MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب
MSA
UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi

The First British Higher Education in Egypt

Cryptography
ECE5632 - Spring 2026

Lecture 4B

Dr. Farah Raad

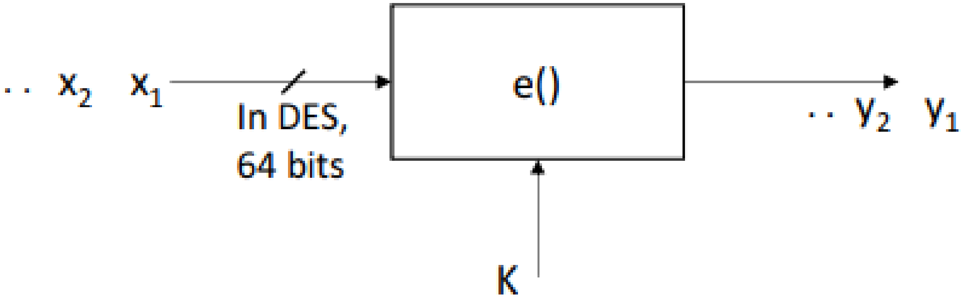
Lecture Topic

Modes of Operation for Block Ciphers

Block Ciphers

Block cipher is an encryption algorithm that takes a fixed size of input say b bits and produces a ciphertext of b bits again.
If the input is larger than b bits it can be divided further.

- **A block cipher is much more than just an encryption algorithm, it can be used:-**
  - ✓ to build different types of block-based encryption schemes
  - ✓ to realize stream ciphers
  - ✓ to construct hash functions
  - ✓ to make message authentication codes
  - ✓ to build key establishment protocols
  - ✓ to make a pseudo-random number generator



- **The security of block ciphers also can be increased by**
  - key whitening
  - multiple encryption

