MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

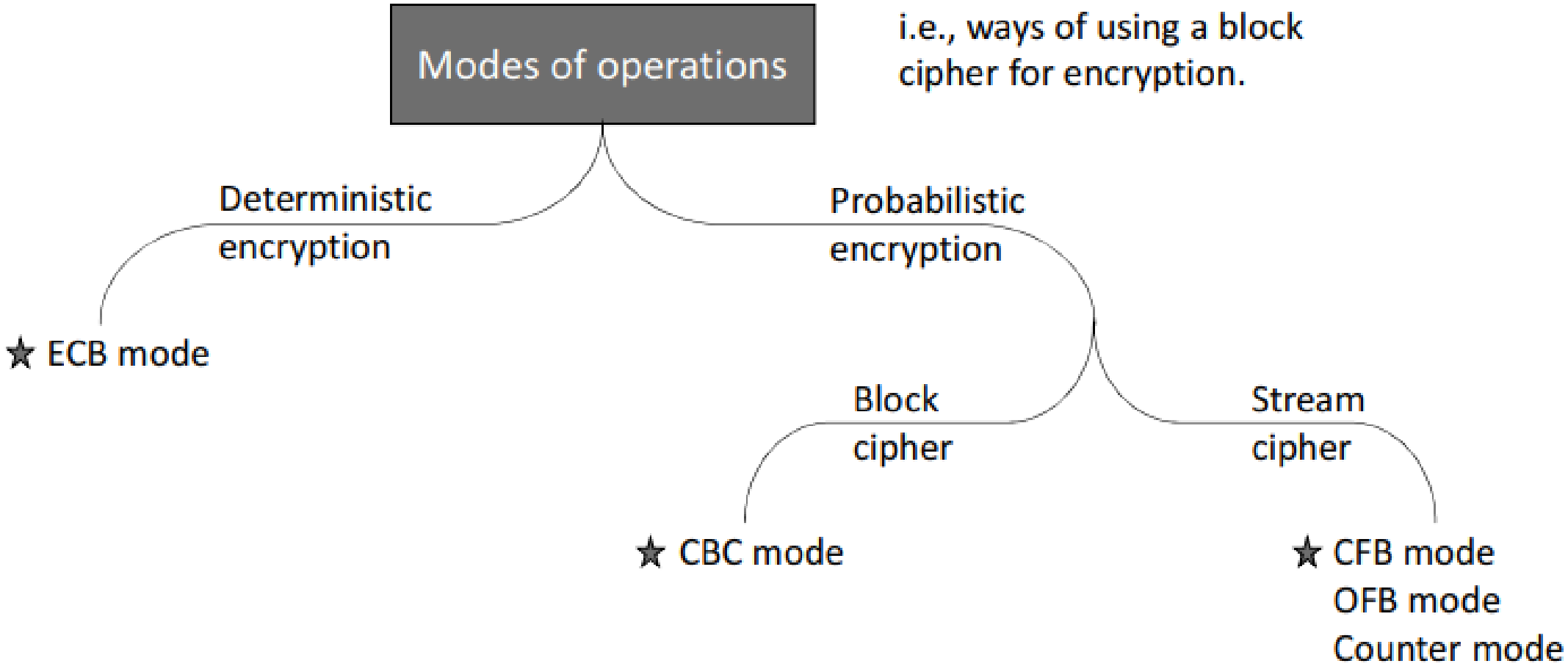
Cryptography
ECE5632 - Spring 2024

Lecture 5A

Dr. Farah Raad

Lecture Topic

Modes of Operation for Block Ciphers


Modes of operations
i.e., ways of using a block cipher for encryption.
Deterministic encryption
Probabilistic encryption
★ ECB mode
Block cipher
Stream cipher
★ CBC mode
★ CFB mode
OFB mode
Counter mode

★ i.e., today.

