الجامعة المستنصرية /كلية التربية / قسم علوم الحاسبات

4th Class
Computers & Data Security

أمنية الحاسوب والبيانات

أستاذ المادة

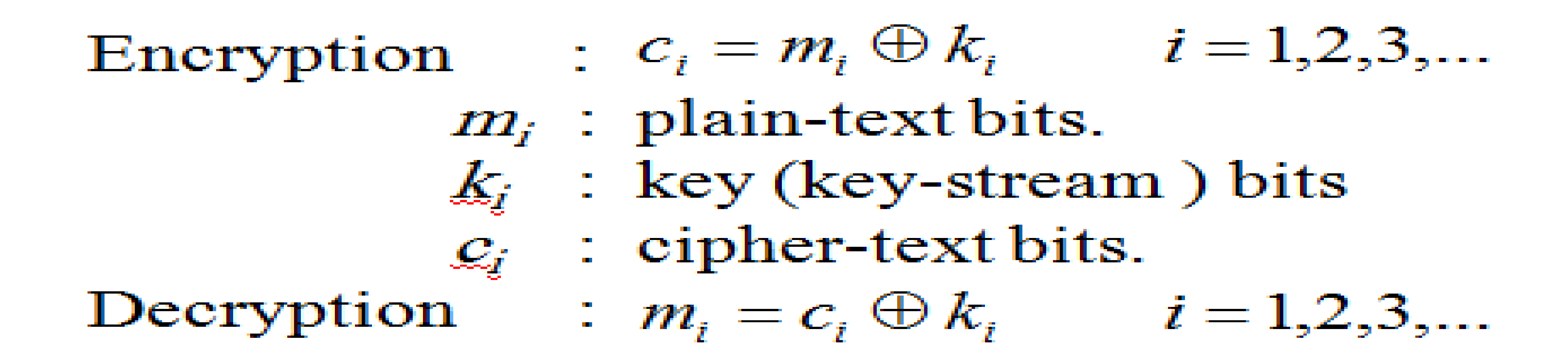
أ.م . د . اخلاص عباس البحراني

Chapter Four
Modern Symmetric Ciphers
(Stream Cipher and Block Cipher)

اعداد: أ.م.د. اخلاص البحراني

Stream cipher

- Is a type of symmetric encryption (means the same key is used for encryption and decryption).
- Basic Idea of stream cipher comes from One-Time-Pad cipher: -



Encryption : $c_i = m_i \oplus k_i \qquad i = 1,2,3,\ldots$

m_i : plain-text bits.

k_i : key (key-stream) bits

c_i : cipher-text bits.

Decryption : $m_i = c_i \oplus k_i \qquad i = 1,2,3,\ldots$

- : ((mi ⊕ ki) ⊕ ki) = mi

- The **drawback of** One-Time-Pad cipher is that the key-stream should be as long as plain-text. Key distribution & Management difficult.
- **Stream Cipher** is the solution (in which key-stream is generated in pseudo-random fashion from relatively short *secret key*.
- **Pseudo-randomness :** sequences appears random to a computationally bounded adversary.