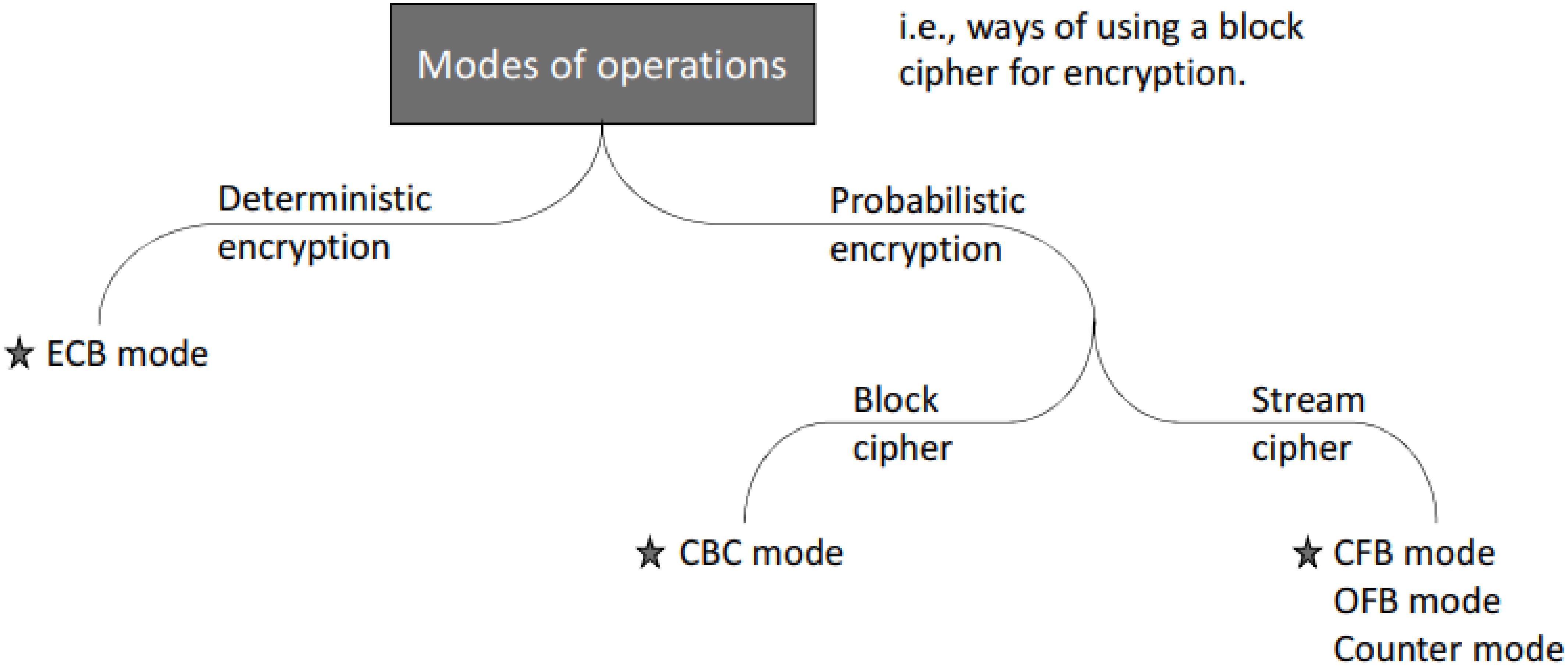
Encryption with Block Ciphers

- There are several ways of encrypting long plaintexts, e.g., an e-mail or a computer file, with a block cipher (“modes of operation”)
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - Output Feedback mode (OFB)
  - Cipher Feedback mode (CFB)
  - Counter mode (CTR)
  - Galois Counter Mode (GCM)
- All of the 6 modes have one goal:
  - In addition to confidentiality, they provide authenticity and integrity:
  - Is the message really coming from the original sender? (authenticity)
  - Was the ciphertext altered during transmission? (integrity)

Deterministic vs Probabilistic Encryption

- In a deterministic encryption scheme, a particular plaintext is mapped to a fixed ciphertext, if the key is unchanged.

- In a probabilistic encryption scheme is non-deterministic.
  i.e., if the same plaintext is encrypted twice, different ciphertexts are obtained.



Modes of operations

i.e., ways of using a block cipher for encryption.

Deterministic encryption

★ ECB mode

Probabilistic encryption

Block cipher

★ CBC mode

Stream cipher

★ CFB mode
OFB mode
Counter mode

★ i.e., today.

Modes of Operation for Block Ciphers

➢ Encryption with Block Ciphers: Modes of Operation

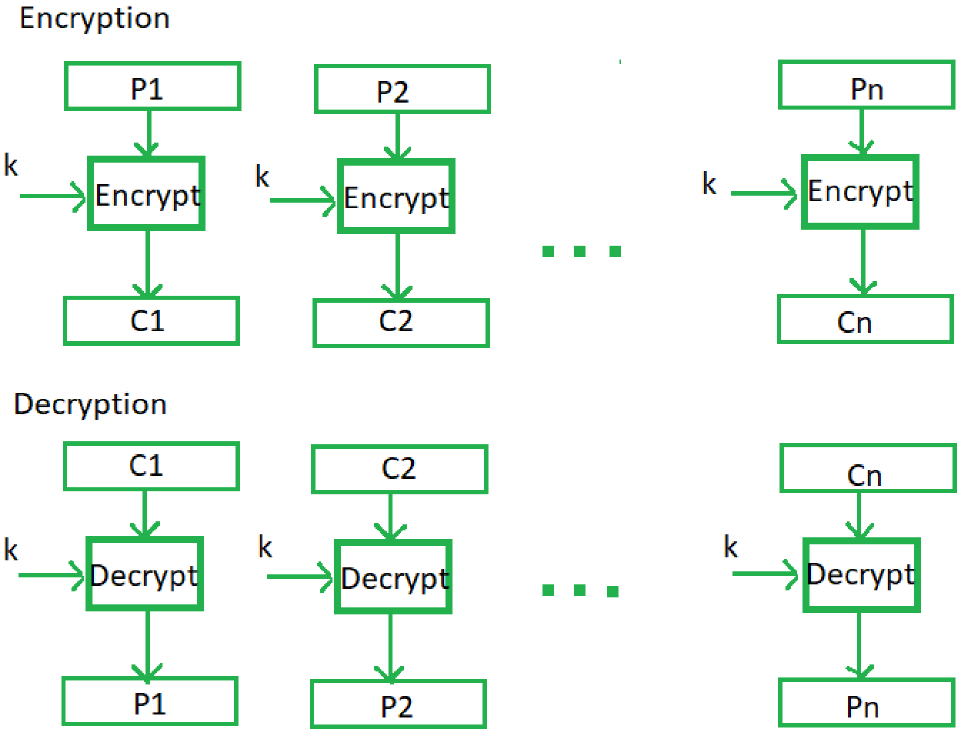
- ✓ **Electronic Codebook Mode (ECB).**
- ✓ Cipher Block Chaining Mode (CBC).
- ✓ Cipher Feedback mode (CFB)
- ✓ Output Feedback mode (OFB)
- ✓ Counter mode (CTR)
- ✓ Galois Counter Mode (GCM)