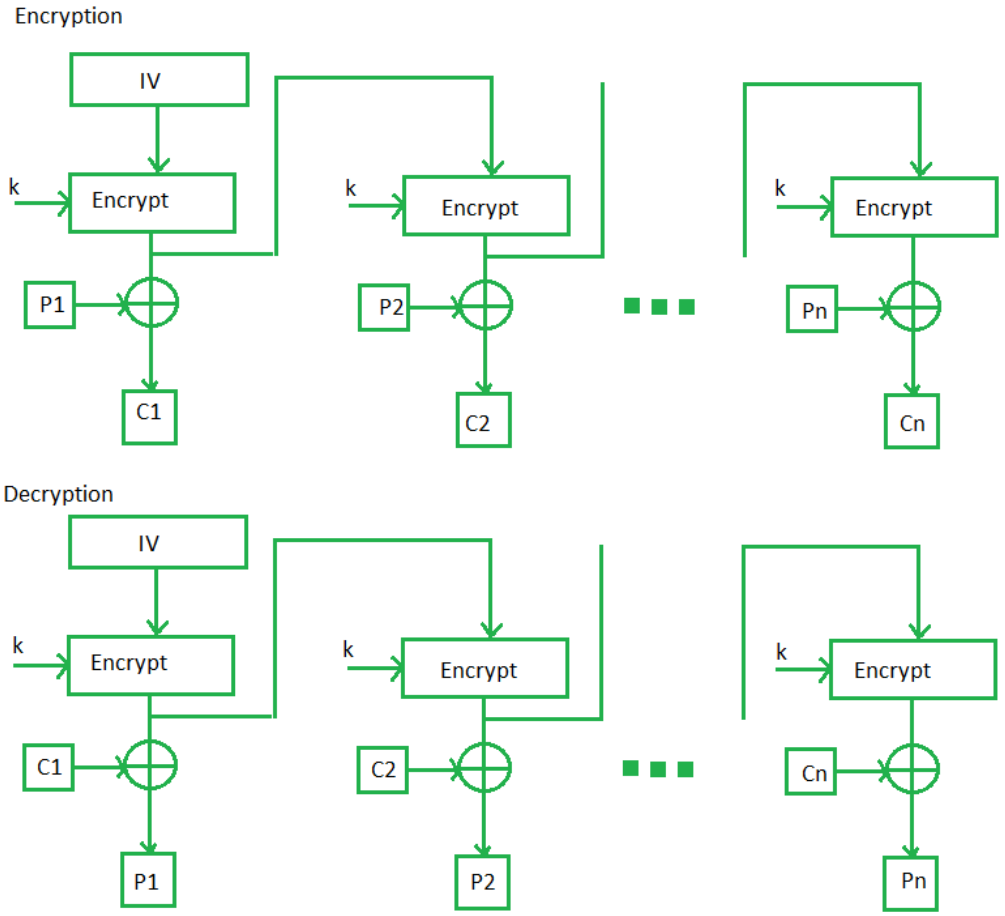
Modes of Operation for Block Ciphers

- 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)

Output Feedback mode (OFB)

- It is used to build a *synchronous* **stream cipher** from a block cipher
- The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output.

- In this output feedback mode, all bits of the block are sent instead of sending selected s bits.
- The Output Feedback mode of block cipher holds great resistance towards bit transmission errors.
- It also decreases the dependency or relationship of the cipher on the plaintext.



Encryption (first block): $s_1 = e_k(\text{IV})$ *and* $y_1 = s_1 \oplus x_1$

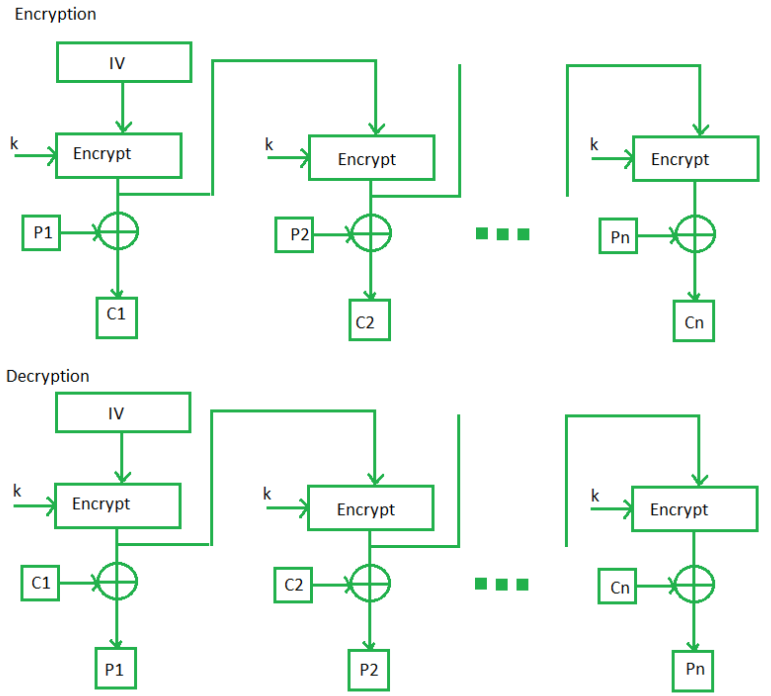
Encryption (general block): $s_i = e_k(s_{i-1})$ *and* $y_i = s_i \oplus x_i, \quad i \geq 2$

