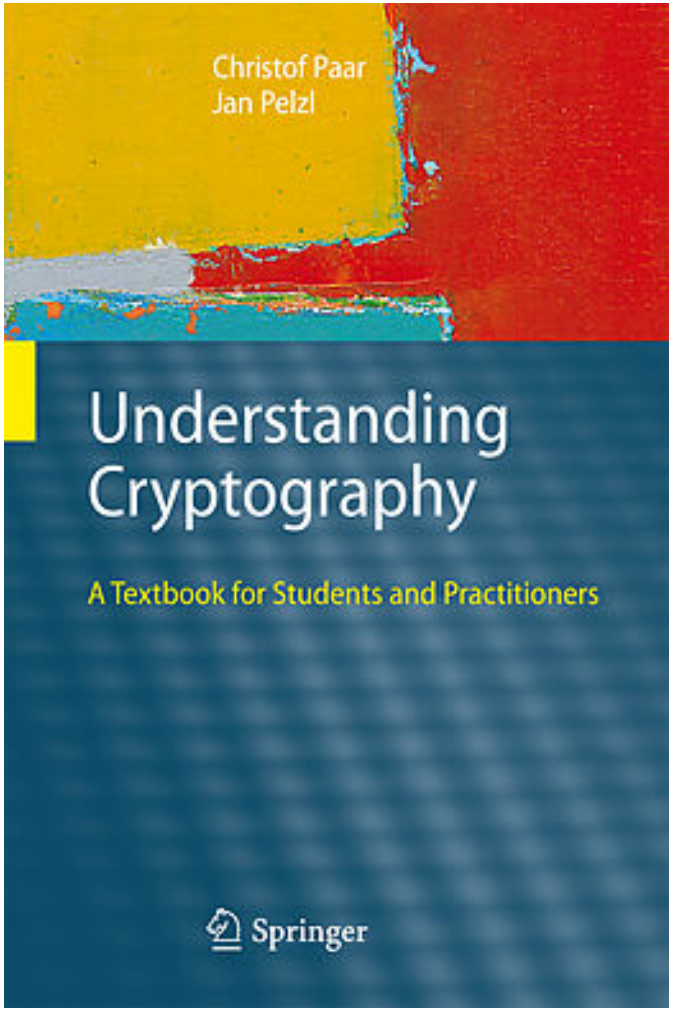
HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

The Data Encryption Standard (DES) and Alternatives

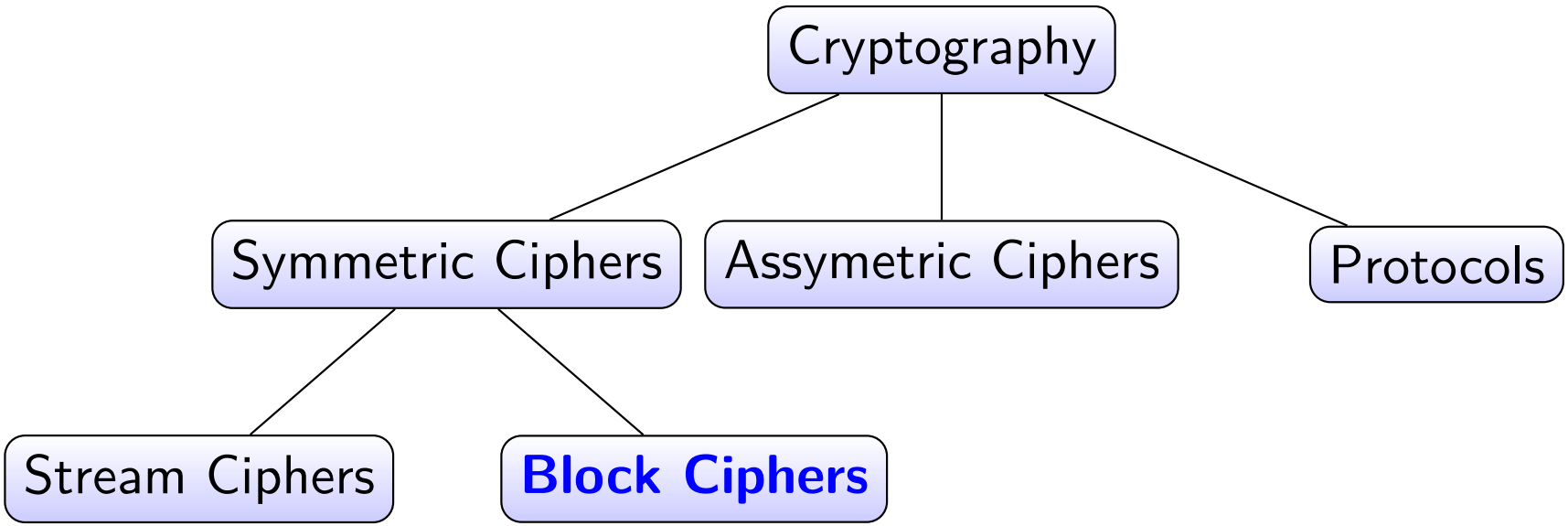
Textbook

https://www.crypto-textbook.com



Outline

Cryptography



Introduction to DES

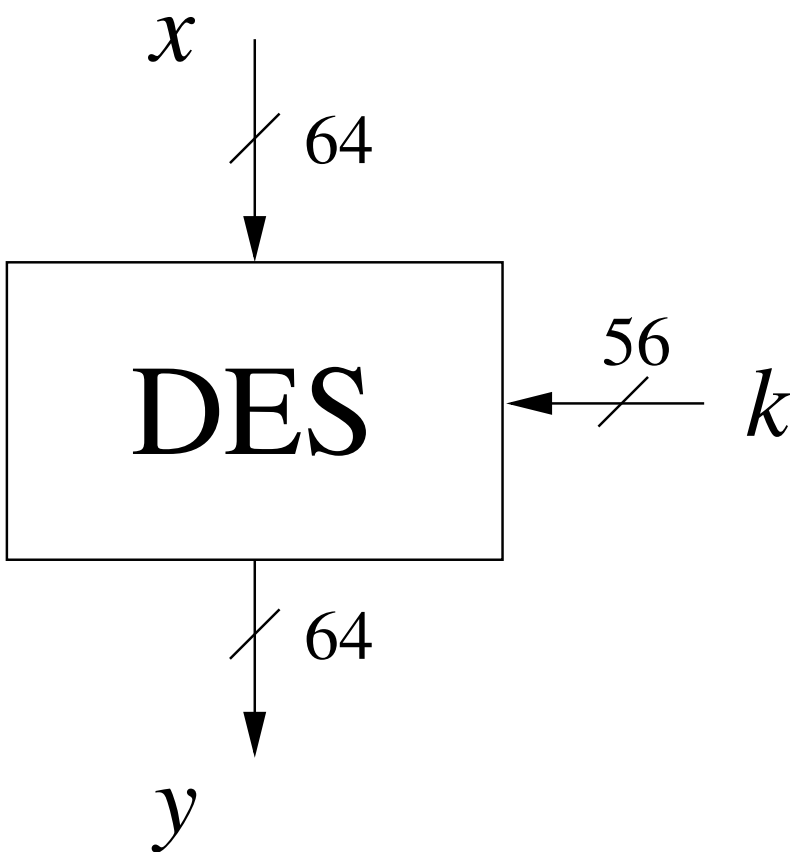
- Proposed by IBM in 1974 based on the cipher *Lucifer*.

  Lucifer is a Feistel cipher which encrypts blocks of 64 bits using a key size of 128 bits.

- It seems certain that the National Security Agency (NSA) influenced changes to the cipher, which was rechristened DES.
- One of the changes that occurred was that DES is specifically designed to withstand differential cryptanalysis, an attack not known to the public until 1990.

Introduction to DES 2

- Allegedly, the NSA also convinced IBM to reduce the Lucifer key length of 128 bit to 56 bit, which made the cipher much more vulnerable to brute-force attacks.
- Some people conjectured that the NSA would be able to search through a key space of 2^{56}, thus breaking it by brute-force.
- Despite of all the criticism and concerns, in 1977 the NBS finally released all specifications of the modified IBM cipher as the Data Encryption Standard (FIPS PUB 46) to the public.