Electronic Code Book mode (ECB)

- It is the easiest block cipher mode of functioning.
- It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext.
- Generally, if a message is large bits in size, it can be broken down into a bunch of blocks and the procedure is repeated
- Each block encrypted independently.
- Identical plaintexts encrypted similarly.
- No chaining, no error propagation
- No need for preprocessing

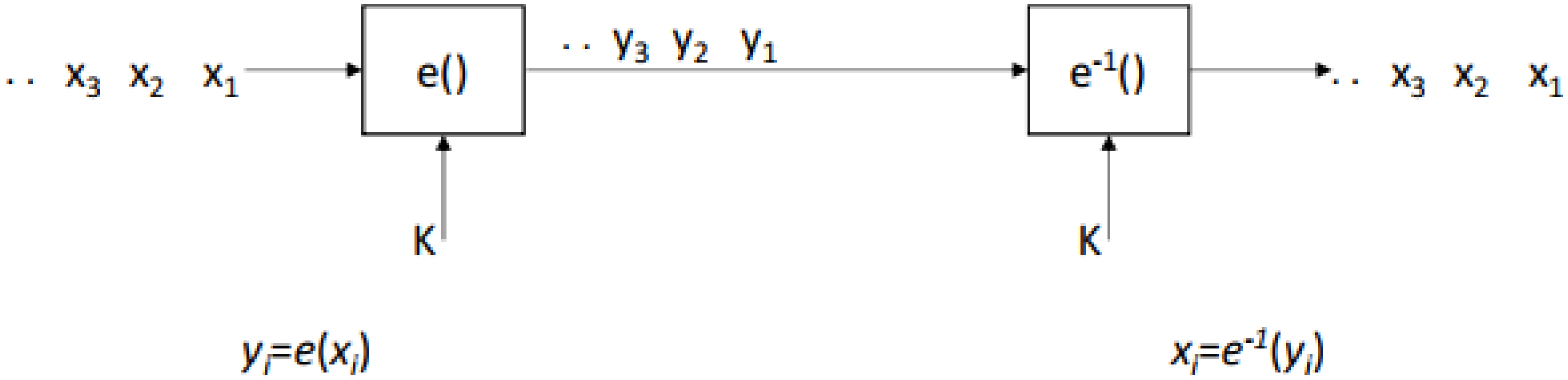
during encryption / decryption

- Allows random access to ciphertext



Electronic Code Book mode (ECB)

- ❑ $e_k(x_i)$ denote the encryption of a *b*-bit plaintext block x_i with key k
- ❑ $e_k^{-1}(y_i)$ denote the decryption of *b*-bit ciphertext block y_i with key k
- ❑ Messages which exceed *b* bits are partitioned into *b*-bit blocks
  - **Each Block is encrypted separately**



Encryption: $y_i = e_k(x_i), \;\; i \geq 1$

Decryption: $x_i = e_k^{-1}(y_i) = e_k^{-1}(e_k(x_i)), \;\; i \geq 1$

Seems like the natural way of doings encryption..
But . . . Not a very good way, as we’re going to see!

Electronic Code Book mode (ECB)

- **Advantages**
  - no block synchronization between sender and receiver is required
  - bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Block cipher operating can be parallelized
  - Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
  - Simple way of the block cipher.

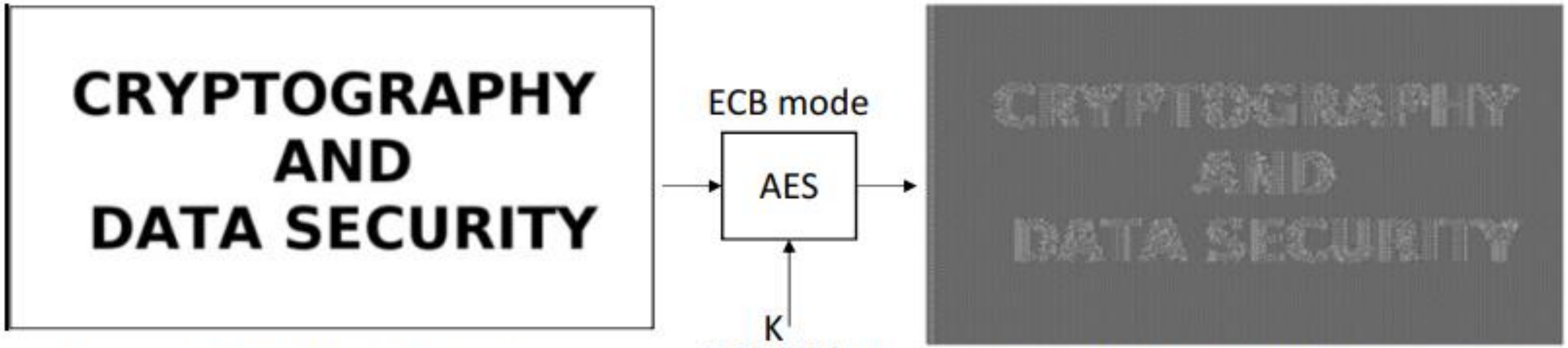
➢ **Disadvantages**

- ECB encrypts highly deterministically (Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext).
- identical plaintexts result in identical ciphertexts
- an attacker recognizes if the same message has been sent twice
- plaintext blocks are encrypted independently of previous blocks
- an attacker may reorder ciphertext blocks which results in valid plaintext

➢ **ECB mode is secure only in case the message is one block.**

ECB

- **Another weakness, Encryption of bitmaps in ECB mode**



Bitmap image before encryption

Encrypted bitmap image using ECB

Simply because ECB is deterministic.

Identical plaintext blocks are mapped into identical cyphertext blocks.