Decryption (first block): $s_1 = e_k(\text{IV})$ *and* $x_1 = s_1 \oplus y_1$

Decryption (general block) : $s_i = e_k(s_{i-1})$ *and* $x_i = s_i \oplus y_i, \quad i \geq 2$

Output Feedback mode (OFB)

- Preprocessing possible (keep enc/decrypting previous output block)
- No random access
- Not parallelizable
- Identical messages: same as CBC (changing IV or the plaintext block results in different ciphertext)
- No chaining dependencies
- Error propagation: Single bit error on Pj may only affect the corresponding bit of Cj
- IV need not be secret, but should be changed if a previously used key is to be used again



Output Feedback mode (OFB)

➢ Advantages of OFB

In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.

➢ Disadvantages of OFB

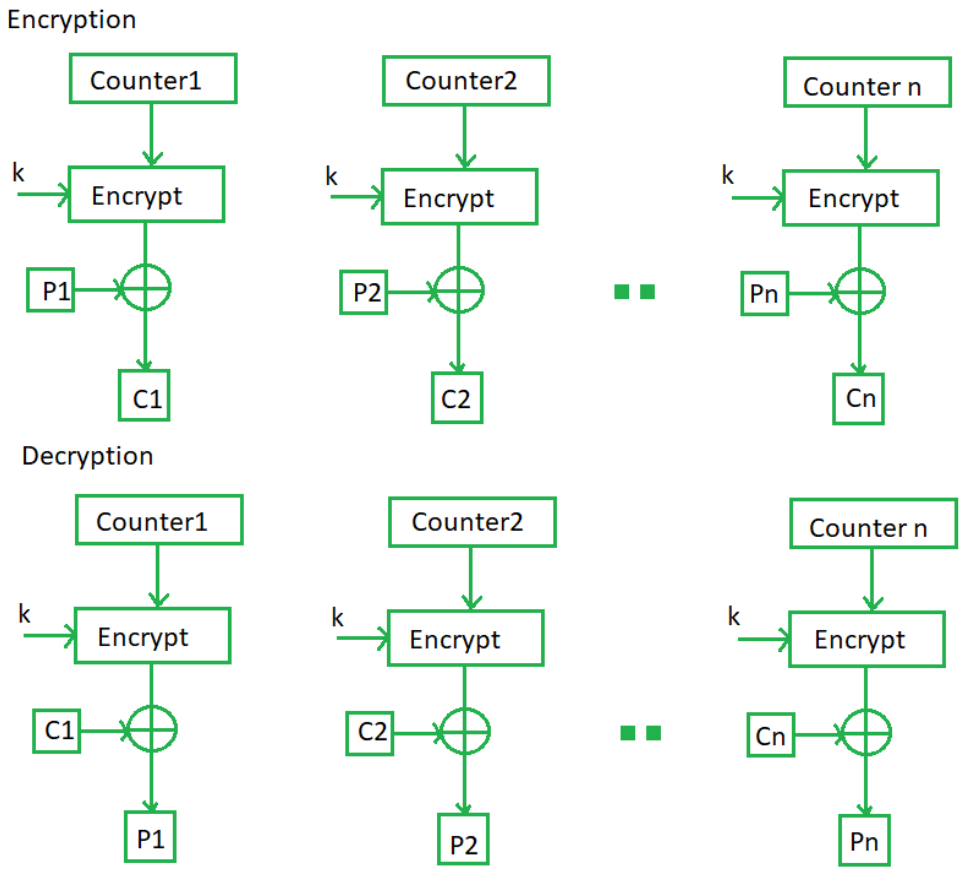
The drawback of OFB is that, because to its operational modes, it is more susceptible to a message stream modification attack than CFB.

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)

Counter mode (CTR)

- It uses a block cipher as a **stream cipher** (like the OFB and CFB modes)
- The Counter Mode is a simple counter-based block cipher implementation.
- Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block.
- The CTR mode is independent of feedback use and thus can be implemented in parallel.
- The input to the block cipher is a counter which assumes a different value every time the block cipher computes a new key stream block.
- Unlike CFB and OFB modes, the CTR mode can be parallelized since the 2nd encryption can begin before the 1st one has finished.
- Desirable for high-speed implementations, e.g., in network routers.

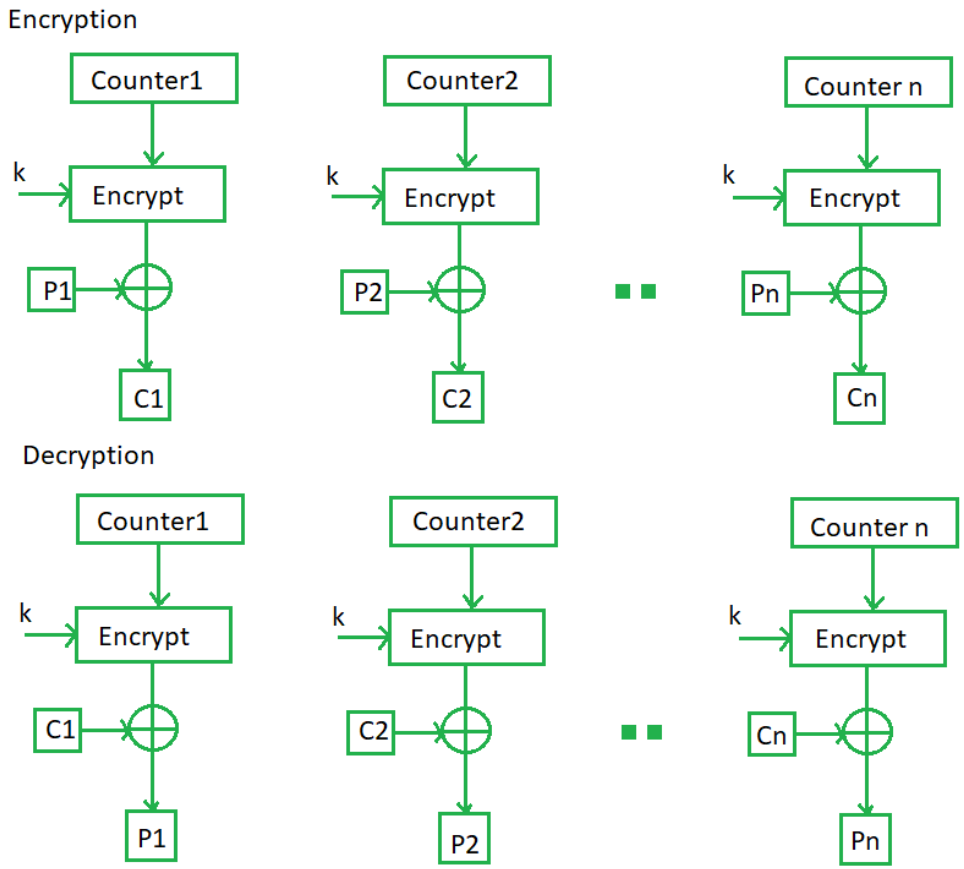


Counter mode (CTR)

- Preprocessing possible (inc/decrement and enc/decrypt counter)
- Allows random access
- Both encryption & decryption are parallelizable : Encrypted counter is sufficient to enc/decrypt
- Identical messages: changing once results in different ciphertext
- No chaining dependencies
- No error propagation
- Counter should be random, and should be changed if a previously used key is to be used again.

Encryption: $y_i = e_k(\text{IV} \parallel \text{CTR}_i) \oplus x_i, \quad i \geq 1$

Decryption : $x_i = e_k(\text{IV} \parallel \text{CTR}_i) \oplus y_i, \quad i \geq 1$



Counter mode (CTR)

➢ Advantages of Counter

• Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext.

• Parallel execution of encryption is possible as outputs from previous stages are not chained as in the case of CBC.

➢ Disadvantages of Counter

• The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is a severe drawback.

