|  |  |
| --- | --- |
|  |  |
| |  | | --- | | **Introduction & Programming with Stream cipher and Block Cipher**  **Chapter-3: Block Ciphers and the Data**  **Encryption Standard ESP8266** | | |

**Mohammad Asif**

**Assistant Professor**

**Department of Computer Science and Engineering**

|  |  |
| --- | --- |
|  |  |
|  | |

|  |  |
| --- | --- |
| |  | | --- | | **Content** | |

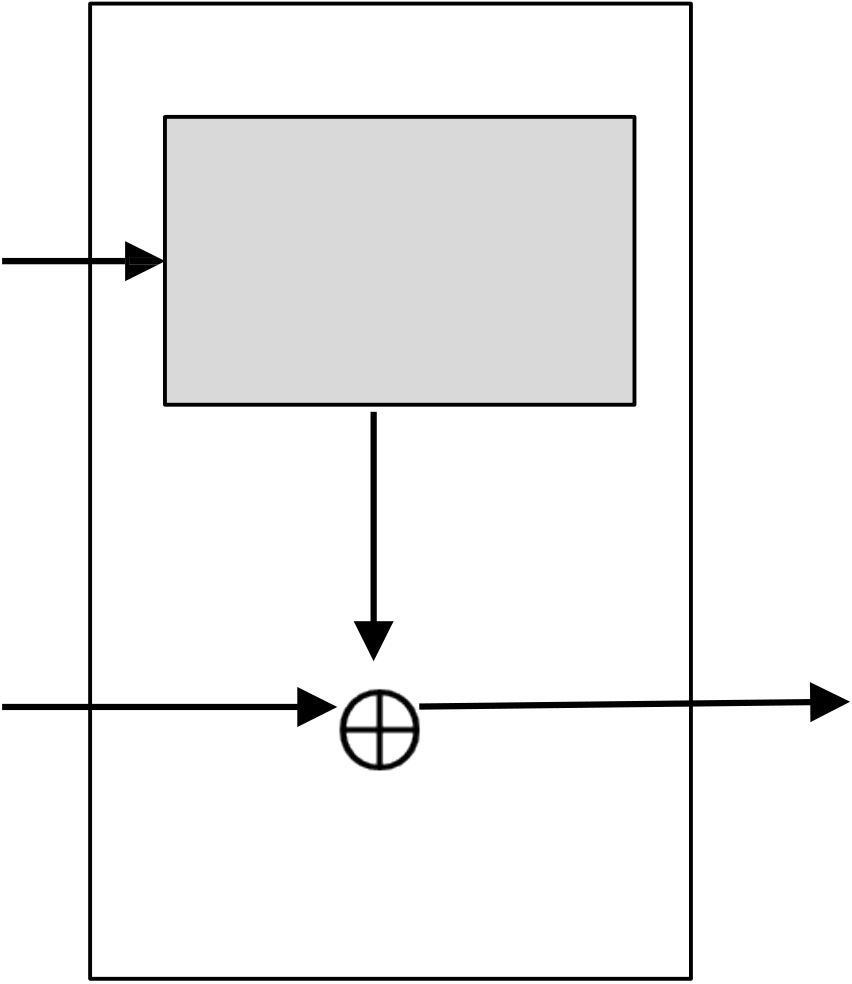
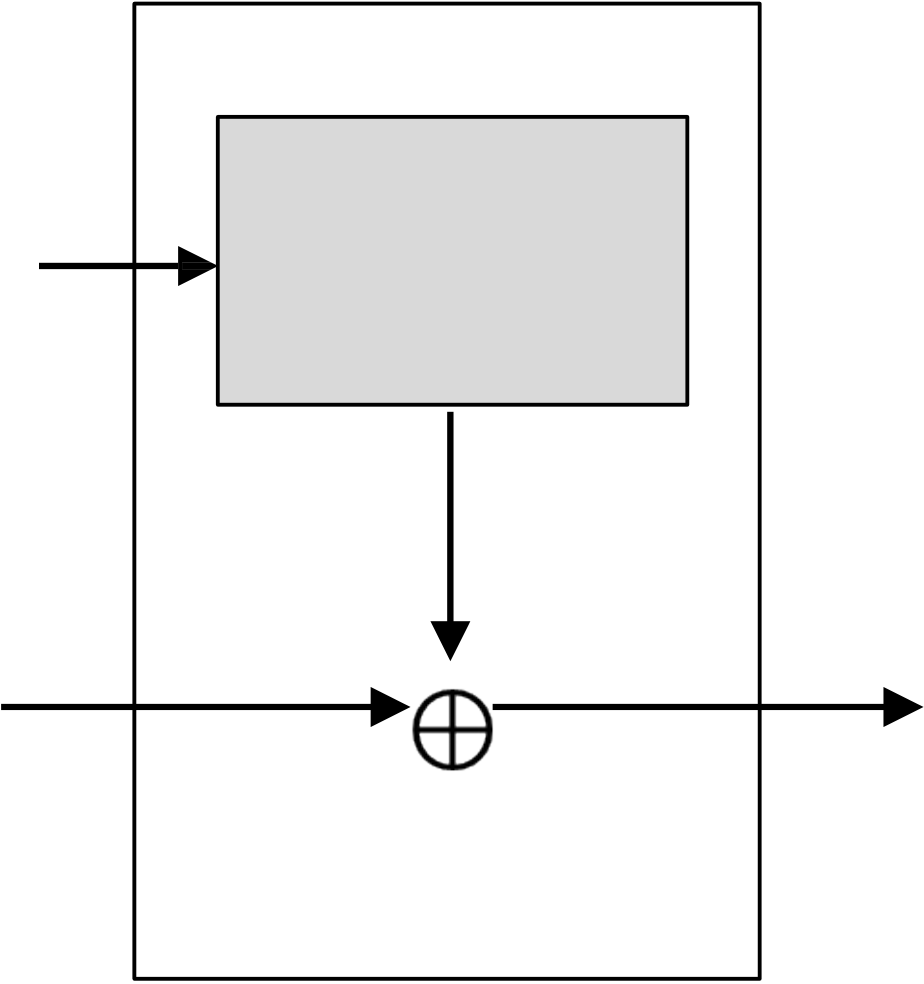
1. Stream ciphers and block ciphers   
2. Block Cipher Principles   
3. Data Stream ciphers and block ciphers 4. Confusion & Diffusion   
5. Data Encryption Standard (DES)   
6. Avalanche Effect   
7. Strength of DES   
8. Design principles of block cipher

|  |  |
| --- | --- |
|  |  |

**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:**

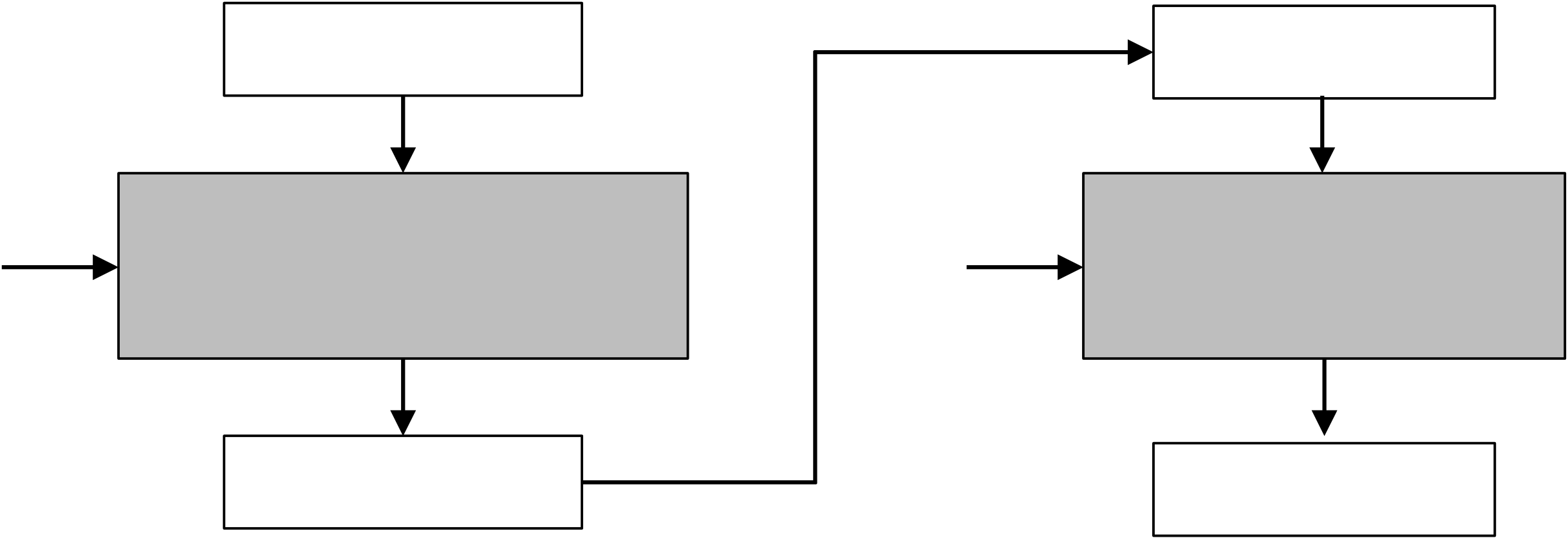
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key(k )i | Bit-stream | Key(ki) | Bit-stream | Plaintext(pi) |
| Generation | Generation |
| 01010 | 010101 |
| algorithm | algorithm |
| 1 |
| Plaintext(pi) | Ki | Ciphertext(ci) | Ki |
| 100101 | ENCRYPTION | 110000 | DECRYPTION | 100101 |