Statistical properties in the plaintext are preserved in the ciphertext

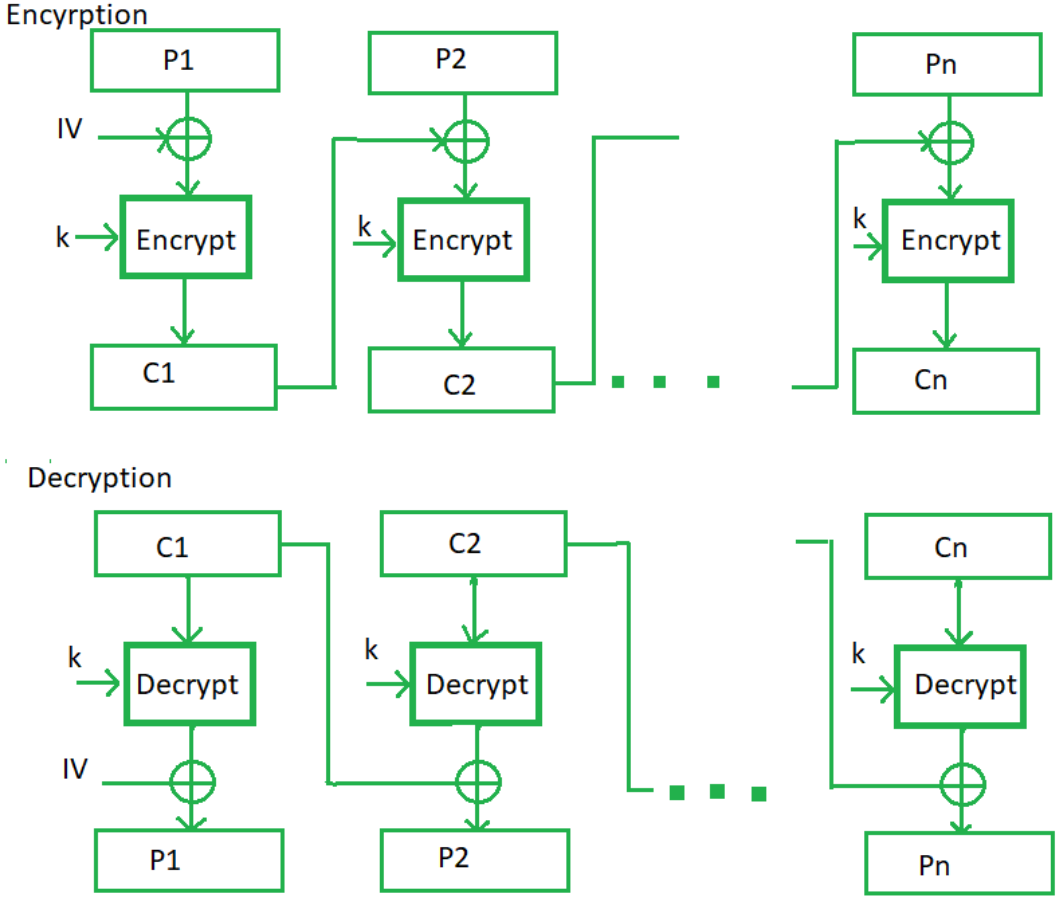
Modes of Operation for Block Ciphers

➢Encryption with Block Ciphers: Modes of Operation

- ✓ Electronic Codebook Mode (ECB)
- ✓ **Cipher Block Chaining Mode (CBC)**
- ✓ Cipher Feedback mode (CFB)
- ✓ Output Feedback mode (OFB)
- ✓ Counter mode (CTR)
- ✓ Galois Counter Mode (GCM)

Cipher Block Chaining Mode (CBC)

- ➢ It is an advancement made on ECB since ECB compromises some security requirements.
- ➢ In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.



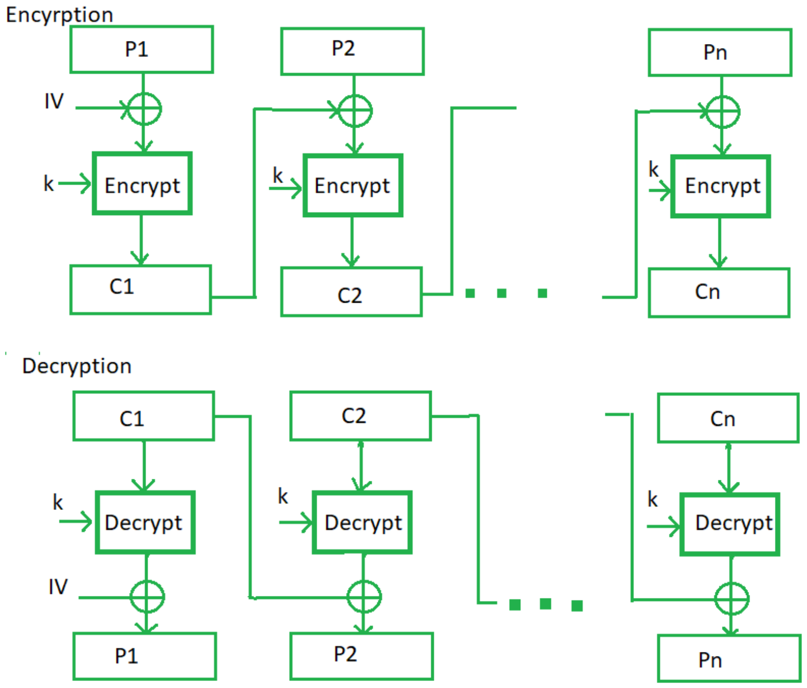
- ➢ In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.
- ❖ **Main goal:** Make the encryption probabilistic
- ❖ **Idea:** Use the ciphertext from the previous block, to impact the current block.
- ➢ No need for preprocessing during encryption / decryption
- ➢ Aallows random access to ciphertext
- ➢ Decryption is parallelizable: Plaintext block xj requires ciphertext blocks cj and cj-1

Cipher Block Chaining Mode (CBC)

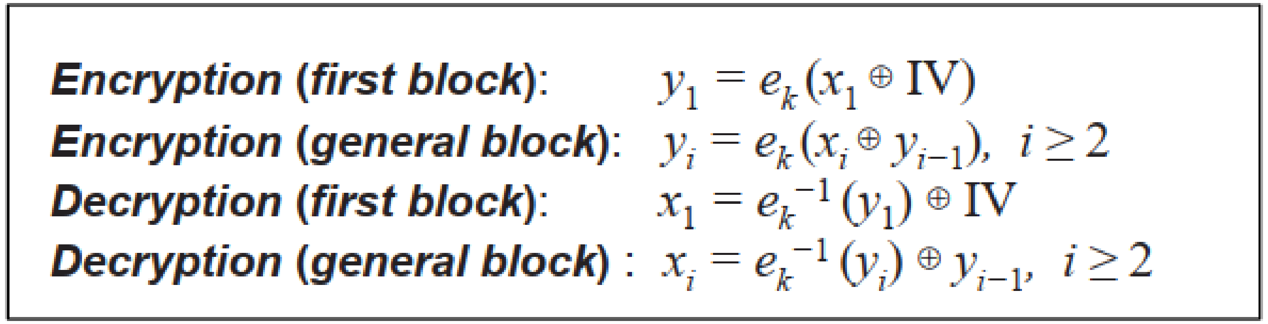
- Identical messages: changing IV or the first plaintext block results in different ciphertext
- Chaining: Ciphertext block cj depends on xj and all preceding plaintext blocks (dependency contained in cj-1)
- Error propagation: Single bit error on cj may flip the corresponding bit on xj+1, but changes xj significantly.
- IV need not be secret, but its integrity should be protected

There are two main ideas behind the CBC mode:

1. The encryption of all blocks are "chained together"
2. ciphertext *yi* depends not only on block *xi* but on all previous plaintext blocks as well



- The encryption is randomized by using an initialization vector (IV)



Encryption (first block): $y_1 = e_k(x_1 \oplus \mathrm{IV})$

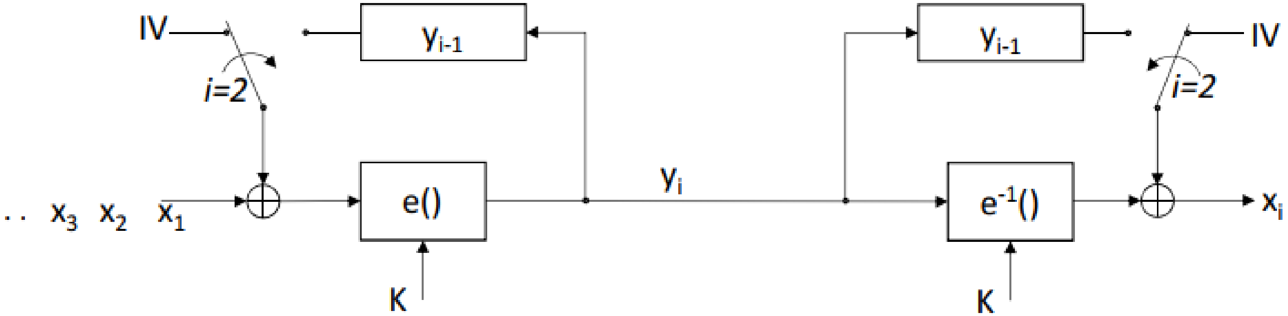
Encryption (general block): $y_i = e_k(x_i \oplus y_{i-1}),\ \ i \geq 2$

Decryption (first block): $x_1 = e_k^{-1}(y_1) \oplus \mathrm{IV}$

Decryption (general block) : $x_i = e_k^{-1}(y_i) \oplus y_{i-1},\ \ i \geq 2$

Cipher Block Chaining Mode (CBC)

- For the first plaintext block x_1 there is no previous ciphertext
  - an IV is added to the first plaintext to make each CBC encryption nondeterministic
  - the first ciphertext y_1 depends on plaintext x_1 and the IV
- The second ciphertext y_2 depends on the IV, x_1 *and* x_2
- The third ciphertext y_3 depends on the IV and x_1, x_2 *and* x_3, and so on



$y_1 = e(x_1 \oplus IV)$
$y_i = e(x_i \oplus y_{i-1})$, $i \geq 2$

$x_1 = e^{-1}(y_1) \oplus IV$
$x_i = e^{-1}(y_i) \oplus y_{i-1}$, $i \geq 2$

IV: Initialization Vector.

Cipher Block Chaining Mode (CBC)

Advantages of CBC

- CBC works well for input with large bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

Disadvantages of CBC

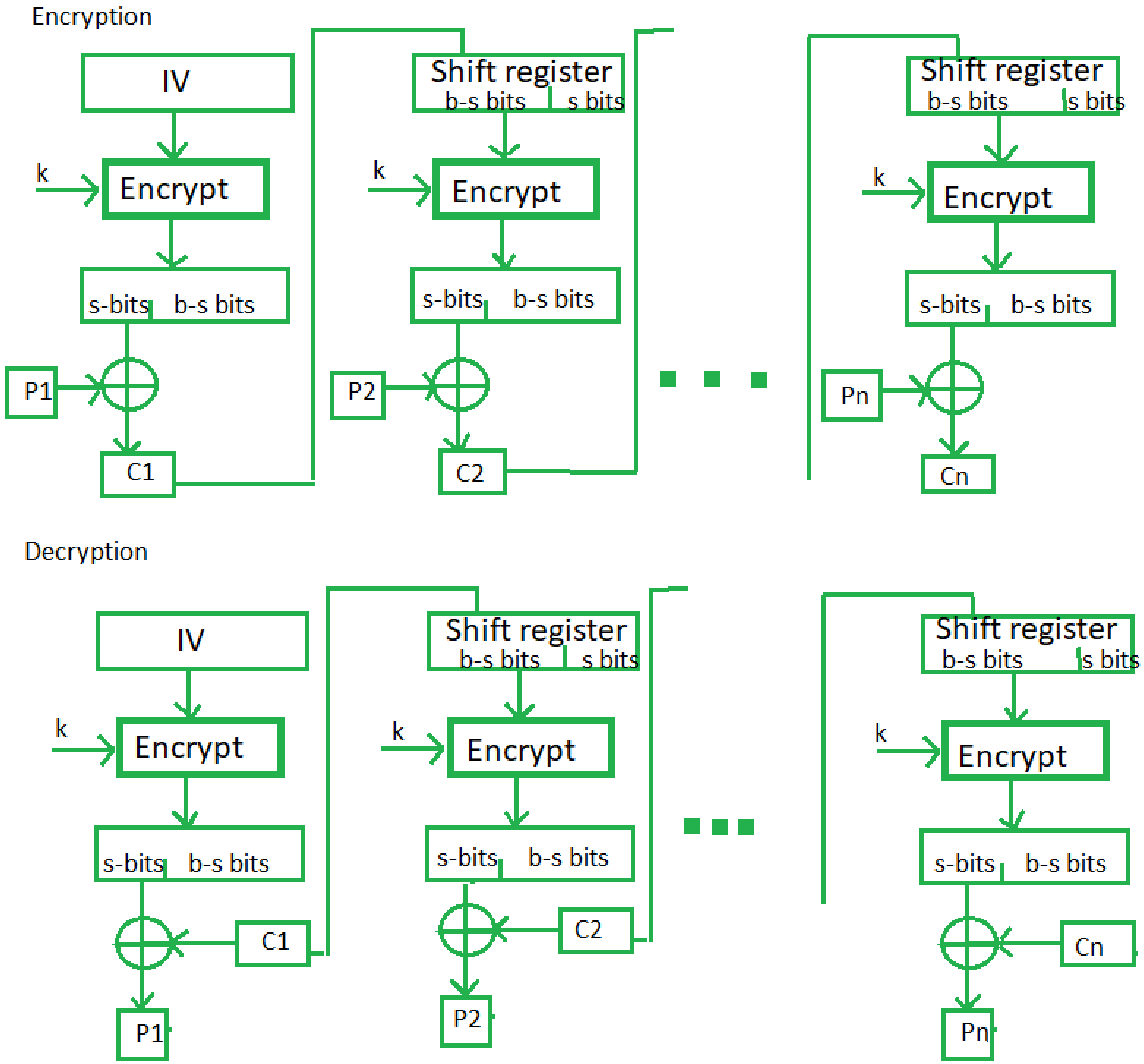
- Parallel encryption is not possible since every encryption requires a previous cipher.
- Doesn’t have to be a secret.
- Error transfer to the end

Modes of Operation for Block Ciphers

- Encryption with Block Ciphers: Modes of Operation
  - ✓ Electronic Codebook Mode (ECB)
  - ✓ Cipher Block Chaining Mode (CBC)
  - ✓ **Cipher Feedback mode (CFB)**
  - ✓ Output Feedback mode (OFB)
  - ✓ Counter mode (CTR)
  - ✓ Galois Counter Mode (GCM)

Cipher Feedback Mode (CFB)

- It uses a block cipher as a building block for an asynchronous **stream cipher**
- In this mode the cipher is given as feedback to the next block of encryption with some new specifications:
  - first, an initial vector IV is used for first encryption
  - output bits are divided as a set of *s* and *b-s* bits.
  - The left-hand side *s* bits are selected along with plaintext bits to which an XOR operation is applied.
  - The result is given as input to a shift register having b-s bits to LHS, and s bits to RHS and the process continues.

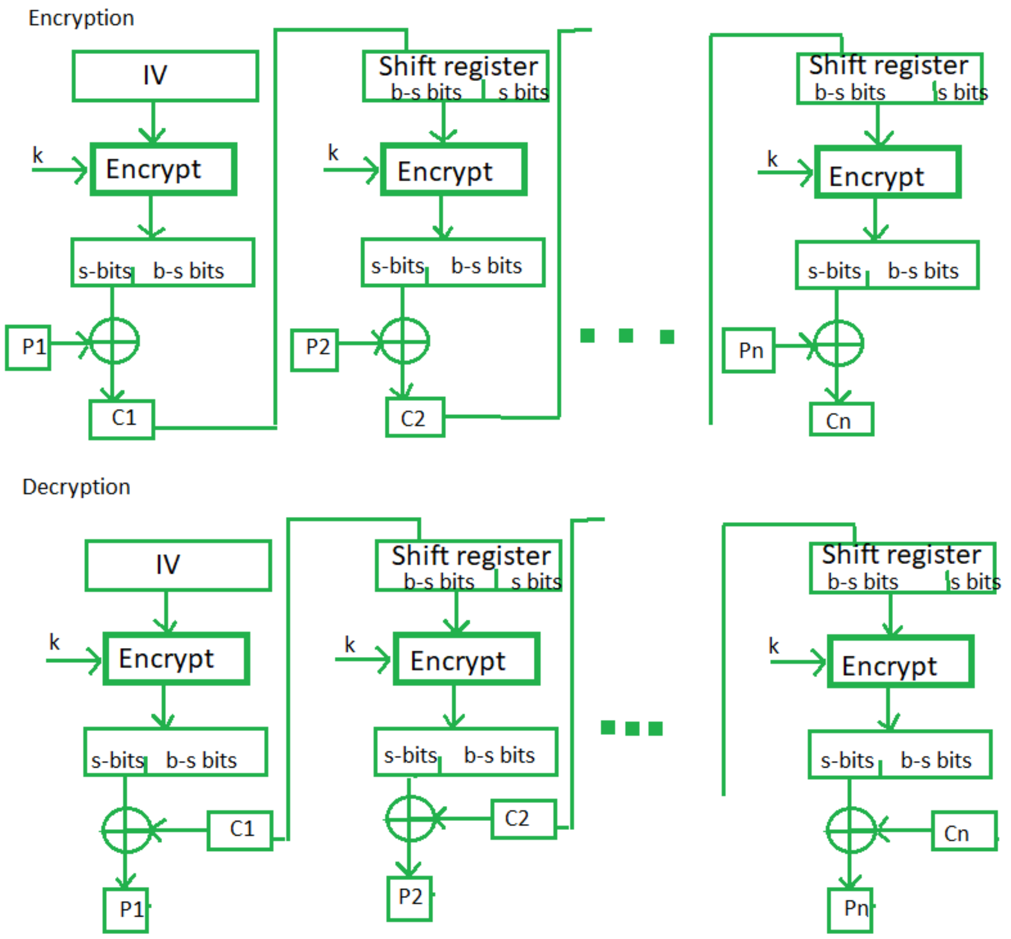


Cipher Feedback Mode (CFB)

Goal: Generate an unpredictable key stream for stream cipher
Idea: Construct the key stream generator using a block cipher

- Allows random access to ciphertext
- Decryption is parallelizable : Plaintext block xj requires ciphertext blocks cj and cj-1
- Identical messages: as in CBC
- Chaining: Similar to CBC
- Error propagation: Single bit error on cj may flip the corresponding bit on xj , but changes xj+1 significantly.
- IV need to be secret (XORed with x1)

Encryption (first block): $y_1 = e_k(\mathrm{IV}) \oplus x_1$
Encryption (general block): $y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$
Decryption (first block): $x_1 = e_k(\mathrm{IV}) \oplus y_1$
Decryption (general block) : $x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$



Cipher Feedback Mode (CFB)

➢ Advantages of CFB

•Since, there is some data loss due to the use of shift register, thus it is difficult for applying cryptanalysis.

➢ Disadvantages of using CFB

- The drawbacks of CFB are the same as those of CBC mode.
- Both block losses and concurrent encryption of several blocks are not supported by the encryption.
- Decryption, however, is parallelizable and loss-tolerant.

MSA
UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!

Any Question?