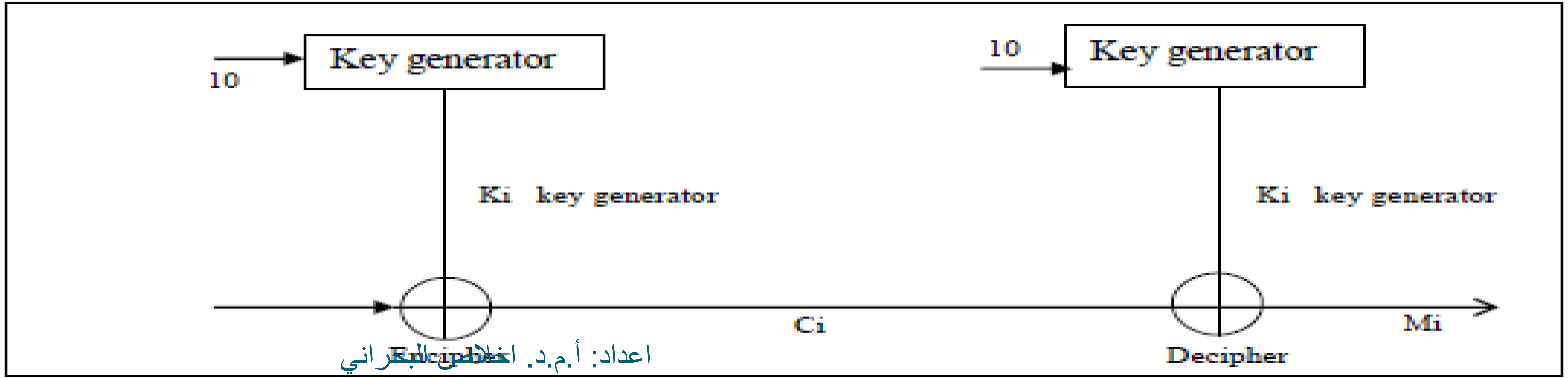
- It is possible to be periodic if reuse the key again after fixed perio
- ds, like Vigenere and Beaufort.
- It is possible to be not periodic if the key is used once like Running Key and OTP.

(i) Encryption
(ii) Decryption
Plaintext m_i
Ciphertext c_i
Key k
Keystream z_i
State σ_i
σ_{i+1}
σ_i
f
g
h
h^{-1}
k
z_i
m_i
c_i

There are two different approaches to stream encryption they are; **synchronous methods** and **self-synchronous methods**.

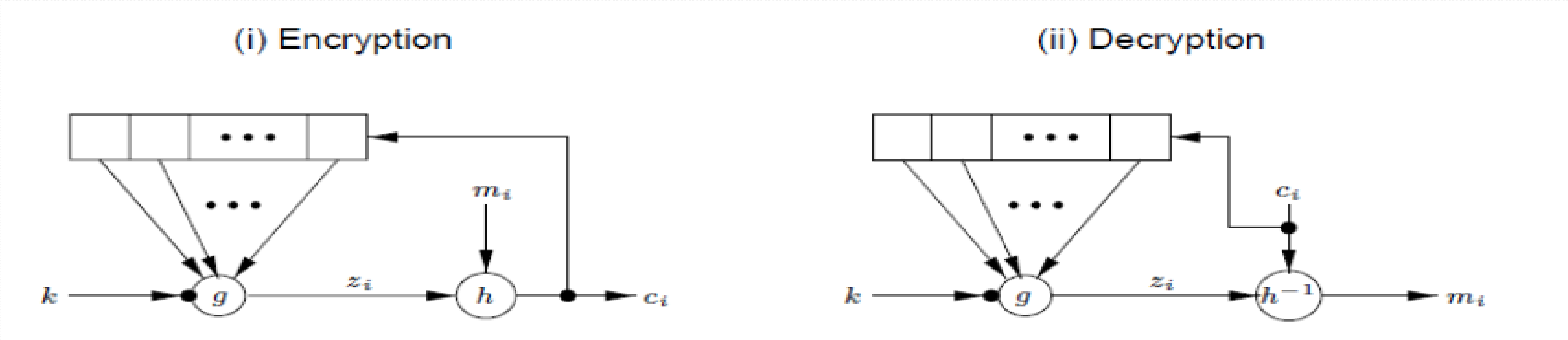
1. Synchronous Stream Ciphers

- Key-stream is independent of plain and cipher-text.
- Both sender &receiver must be synchronized.
- Resynchronization can be needed (This means that if a ciphertext is lost during transmission, the sender and receiver must resynchronize their key generators before they can proceed).
- Synchronous stream ciphers have the advantage of not propagating errors. A transmission error effecting one character will not affect subsequent characters. From another point of view; this is a disadvantage in that it is easier for an opponent to modify (with out detection) a single ciphertext character.
- Active attacks can easily be detected (disadvantage).



2. Self-Synchronizing Stream Ciphers

- Key-stream is a function of fixed number *t* of cipher-text bits. This is done by using a cipher feed back mode (CFB) because the ciphertext characters participate in the feed back loop.
- It is some times called **chaining**, because each ciphertext character depend on preceding cipher-text character (chain) the feed back
- Limited error propagation (up to *t* bits).
- Active attacks cannot be detected.
- At most *t* bits later, it resynchronizes itself when synchronization is lost.
- It helps to diffuse plain-text statistics.