|  |  |
| --- | --- |
|  |  |

**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:**

|  |  |  |  |
| --- | --- | --- | --- |
| Key | b bits | Key | b bits |
|  |  |
| Plaintext | Ciphertext |
| Encryption Algorithm | Decryption |
| (K) | (K) |
| Algorithm |
| Ciphertext | Plaintext |
|  |  |
| b bits | b bits |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Block Cipher Principle – Fiestel Structure** | 1. | Plaintext is split into 32- |
| bit halves Li and Ri |
| 2. |
| Ri is fed into the |
| 3. | function F. |
| The output of function F |
| 4. | is then XORed with Li |
| Left and right half are |
| swapped. |
|  |
| **Li = R i – 1** |

|  |  |
| --- | --- |
|  |  |

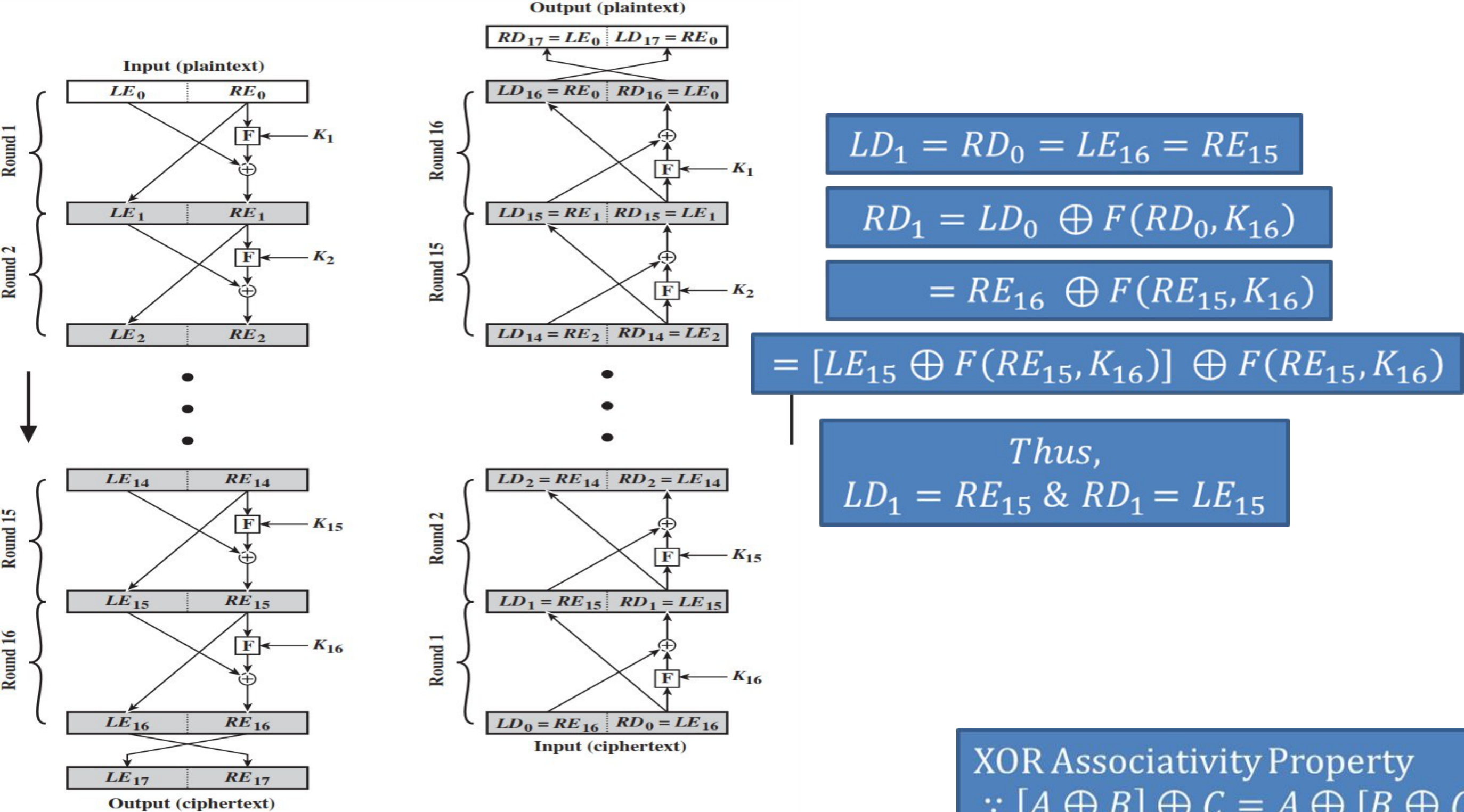
**Block Cipher Principle – Fiestel Structure**

|  |  |
| --- | --- |
| **1.**  **2.**  **3.**  **4.**  **5.** | **Block size:** Common block size of 64-bit. However, the new algorithms uses a 128-bit, 256-bit block size.  **Key size:** Key sizes of 64 bits or less are now widely considered to be  insufficient, and 128 bits has become a common size.  **Number of rounds**: A typical size is 16 rounds.  **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.  **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: |

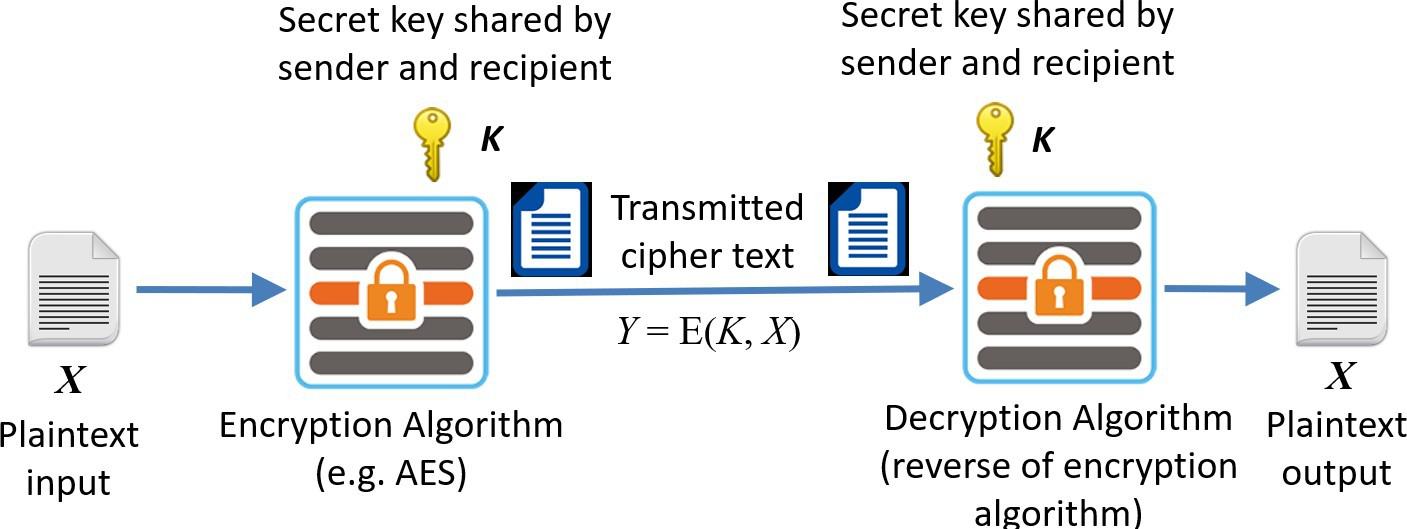


|  |  |
| --- | --- |
|  |  |

**Block Cipher Principle – Fiestel Structure**   
 On Decryption Side:

|  |  |
| --- | --- |
|  |  |

**Symmetric Cipher Model**

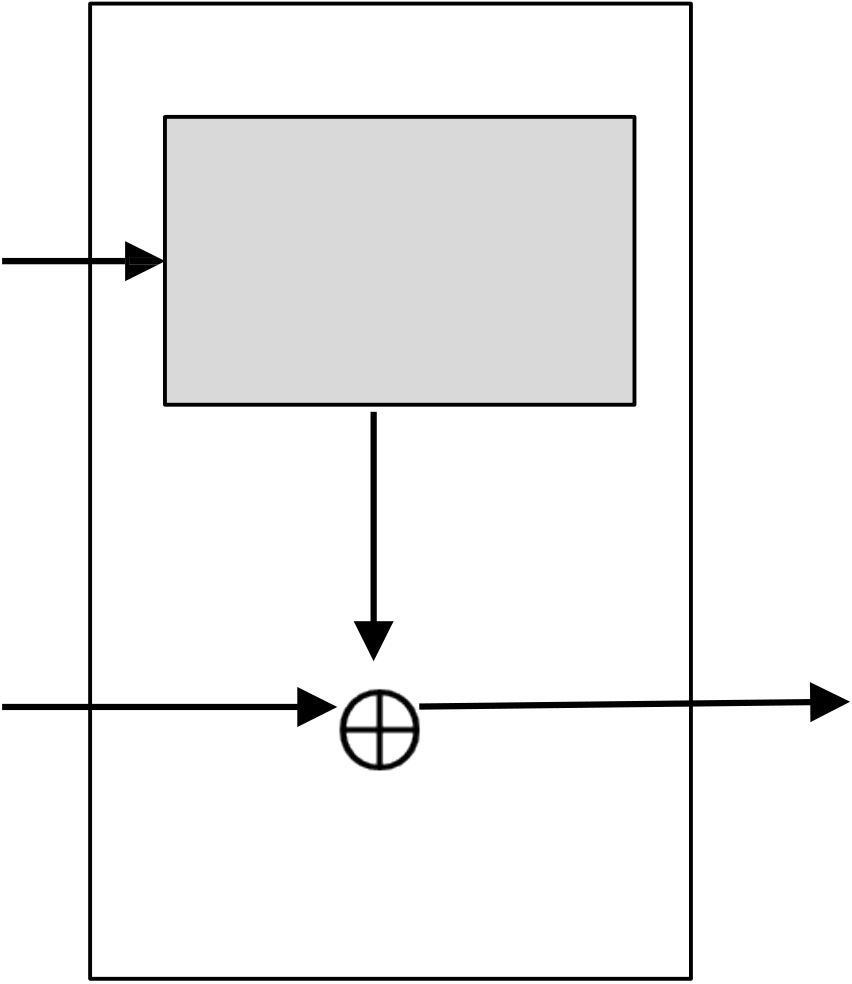
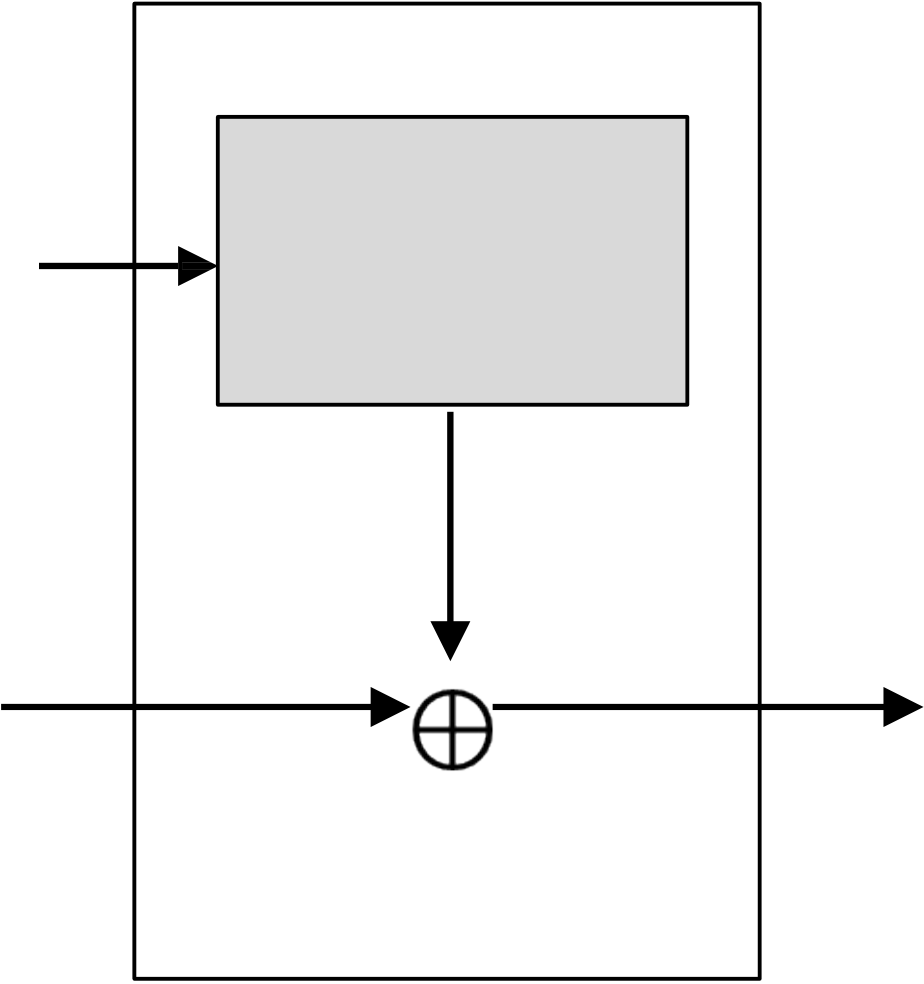


|  |  |
| --- | --- |
|  |  |

**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:**

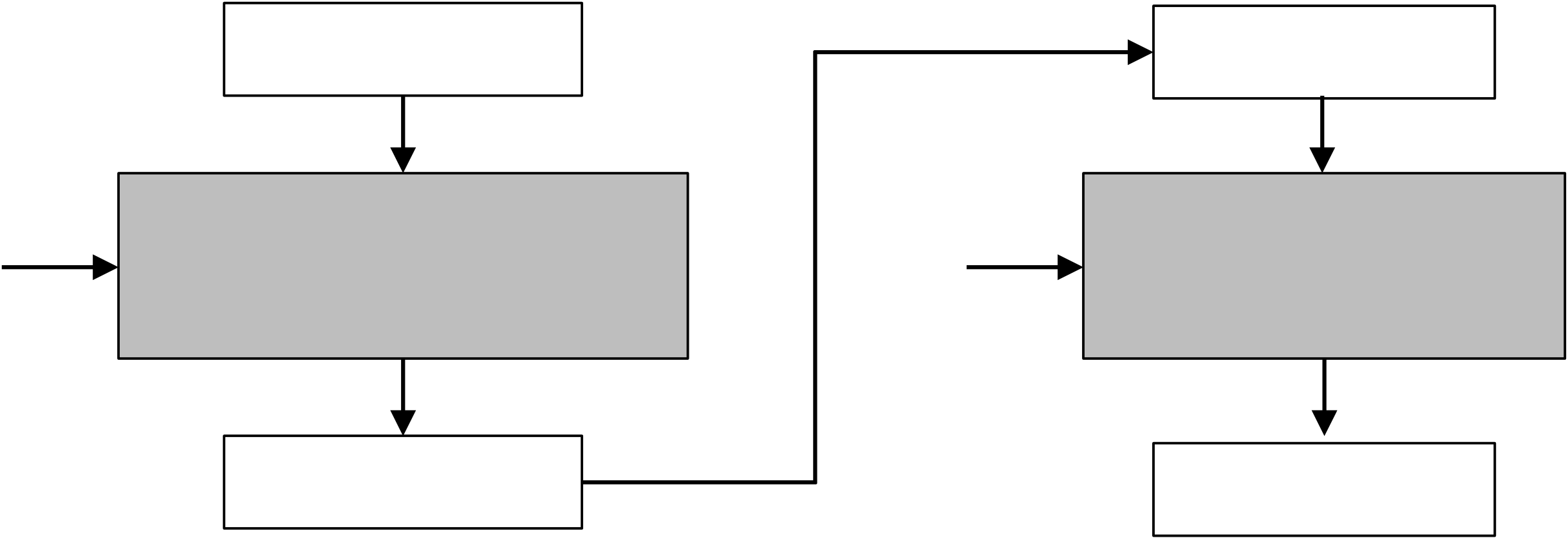
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key(k )i | Bit-stream | Key(ki) | Bit-stream | Plaintext(pi) |
| Generation | Generation |
| 01010 | 010101 |
| algorithm | algorithm |
| 1 |
| Plaintext(pi) | Ki | Ciphertext(ci) | Ki |
| 100101 | ENCRYPTION | 110000 | DECRYPTION | 100101 |

|  |  |
| --- | --- |
|  |  |

**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:**

|  |  |  |  |
| --- | --- | --- | --- |
| Key | b bits | Key | b bits |
|  |  |
| Plaintext | Ciphertext |
| Encryption Algorithm | Decryption |
| (K) | (K) |
| Algorithm |
| Ciphertext | Plaintext |
|  |  |
| b bits | b bits |



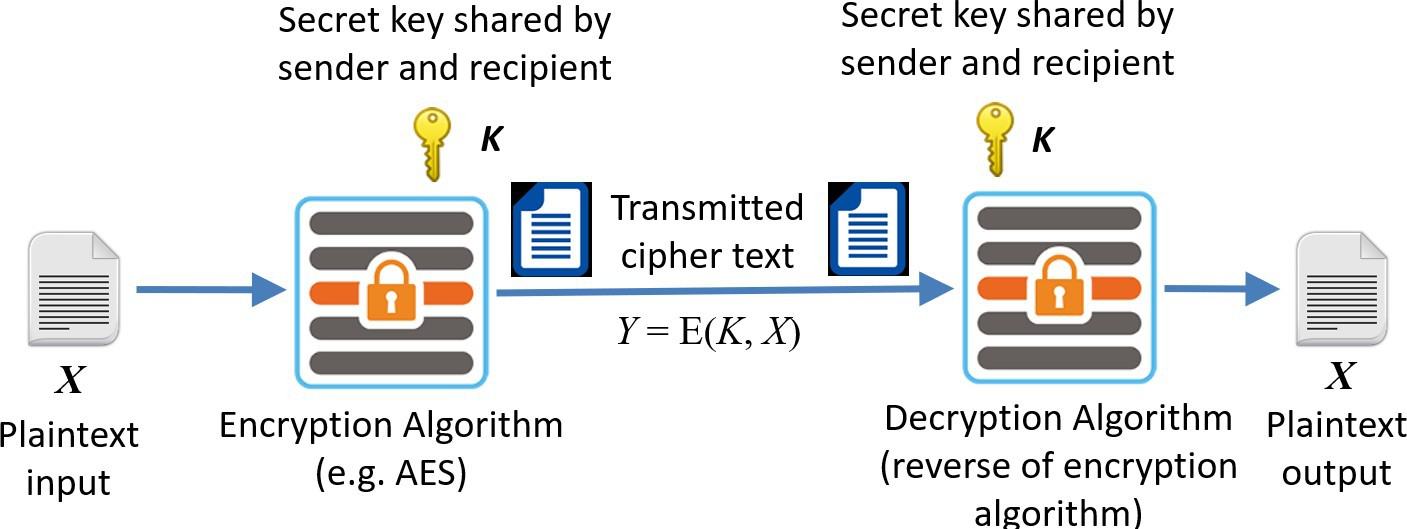
|  |  |
| --- | --- |
|  |  |

**Confusion & Diffusion:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| •  • | **Confusion** | |  | | **Diffusion** | | | | | | | |
| Confusion hides the relationship between the cipher text and the key. | | • Diffusion | | hides | | the | relationship | | |
| between | | the | cipher | | text | and | the |
| plaintext. | | | | | | | |
| This is achieved by the use of a complex substitution algorithm. | |
| • This | is | achieved | | by | changing | | one |
| plaintext digit which affect the value of | | | | | | | |
| many cipher text digits. | | | | | | | |
| X1=0010 1011 | | | Y1=1011 1001 | | | | | | | | |
| X2=0000 1011 | Diffusion | | | | | Y2=0110 1100 | | | | | |
|  | | |  | | |
|  |
| Single bit flip |  | | | | | | | Many bit flips | | | |

|  |  |
| --- | --- |
|  |  |

**Symmetric Cipher Model**

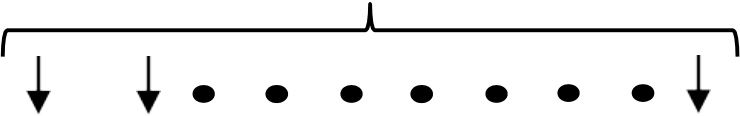
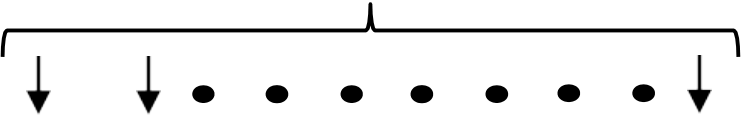
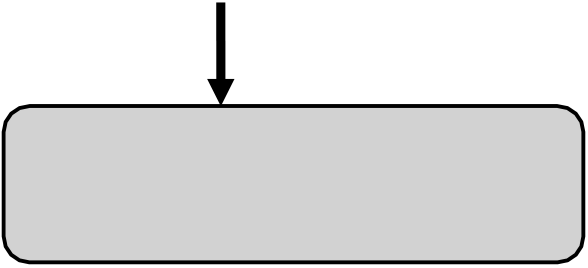
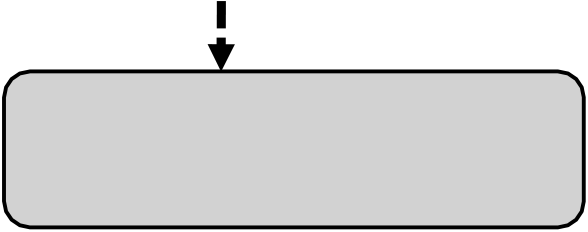
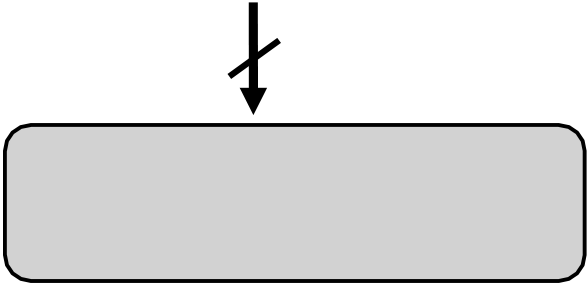
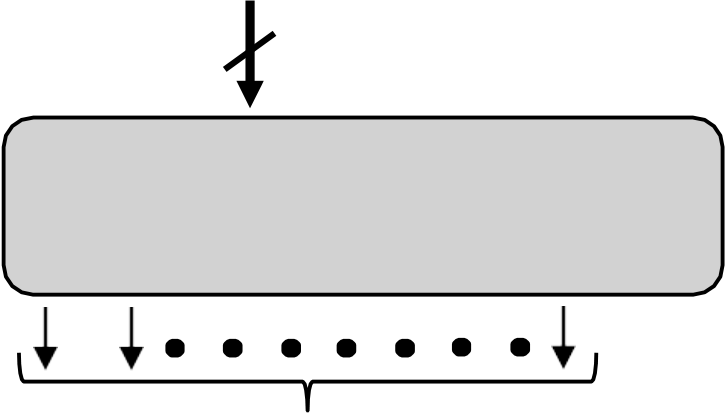
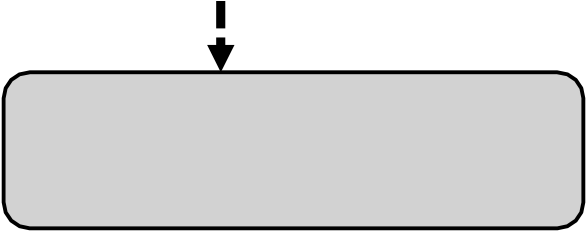
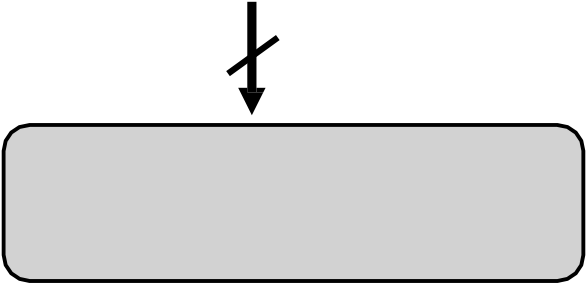
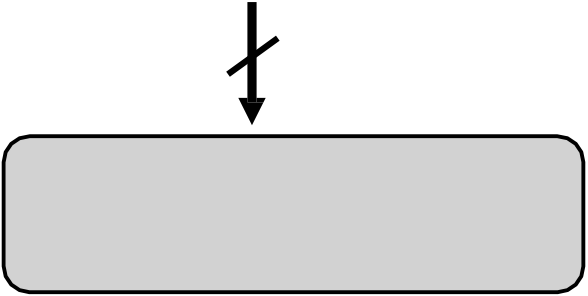


|  |  |
| --- | --- |
|  |  |

**Data Encryption Standard (DES):**

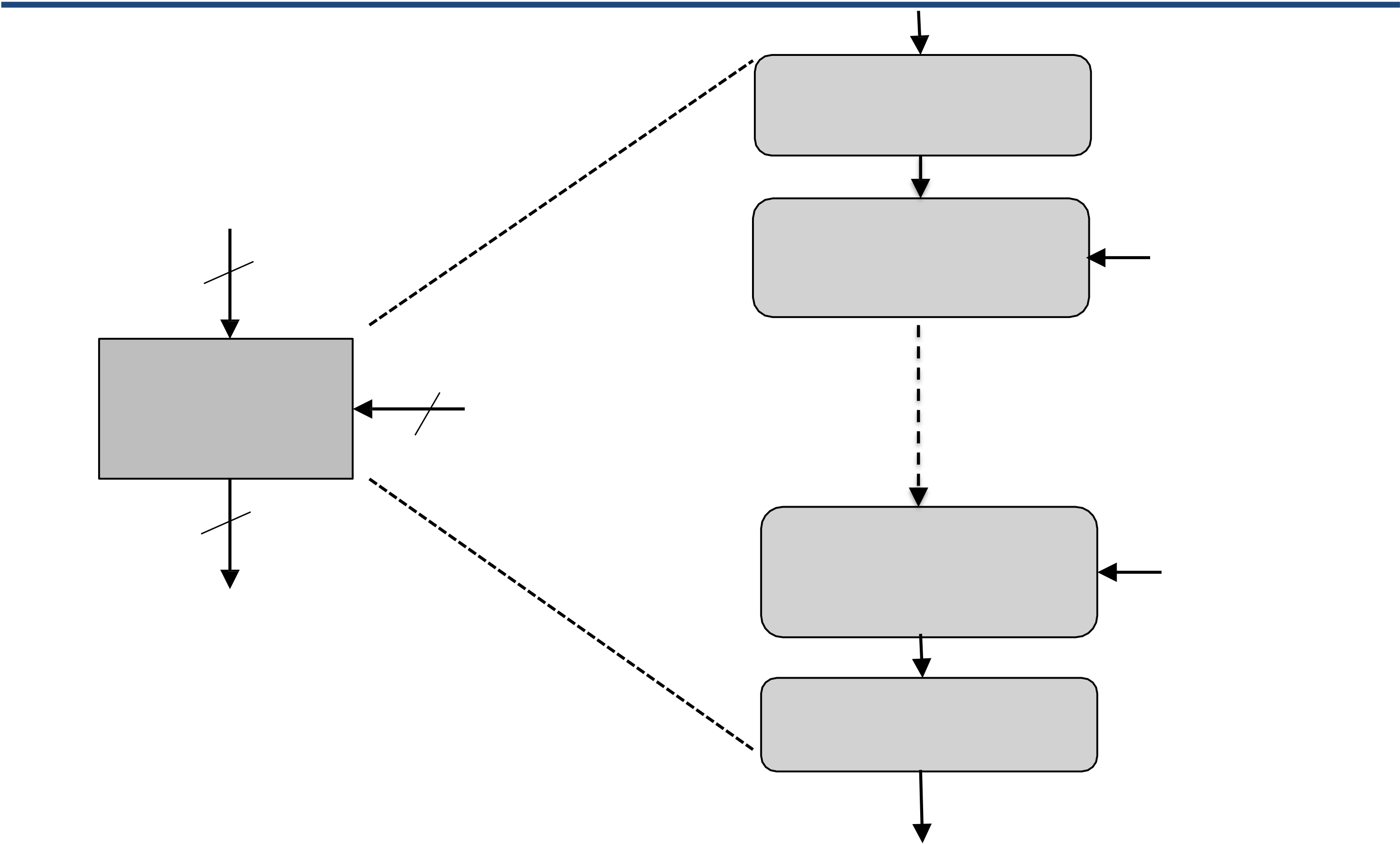
Type: Block Cipher   
Block Size : 64-bit   
Key Size: 64-bit,   
with only 56-bit   
effective   
Number of   
Rounds: 16

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 64-bit plaintext | |  |  |  | 64-bit key |
| |  |  |  | | --- | --- | --- | | |  | | --- | | Permutation |  |  | | --- | | Initial | | | |  |  |  | |  | | --- | |  |  |  | | --- | | Permuted |   choice 1 |
| 6 | | 4 | Permuted | 5 |  |
| 5  6   |  | | --- | | shift |  |  | | --- | | Left circular | |
| 4  Round 1 | K1 |
| 8 |
| 6 |
| choice 2 |
| 6 | | 4 |  | 5 | 5 |
| 4  Round 2 | K2 | Permuted | Left |
| 8 | 6 |
| choice 2 | ci6rcular |
| Round 16 | K1  6 | 4 | Permuted | 5 | Left circular |
| 8 | 6 |
| choice 2 | shift |

32-bit swap   
6

4

Inverse   
Initial Permutation   
64-bit

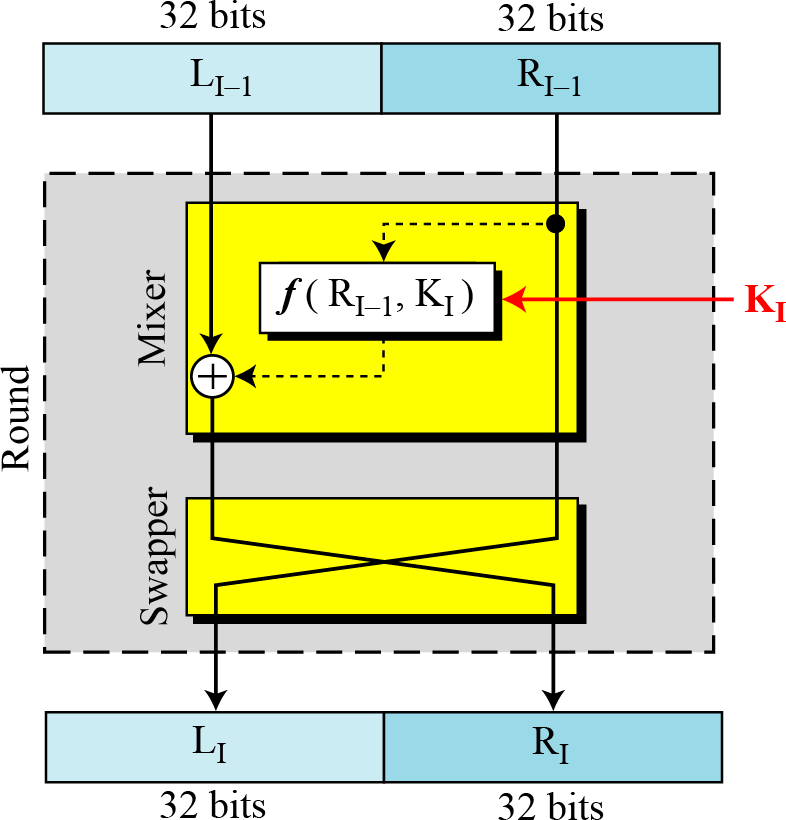


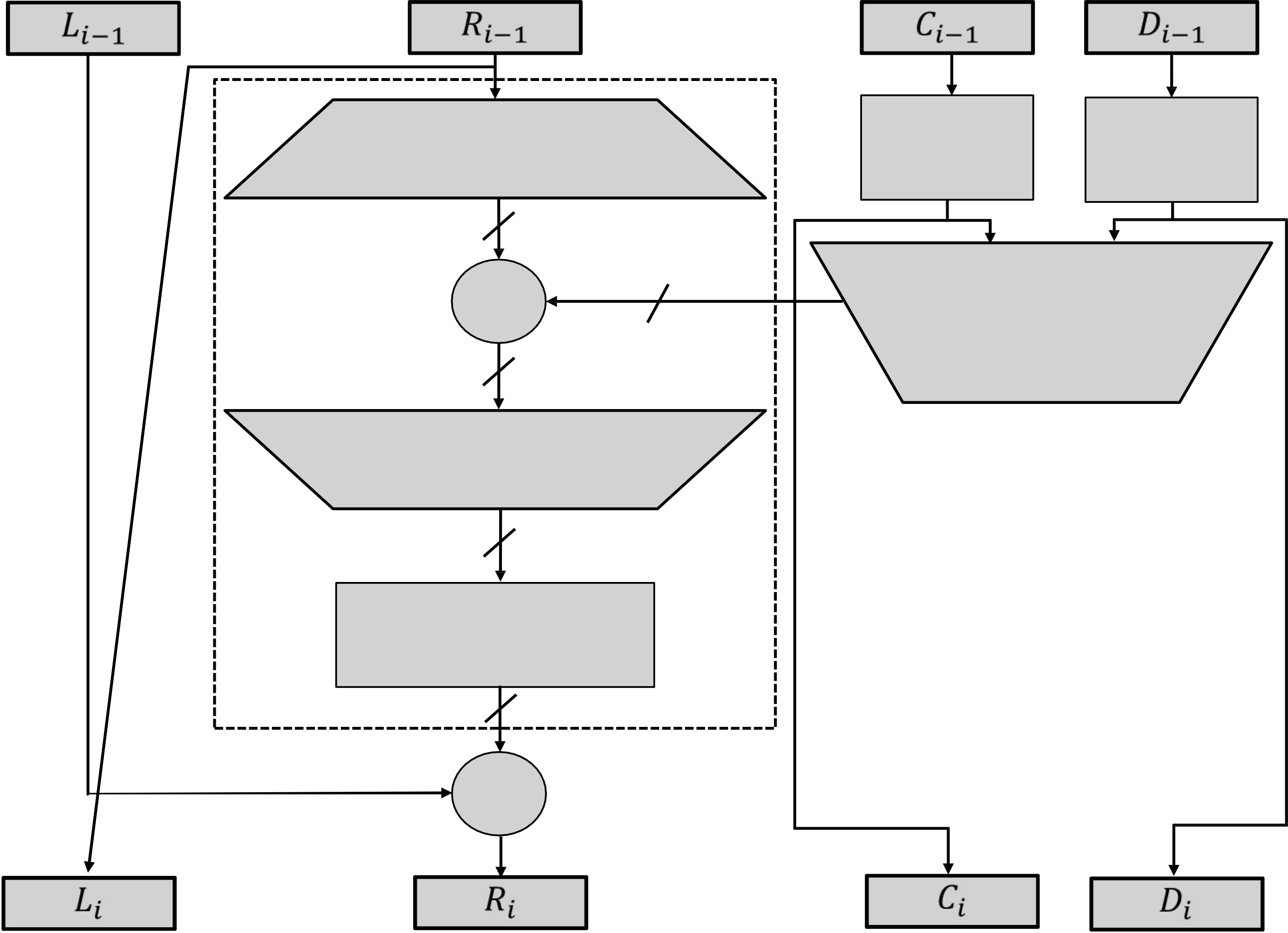
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Encryption Standard (DES):**  X  64 | | | X  Initial Permutation | |
| Encryption  Round 1 | K1 |
| DES | 56 | Ki | Encryption | |
| 64   Y | | |
| Round 16 | K16 |

Final permutation   
Y

|  |  |
| --- | --- |
|  |  |

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





|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 32-bits |  |  | 32-bits |  |  | 28-bits |  |  | 28-bits |  |
| Expansion/ permutation | | | Left Shift | Left Shift |
| (E table) | | |
| (S) | (S) |

48

|  |  |  |  |
| --- | --- | --- | --- |
| XOR | 48 | *Ki* | Permutation/ compression |
| (Permuted choice 2) |

48

Substitution/choice   
(S-box)

32

Permutation   
(P)

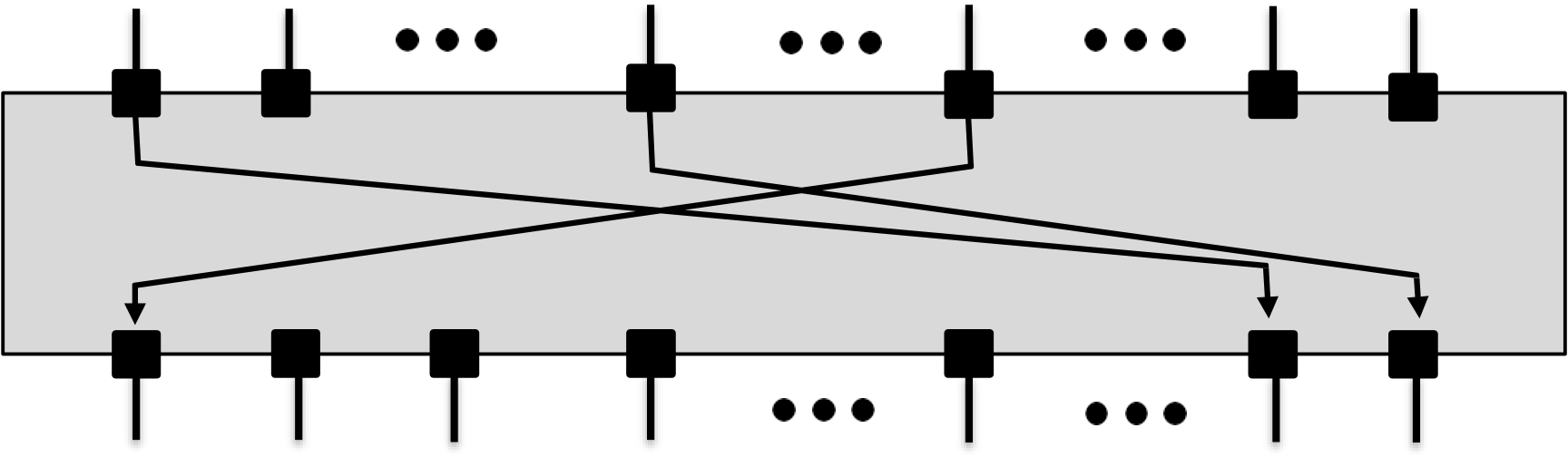
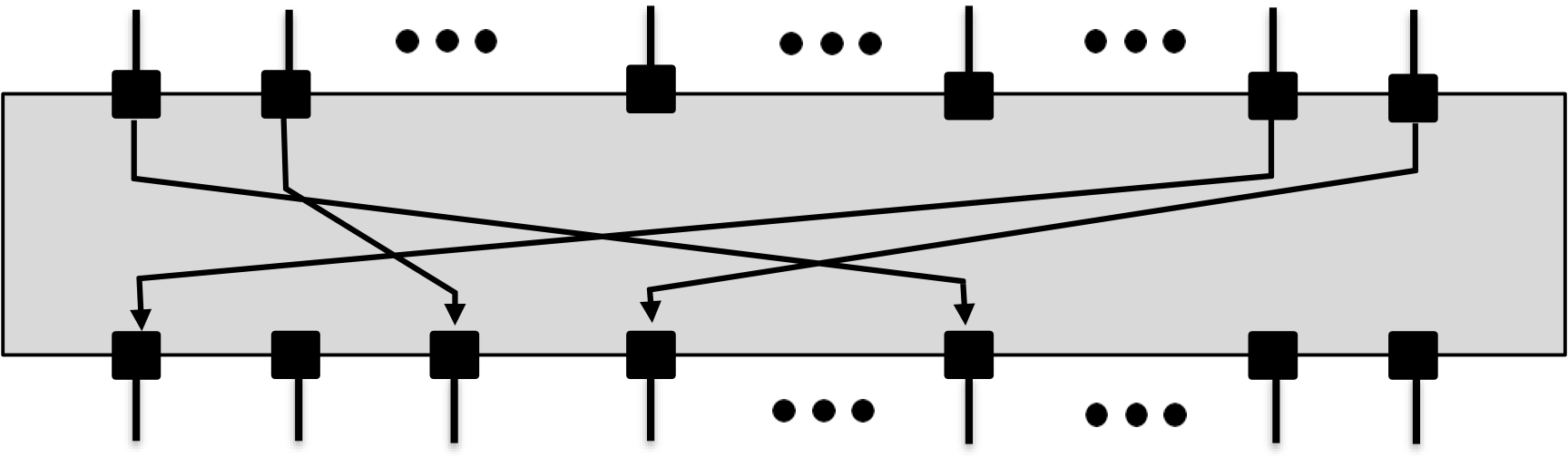
32

XOR

|  |  |
| --- | --- |
|  |  |

**Data Encryption Standard (DES):**

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



|  |  |
| --- | --- |
|  |  |

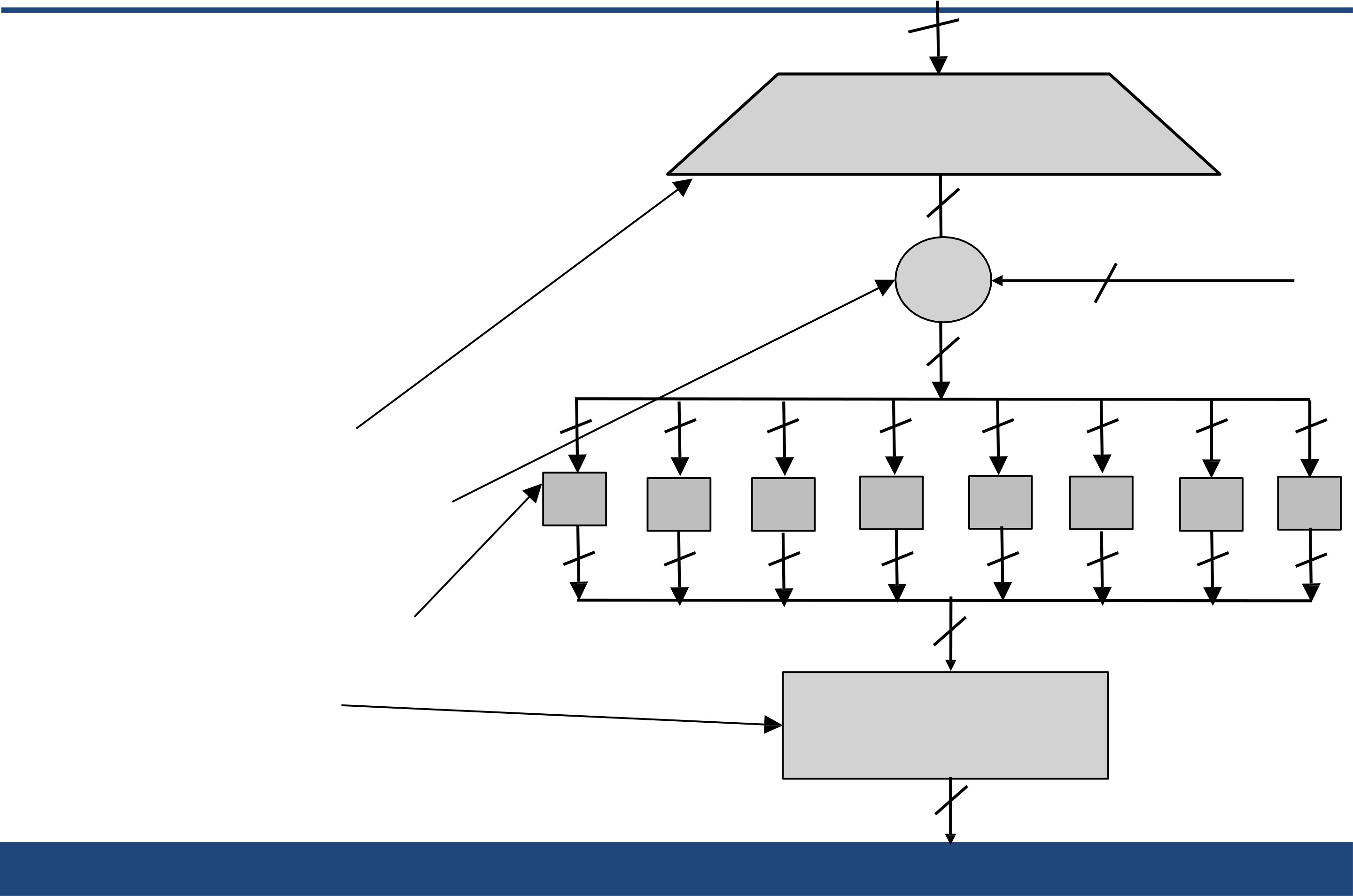
**Data Encryption Standard (DES): - Initial Permutation**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| The | initial | | | 1 | 2 | 25 | | 40 | | 58 | 64 |
| permutation | | of | the | 1 | 2 | 8 | 25 | | 40 | 58 | 64 |
| 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. | | | |
| |  | | --- | | 16 Rounds | | | | | | | | |
| 1 | 2 | 25 | | 40 | | 58 | 64 |
| 1 | 2 | 8 | 25 | 40 | | 58 | 64 |

|  |  |
| --- | --- |
|  |  |

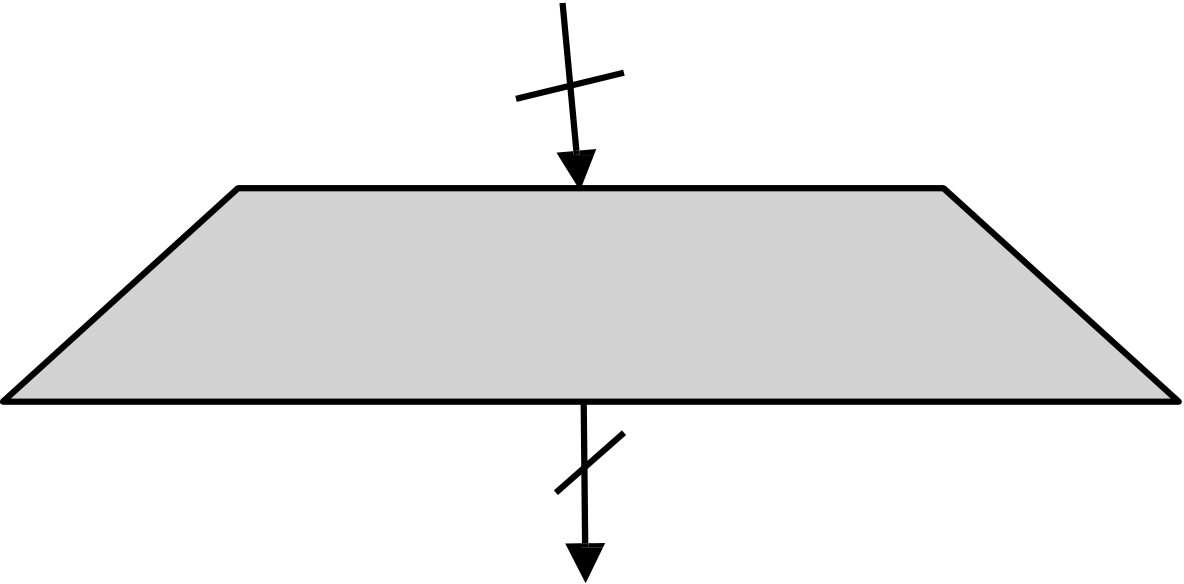
**Data Encryption Standard (DES): Initial and Final Permutation**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 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 | |



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ri-132  **Data Encryption Standard (DES): The f Function**  Expansion/permutation | | | | | | | | | | | | | |
| 1. | Main operation of DES | | | (E table) | | | | | | 48 | *Ki* | | |
| 48 | | | | | |
| f-function inputs: | | | |
| *Ri-1* and round key *ki* | | | | XOR | | | | | |
| **4 Steps**: | | | | 48 | | | | | |
| 1. Expansion E | | 6 | | 6 | | 6 | | 6 | 6 | 6 | 6 | | 6 |
| 2. XOR with round key | | | S1 | S2 | S3 | | S4 | | S5 | S6 | S7 | S8 | |
| 4 | | | | 4 | | 4 | | 4 | 4 | 4 | 4 | 4 | |
| 3. S-box substitution | | | | 32 | | | | | | | | | |
| 4. Permutation | | | | Permutation  (P) | | | | | | | | | |

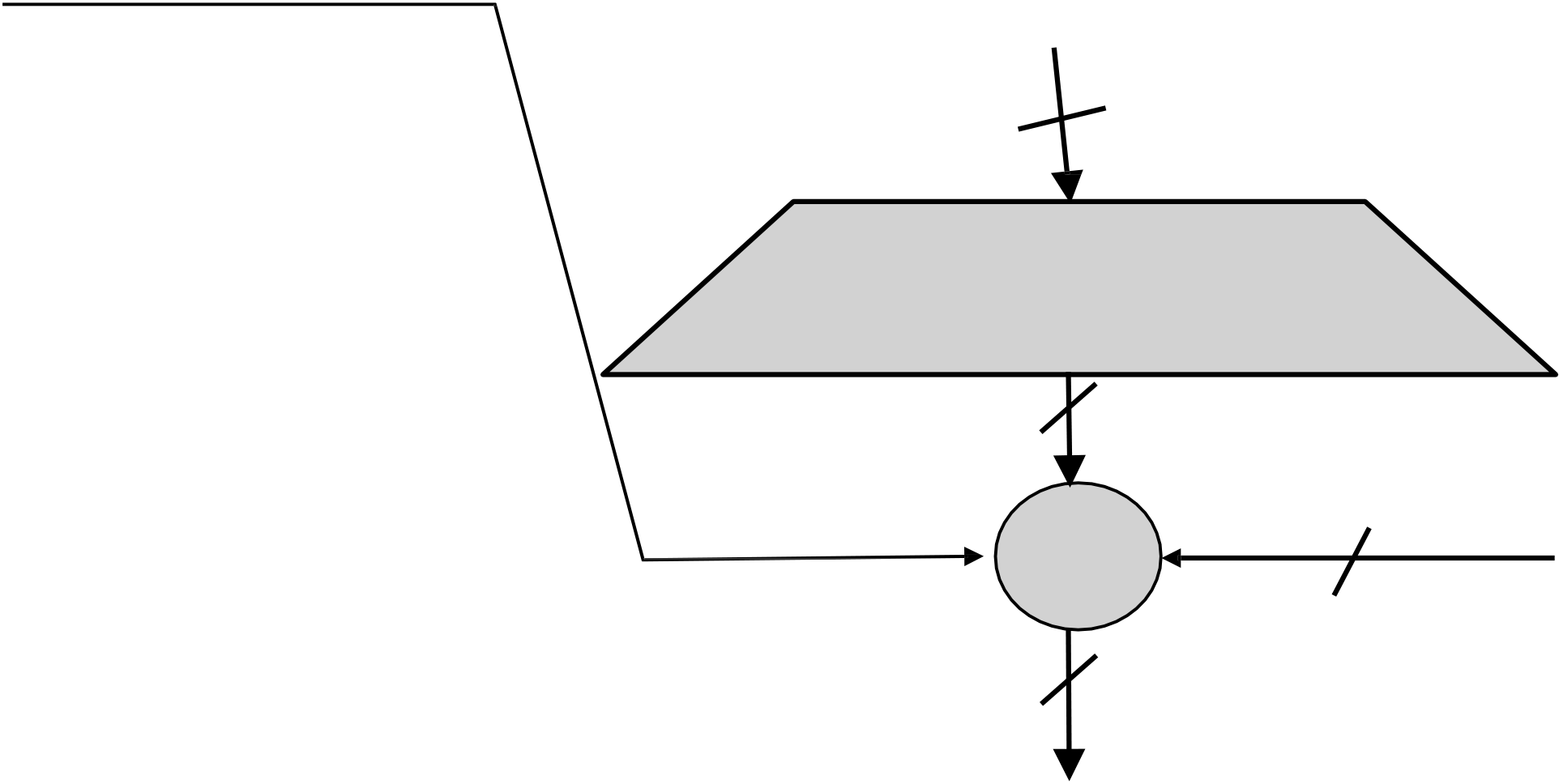
32



|  |  |
| --- | --- |
|  |  |
| **Data Encryption Standard (DES): The f Function – The Expansion** 32  **Function** | |
| Main purpose: **Increases diffusion** | Expansion/permutation  (E table) |

48

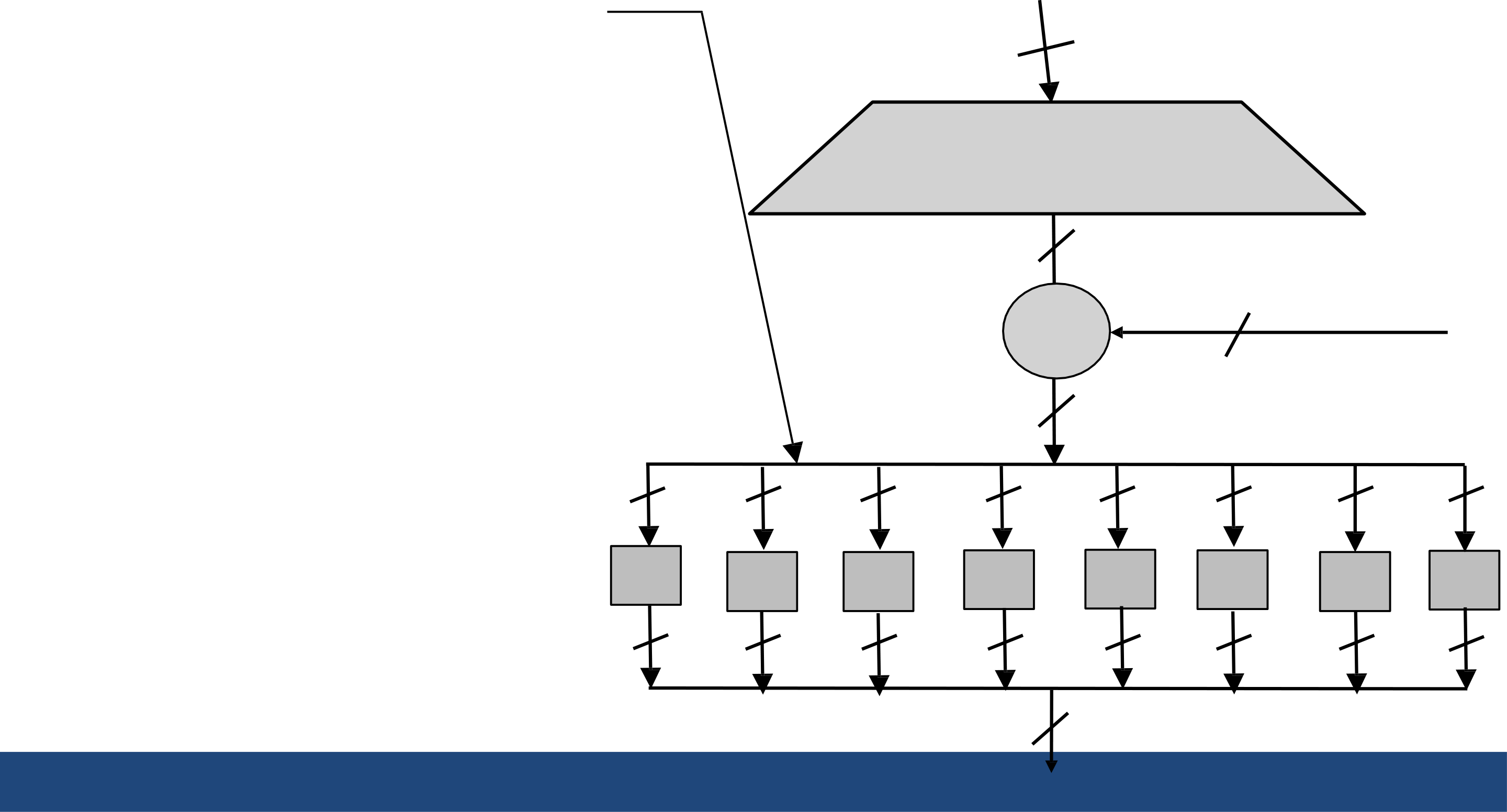
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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** | | | Ri-1 | 48 | *Ki* |
| After | the | expansion |
| 32 |
| permutation, DES uses | | | Expansion/permutation |
| the XOR operation on the | | |
| (E table) |
| expanded right section | | |
| 48 |
| and the round key. | | |
| Note that both the right | | | XOR |
| section and the key are | | | 48 |
| 48-bits in length now. | | |

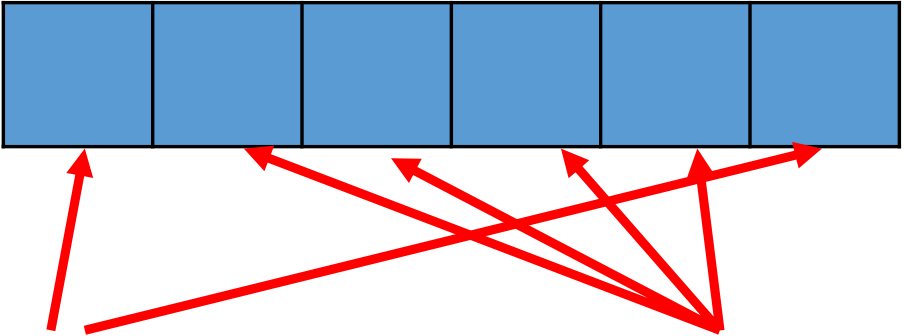
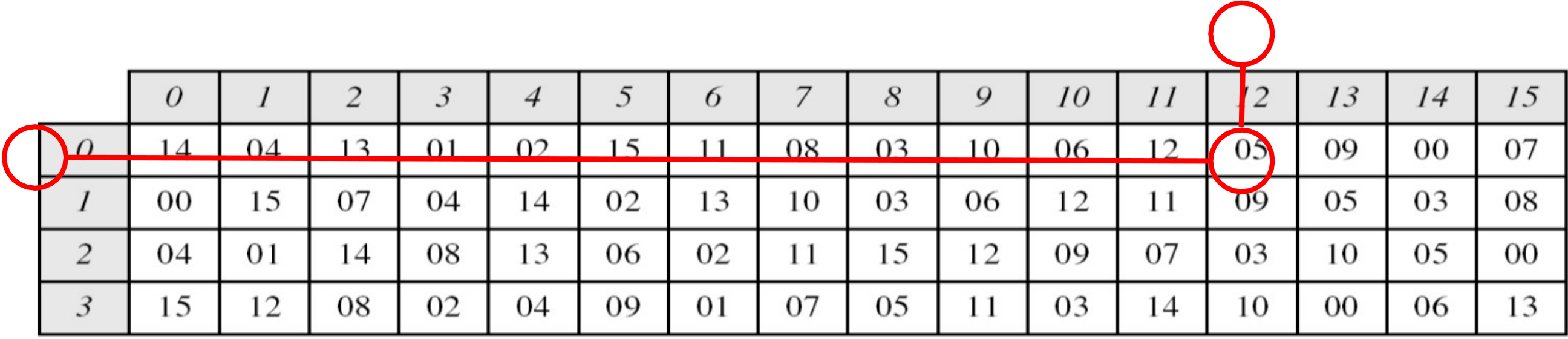
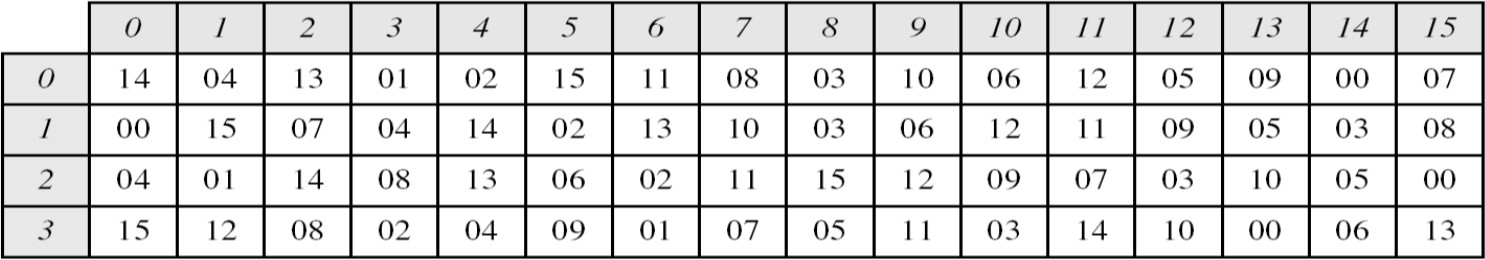


|  |  |
| --- | --- |
|  |  |

**Data Encryption Standard (DES): S-Box substitution**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| • | Eight substitution tables. | 6 | 6 | 6 | Ri-1 | | 48 | *Ki* | 6 | 6 |
| 32 | |
| • | 6 bits of input |
| • | 4 bits of output. | Expansion/permutation | |
| (E table) | |
| • | Convert 48 bits to 32 bits |
| • | Non-linear and resistant to | 48 | |
| • | differential cryptanalysis. | XOR | |
| Crucial element for DES |
| • | security! | 48 | | 6 |
| Introduces confusion. |
| 6 | 6 |
| S1 | 4 | S2 | S3 | S4 | S5 | S6 | S7 |
| S8 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 |

32



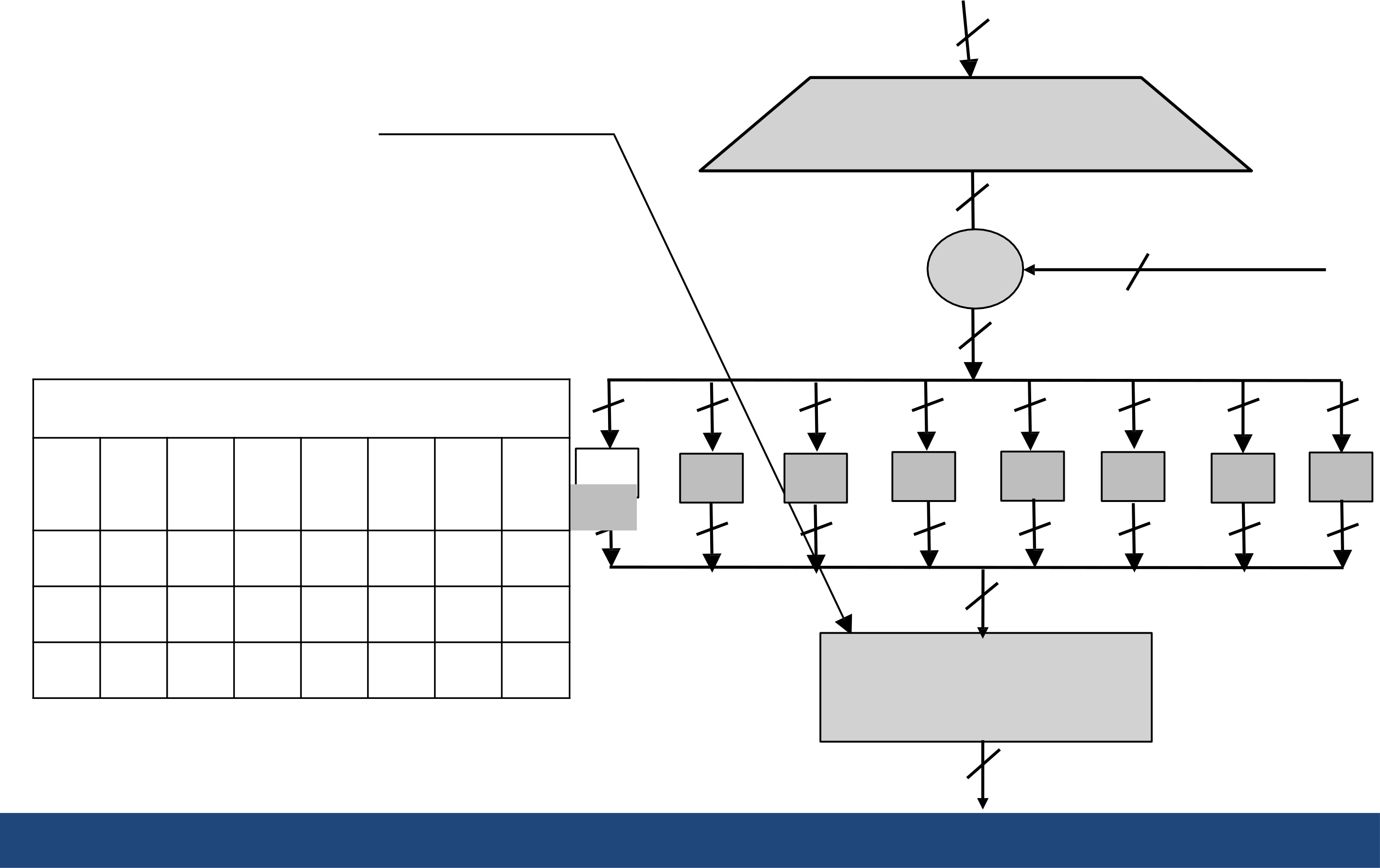
|  |  |
| --- | --- |
|  |  |

**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.

**S-box 1**Example:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input | 0 | 1 | 1 | 0 | 0 | 1 | Output | |  |  |  |  | | --- | --- | --- | --- | | 1 | 0 | 0 | 1 | |
| Row | Column | |



|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| **Data Encryption Standard (DES): The Permutatio**3**n**2  Permutation P | | Ri-1  Expansion/permutation  (E table)  48  *Ki* | |
| • | Bitwise permutation. |
| • | **Introduces diffusion.** |
| XOR | 48 |

48

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 7 | **Permutation Table P** | | | | 28 | 17 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 20 | 21 | 29 | 12 |
| S2 | S3 | S4 | S5 | S6 | S7 | S8 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 | S1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 4 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 | 32 | |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 | Permutation | |
| (P) | |

32

|  |  |
| --- | --- |
|  |  |

**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.



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.  2. | 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.  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.

