INT 307
Multimedia Security System

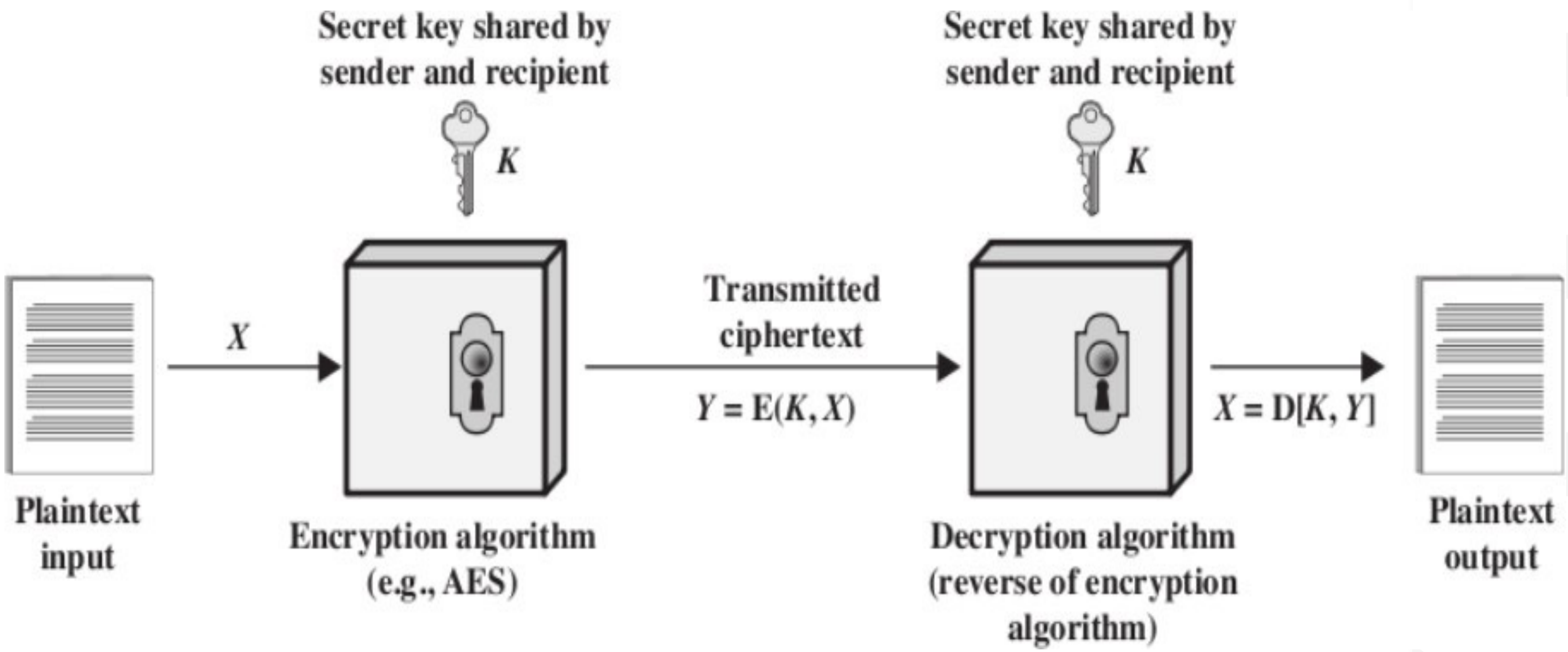
Multimedia Encryption (II)

Sichen.Liu@xjtlu.edu.cn

XJTLU | SCHOOL OF FILM AND TV ARTS

Xi'an Jiaotong-Liverpool University
西交利物浦大学

Simplified Model of Symmetric Encryption

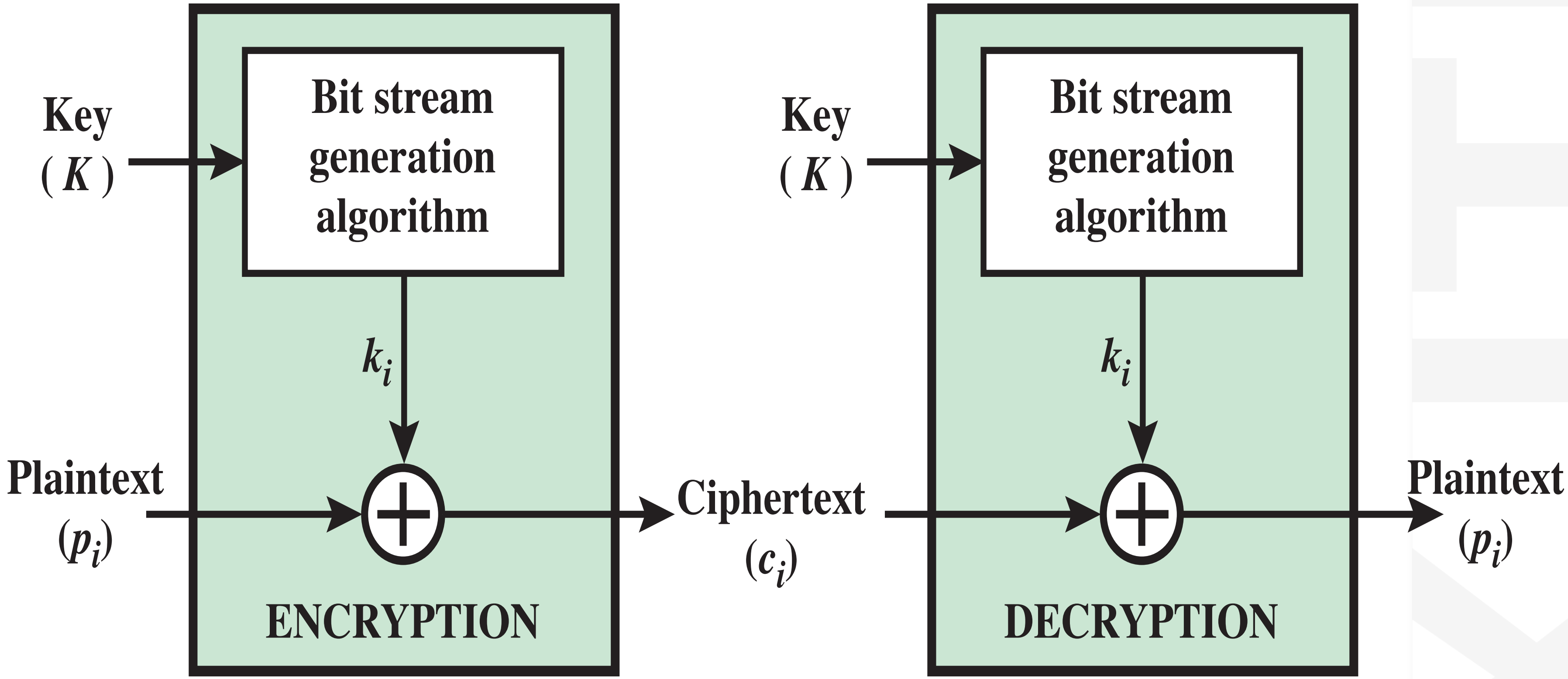


Example: One-Time Pad

- Message 0100010
- Key 1001011
- Encrypted Message 1101001 = Message $\oplus$ Key
- Message = Encrypted Message $\oplus$ Key

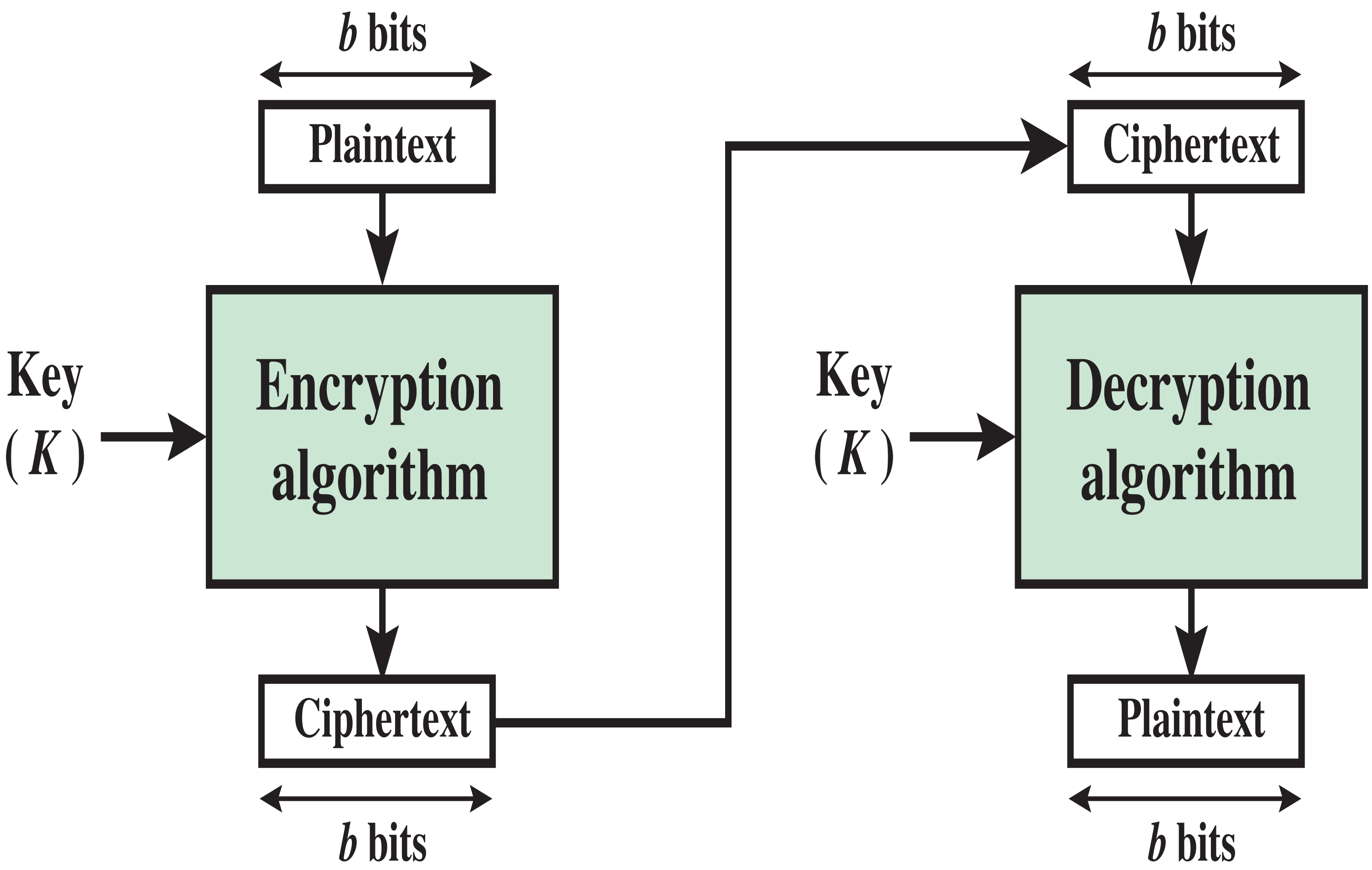
Encryption Types

- Stream Cypher



Encryption Types

- Block Cypher: DES, AES,Triple-DES

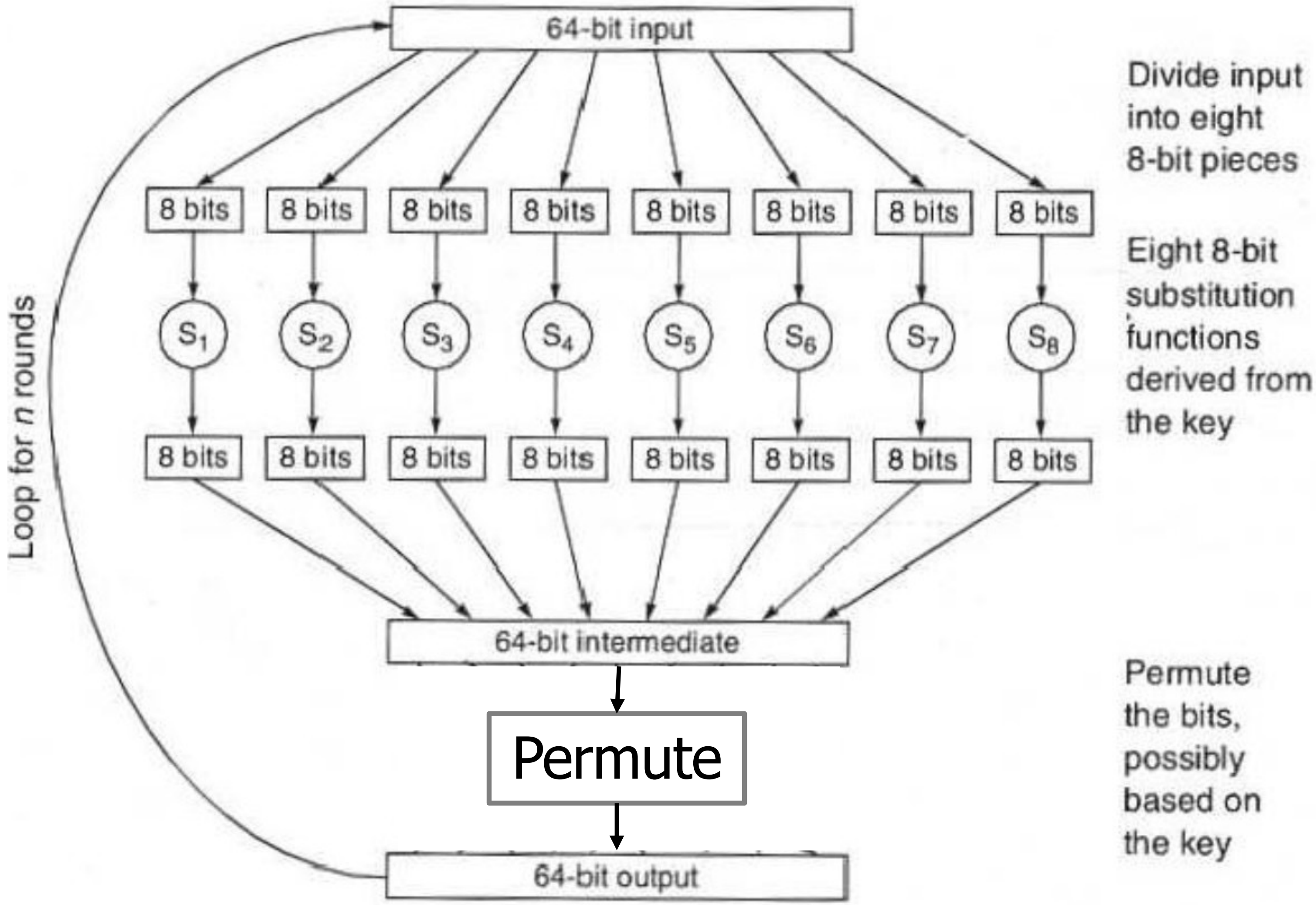


Substitution and Permutation

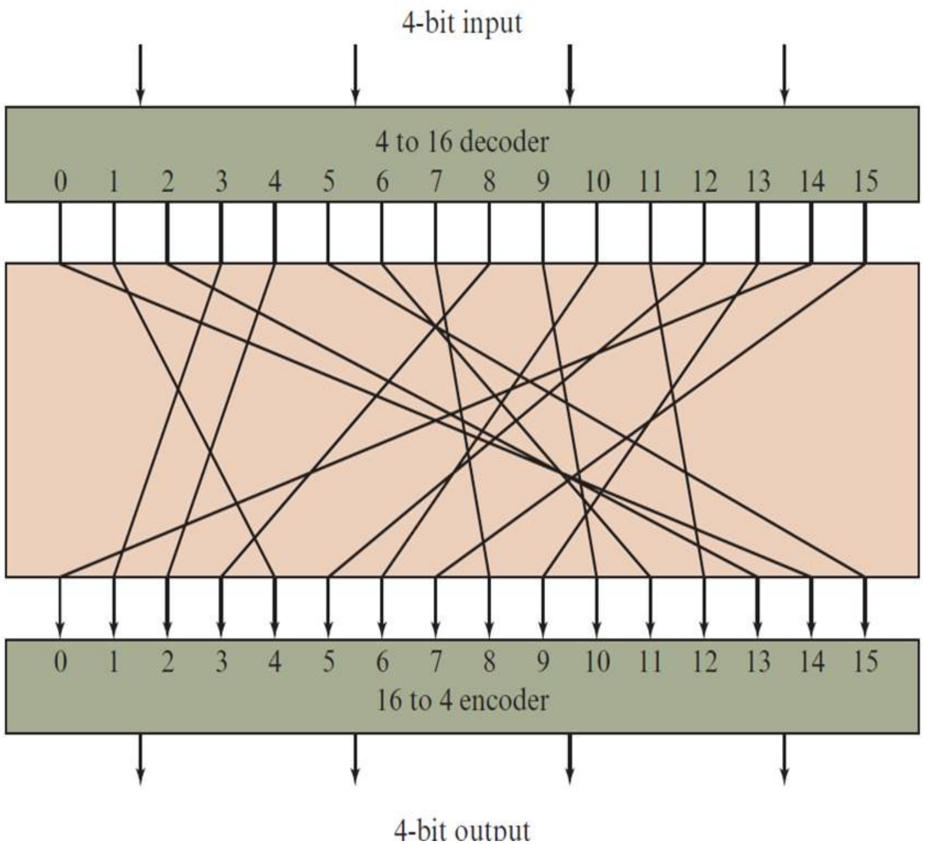
- **Substitution:** replacing an element of the plaintext with an element of ciphertext
- Overall substitution rule or varying ones for every element of the plaintext.
- **Permutation:** rearrange the order of appearance of the element of the plaintext.
- Multiple rounds of interlaced transpositions and substitutions.

Block Cypher Example

- Block cypher



Block Cypher Example



Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - DES is a block cipher - the plaintext is processed in 64-bit blocks
  - The key is 56-bits in length
  - Based on Feistel Cipher Structure
- Triple DES
  - Effective key length of 112/168 bits
- Advanced Encryption Standard (AES)
  - 128-bit data, 128/192/256-bit keys
  - Stronger & faster than Triple-DES
- Public key encryption: asymmetric key (e.g., RSA)

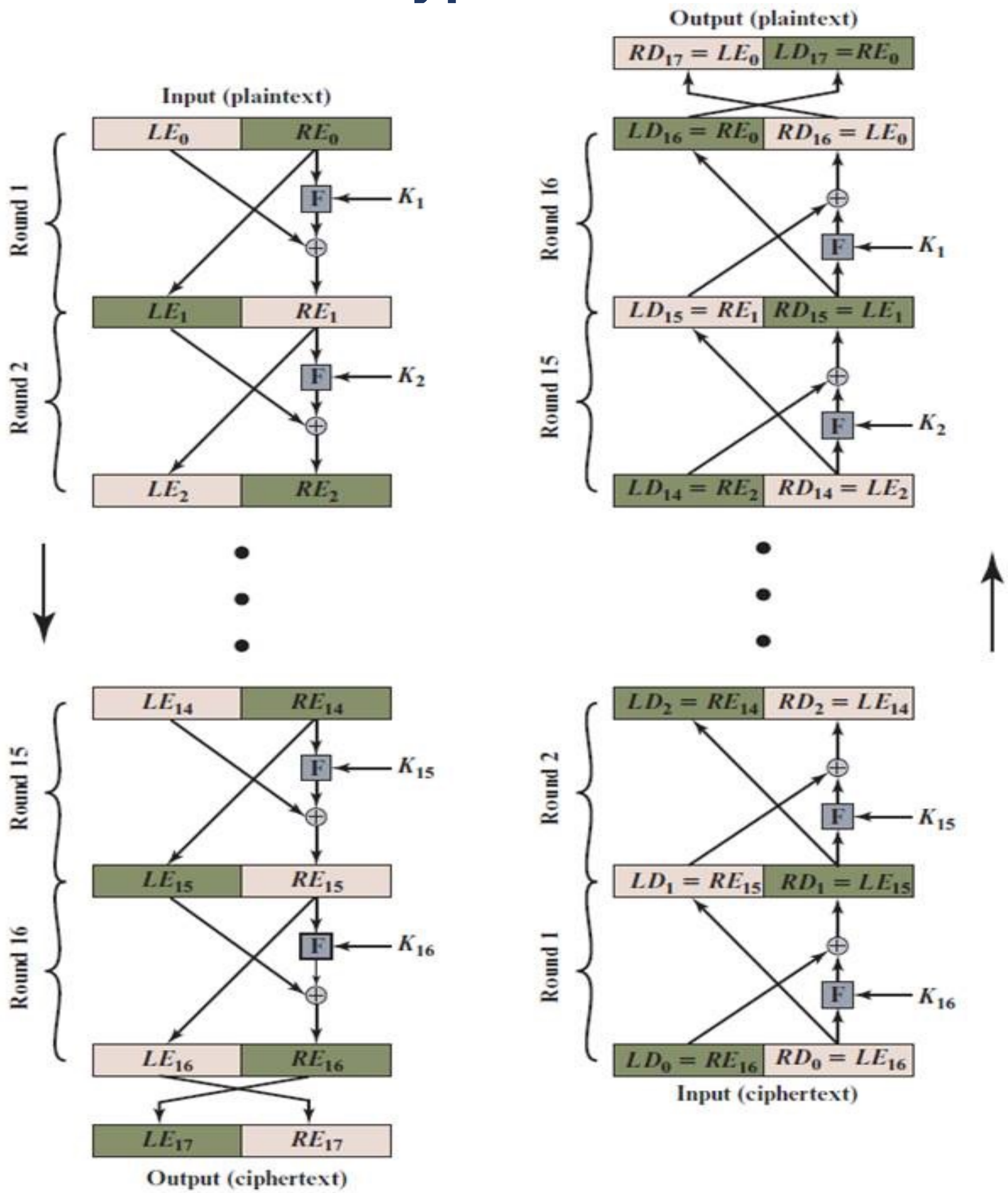
Feistel Encryption Framework

- Milestone Paper of encryption in 1973

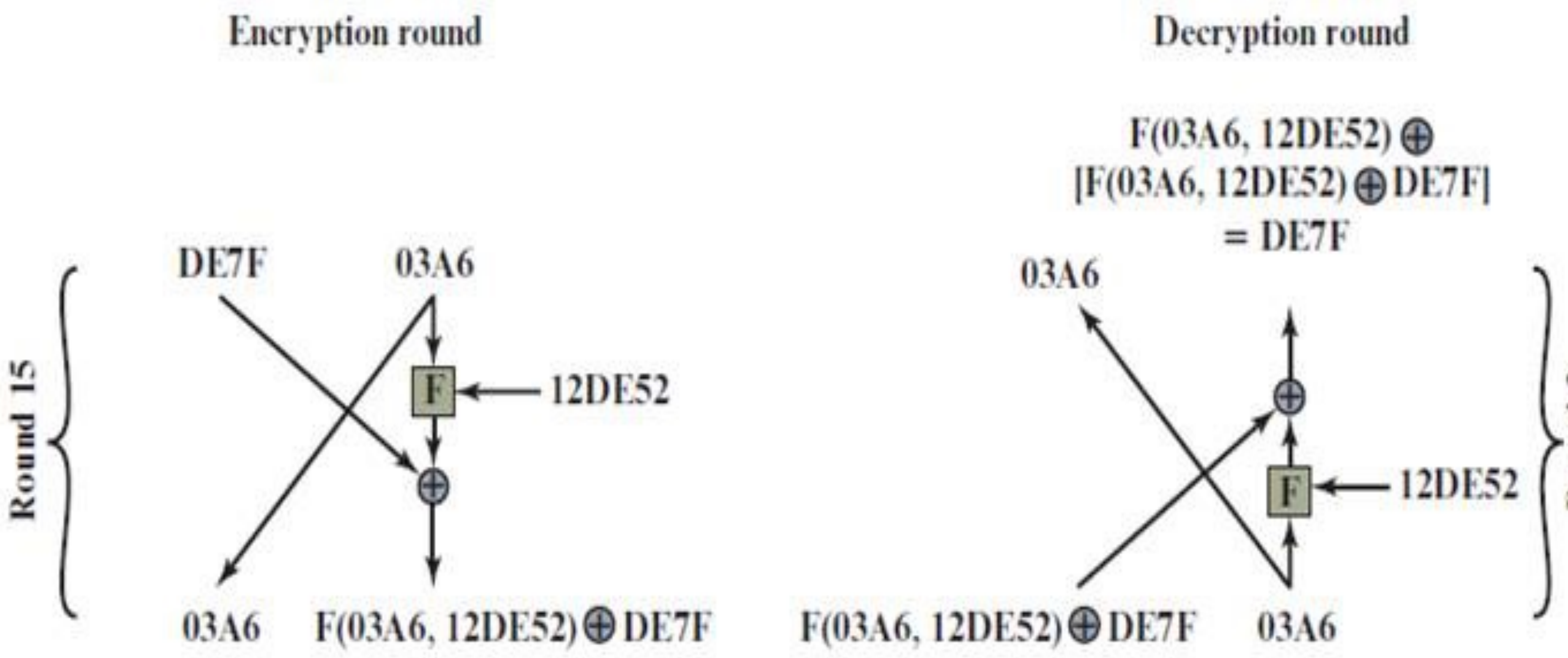
- Most famous encryption algorithms are based on Feistel structure
  - DES
  - Triple DES
  - AES

Feistel Encryption Structure

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



Feistel Example



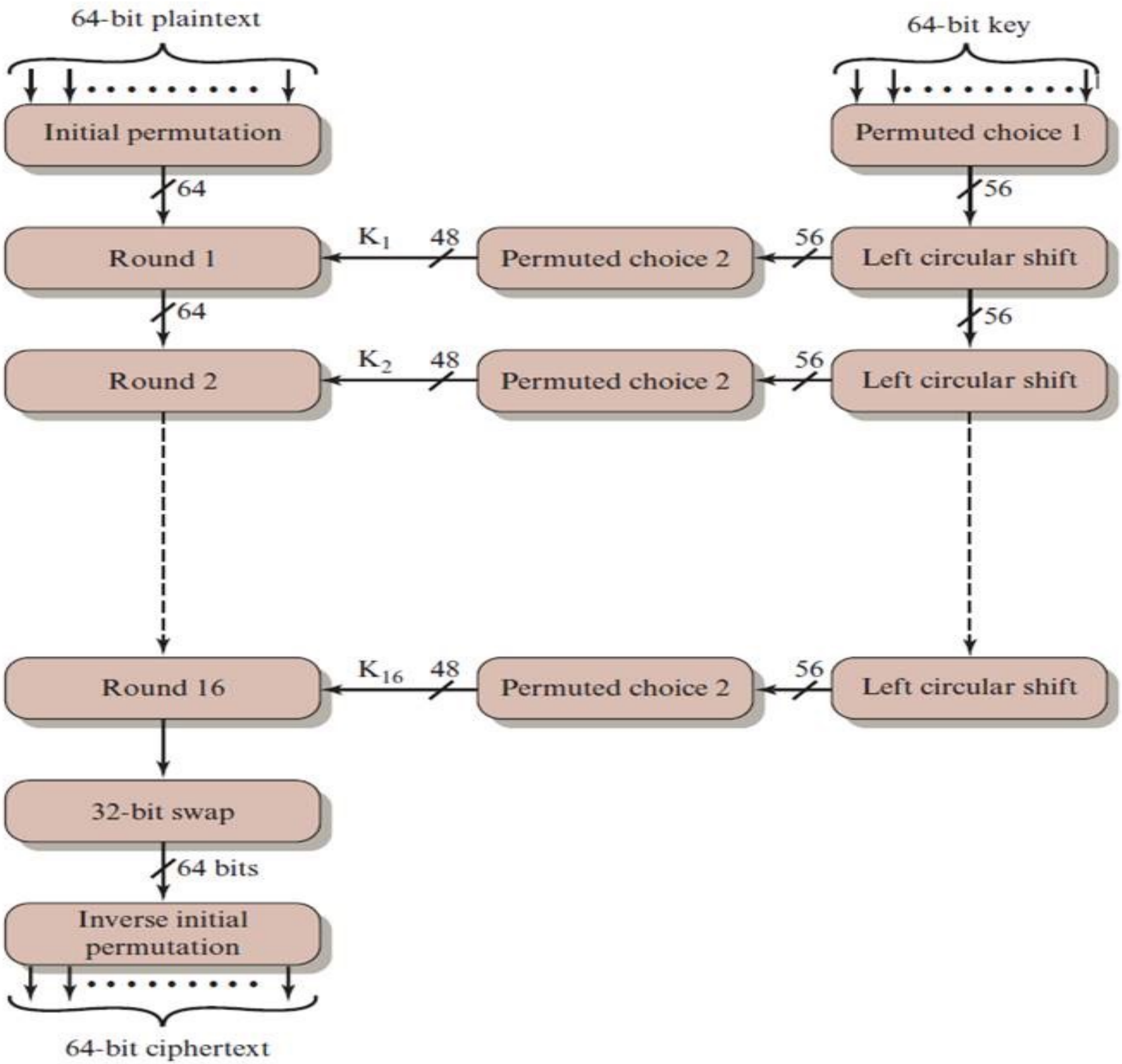
Major Concerns in Feistel Encryption Framework

- Block size:
  - Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm. Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design.
- Key size:
  - Larger key size means greater security but may decrease encryption/decryption speed.
- Number of rounds:
  - The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- Subkey generation algorithm:
  - Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- Round function F:
  - Greater complexity generally means greater resistance to cryptanalysis.

Data Encryption Standard (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Standard (DES)
  - Data are encrypted in 64-bit blocks using a 56-bit key
  - The algorithm transforms 64-bit input in a series of steps into a 64-bit output
  - The same steps, with the same key, are used to reverse the encryption

DES Structure



DES-Initial Permutation and Final Permutation

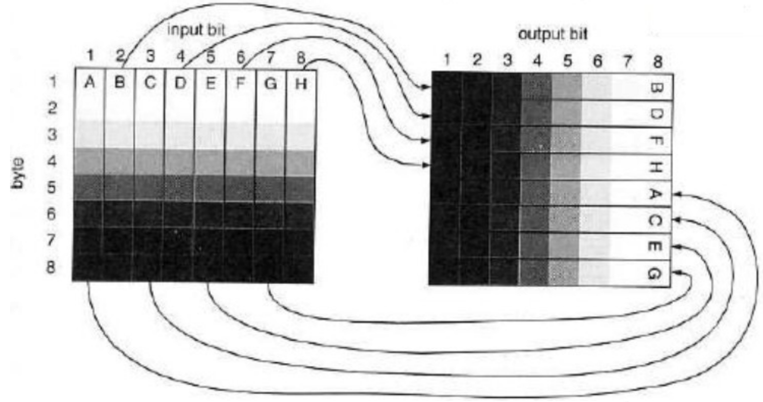
- Objective: Make the output data more random and do not increase security level

(a) Initial Permutation (IP)

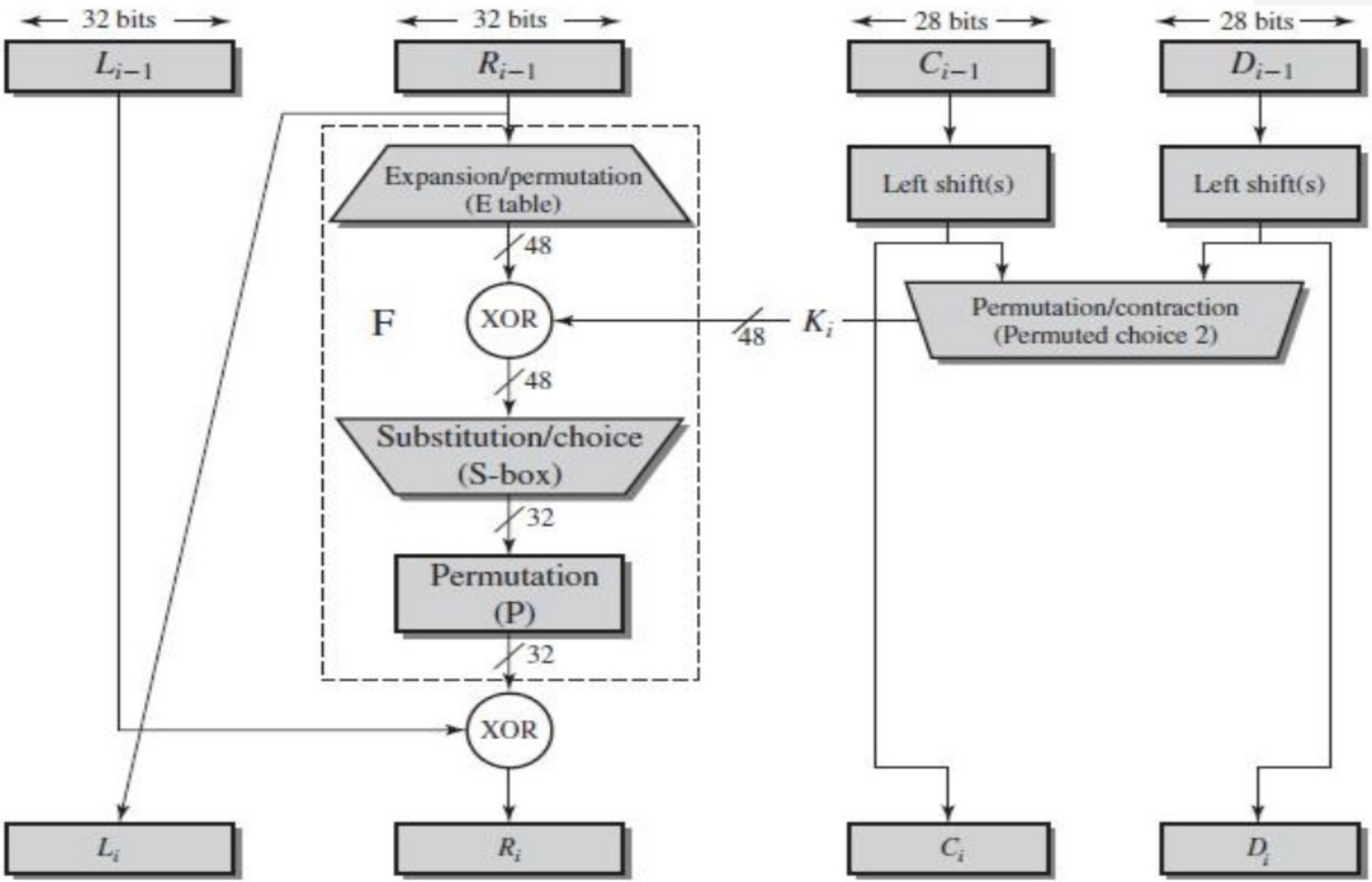
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial 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



Encryption in a DES Round



DES Expansion (E) and Permutation (P)

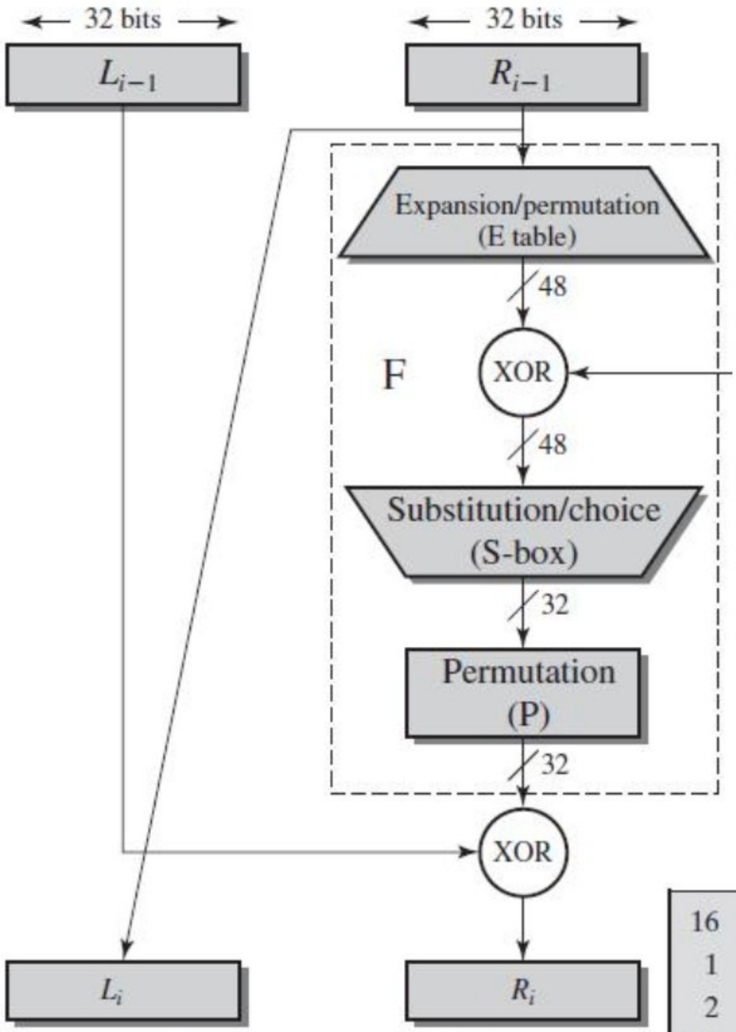


Figure 3.6 Single Round of DES Algorithm

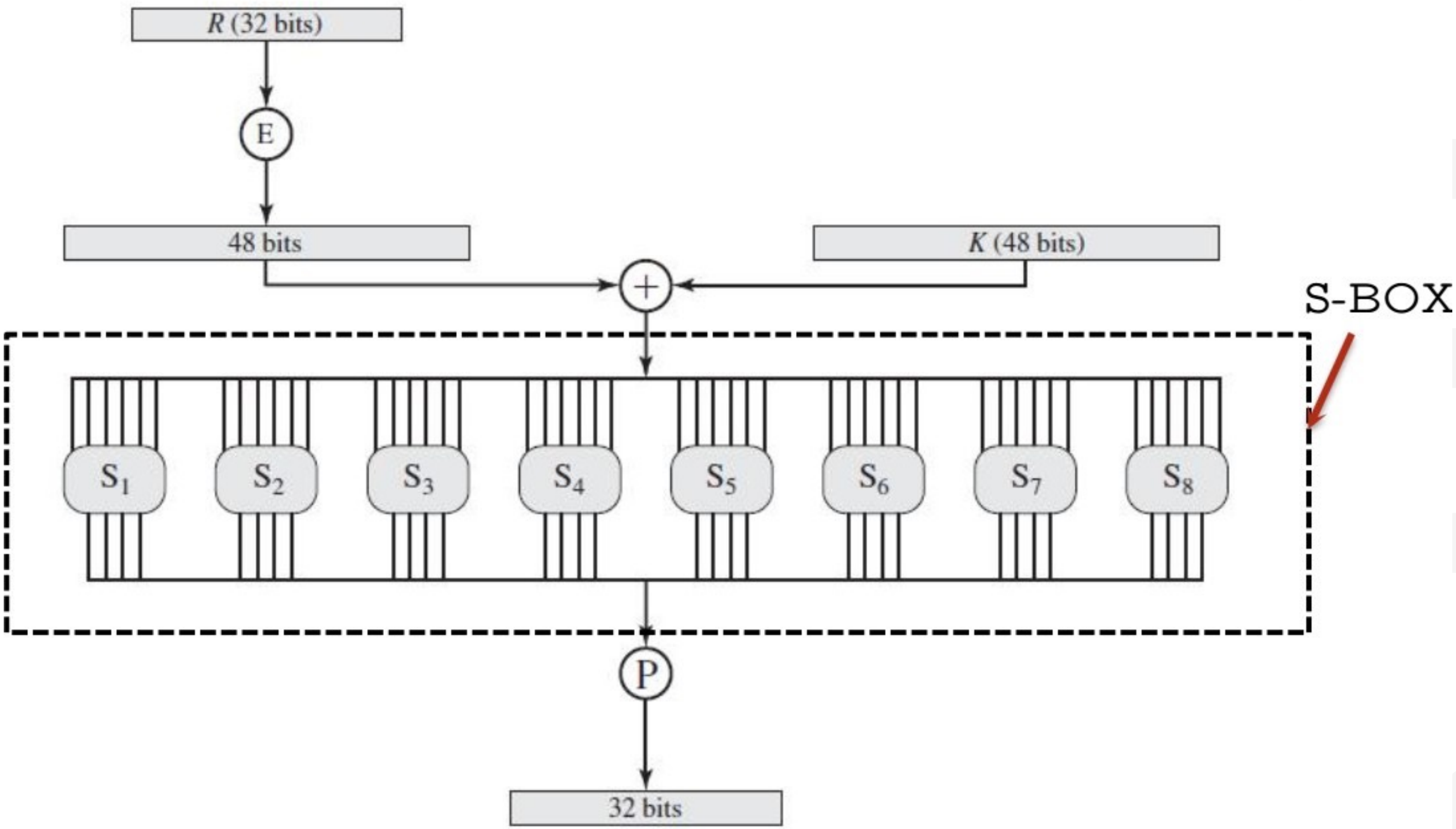
(c) Expansion Permutation (E)

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

(d) Permutation Function (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

DES S-Box

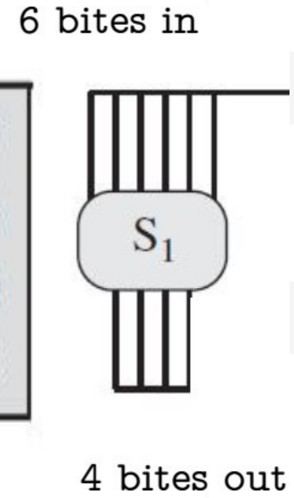


S-Box

- The first and last bits of the input to box form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i.

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



- The middle four bits select one of the sixteen columns. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output.
- For example, in S1, for input 011001, the row is 01 (row 1) and the column is 1100 (column 12).The value in row 1, column 12 is 9, so the output is 1001.

S-Box

- 8 S-box, each containing different table values

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

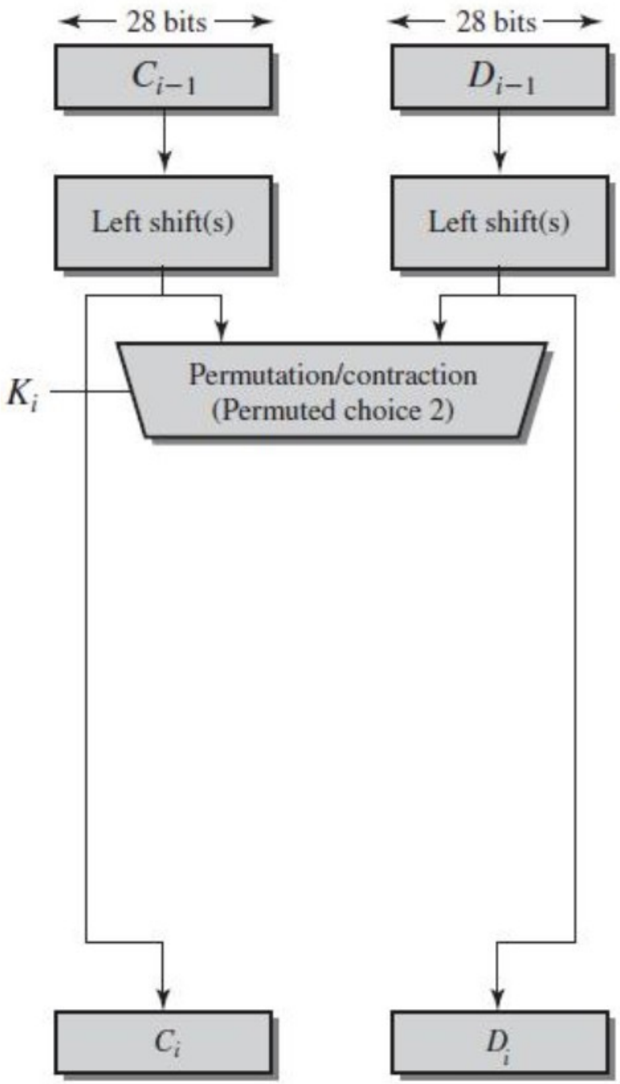
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

⋮

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Key Generation for Each Round



(a) Input Key

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

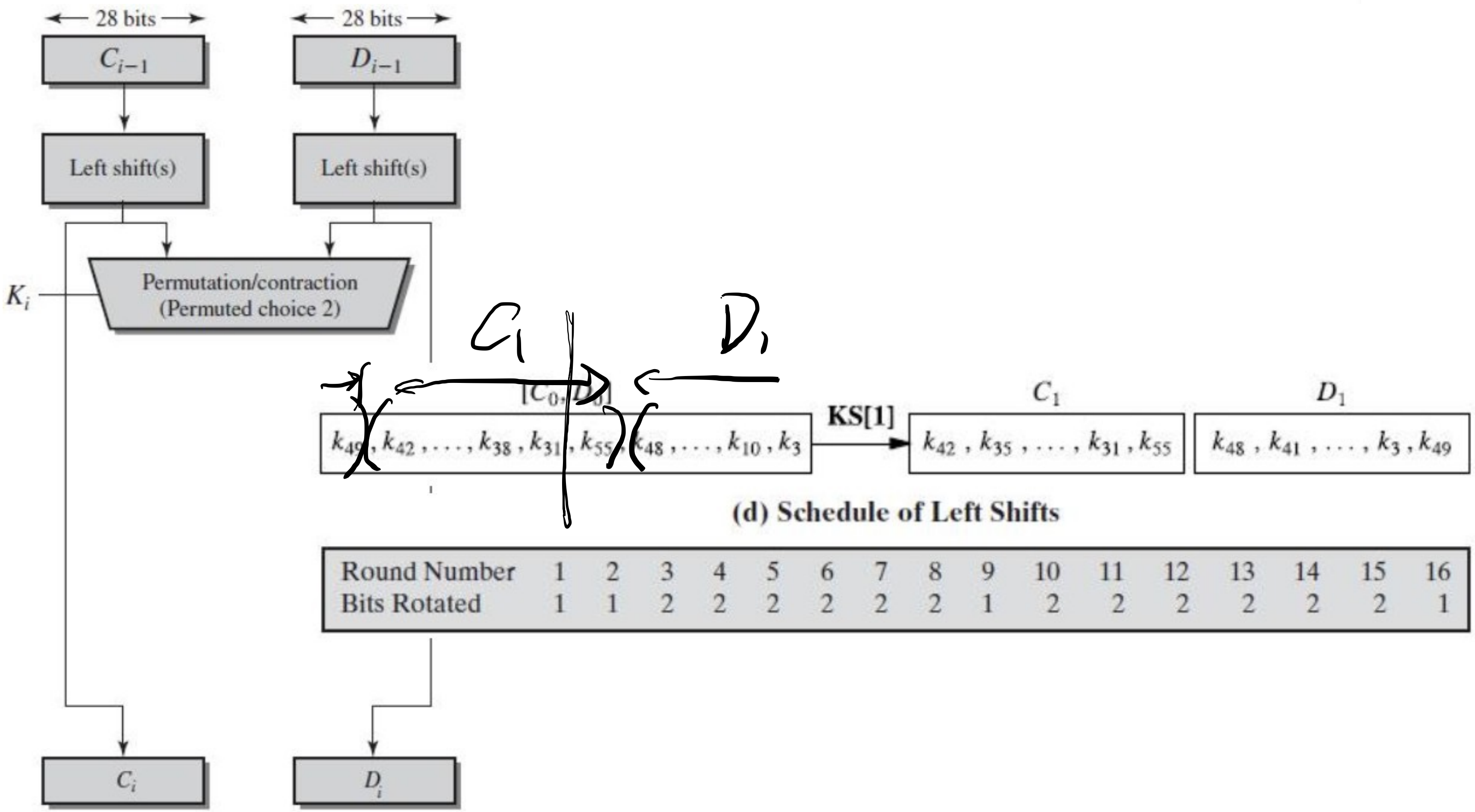
C_0

(b) Permuted Choice One (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

D_0

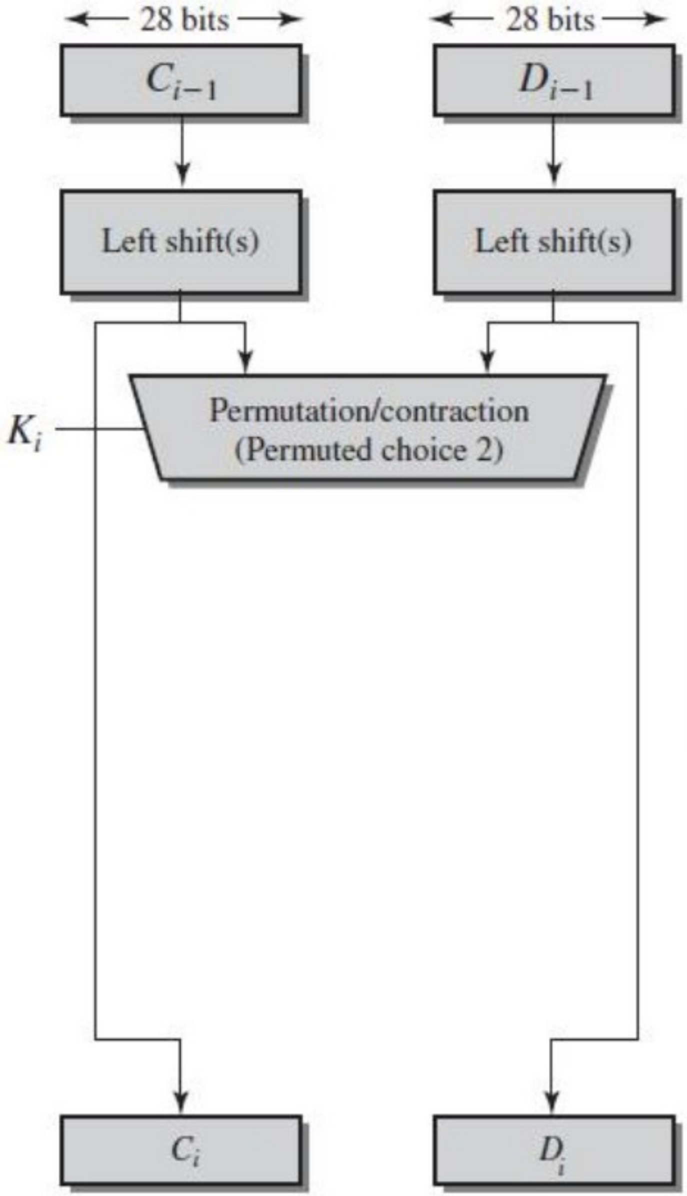
Key Generation for Each Round



(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

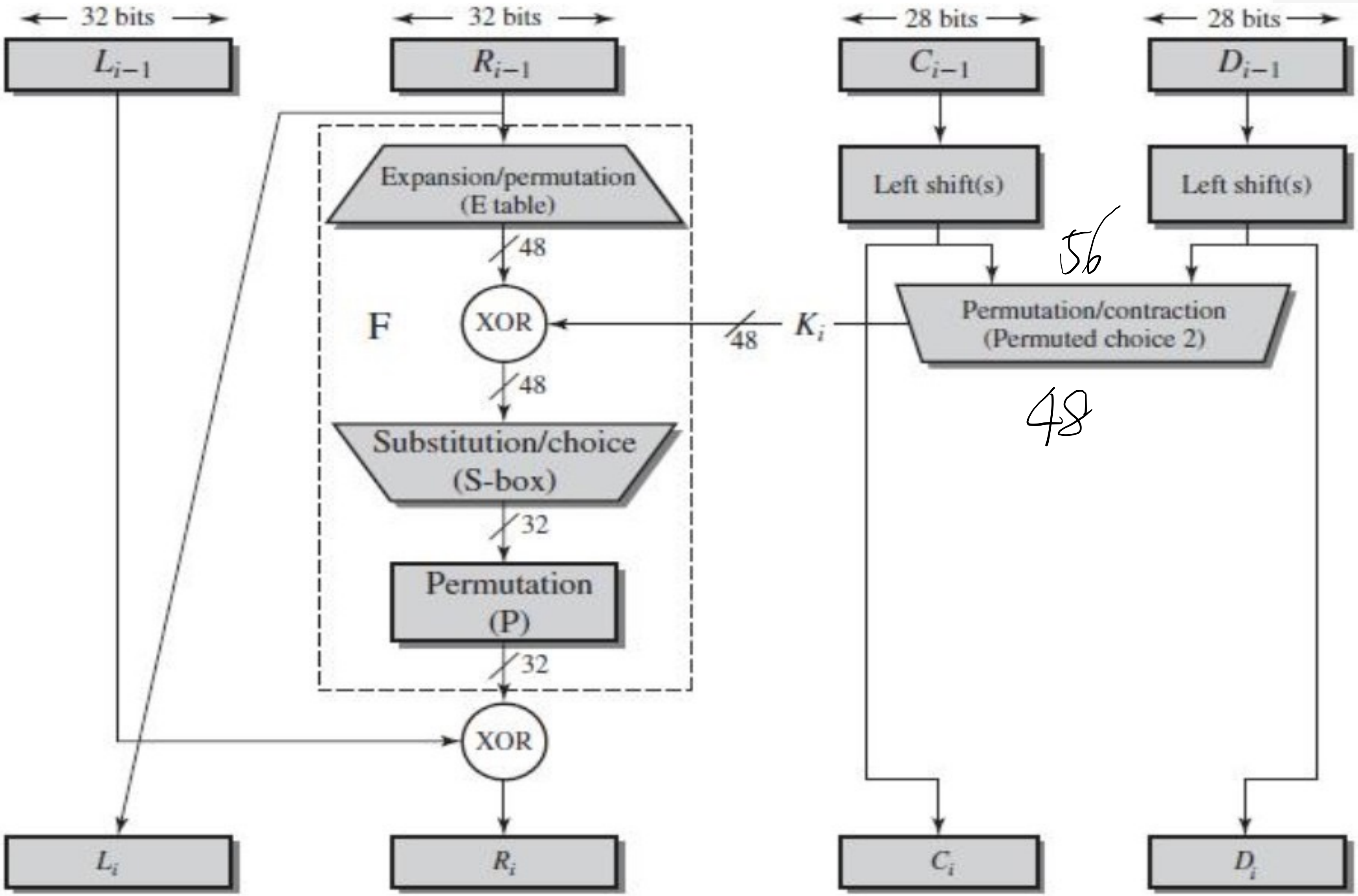
Key Generation for Each Round



(c) Permuted Choice Two (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

Encryption in a DES Round



More Secure Techniques

- Triple DES
- Effective key length of 112/168 bits
- Advanced Encryption Standard (AES)
- 128-bit data, 128/192/256-bit keys
- Stronger & faster than Triple-DES

Triple DES

- The availability of increasing computational power made brute-force attacks feasible
- A simple method to increase the key size of DES
- Key bundle comprise three DES key K_1, K_2 and K_3 (56 bits)
- Encryption

$$\text{ciphertext} = E_{K_3} D_{K_2} E_{K_1} (\text{plaintext})$$

- Decryption

$$\text{plaintext} = D_{K_1} E_{K_2} D_{K_3} (\text{ciphertext})$$

Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
26 characters permutation	Monoalphabetic	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Format Compliant Encryption

- For mobile applications
- Recall: mobile device-limited resource
  - Selective encryption- computational complexity
  - Security level → target application
  - Encryption algorithm selection-computation power
- Compression: wireless communication-limited bandwidth; multimedia data stream-large
- If selective encryption is not done smartly → Compression + encryption = bitrate increase

Example: MPEG I Frame Intra Block Shuffling

24	20	18	17	10	8	4	1
21	16	13	9	6	3	0	0
15	10	4	2	0	0	0	0
10	7	3	0	0	0	0	0
6	2	0	0	0	0	0	0
4	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

shuffle

transpositions

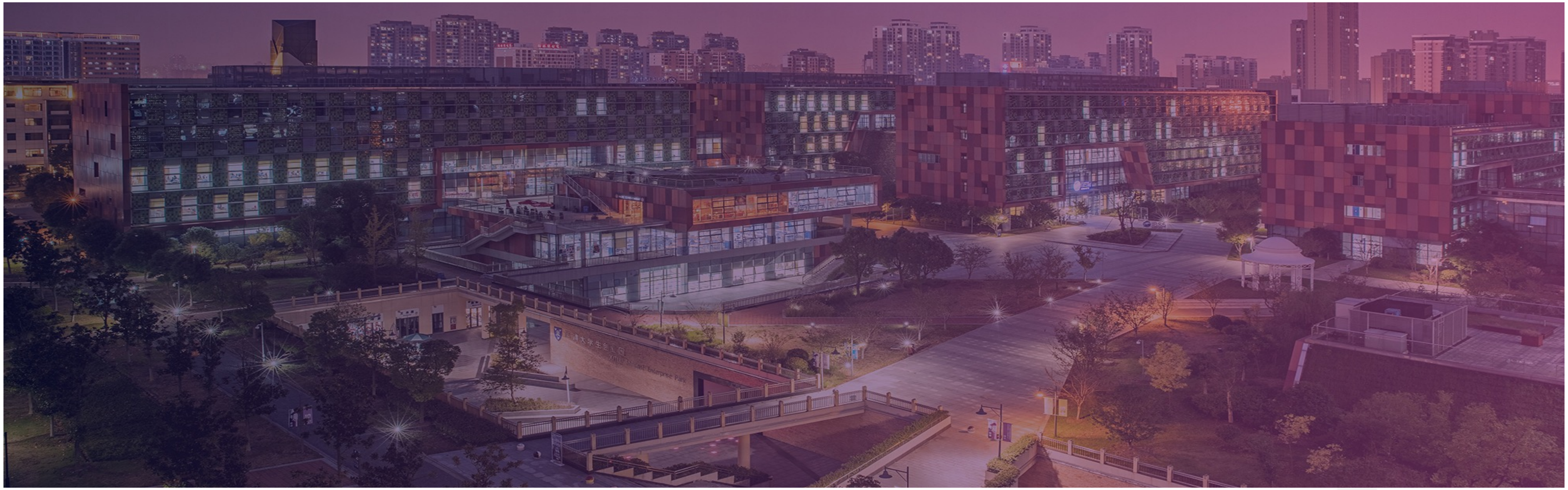
7	0	1	0	4	8	0	10
0	6	0	0	3	0	0	4
0	0	4	2	0	15	0	0
3	0	10	0	13	0	0	0
6	2	0	0	0	0	21	0
9	0	10	0	0	24	0	0
0	16	0	18	0	0	0	0
0	0	0	0	17	0	0	20

0s – clustered together → not any more

bitrate ↑

Joint Encryption and Compression

- To achieve improved overall performance:
  - E.g., Zigzag-Permutation (Tang 96)
  - Simple, but significantly lower compression ratio.
  - Local scrambling → spatial energy distribution unchanged → less effective scrambling
  - Spatially shuffle coefficients/ MVs (Zeng & Lei 99)
  - Coefficient block shuffling, block rotation, and coefficient shuffling within a segment.
  - Local statistics largely unchanged → good coding efficiency
  - Global spatial configuration changed → good security



THANK YOU

VISIT US

WWW.XJTLU.EDU.CN

FOLLOW US

@XJTLU

Xi'an Jiaotong-Liverpool University
西交利物浦大学

XJTLU | SCHOOL OF FILM AND TV ARTS