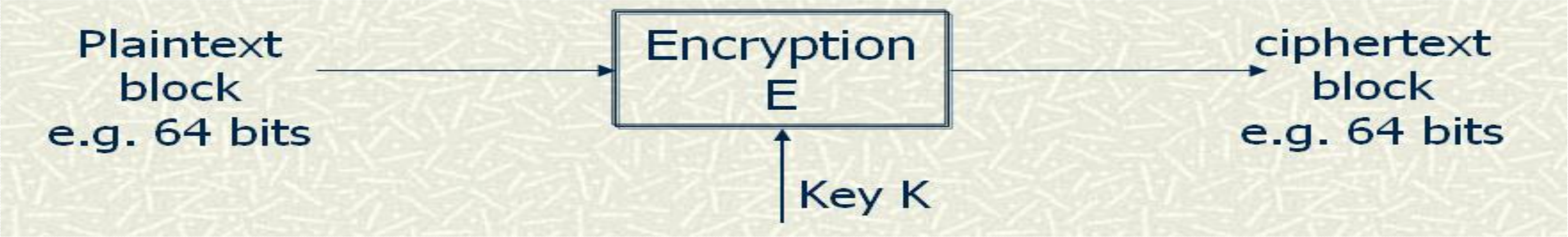
(i) Encryption

(ii) Decryption

Block cipher

- **Block cipher :** - Is a type of symmetric encryption which operates on blocks of data (means the same key is used for encryption and decryption). It encrypts a block of clear text into a block of cipher text of the same length.
- In this case, a block cipher can be viewed as a simple substitute cipher with character size equal to the block size.

- Popular block ciphers are (***Hill Cipher, Playfair Cipher, DES-Data Encryption Standard-, ECB***) with using the same key.



Advantages and Disadvantages of Block Cipher:-

- **Advantages**
  - 1. The possibility of parallel processing for more than one block at the same time.
  - 2. Encryption is quick because all the time implemented n of encryption.
  - 3. Error that occurs in a given block does not affect the other.
  - 4. Each block in the Plaintext is encrypted independently.
- **Disadvantages**
  - 1. The similar blocks in the plaintext also generate similar blocks in the Ciphertext because all blocks using the same key.
  - 2. Easy addition or deletion can be implemented on blocks.

Block cipher operation modes: -

1. **ECB Operation Mode.**

- ECB stands for **Electronic Code Book.** Blocks of clear text are encrypted independently.
- Strength: it's simple.
- Weakness :

1- Repetitive information contained in the plaintext may show in the ciphertext, if aligned with blocks.

2. If the same message is encrypted (with the same key) and sent twice, their ciphertext are the same.

- Typical application: secure transmission of short pieces of information (e.g. a temporary encryption key)