- Currently, DES is no longer secure due to the short key size.
- But 3DES is secure.

Principle of building block cipher

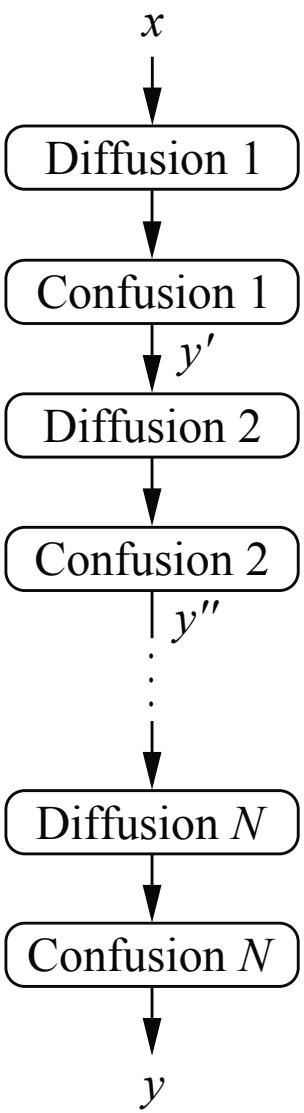
According to Claude Shannon

- **Confusion** is an encryption operation where the relationship between key and ciphertext is obscured.
- **Diffusion** is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext.

Example

Principle of diffusion of a block cipher

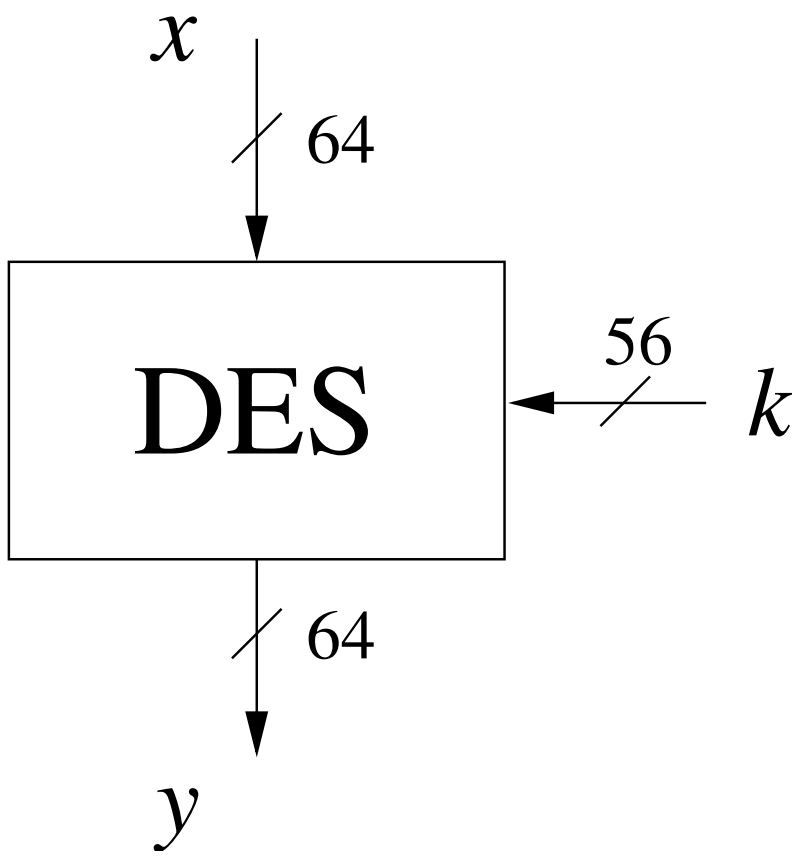
Principle of building block cipher



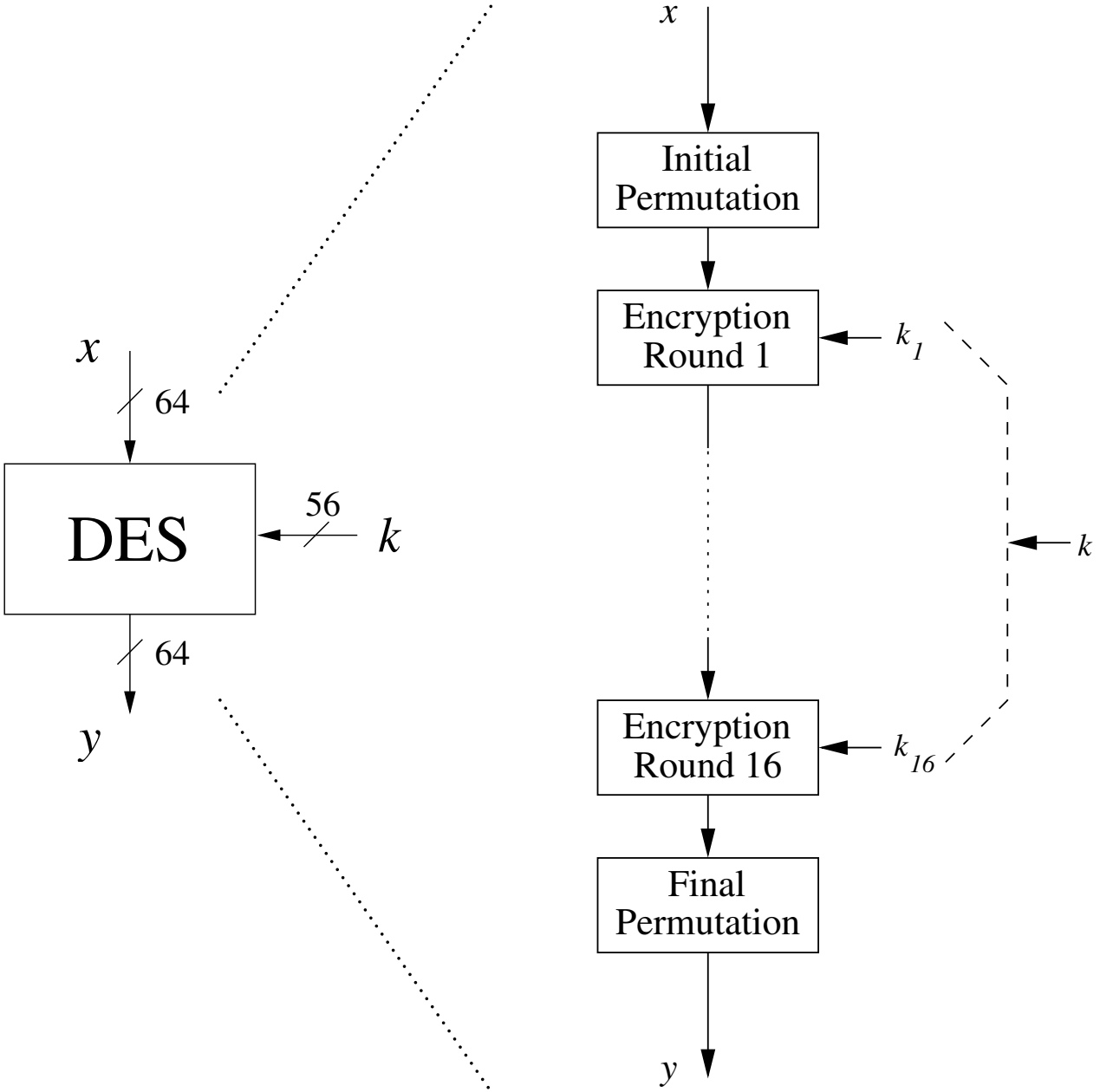
Principle of an N round product cipher, where each round performs a confusion and diffusion operation

Outline

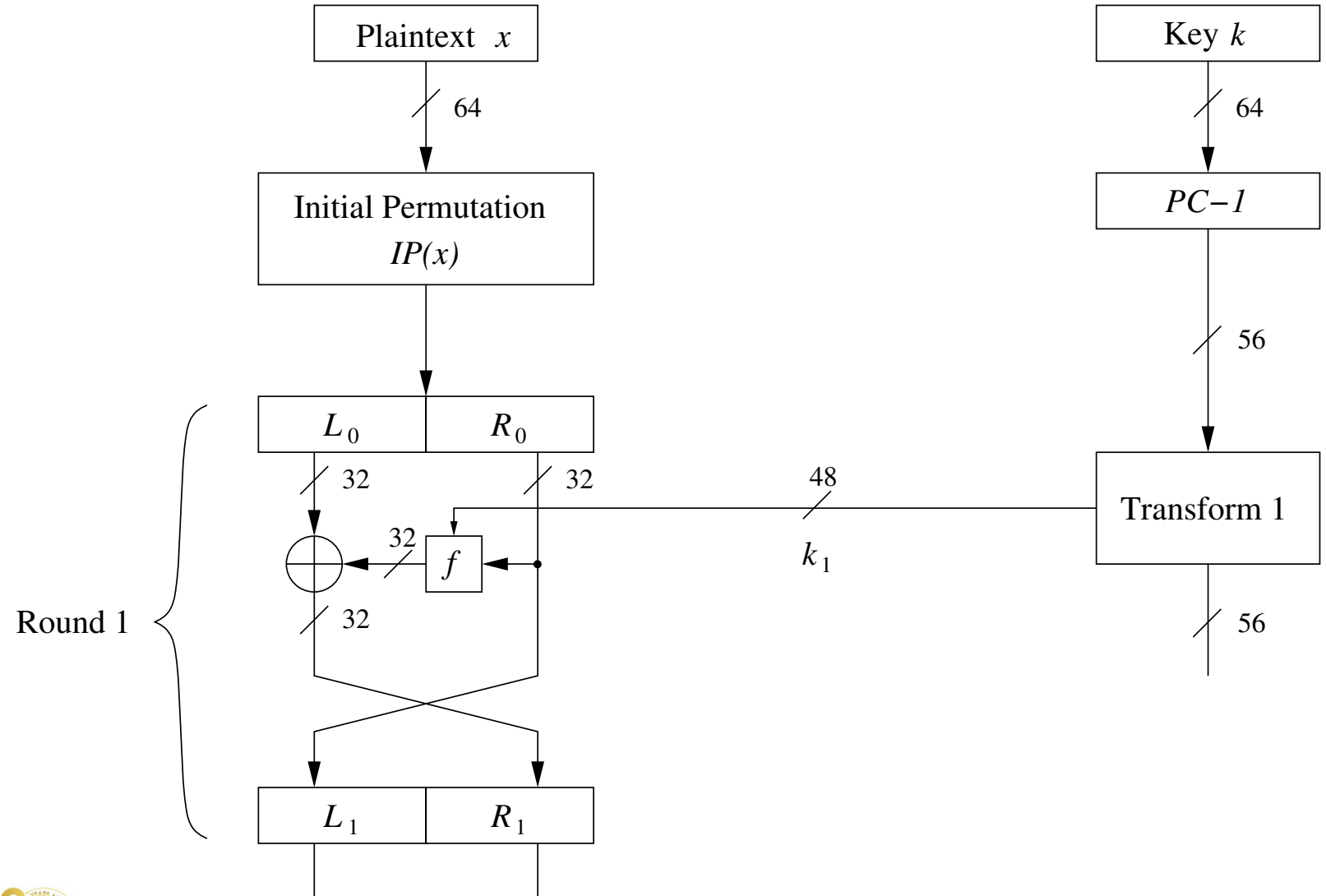
DES



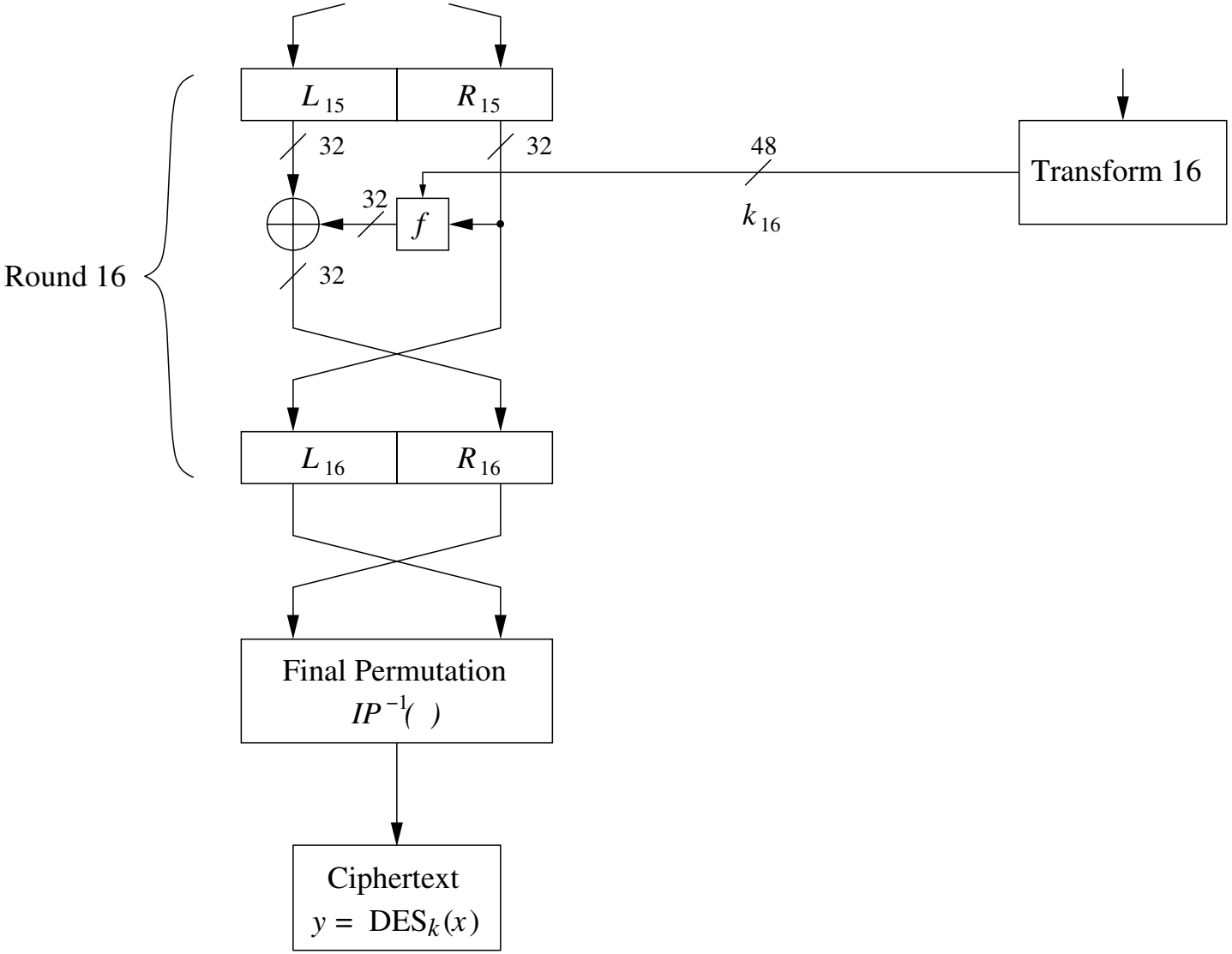
- The block size is 64 bits
- The key length is 56 bits.


x
64
DES
56
k
64
y
x
Initial Permutation
Encryption Round 1
k1
k
Encryption Round 16
k16
Final Permutation
y

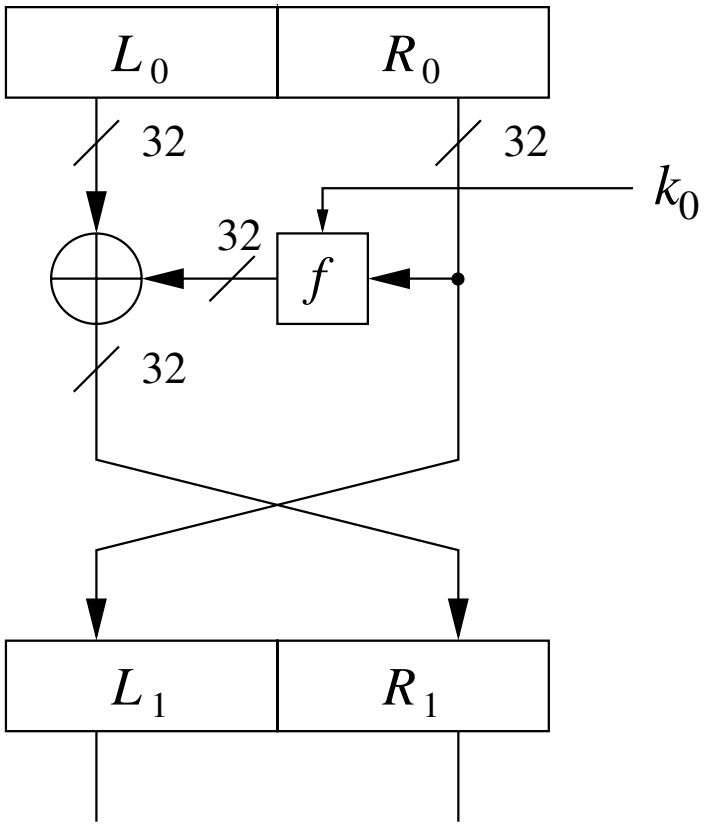
Feistel network: Round 1



Feistel network: Round 16



The Feistel structure of DES



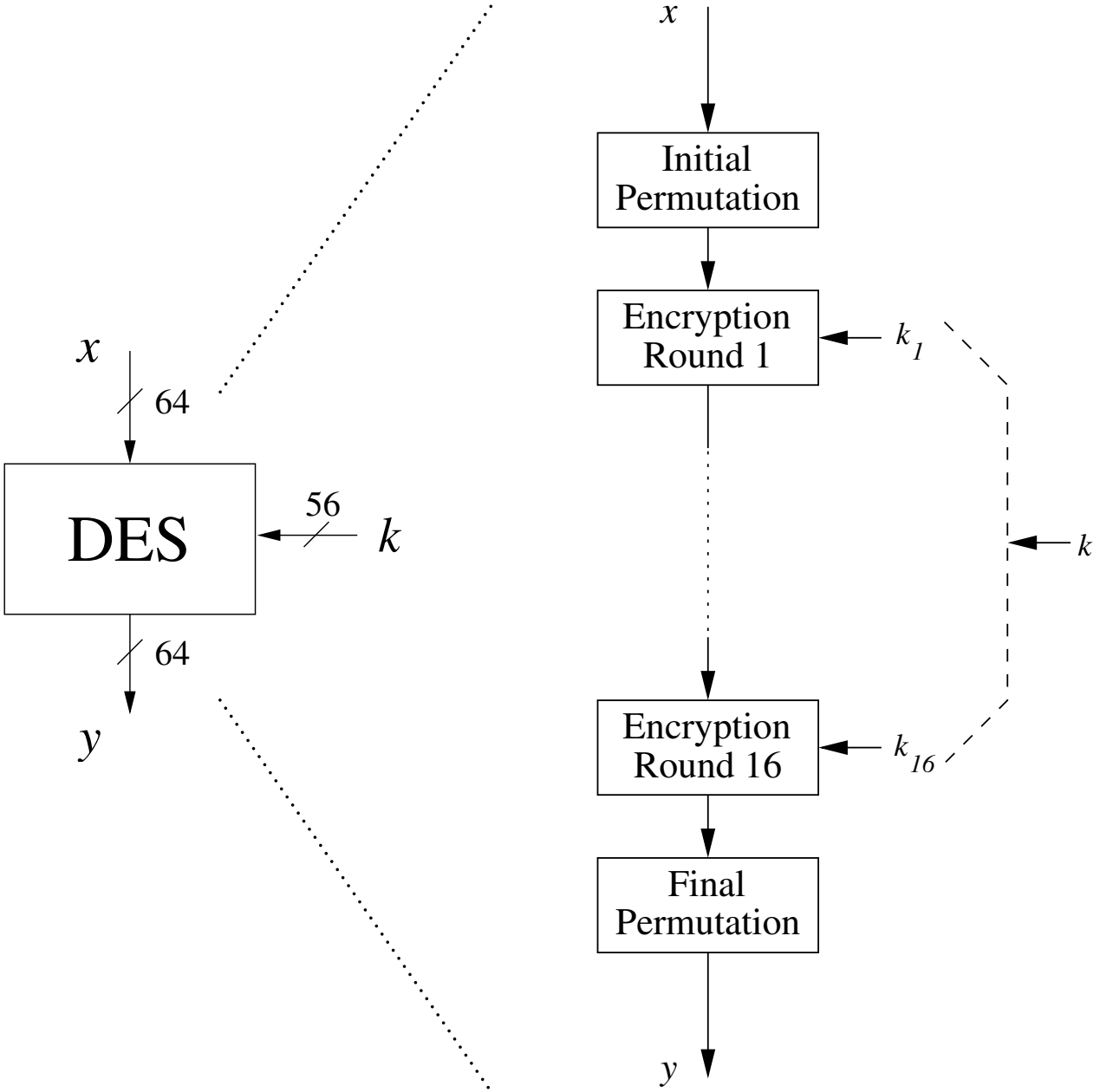
- In symbols:

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

- How to compute the inverses?

$$(L_i,\ R_i) \longrightarrow (L_{i-1},\ R_{i-1})$$

Outline


x
64
DES
56
k
64
y
x
Initial Permutation
Encryption Round 1
k1
k
Encryption Round 16
k16
Final Permutation
y

Initial and Final Permutation

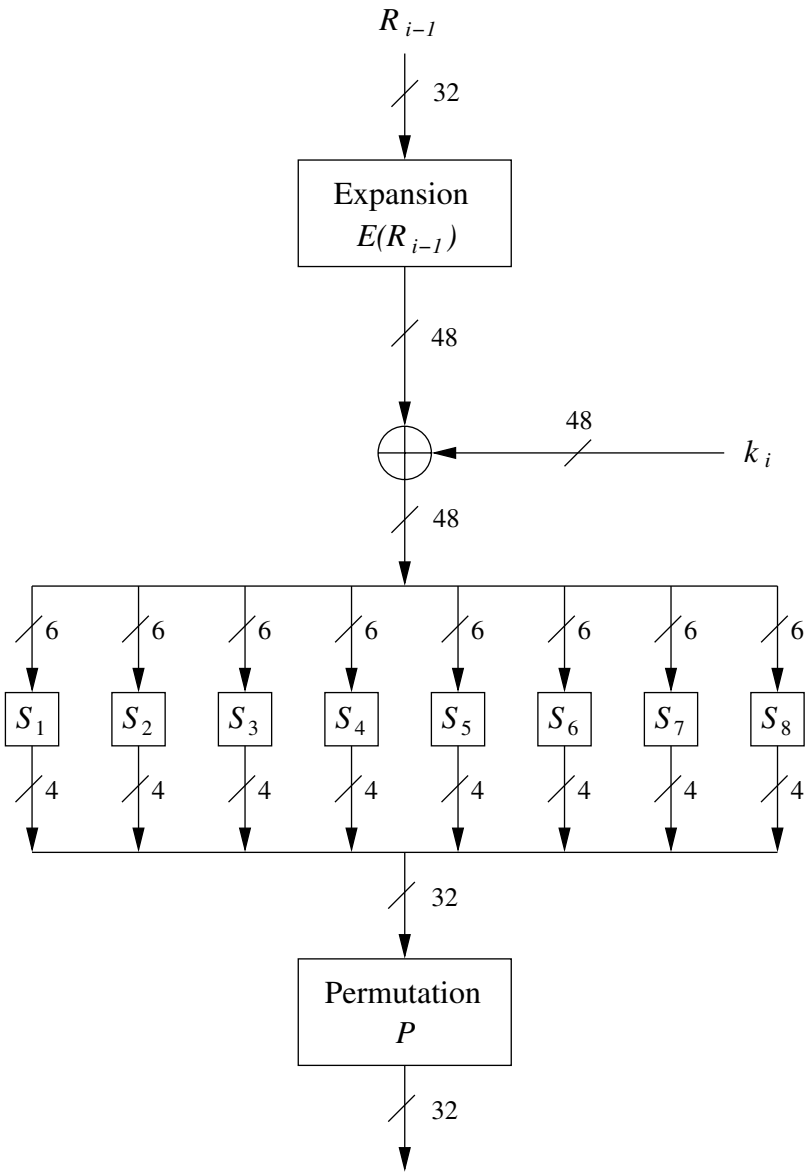
IP

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

IP^{-1}

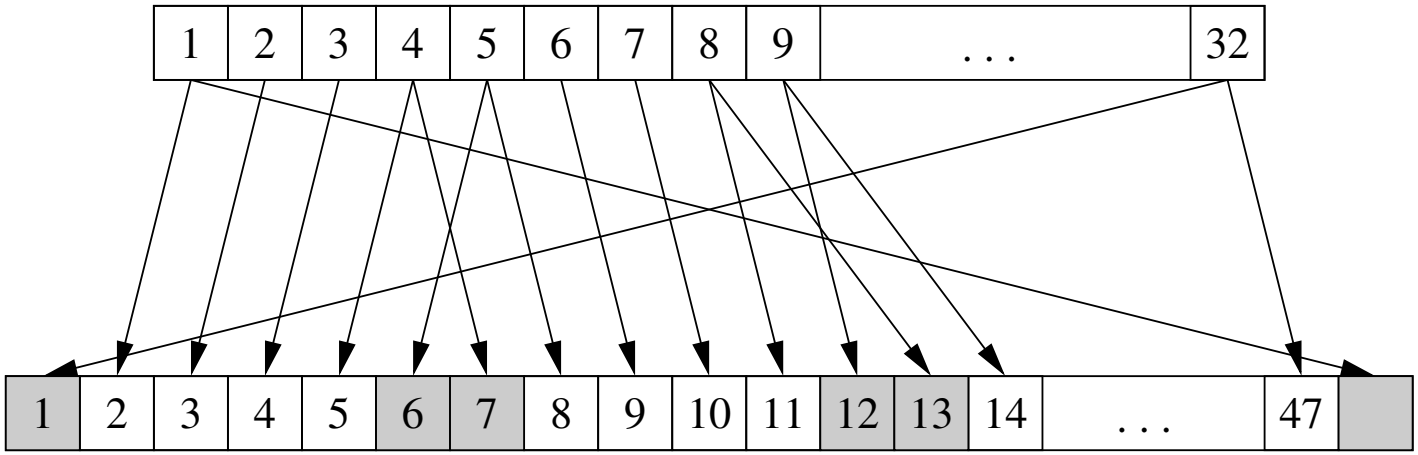
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

The f – function



- Expansion $E(R_{i+1})$
- XOR with current round key i
- substition boxes S-box
- P permutation

Expansion E



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

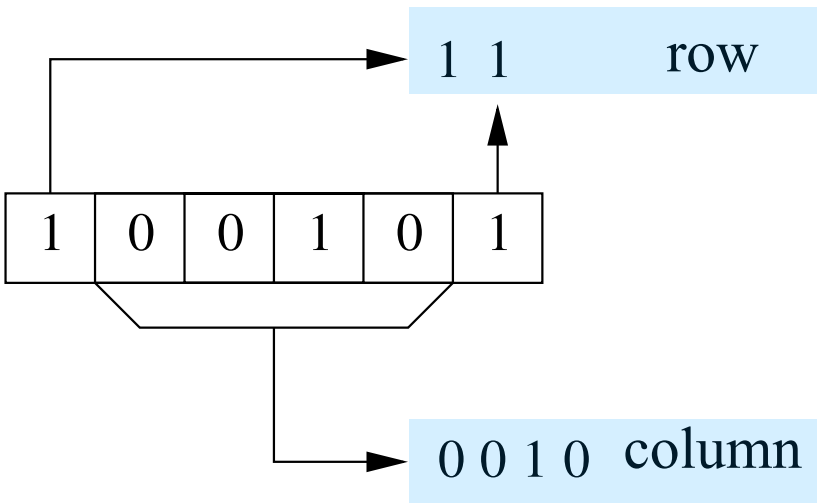
S-Box

- S-box is a lookup table that maps a 6-bit input to a 4-bit output.
- DES has 8 S-boxes that are nonlinear functions

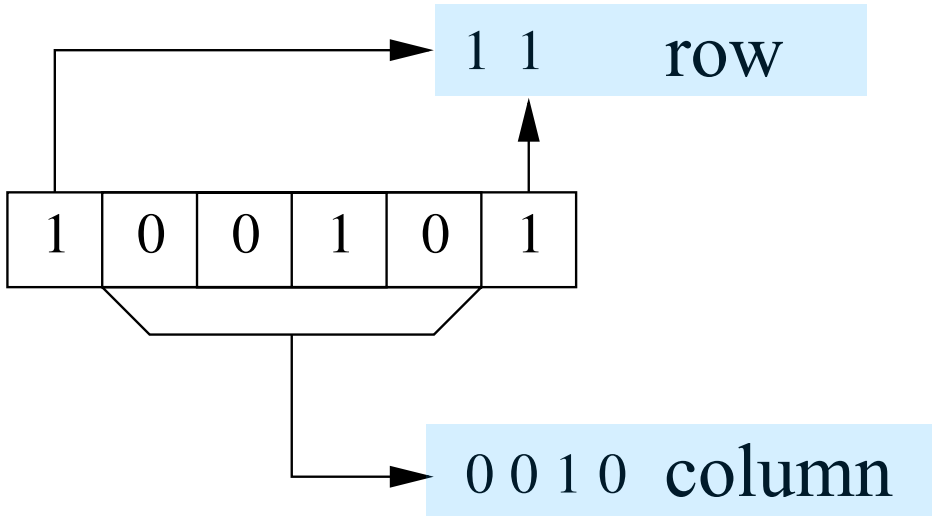
$$S(a) \oplus S(b) \neq S(a \oplus b).$$

(against differential cryptanalysis)

- The S-box is decrypted in a special way:



S-box



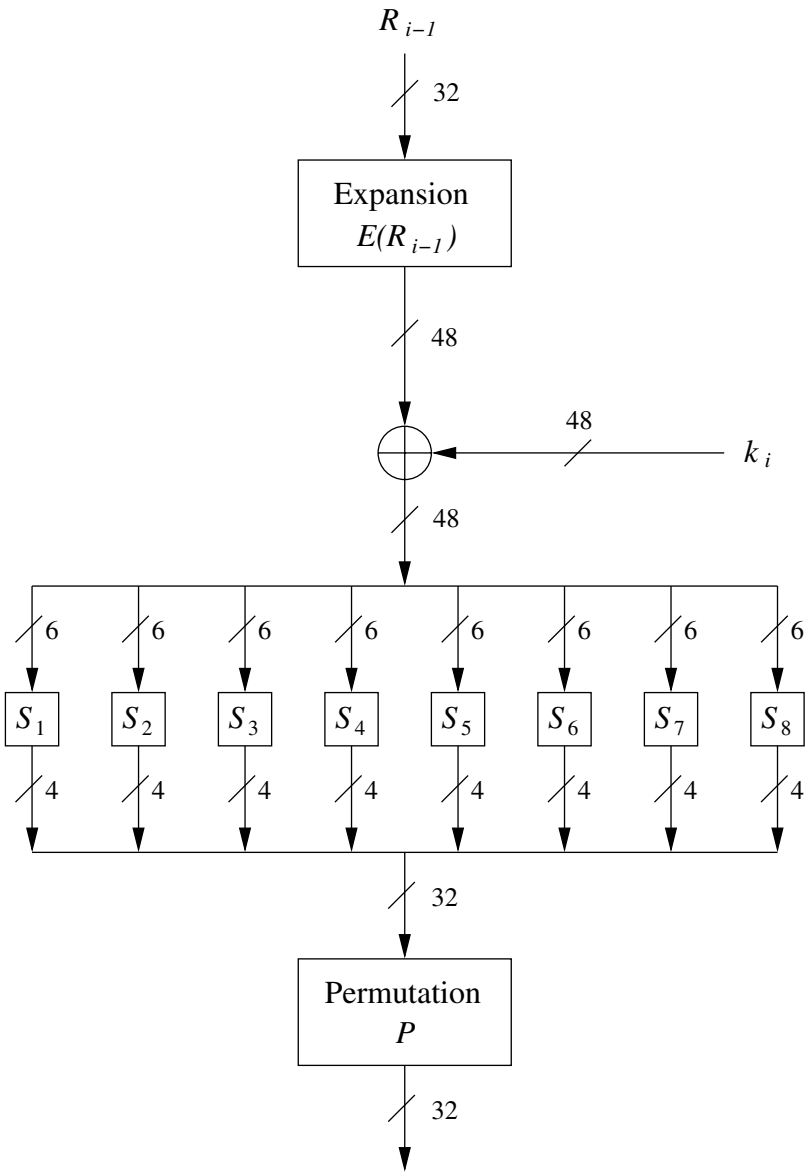
S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

P Permutation

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

Figure: The permutation P introduces diffusion because the four output bits of each S-box are permuted in such a way that they affect several different S-boxes in the following round.

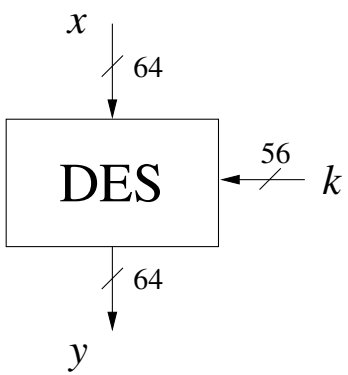
The f – function

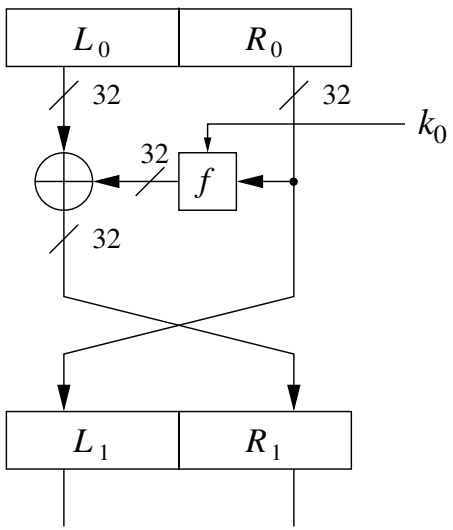


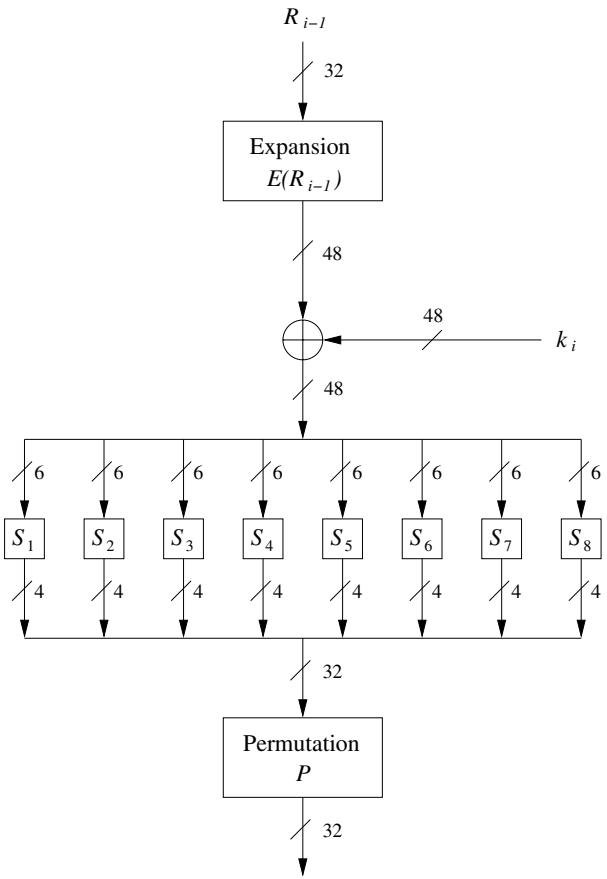
- Expansion $E(R_{i+1})$
- XOR with current round key i
- substition boxes S-box
- P permutation

Outline

Recall: Internal Structure of DES



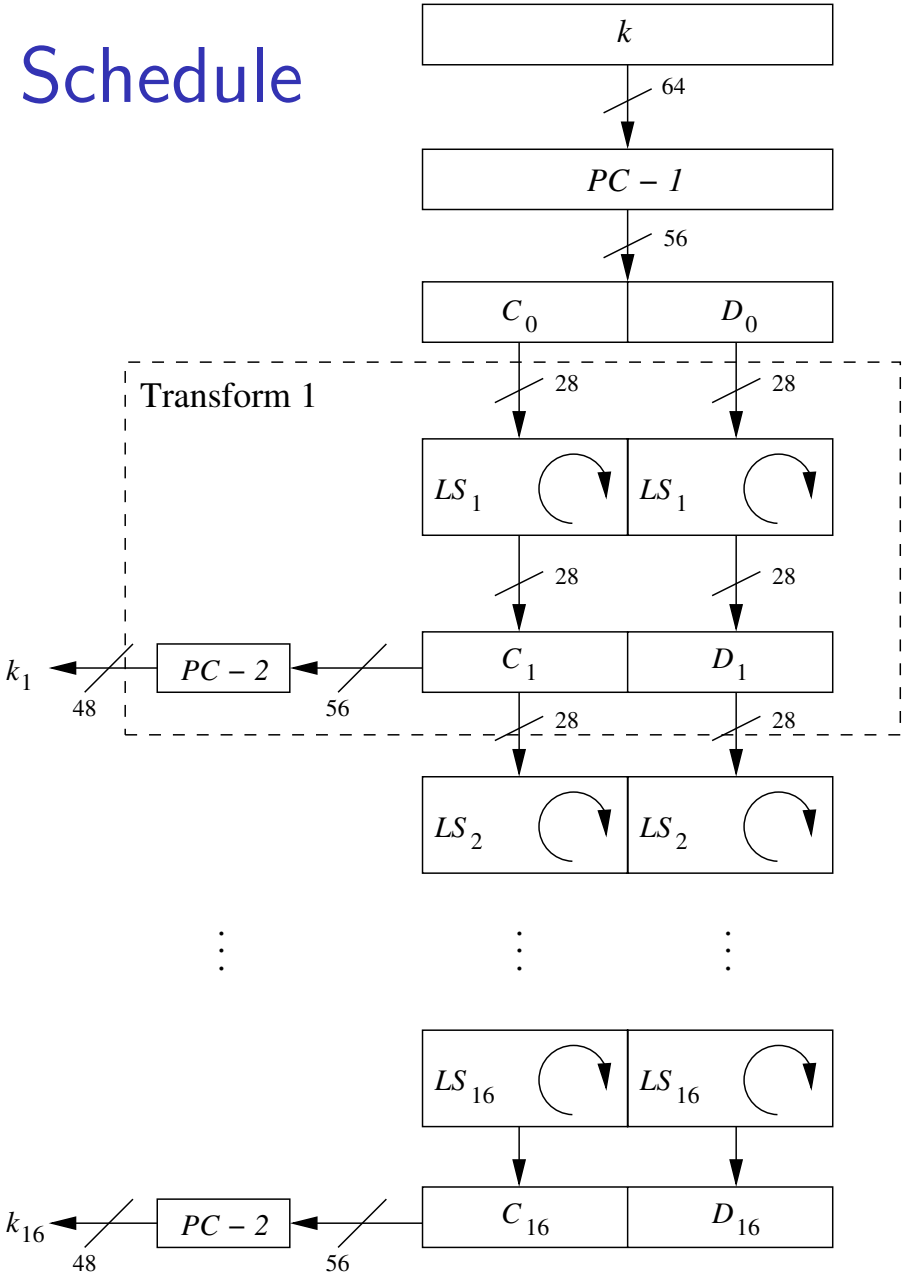




Key Schedule

- Question: How to calculate 16 subkey $k_1, \ldots, k_{16}$?
- Key schedule uses only simple operations (permutations and left rotation) on bits.

Key Schedule

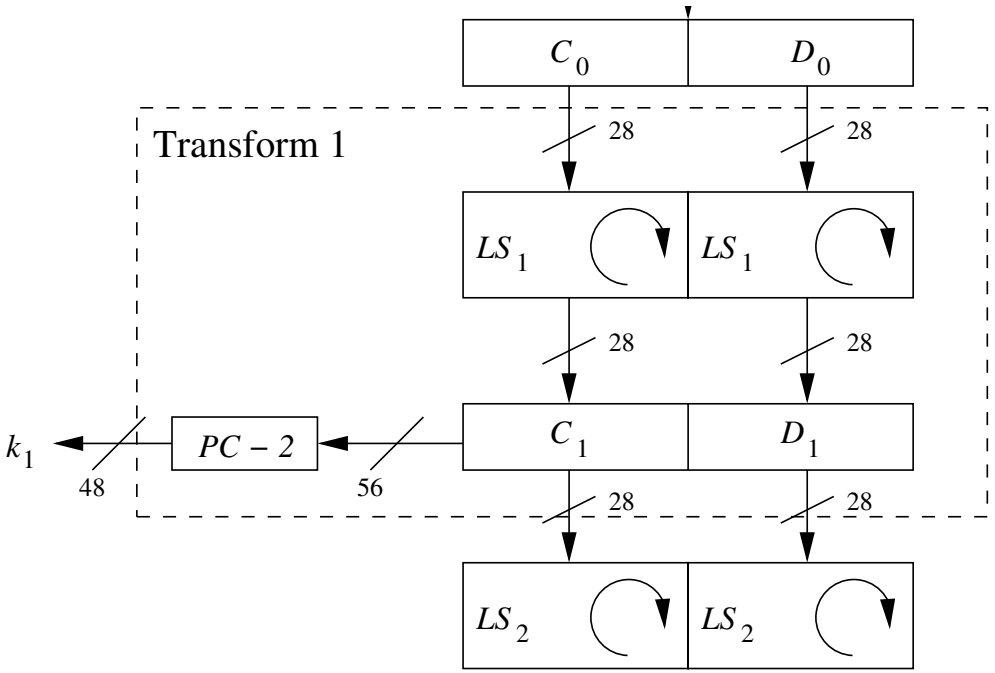


Initial Key Permutation PC-1

- Remove the $8, 16, 24, \ldots, 64$ bits of key k of size 64 bits.
- The real DES key is just $(64 - 8) = 56$ bits.

$PC-1$							
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

LS_i: Left shift (left rotate)



$$LS_i = \begin{cases} \text{Left Rotate } 1 \text{ position} & \text{if } i = 1, 2, 9, 16 \\ \text{Left rotate } 2 \text{ positions} & \text{otherwise.} \end{cases}$$

Remark: Total number of bits rotated is $4 \times 1 + 12 \times 2 = 28$, thus

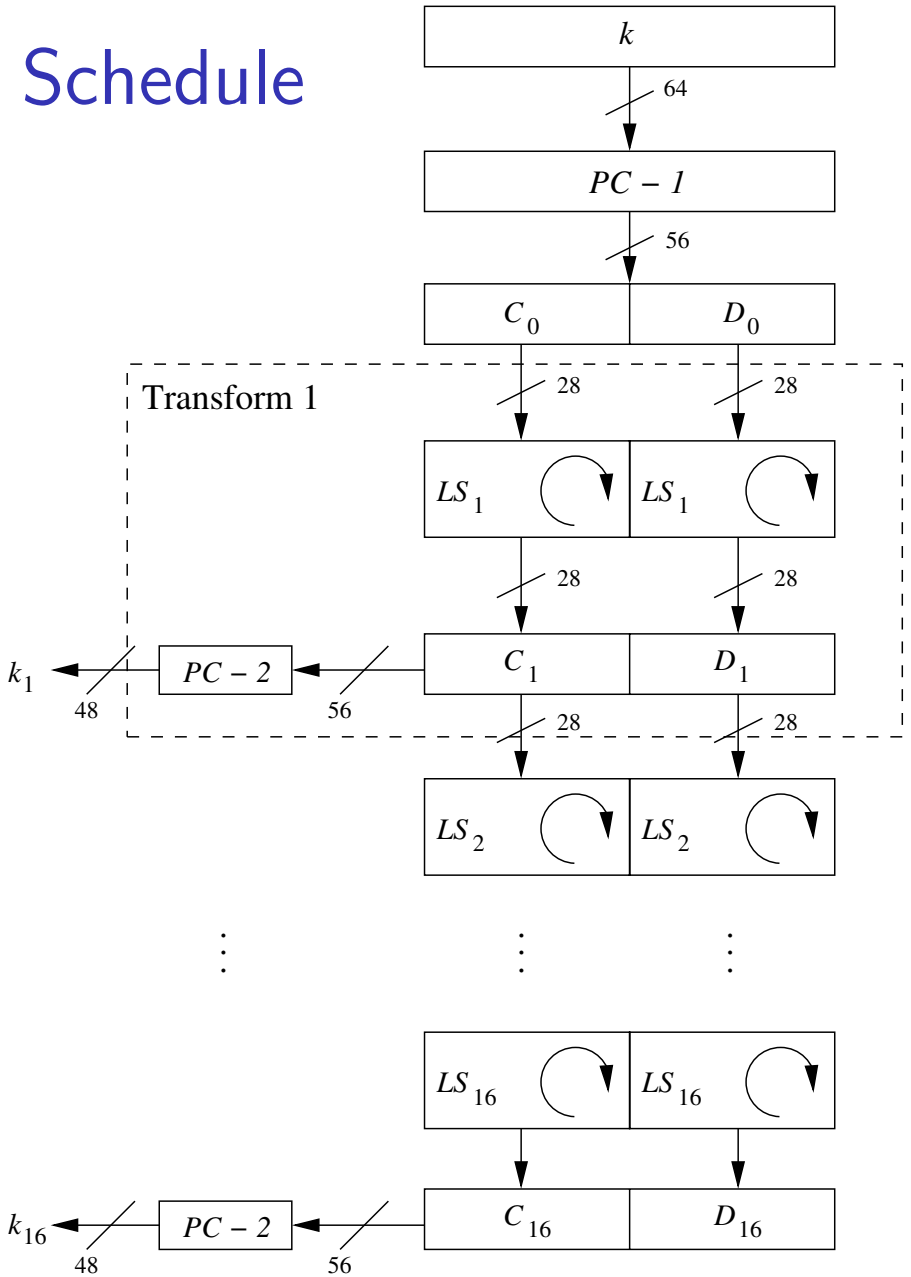
$$C_{16} = C_0;\ D_{16} = D_0.$$

Round Key Permutation PC-2

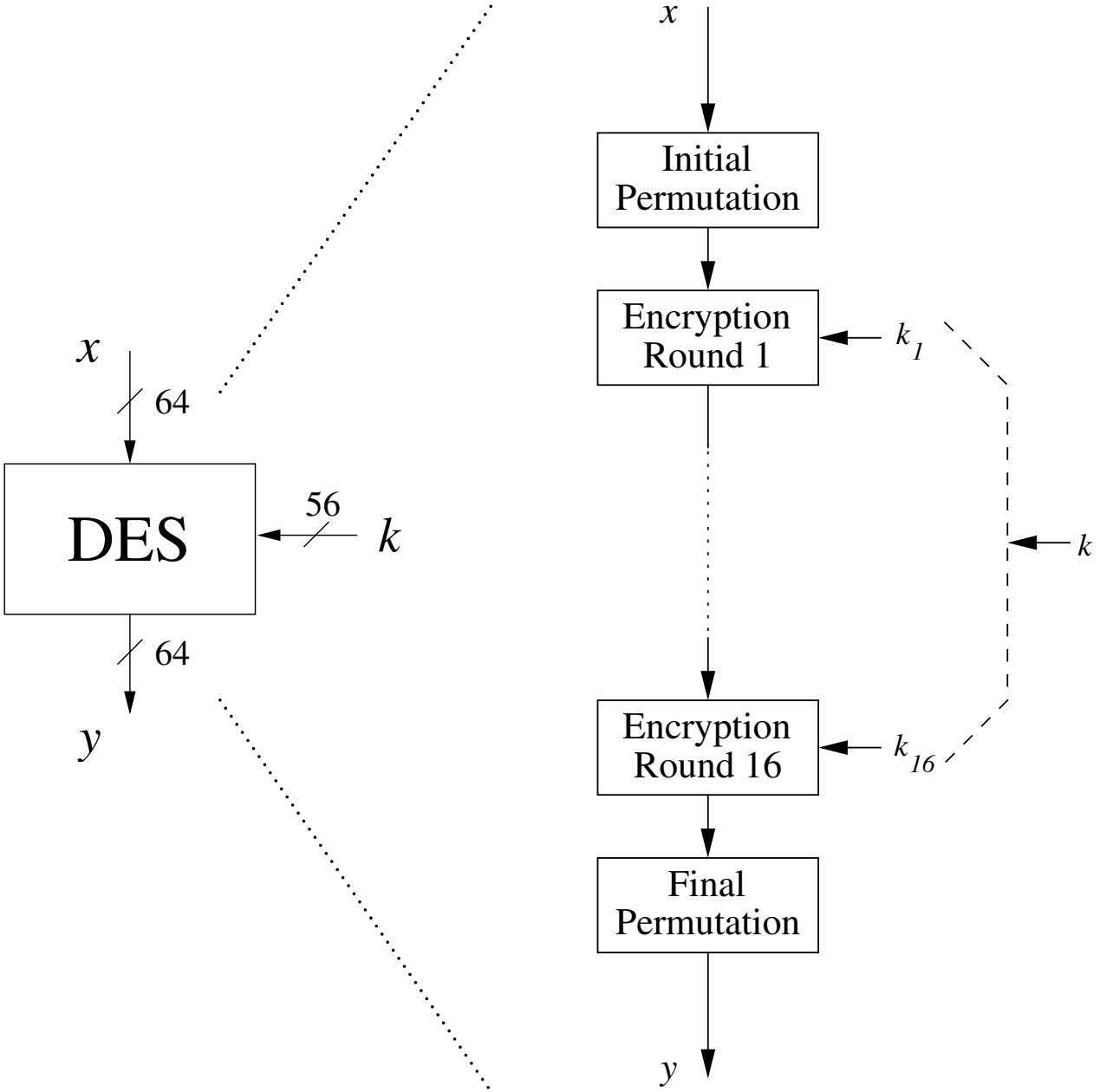
- Remove 8 bits of $\boxed{C_i}\boxed{D_i}$;
- The bit length of subkey k_i is $56 - 8 = 48$ bit

$PC-2$							
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

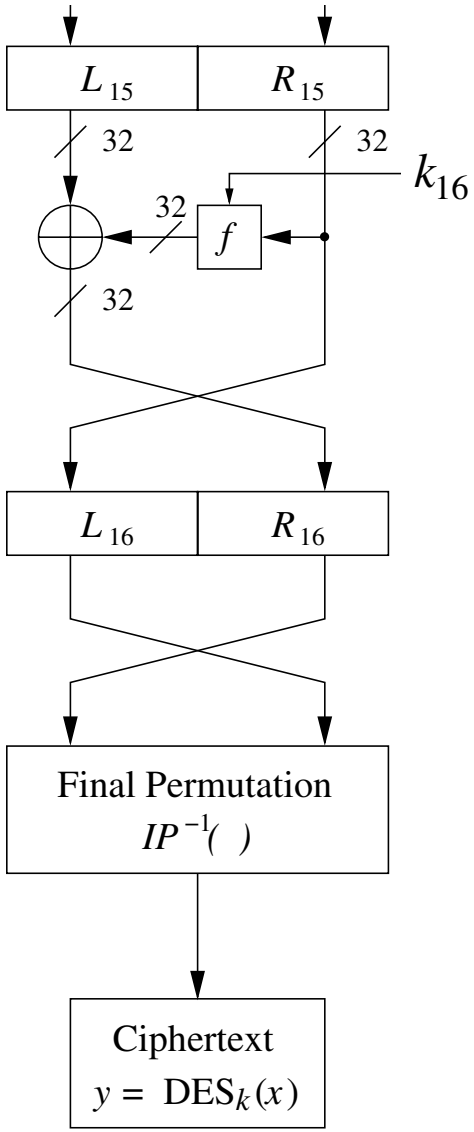
Key Schedule

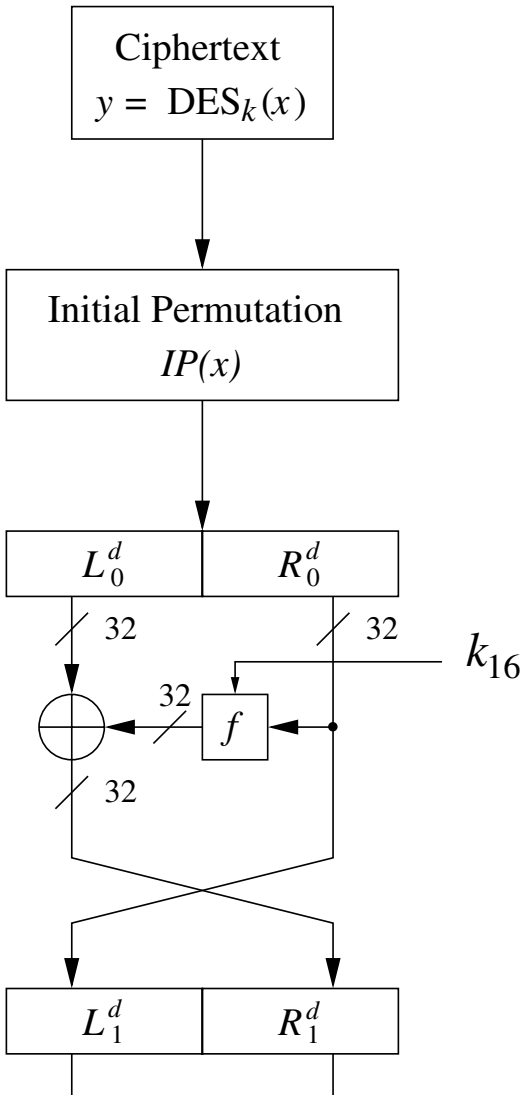


Outline


x
64
DES
56
k
64
y
x
Initial Permutation
Encryption Round 1
k1
k
Encryption Round 16
k16
Final Permutation
y

DES decryption





Outline

Exhaustive Key Search

Problem

- given a few input output pairs

$$(x_i, y_i = \mathsf{Enc}(k, x_i))$$

  for $i = 1, 2, 3$.
- find key k.

Lemma

Suppose DES is an ideal cipher (2^{56} random invertible functions $\pi_i : \{0,1\}^{64} \to \{0,1\}^{64}$)

*then $\forall x, y$ there is at most **one** key k such that*

$$y = DES(k, x)$$

with probability $\geq 1 - 1/256 \approx 99.5\%$.

Exhaustive Search for block cipher key

- For two DES pairs :

$$(x_1, y_1 = DES(k, x_1)) \text{ and } (x_2, y_2 = DES(k, x_2))$$

  unicity probability $\approx 1 - 1/2^{71}$.
- For AES-128: given two input/output pairs, unicity prob. $\approx 1 - 1/2^{128}$
- Thus two input/output pairs are enough for Exhaustive Key Search.

DES challenge

```
msg = "The unknown messages is : XXXX ... "
CT  =      y1        y2        y3          y4
```

Goal: find key $k \in \{0,1\}^{56}$ such that $DES(k, x_i) = y_i$ for $i = 1, 2, 3$.

- 1997: DESCHALL project with internet search – 96 days
- 1998: EFF machine (DeepCrack) – 3 days (250K \$)
- 1999: combined search – 22 hours
- 2006: COPACOBANA (120 FPGA) – 7 days (10K \$).

56 bit ciphers should not be used !! 128-bit key $\Rightarrow 2^{72}$ days.

ĐẠI HỌC BÁCH KHOA

25 YEARS ANNIVERSARY SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you!

soict.hust.edu.vn/ fb.com/groups/soict