Parul® University

NAAC A++

Stream cipher and Block Cipher

Chapter-3: Block Ciphers and the Data Encryption Standard

Mohammad Asif
Assistant Professor
Department of Computer Science and Engineering

Parul® University

NAAC A++

Content

INDEX

Stream cipher and Block Cipher:

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Examples:

Autokeyed Vigenère cipher

A5/1

RC4

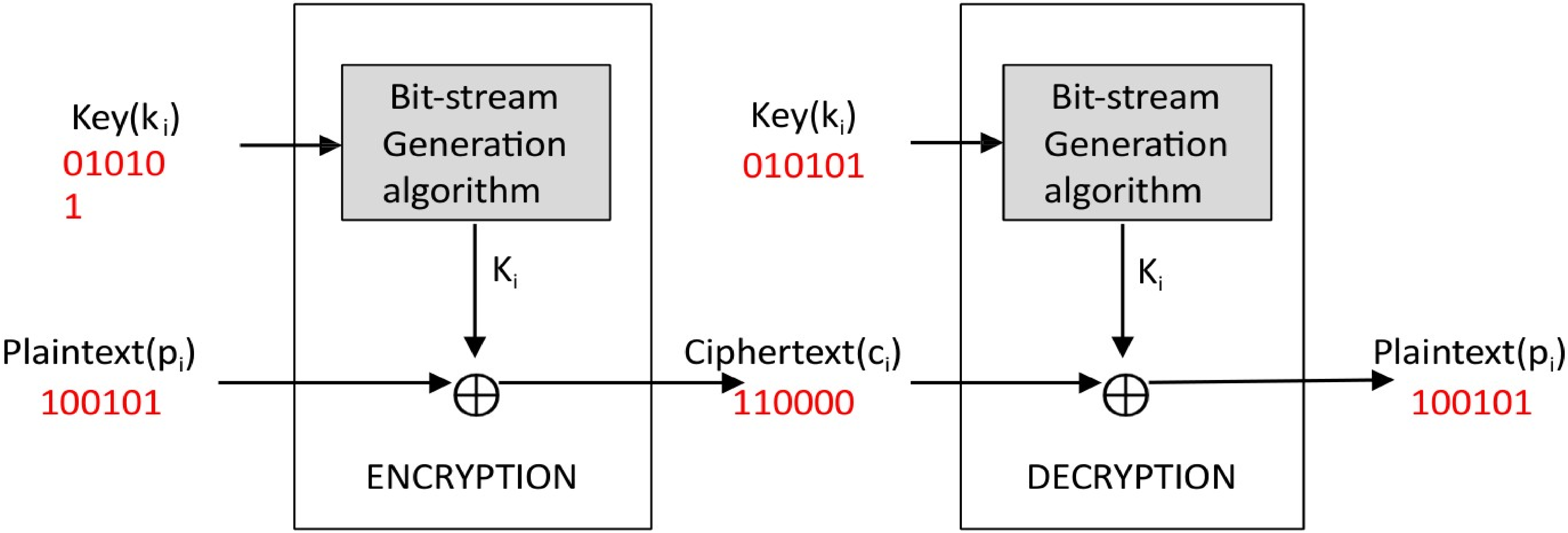
Vern

am

ciph

er.

Stream cipher and Block Cipher:



Stream cipher and Block Cipher:

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used.

Examples:

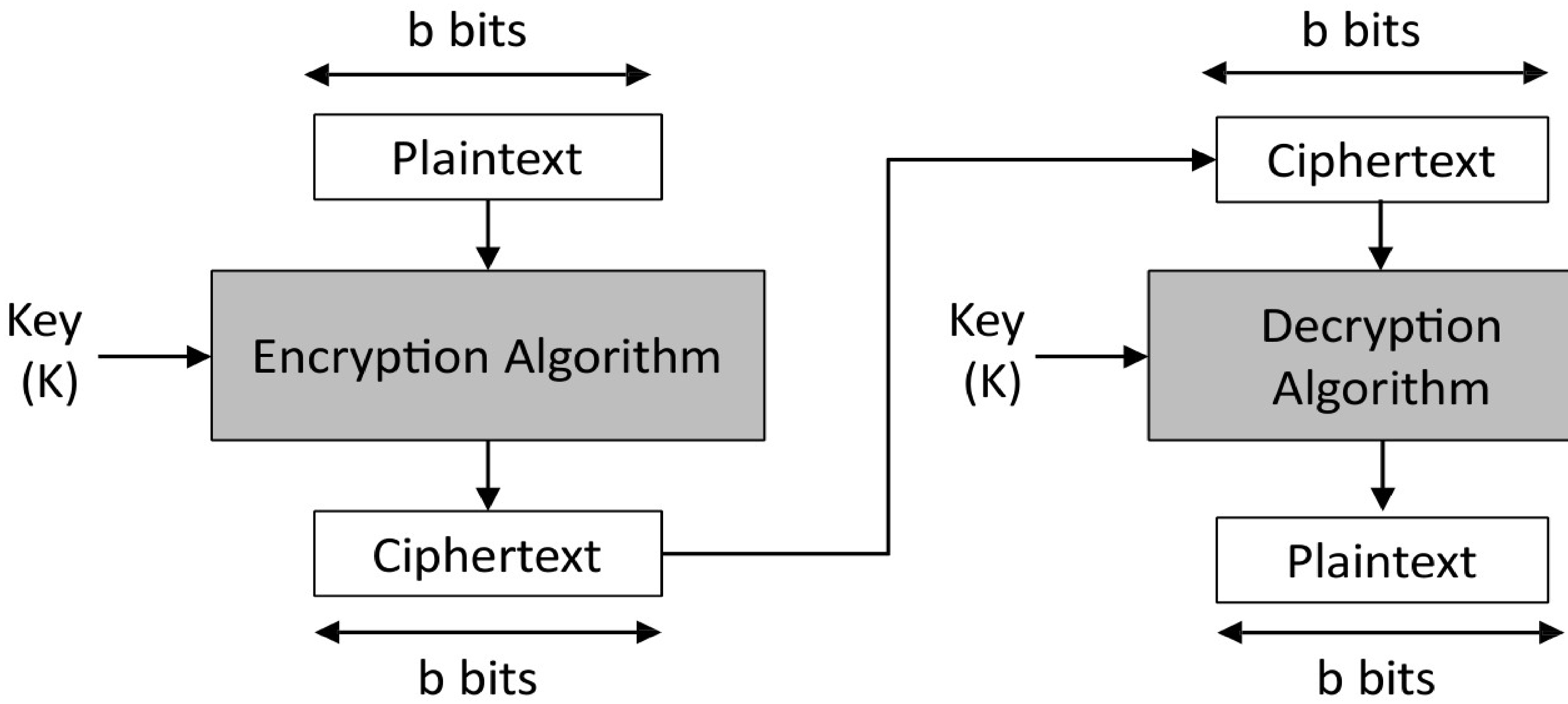
Feistel cipher

DES

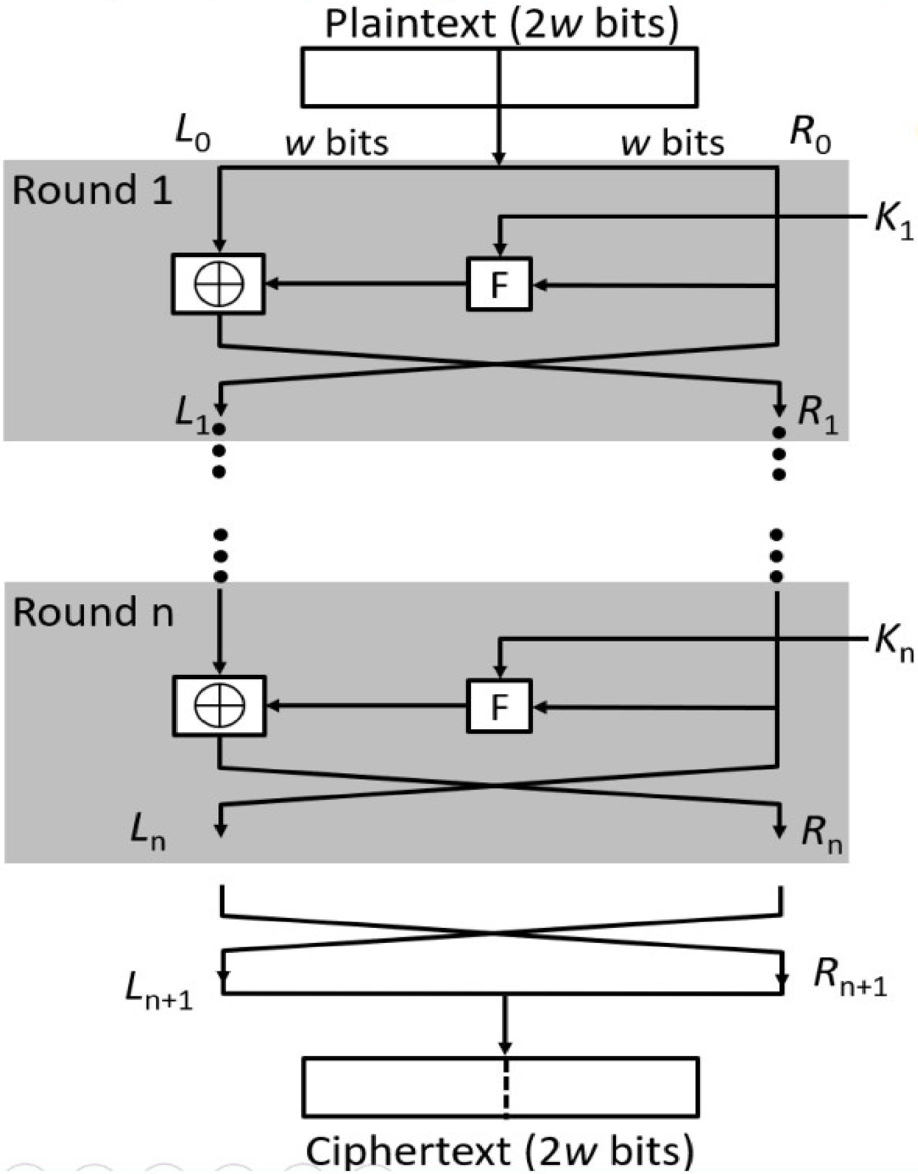
Triple DES

AES

Stream cipher and Block Cipher:



Block Cipher Principle – Fiestel Structure



1. Plaintext is split into 32-bit halves L_i and R_i
2. R_i is fed into the function F.
3. The output of function F is then XORed with L_i
4. Left and right half are swapped.

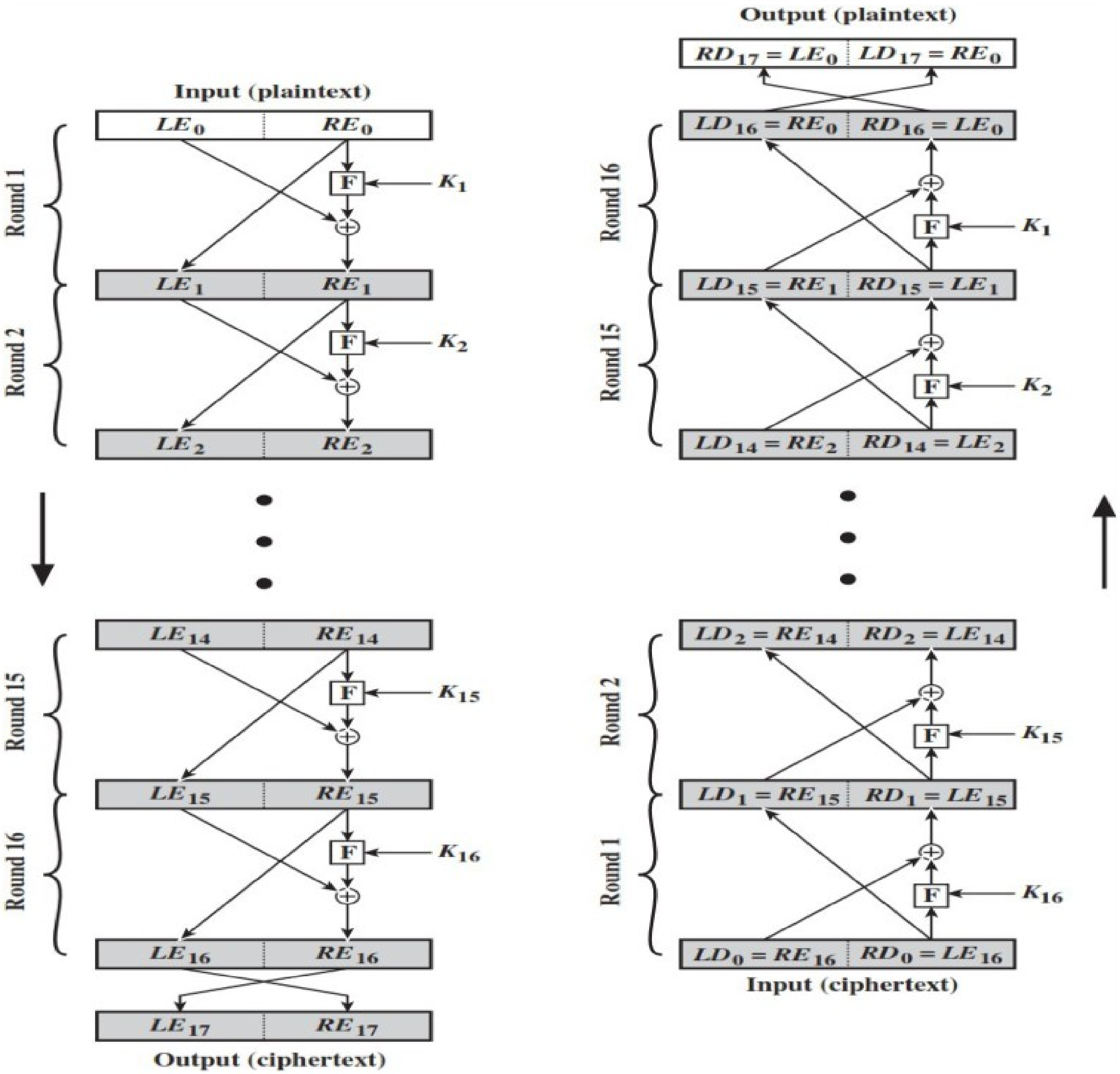
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

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

Block Cipher Principle – Fiestel Structure

1. **Block size:** Common block size of 64-bit. However, the new algorithms uses a 128-bit, 256-bit block size.
2. **Key size:** Key sizes of 64 bits or less are now widely considered to be
   insufficient, and 128 bits has become a common size.
3. **Number of rounds**: A typical size is 16 rounds.
4. **Round function F:** This phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions. Again, greater complexity generally means greater resistance to cryptanalysis.
5. **Subkey generation algorithm:** For each of the sixteen rounds, a different subkey (Ki) derived from main key by the combination of a left circular shift and a permutation. Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

Block Cipher Principle – Fiestel Structure



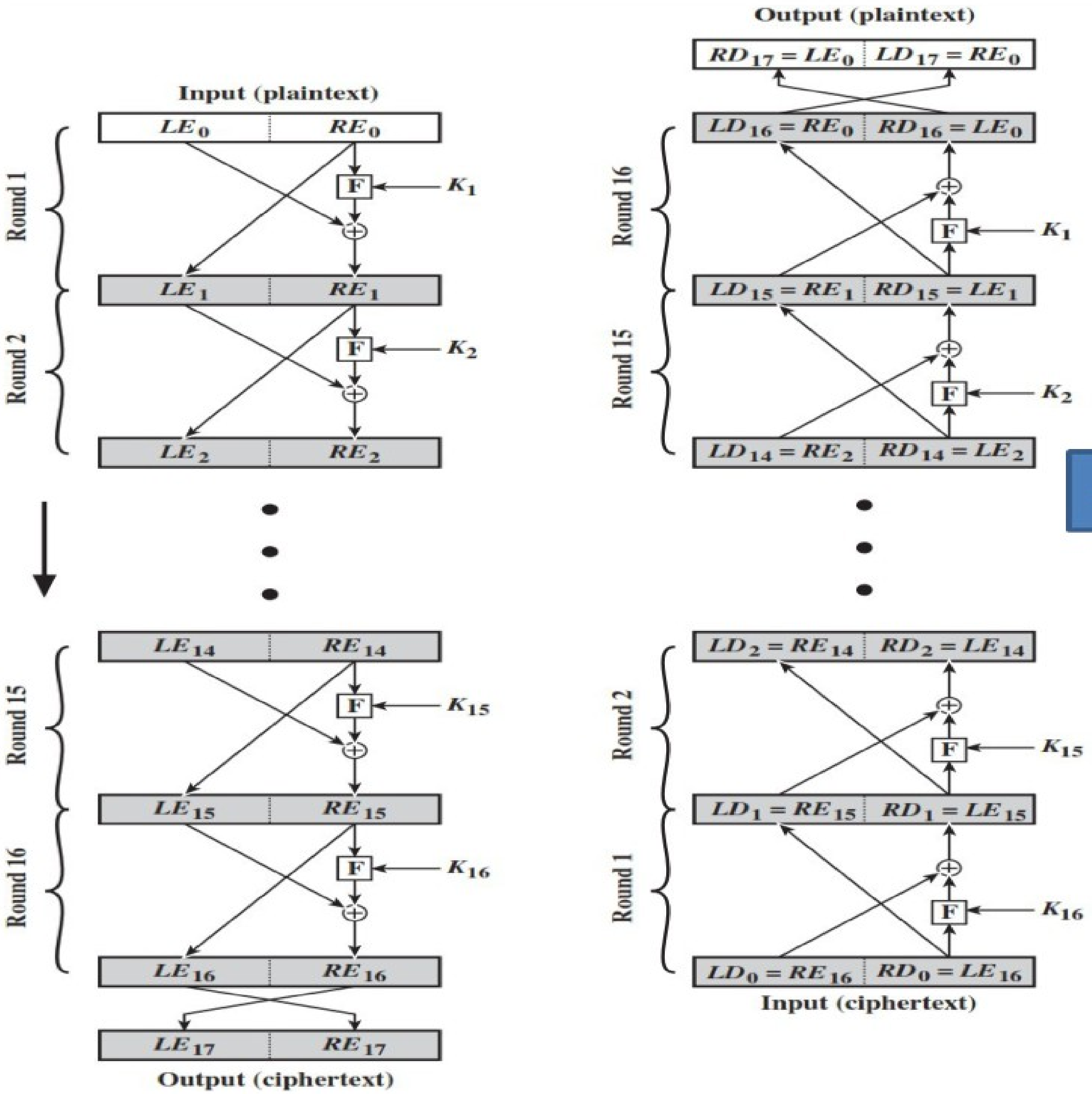
Prove that o/p of first round of Decryption is equal to 32-bit swap o i/p of 16th round of Encryption
LD1=RE15 & RD1=LE15

On Encryption Side:

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

Block Cipher Principle – Fiestel Structure



On Decryption Side:

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \oplus F(RD_0, K_{16})$$

$$= RE_{16} \oplus F(RE_{15}, K_{16})$$

$$= [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16})$$

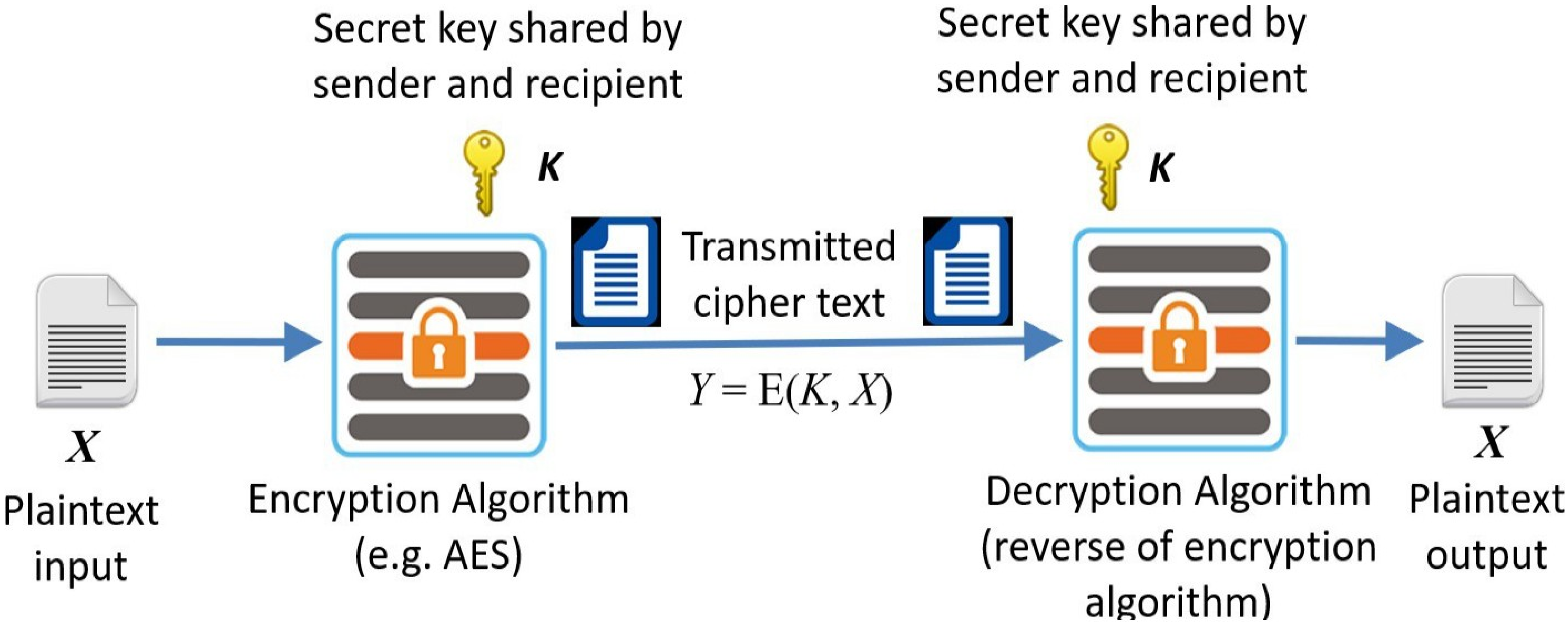
Thus,

$$LD_1 = RE_{15} \;\&\; RD_1 = LE_{15}$$

XOR Associativity Property

$$\because [A \oplus B] \oplus C = A \oplus [B \oplus C]$$

Symmetric Cipher Model



Stream cipher and Block Cipher:

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Examples:

Autokeyed Vigenère cipher

A5/1

RC4

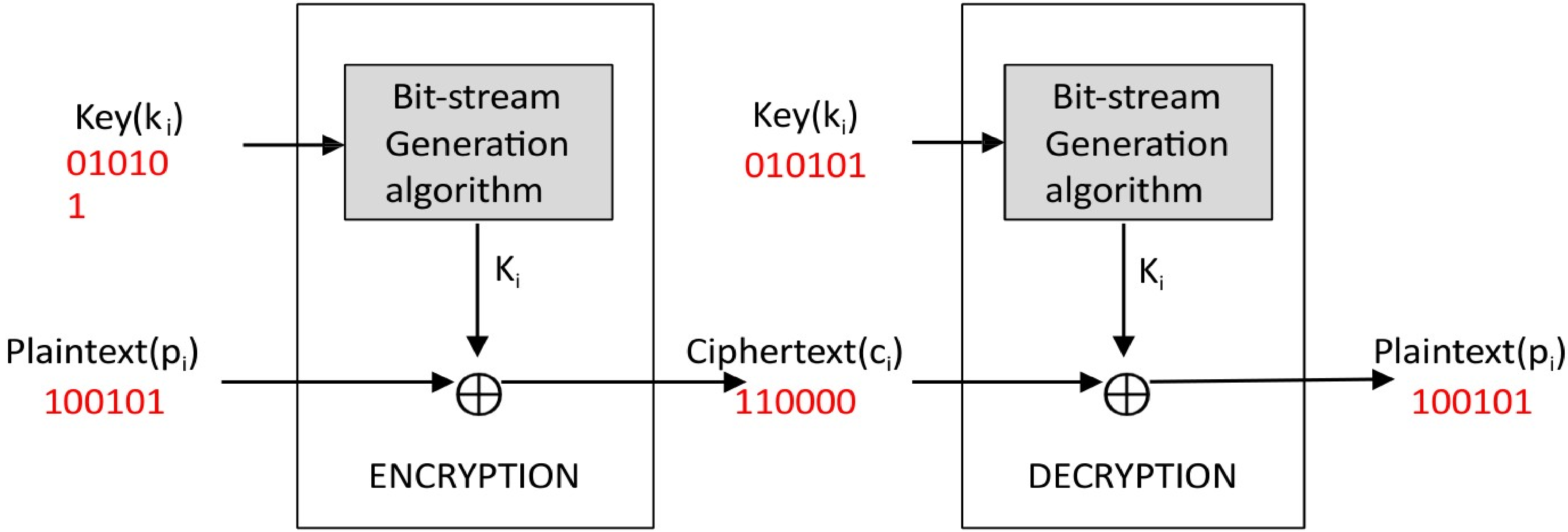
Vern

am

ciph

er.

Stream cipher and Block Cipher:



Stream cipher and Block Cipher:

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used.

Examples:

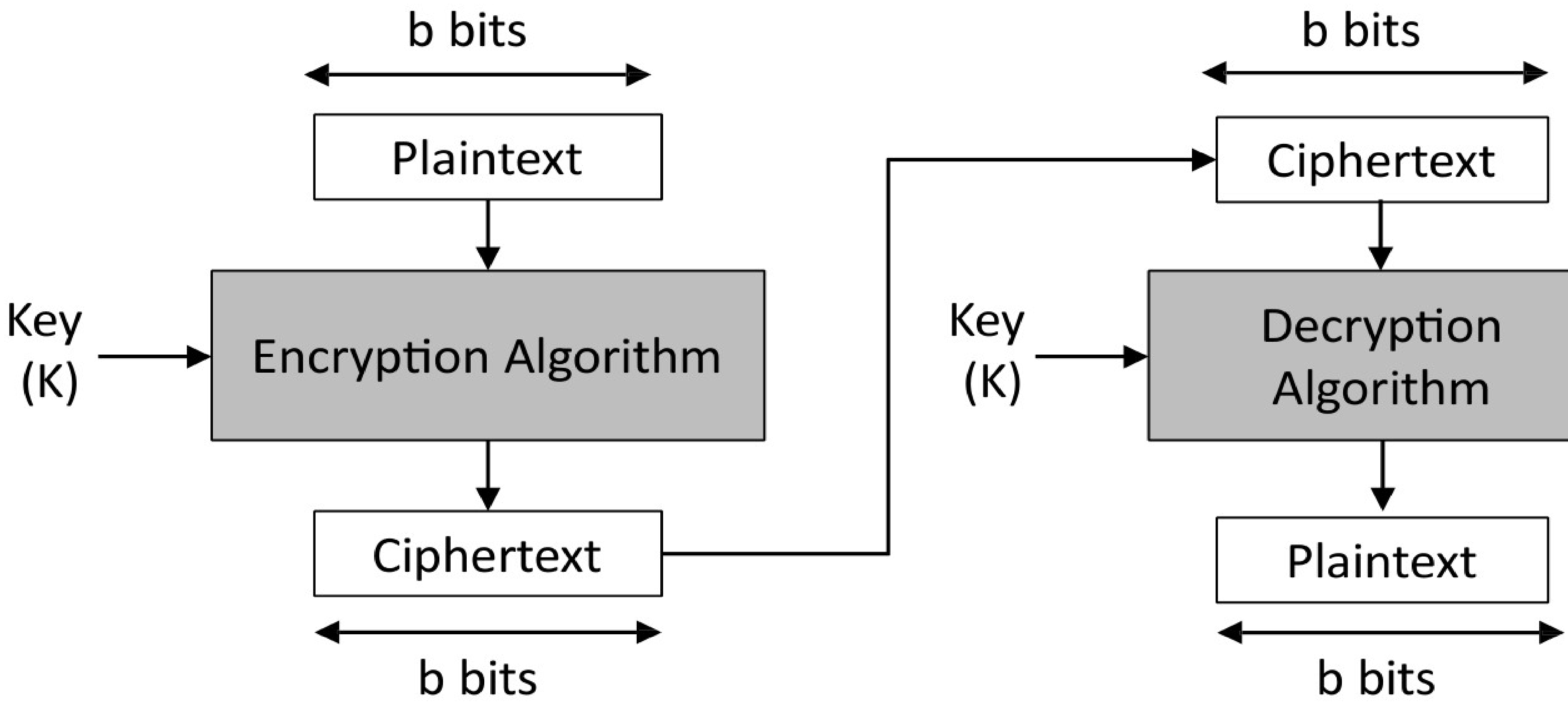
Feistel cipher

DES

Triple DES

AES

Stream cipher and Block Cipher:



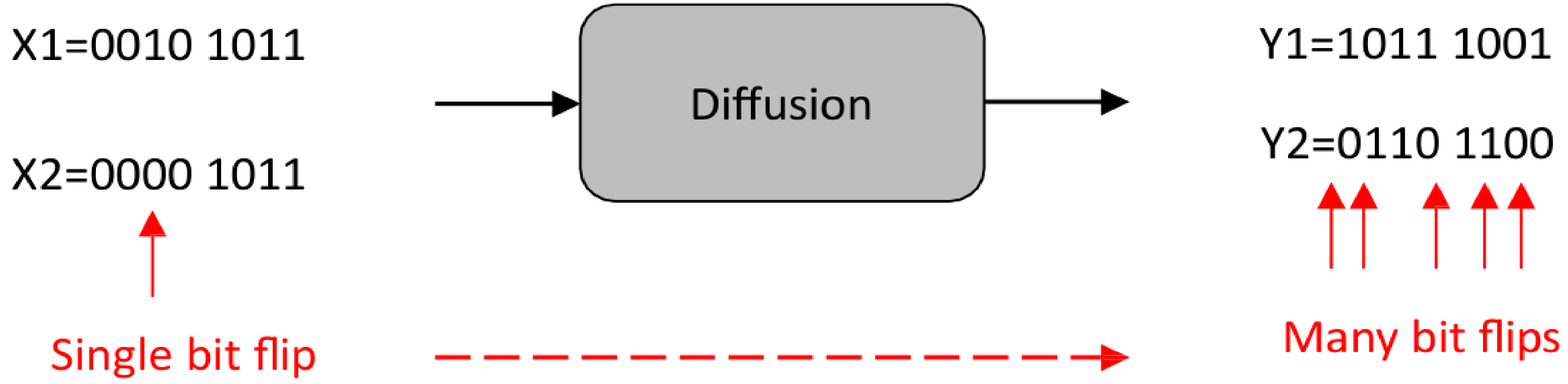
Confusion & Diffusion:

Confusion

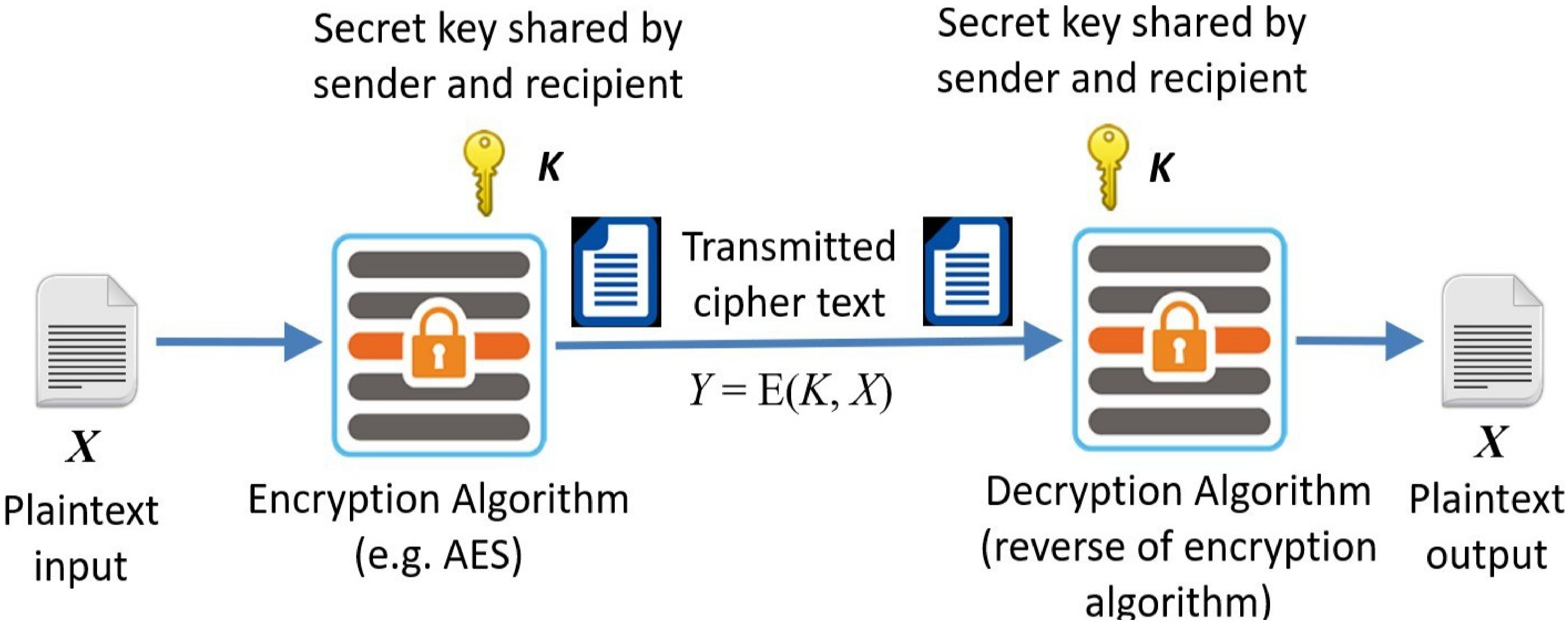
- Confusion hides the relationship between the cipher text and the key.
- This is achieved by the use of a complex substitution algorithm.

Diffusion

- Diffusion hides the relationship between the cipher text and the plaintext.
- This is achieved by changing one plaintext digit which affect the value of many cipher text digits.

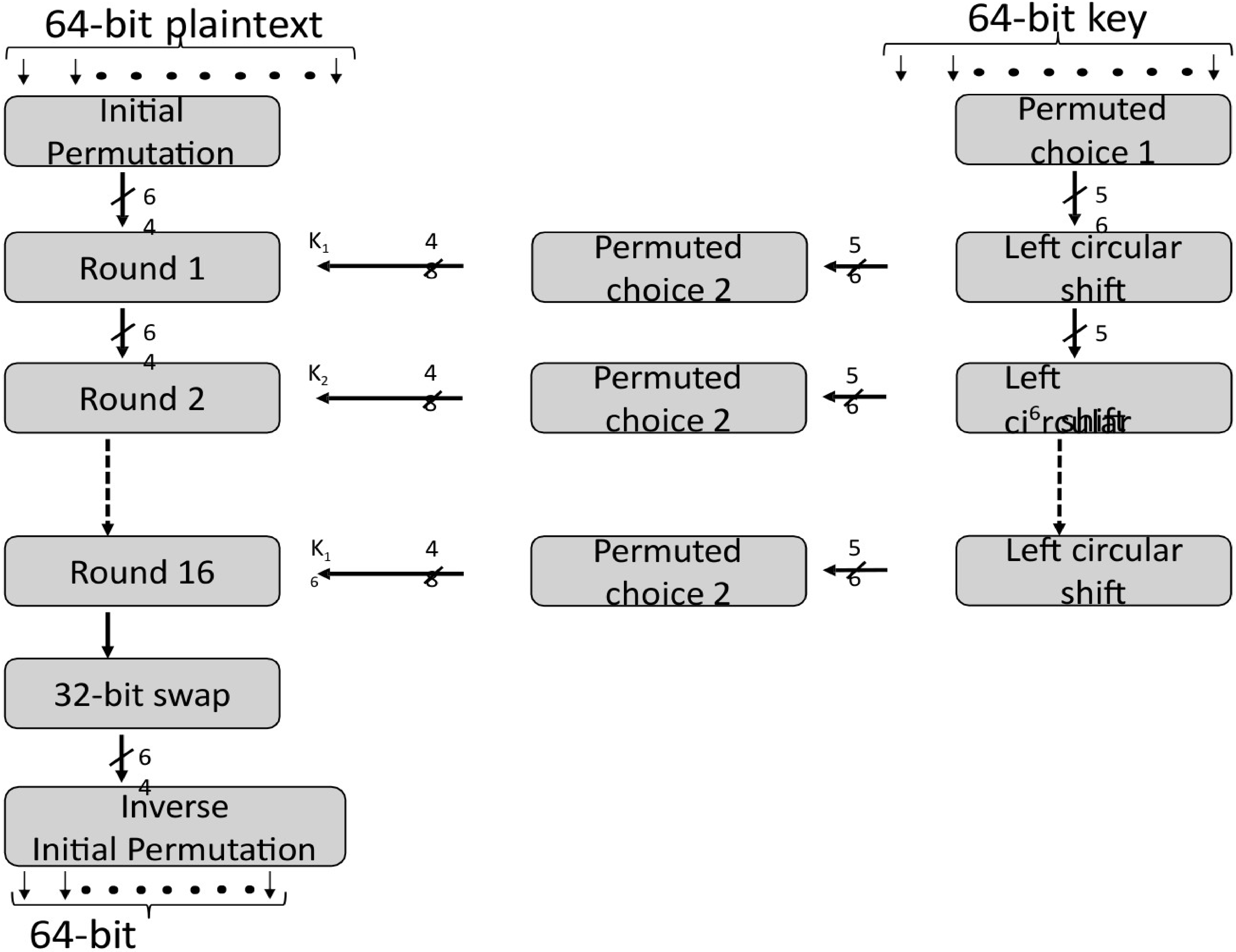


Symmetric Cipher Model



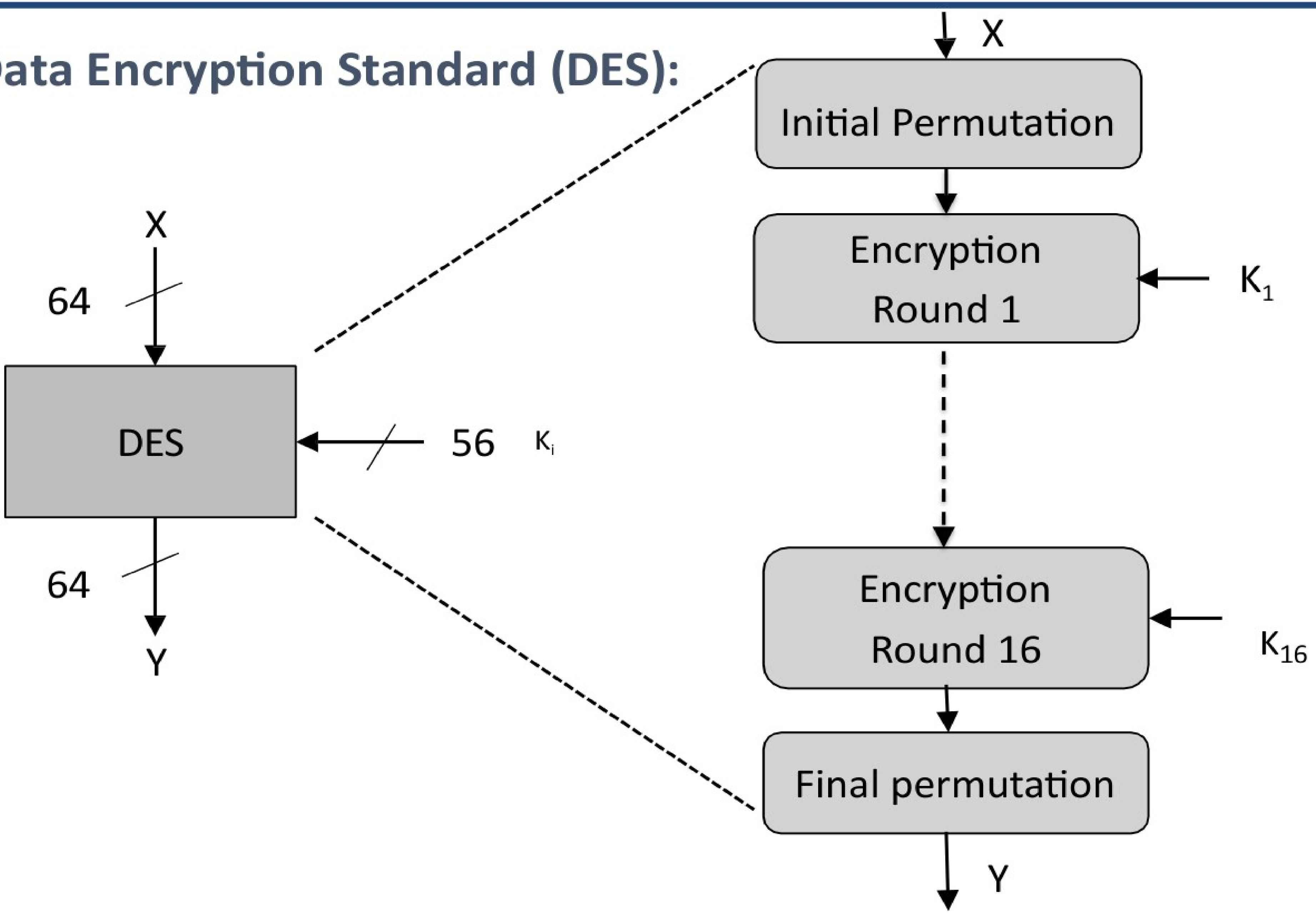
Data Encryption Standard (DES):

Type: Block Cipher
Block Size : 64-bit
Key Size: 64-bit,
with only 56-bit
effective
Number of
Rounds: 16

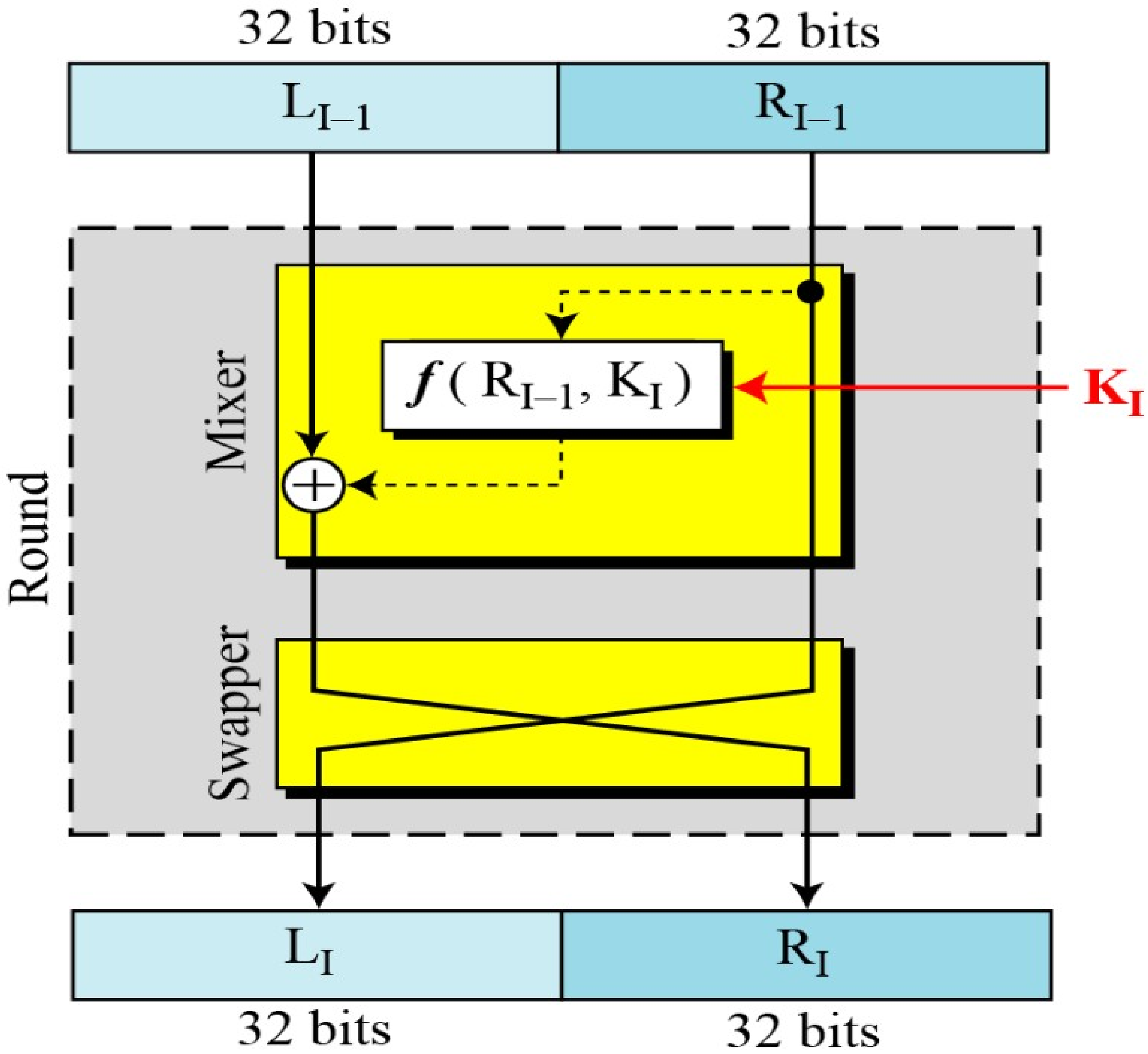


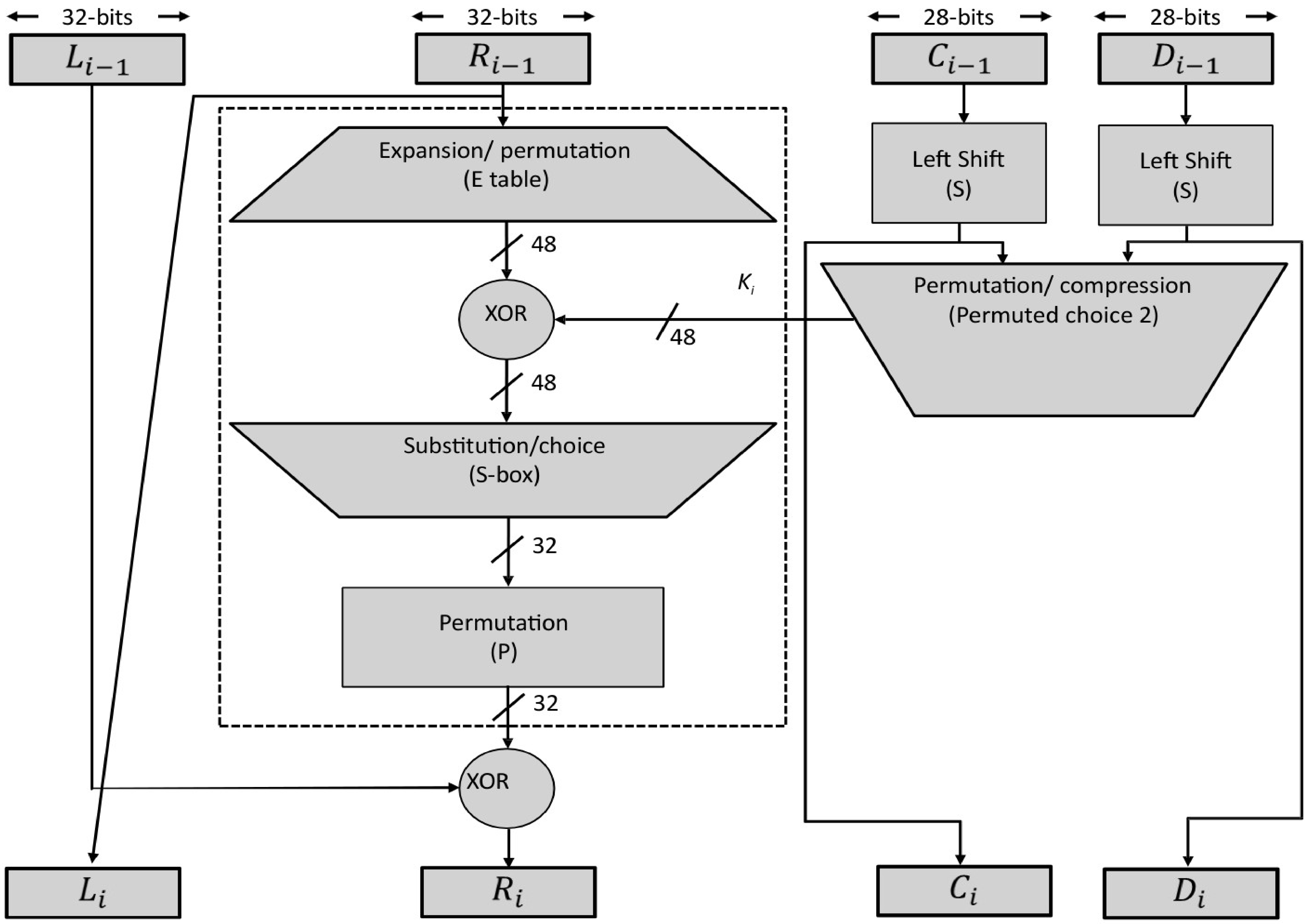
64-bit plaintext
64-bit key
Initial Permutation
Permuted choice 1
64
56
Round 1
K_1
48
Permuted choice 2
56
Left circular shift
Round 2
K_2
Round 16
K_{16}
32-bit swap
Inverse Initial Permutation
64-bit

Data Encryption Standard (DES):



Data Encryption Standard (DES) – Single round of DES:





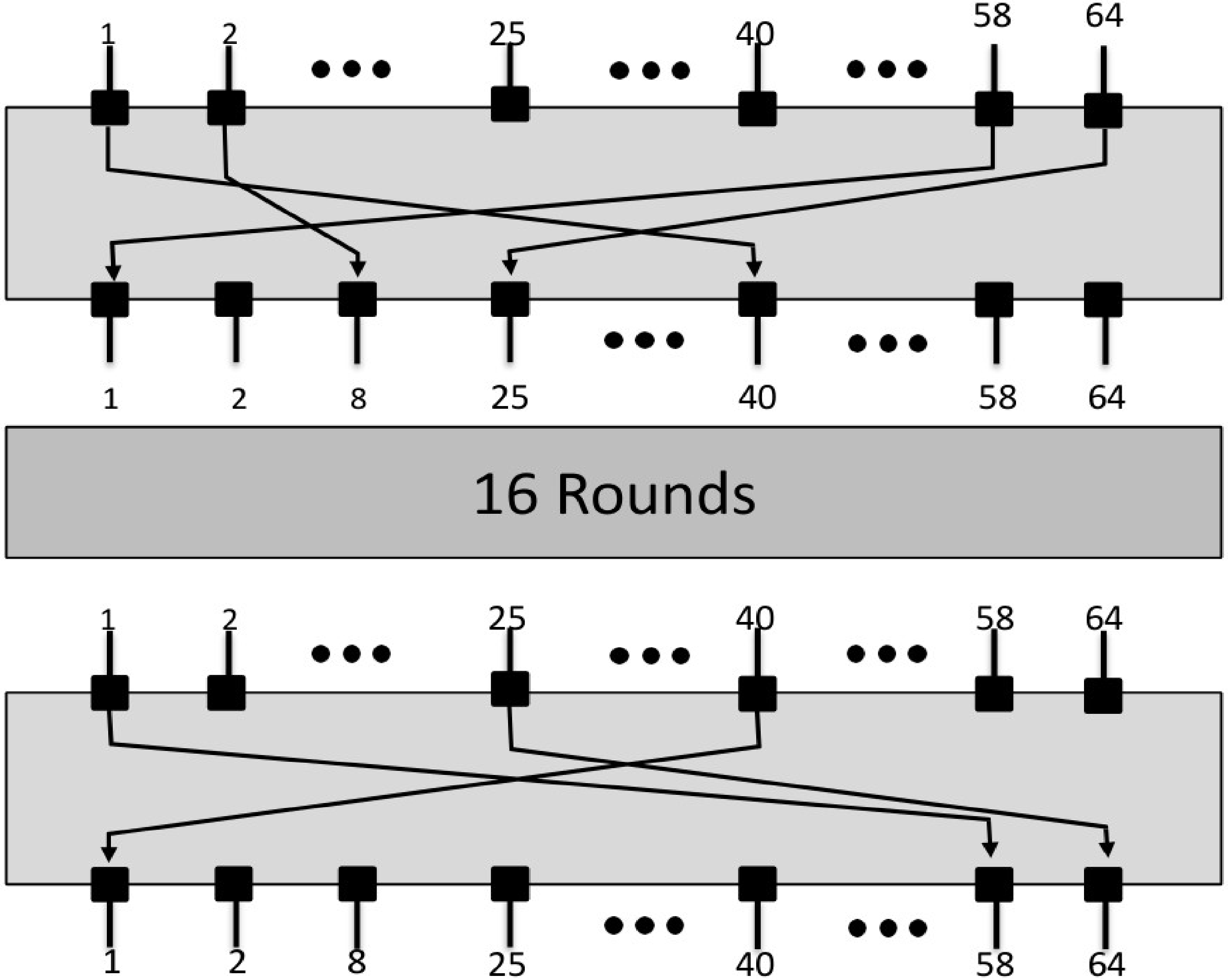
32-bits
32-bits
28-bits
28-bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/ permutation
(E table)
48
XOR
48
Substitution/choice
(S-box)
32
Permutation
(P)
32
XOR
K_i
48
Left Shift
(S)
Left Shift
(S)
Permutation/ compression
(Permuted choice 2)
L_i
R_i
C_i
D_i

Data Encryption Standard (DES):

1. Initial permutation: First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
2. The F function: This phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.
3. Swap: L and R swapped again at the end of the cipher, i.e., after round 16 followed by a final permutation.
4. Inverse (Final) permutation: It is the inverse of the initial permutation.
5. Subkey generation: For each of the sixteen rounds, a different subkey (Ki) derived from main key by the combination of a left circular shift and a permutation.

Data Encryption Standard (DES): - Initial Permutation

The initial permutation of the DES algorithm changes the order of the plaintext prior to the first round of encryption



The final permutation occurs after the sixteen rounds of DES are completed. It is the inverse of the initial permutation.

Data Encryption Standard (DES): 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

Data Encryption Standard (DES): The f Function

1. Main operation of DES

- f-function inputs:

  Ri-1 and round key *ki*

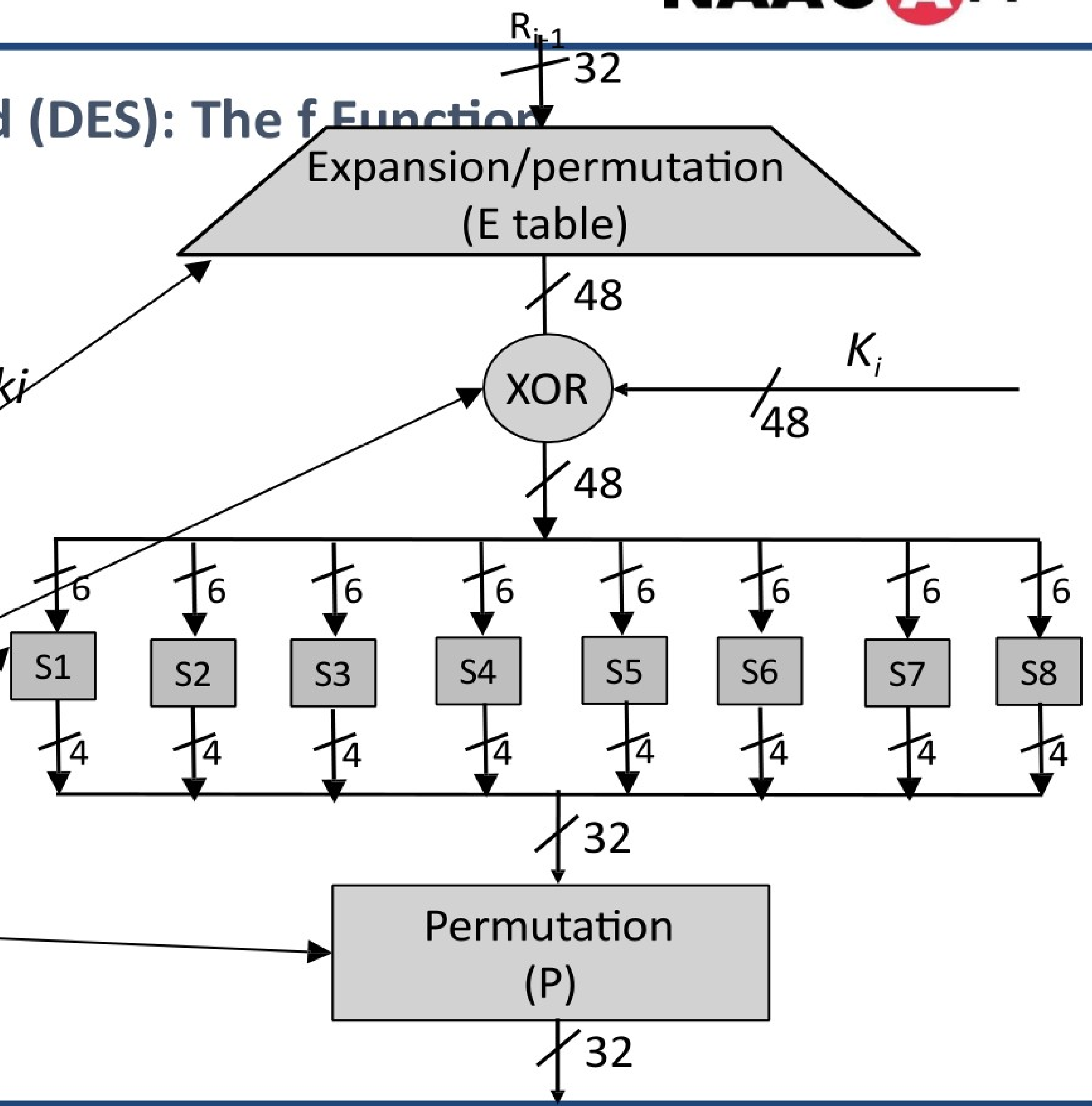
- **4 Steps**:

1. Expansion E

2. XOR with round key

3. S-box substitution

4. Permutation

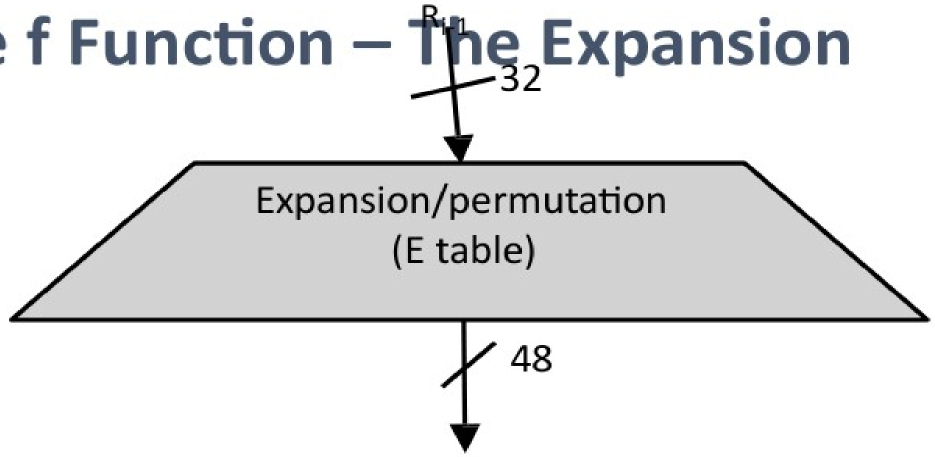


Data Encryption Standard (DES): The f Function – The Expansion Function

Main purpose: **Increases diffusion**

Since Ri-1 is a 32-bit input and Ki is a 48-bit key, we first need to expand Ri-1 to 48 bits.

Input: (8 blocks, each of them consisting 4 bits) - 32 bits
Output: (8 blocks, each of them consisting 6 bits) – 48 bits



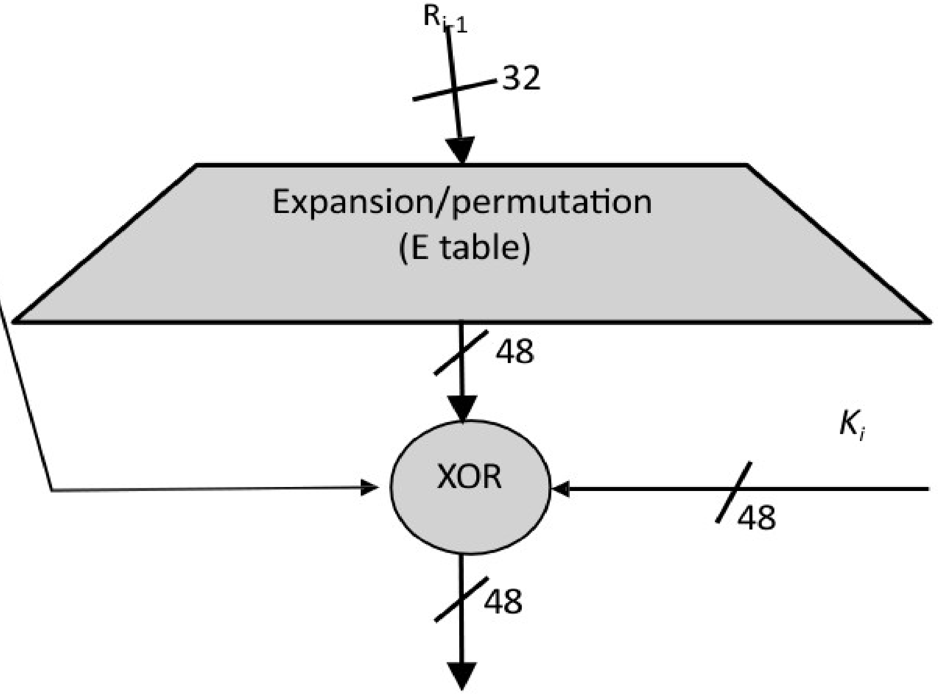
Expansion Table E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Data Encryption Standard (DES): XOR round Key

XOR Round Key

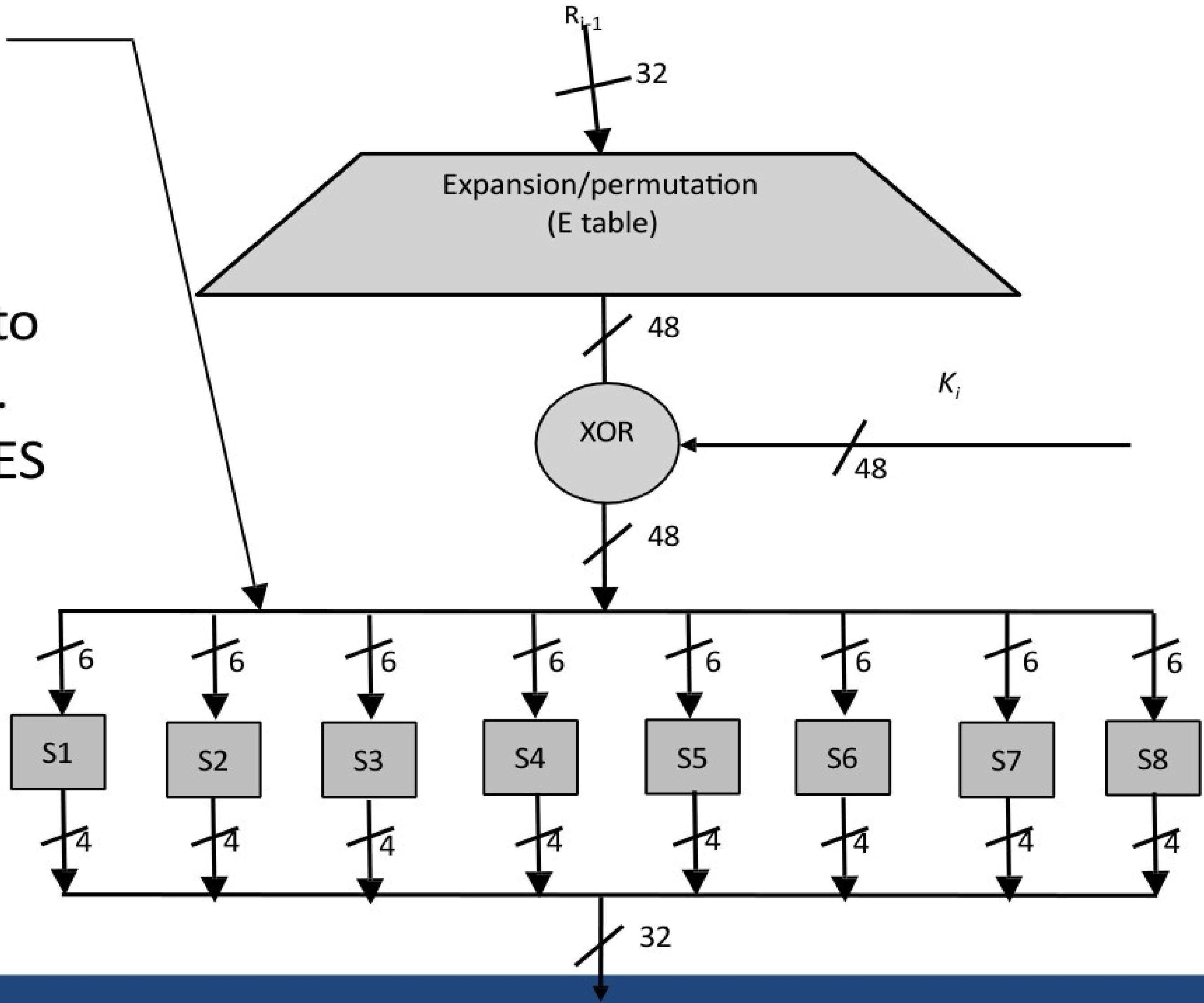
After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.

Note that both the right section and the key are 48-bits in length now.



Data Encryption Standard (DES): S-Box substitution

- Eight substitution tables.
- 6 bits of input
- 4 bits of output.
- Convert 48 bits to 32 bits
- Non-linear and resistant to differential cryptanalysis.
- Crucial element for DES security!
- Introduces confusion.



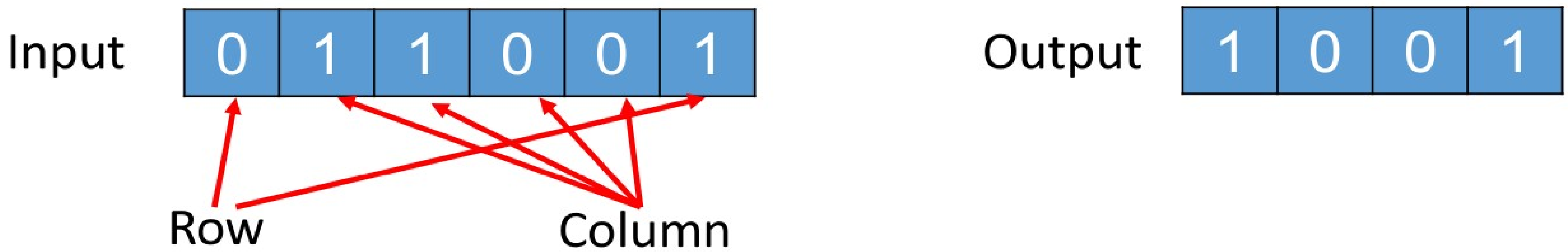
Data Encryption Standard (DES): S-Box substitution

The outer two bits of each group select one row of an S-box.
Inner four bits selects one column of an S-box.

	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

S-box 1

- Example:

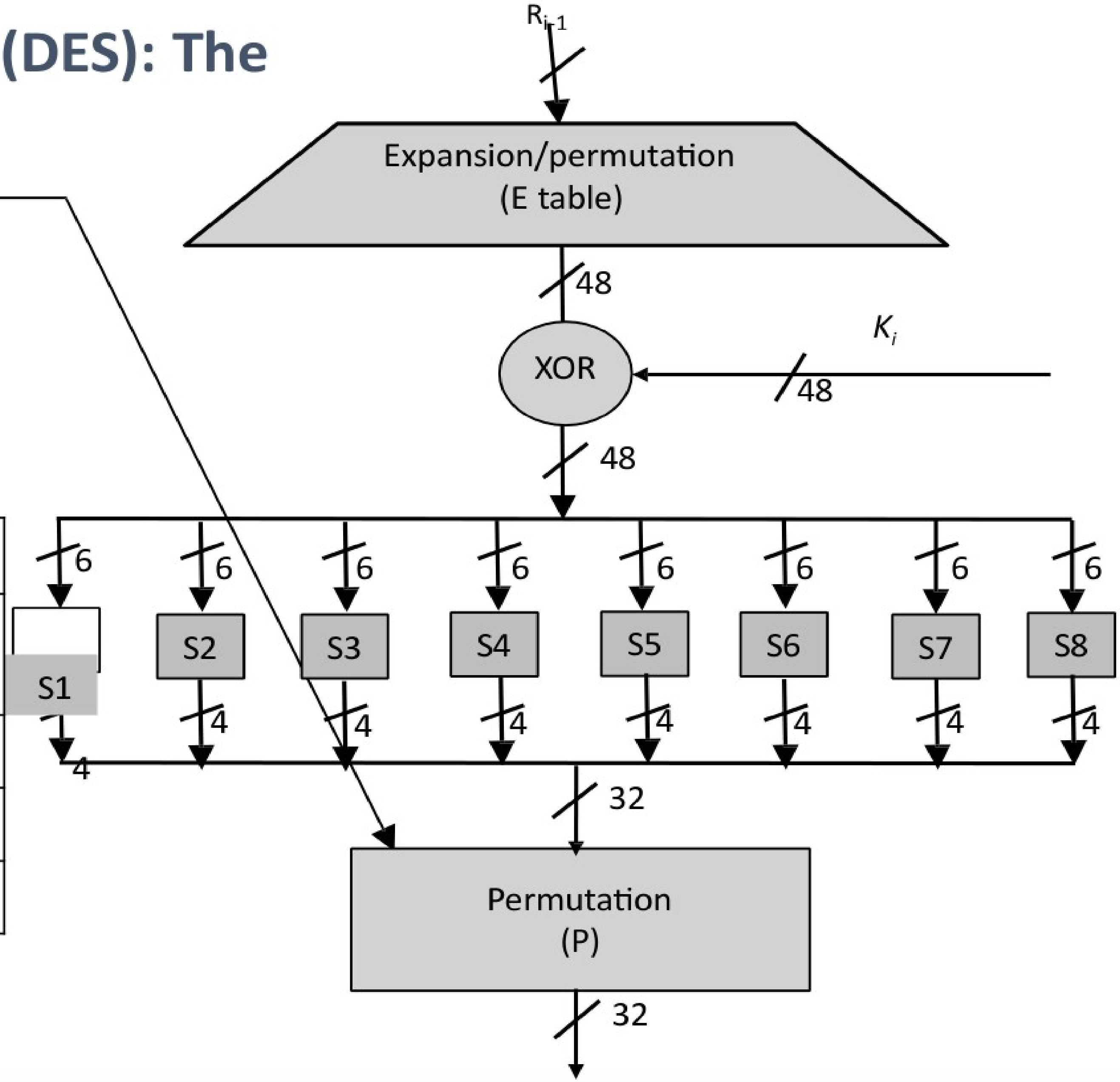


Data Encryption Standard (DES): The Permutatio3n2

Permutation P

- Bitwise permutation.
- **Introduces diffusion.**

Permutation Table P							
16	7	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25



Avalanche Effect

Desirable property of any encryption algorithm is that a change in one bit of the plaintext or of the key should produce a change in many bits of cipher text.

DES performs strong avalanche effect.

Plaintext: 0000000000000000 Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1

Plaintext: 000000000000000<u>1</u> Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3

Although the two plaintext blocks differ only in the rightmost bit, the cipher text blocks differ in 29 bits.

This means that changing approximately 1.5 % of the plaintext creates a change of approximately 45 % in the ciphertext.

Strength of DES

The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.

The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Design Principle of Block Cipher :

1. ConfusionPurpose: Make the relationship between the ciphertex and the encryption key as complex as possible.Achieved by: Using substitution operations (like S-boxes).
   Effect: Even a small change in the key or plaintext causes major,
   unpredictable changes in ciphertext.

2. DiffusionPurpose: Spread the influence of a single plaintext bit across many ciphertext bits. Achieved by: Using permutation and mixing operations.
   Effect: Changing one bit of the plaintext affects many bits of the ciphertext.

Design Principle of Block Cipher :

3.Kerckhoffs's Principle : A cipher should remain secure even if everything about the system (except the key) is public knowledge. Focuses security entirely on the secrecy of the key, not the algorithm.

4.Iterative Structure (Rounds)Instead of a single operation, block ciphers apply multiple rounds of transformations. Each round improves confusion and diffusion.
Example: AES uses 10, 12, or 14 rounds depending on key size.

5.Key Expansion The key schedule algorithm generates a different subkey for each round from the original key. Strong key expansion ensures better security.

Parul® University | NAAC GRADE A++

https://paruluniversity.ac.in/