Encryption: $C_i = E_K(P_i)$ Decryption: $P_i = D_K(C_i)$

E: Encryption D: Decryption

P_i: Plaintext block i C_i: Ciphertext block i

K: Secret key

P_1
P_2
P_N
n bits
K
E
D
•••
C_1
C_2
C_N

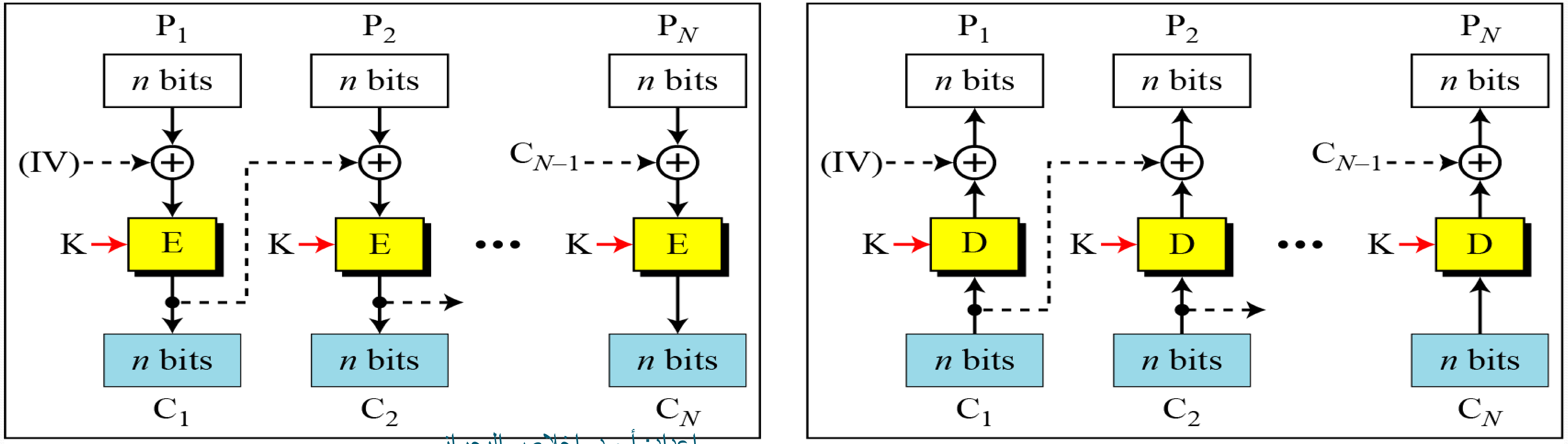
Encryption Decryption

2. CBC Operation Mode.

- **CBC** stands **for Cipher-Block Chaining** The previous cipher text block is XORed with the clear text block before applying the encryption mapping.
- Solve security deficiencies in ECB where Repeated same plaintext block result different ciphertext block
- Use Initial Vector (IV) to start process

Ci = EK (Pi XOR Ci-1)

E: Encryption D : Decryption
P_i: Plaintext block *i* C_i : Ciphertext block *i*
K: Secret key IV: Initial vector (C_0)



Encryption

Decryption

3. Cipher FeedBack (CFB).

- Message is treated as a stream of bits , Bitwise-added to the output of the block cipher , Result is feedback for next stage (hence name).its Uses for stream data encryption, authentication
- Use Initial Vector to start process.
- Plaintext is treated as a stream of bits. Any number of bit (1, 8 or 64 or whatever) to be feed back (denoted CFB-1, CFB-8, CFB-64)

IV
Shift register
64 − s bits
s bits
64
K
Encrypt
Select
s bits
Discard
64 − s bits
s
P_1
C_1
P_2
C_2
C_{M-1}
P_M
C_M
(a) Encryption
Select
j bits
Discard
64 − j bits
Decrypt
(b) Decryption

اعداد: أ.م.د. اخلاص البحراني

4. Output Feedback Mode (OFM).

- The block cipher is used as a stream cipher, it produces the random key stream.
- Very similar to CFB But output of the encryption function output of cipher is fed back (hence name), instead of ciphertext.

IV
Shift register
64 − s bits
s bits
64
K
Encrypt
64
Select
s bits
Discard
64 − s bits
s
P1
C1
P2
C2
O_{M−1}
PM
CM
• • •
Select
j bits
Discard
64 − j bits
Decrypt
P1
P2
PM

(a) Encryption

(b) Decryption

Block Cipher & Stream Cipher Comparison:-

	Block Cipher	Stream Cipher
1	Processing or encoding plaintext is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding plaintext is done bit by bit. The block size here is simply one bit.
2	The same key is used to encrypt each of the blocks.	A different key is used to encrypt each of the bits.
3	Usually more complex and slower in operation.	Usually very simple and much faster.
4	More secure in most cases.	Equally secure if properly designed.
5	The key to the cipher text relationship could be very complicated.	Key is often combined with an initialization vector.
6	An error will affect the transformation of all characters in the same block.	An error in the encryption process affects only that character, because each symbol is separately encoded.
7	Slowness of encryption, the person using a block cipher must wait until entire block of plaintext symbols has been received before starting the encryption process.	Speed of transformation, because each symbol is encrypted without regard for any other plaintext symbols, each symbol is encrypted as soon as it is read, so the time required to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext.