# SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

**An Autonomous Institution**

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

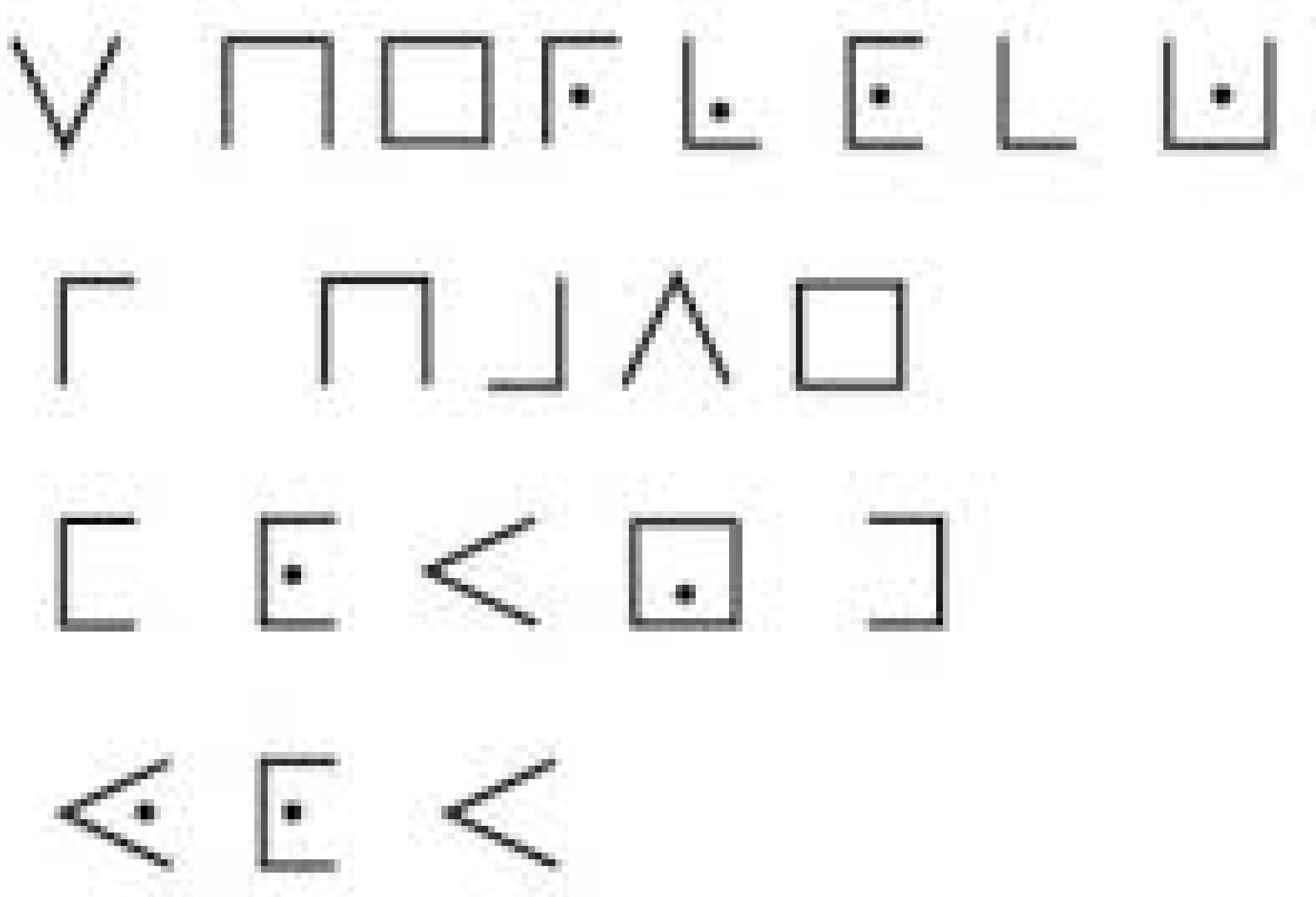
## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

## COURSE NAME : 19CS503 Cryptography and Network Security

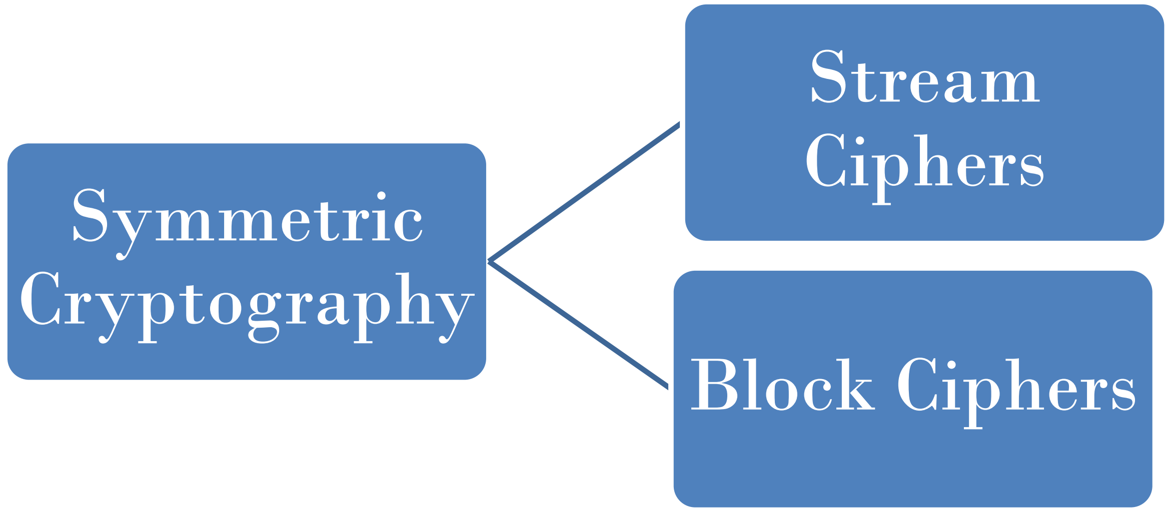
III YEAR /V SEMESTER

## Unit 2- SYMMETRIC KEY CRYPTOGRAPHY

Topic : Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation

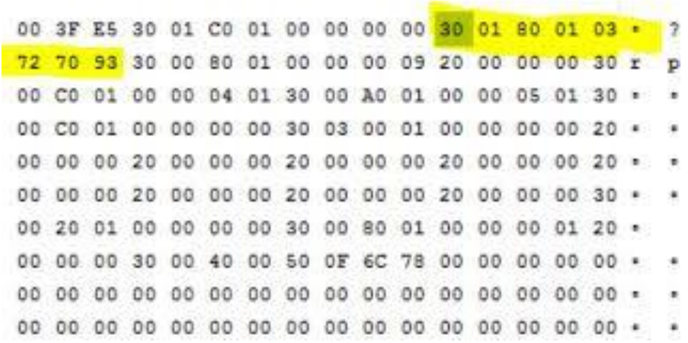


# Stream and Block Ciphers




**Stream ciphers** process messages a bit or byte at a time when en/decrypting

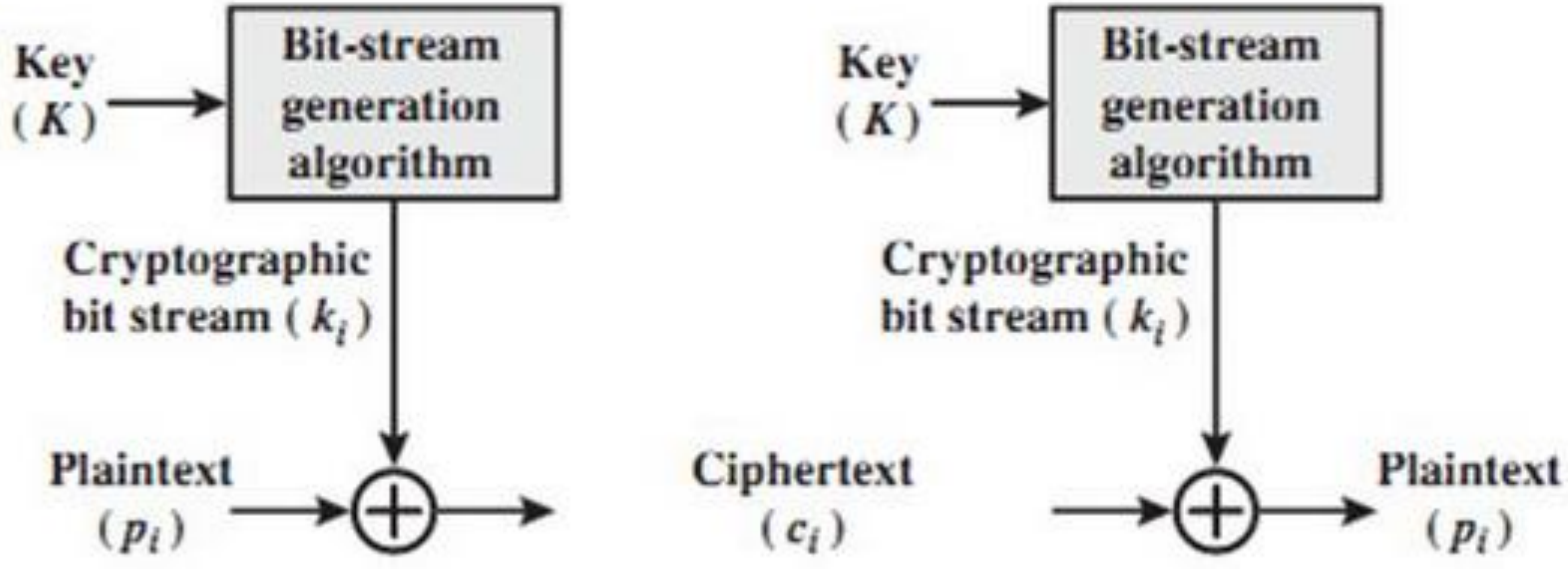
**Block ciphers** process messages into blocks, each of which is then en/decrypted

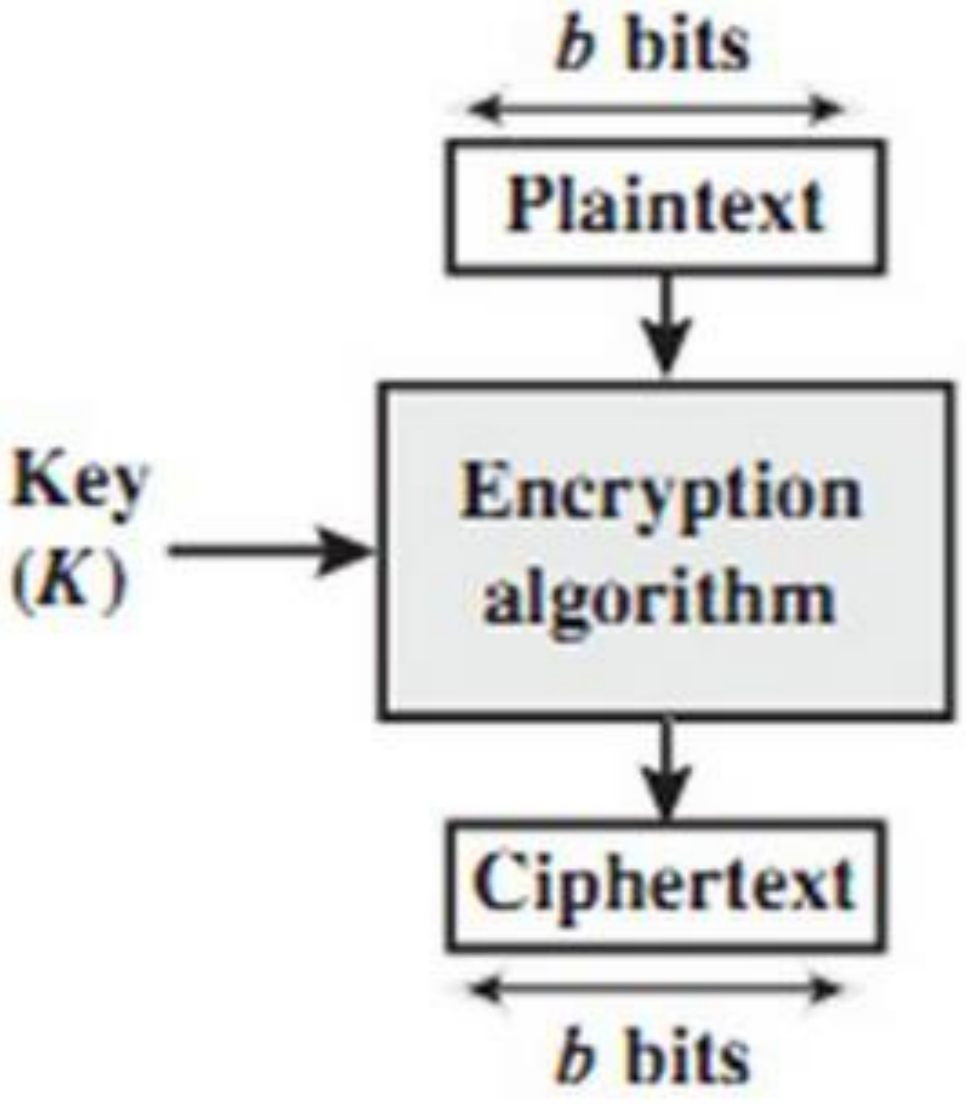



Simple substitution is an example of a stream cipher.

Columnar transposition is a block cipher

# Stream and Block Ciphers



# Block vs Stream Cipher

| Block Cipher | Stream Cipher |
|---|---|
| Block Cipher Converts the plain text into cipher text by taking plain text's block at a time. | Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time. |
| Block cipher uses either 64 bits or more than 64 bits. | While stream cipher uses 8 bits. |
| The complexity of block cipher is simple. | While stream cipher is more complex. |
| Block cipher Uses confusion as well as diffusion. | While stream cipher uses only confusion. |
| In block cipher, reverse encrypted text is hard. | While in stream cipher, reverse encrypted text is easy. |
| The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining). | The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback). |

# Feistel Cipher Structure

**Reversible Mapping**

| Plaintext | Ciphertext |
|---|---|
| 00 | 11 |
| 01 | 10 |
| 10 | 00 |
| 11 | 01 |

Each time unique ciphertext block is created.

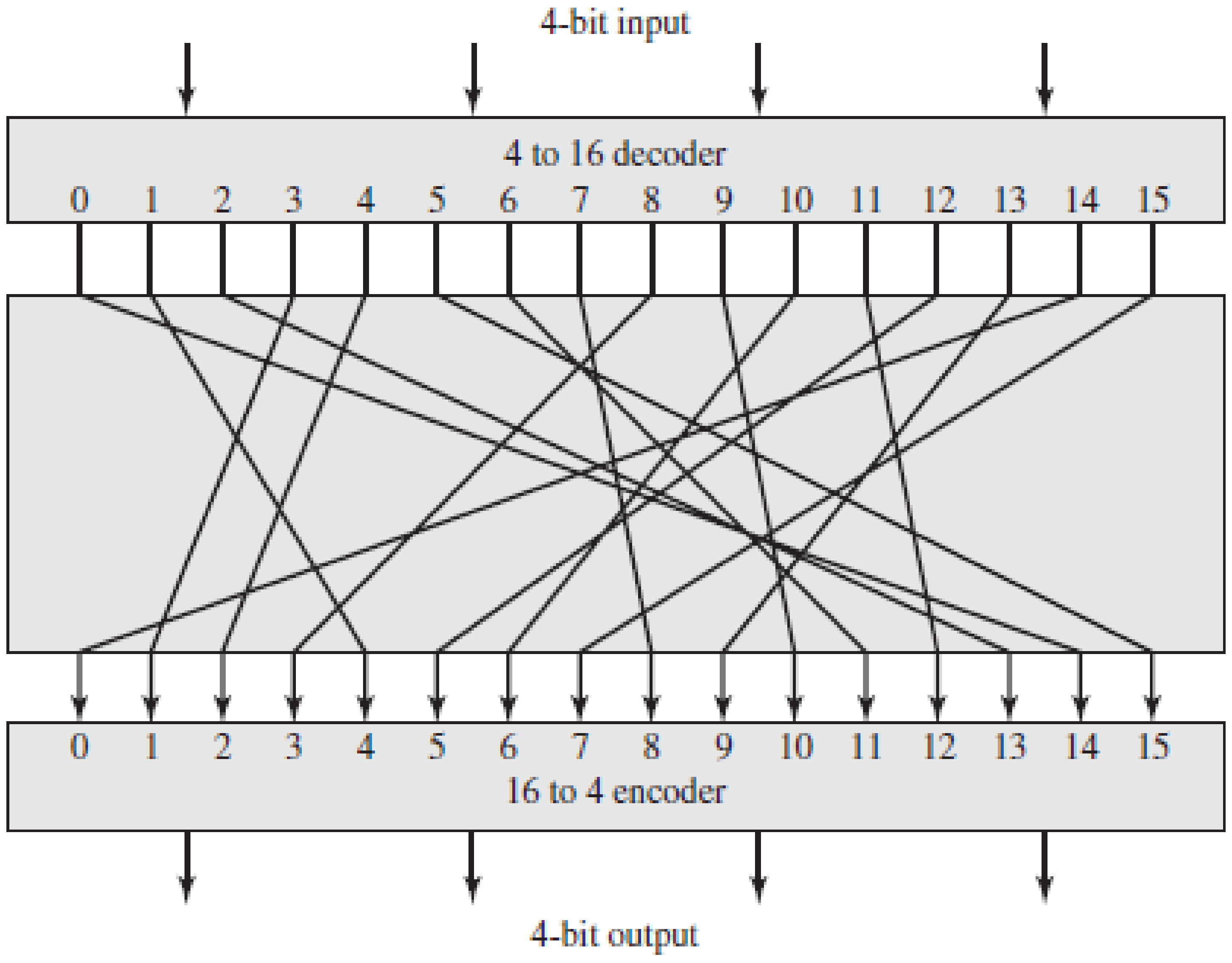
**Irreversible Mapping**

| Plaintext | Ciphertext |
|---|---|
| 00 | 11 |
| 01 | 10 |
| 10 | 01 |
| 11 | 01 |

Ciphertext of 01 have been produced by one of two plaintext.

# Message Authentication and Digital Signature

- 4-bit input ,16 possible input states - mapped by the substitution cipher - 16 possible output states, 4 ciphertext bits.
- Referred as Ideal Block Cipher
  - Because it allows plaintext-ciphertext mapping for all possible inputs.




key is mapping ; Key length **16 × 4 bits = 64 bits . i.e. concatenate all bits of ciphertext table**

# Problems with Ideal Block Cipher

- Small block size
  - equivalent to classical substitution cipher
  - cryptanalysis based on statistical characteristics feasible
- Large block size:
  - key must be very large
  - performance/ implementation problems.

# Activity

# Feistel Cipher

- Feistel proposed applying two or more simple ciphers in sequence so final result cryptographically stronger than component ciphers
- **n-bit block length; k-bit key length; 2k transformations (rather than 2n !)**
- Feistel cipher alternates: substitutions, transpositions (permutations)

**Subtitution**

plaintext element or group of elements is uniquely replaced

**Permutation**

The order of plaintext element is changed

# Diffusion and Confusion

- To suppress statistical cryptanalysis

| Diffusion | Confusion |
| --- | --- |
| • Each plaintext digit affects the value of many ciphertext digits. | • Achieved with the use of complex substitution algorithm |

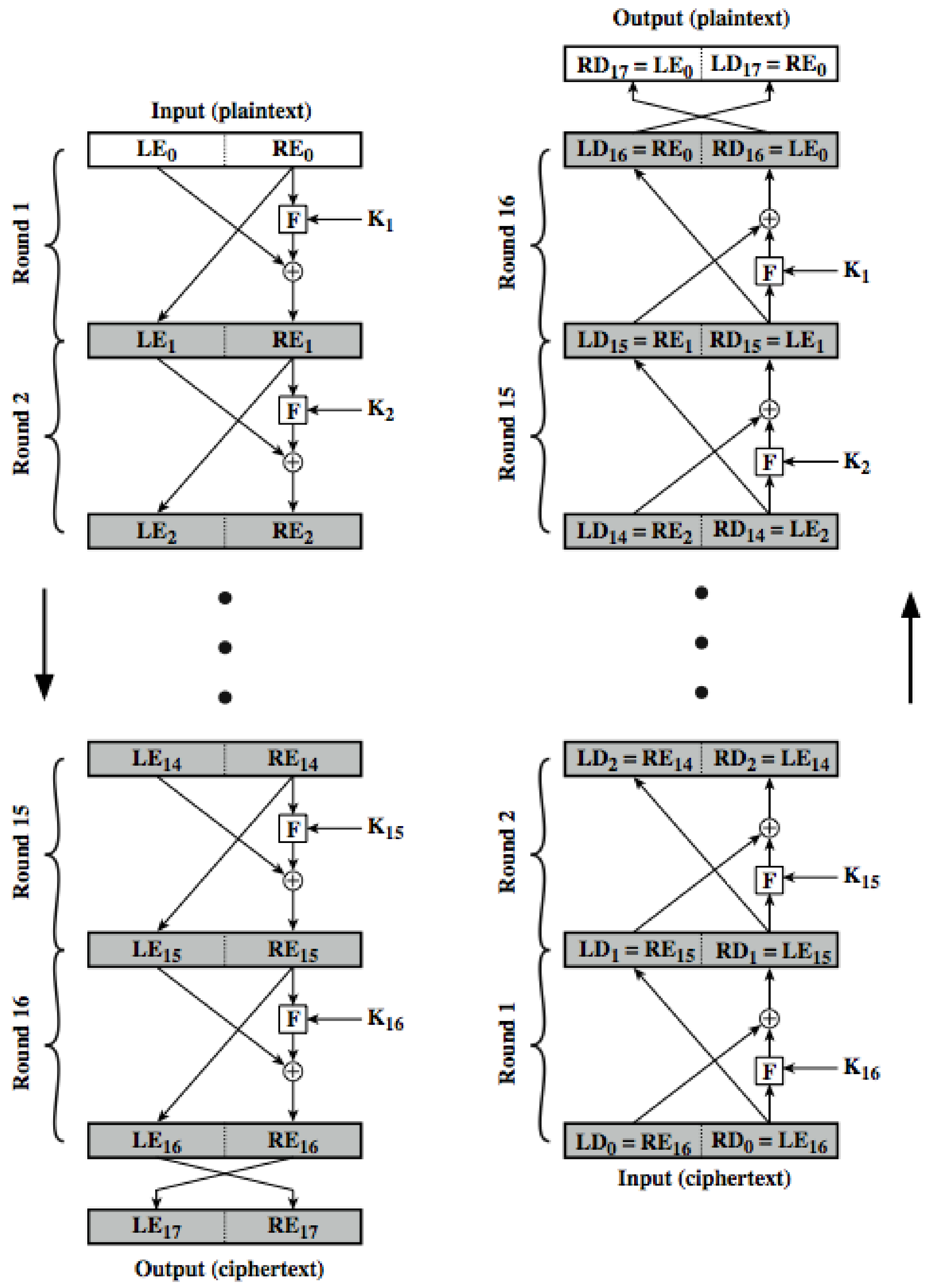
Message M=m1,m2,m3.. of characters encrypted as

$$y_n = \left( \sum_{i=1}^{k} m_{n+i} \right) \bmod 26$$

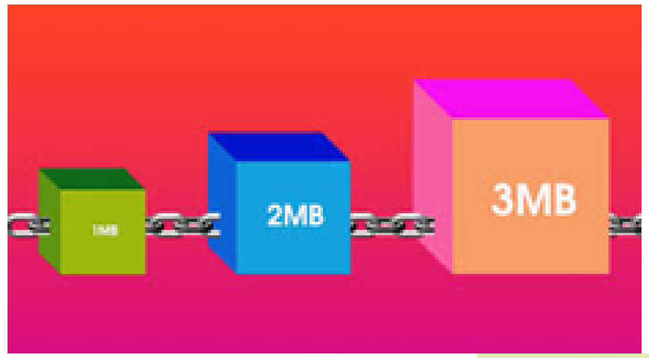
Statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

# Feistel Cipher Structure

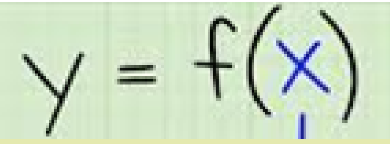
- Left – Hand Side
  - Plaintext 2w bits and Key k
  - $L_0$ and $R_0$
  - N rounds of processing
    - (fig has 16 rounds)
  - Subkey $K_I$
  - Substitution – Left half
  - Round Function F to Right half
  - $F(RE_i, K_{i+1})$
  - Permutation to both halves



# Feistel Cipher Design Elements

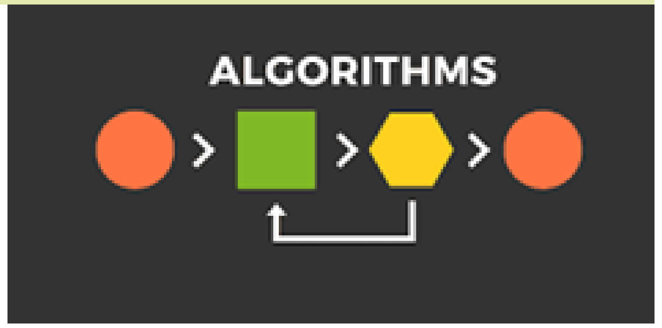



block size - increasing size improves security, but slows cipher




round function - greater complexity can make analysis harder, but slows cipher

key size - increasing size improves security, makes exhaustive key searching harder, but may slow cipher




number of rounds - increasing number improves security, but slows cipher

subkey generation algorithm - greater complexity can make analysis harder, but slows cipher

fast software en/decryption - more recent concern for practical use
ease of analysis - for easier validation & testing of strength

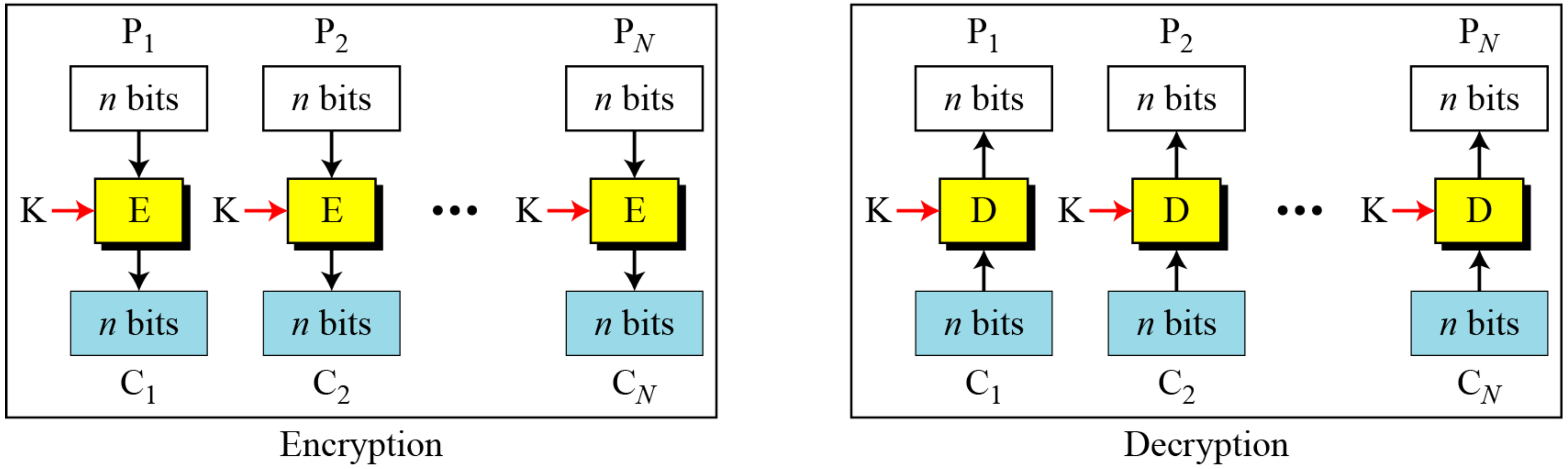
# Block Cipher – Modes of operation

| | |
|---|---|
| Electronic Code Book (ECB) | • Each block encoded independently using the same key. |
| Cipher Block Chaining (CBC) | • XOR of the next block of plaintext and the preceding block of ciphertext. |
| Cipher Feedback(CFB) | • pseudorandom output (Preceding ciphertext) XORed with plaintext to produce next unit of ciphertext |
| Output Feedback (OFB) | • Same as CFB except preceding encryption output, and full blocks are used. |
| Counter (CTR) | • ORed with an encrypted counter. CTR is incremented for each subsequent block |

# Electronic Code Book (ECB)

| ECB | $C_j = E(K, P_j) \quad j = 1, \ldots, N$ | $P_j = D(K, C_j) \quad j = 1, \ldots, N$ |
|---|---|---|

E: Encryption
D: Decryption
$P_i$: Plaintext block $i$
$C_i$: Ciphertext block $i$
K: Secret key




Application: Secure transmission of single values (e.g., an encryption key)

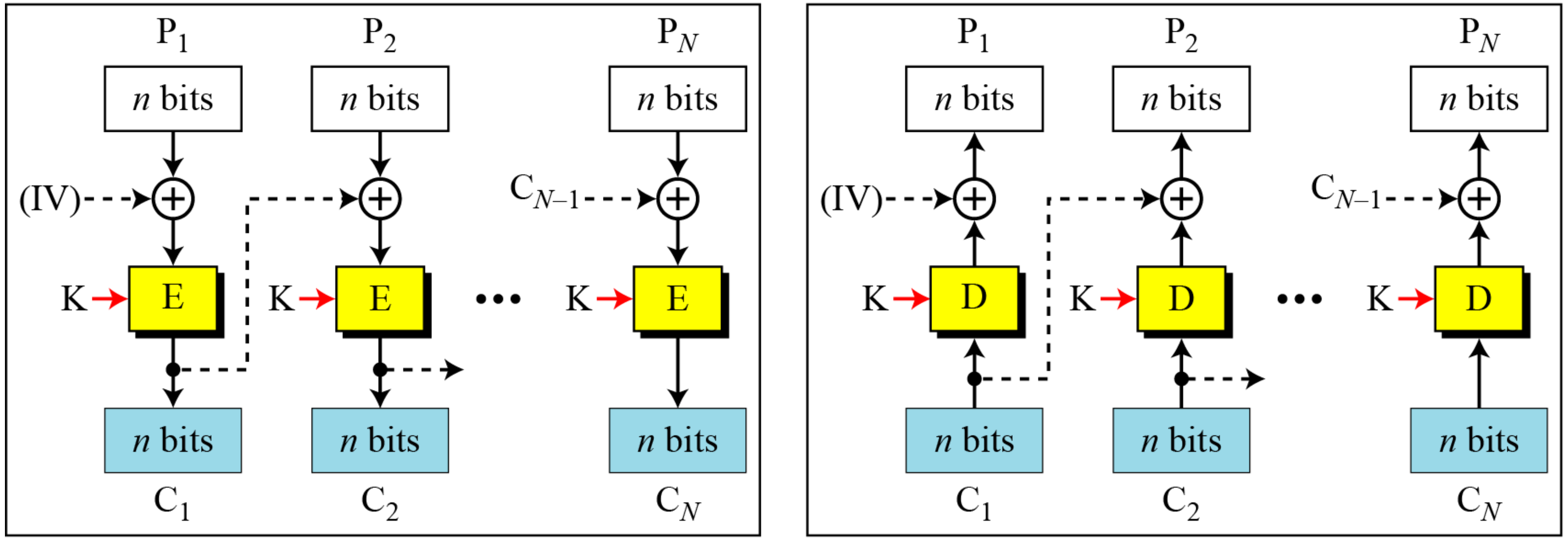
# Cipher Block Chaining (CBC)

| | | |
|---|---|---|
| CBC | $C_1 = E(K, [P_1 \oplus IV])$<br>$C_j = E(K, [P_j \oplus C_{j-1}])\ j = 2, \ldots, N$ | $P_1 = D(K, C_1) \oplus IV$<br>$P_j = D(K, C_j) \oplus C_{j-1}\ j = 2, \ldots, N$ |

E: Encryption
$P_i$: Plaintext block $i$
K: Secret key

D : Decryption
$C_i$ : Ciphertext block $i$
IV: Initial vector ($C_0$)

Application: General-purpose block oriented transmission and Authentication



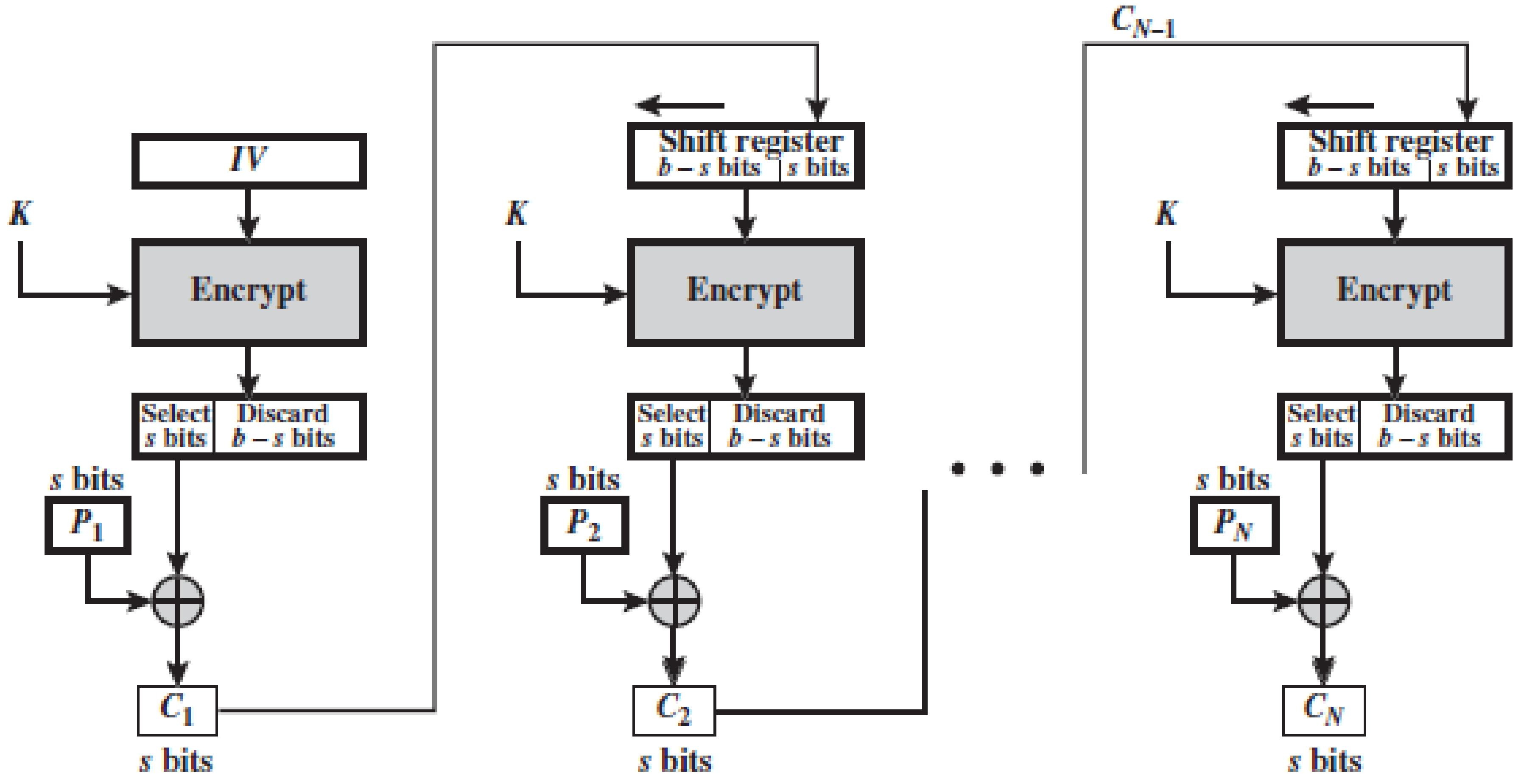

Encryption

Decryption

# Cipher Feedback(CFB)

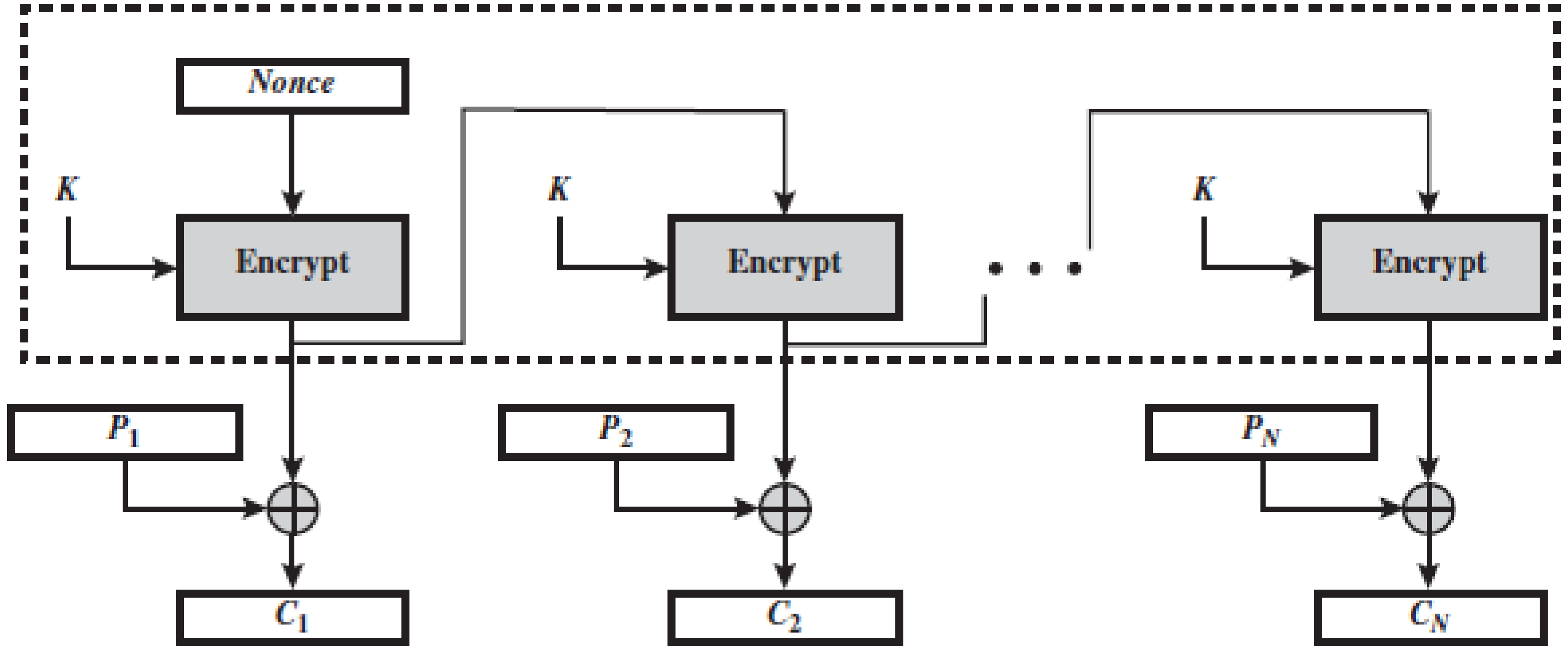
| | | |
|---|---|---|
| CFB | $I_1 = IV$<br>$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1} \quad j = 2, \ldots, N$<br>$O_j = \text{E}(K, I_j) \quad j = 1, \ldots, N$<br>$C_j = P_j \oplus \text{MSB}_s(O_j) \quad j = 1, \ldots, N$ | $I_1 = IV$<br>$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1} \quad j = 2, \ldots, N$<br>$O_j = \text{E}(K, I_j) \quad j = 1, \ldots, N$<br>$P_j = C_j \oplus \text{MSB}_s(O_j) \quad j = 1, \ldots, N$ |

Application: General-purpose stream oriented transmission and Authentication



# Output FeedBack (OFB)

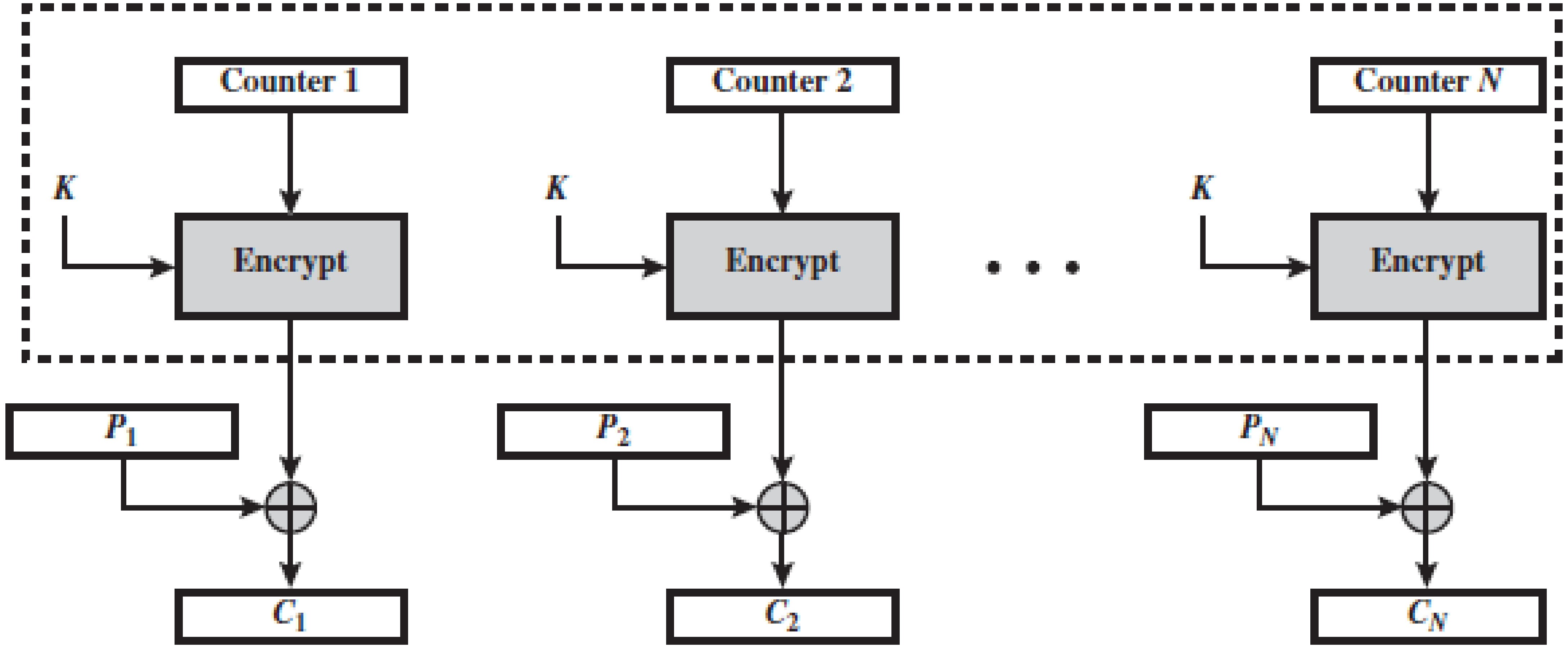
| | | |
|---|---|---|
| OFB | $I_1 = Nonce$<br>$I_j = O_{j-1} \quad j = 2, \ldots, N$<br>$O_j = E(K, I_j) \quad j = 1, \ldots, N$<br>$C_j = P_j \oplus O_j \quad j = 1, \ldots, N-1$<br>$C_N^* = P_N^* \oplus MSB_u(O_N)$ | $I_1 = Nonce$<br>$I_j = O_{j-1} \quad j = 2, \ldots, N$<br>$O_j = E(K, I_j) \quad j = 1, \ldots, N$<br>$P_j = C_j \oplus O_j \quad j = 1, \ldots, N-1$<br>$P_N^* = C_N^* \oplus MSB_u(O_N)$ |




Application: Stream-oriented transmission over noisy channel (e.g., satellite communication)

# Counter (CTR)

| | | |
|---|---|---|
| CTR | $C_j = P_j \oplus E(K, T_j) \quad j = 1, \ldots, N-1$<br>$C^*_N = P^*_N \oplus MSB_u[E(K, T_N)]$ | $P_j = C_j \oplus E(K, T_j) \quad j = 1, \ldots, N-1$<br>$P^*_N = C^*_N \oplus MSB_u[E(K, T_N)]$ |




Application: General-purpose block oriented transmission and Useful for high-speed requirements

# Summary

| Operation Mode | Description | Type of Result | Data Unit Size |
|---|---|---|---|
| ECB | Each *n*-bit block is encrypted independently with the same cipher key. | Block cipher | *n* |
| CBC | Same as ECB, but each block is first exclusive-ored with the previous ciphertext. | Block cipher | *n* |
| CFB | Each *r*-bit block is exclusive-ored with an *r*-bit key, which is part of previous cipher text | Stream cipher | $r \leq n$ |
| OFB | Same as CFB, but the shift register is updated by the previous *r*-bit key. | Stream cipher | $r \leq n$ |
| CTR | Same as OFB, but a counter is used instead of a shift register. | Stream cipher | *n* |

# Assessment 1

1 Confusion hides the relationship between the ciphert
plaintext.
a) True
b) False

2. The S-Box is used to provide confusion, as it is depe
unknown key.
a) True
b) False

# REFERENCES


1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.


# THANK YOU