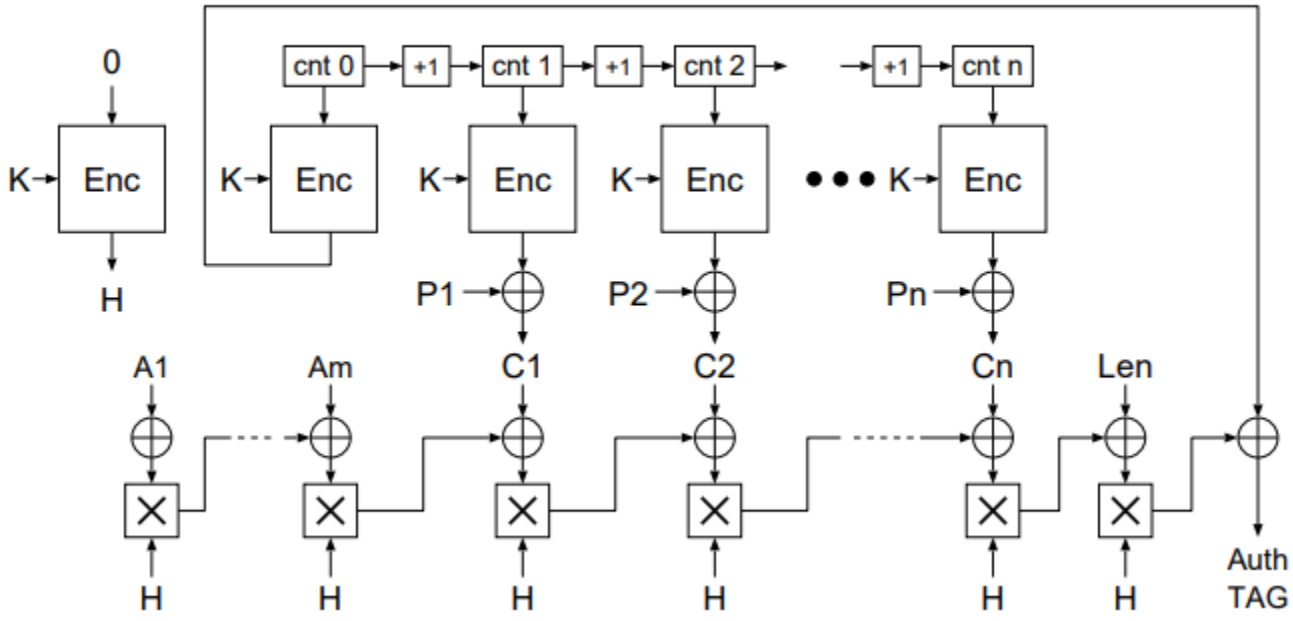
• The recovery of plaintext is erroneous when synchronization is lost.

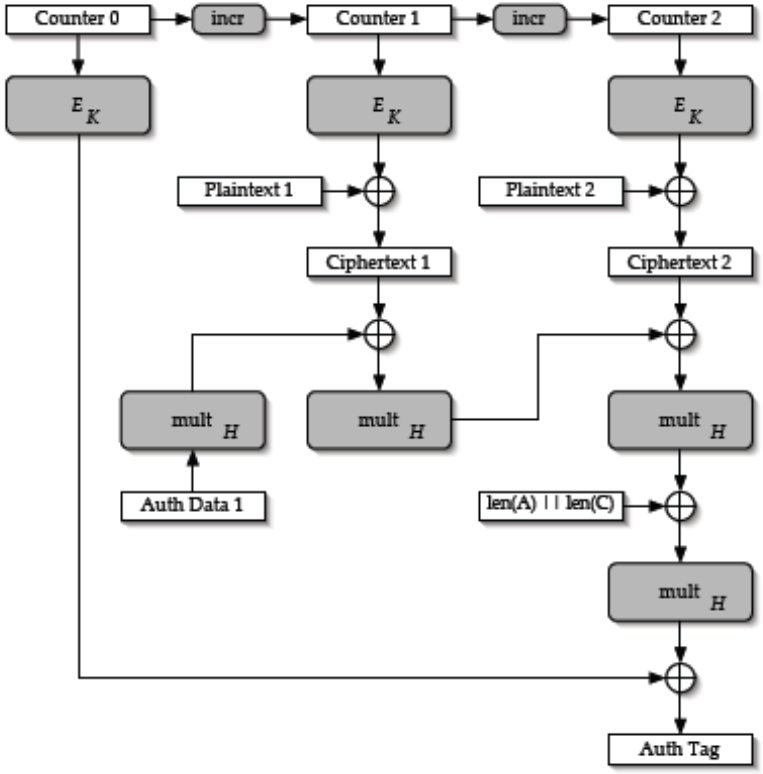
Modes of Operation for Block Ciphers Basic Features

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No	Yes	Yes	Yes	Yes
Basic speed	s_{ECB}	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx s_{ECB}$
Capability for parallel processing and pipelining	Encryption and decryption	Encryption and decryption	None	Decryption only	Decryption only
Cipher operations	Encryption and decryption	Encryption only	Encryption only	Encryption only	Encryption and decryption
Preprocessing	No	Yes*	Yes*	No	No
Random access	**Yes**	**Yes**	No	**Yes**	**Yes**

Galois Counter Mode (GCM)

- Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption.
- It also computes a *message authentication code* (MAC), i.e., a cryptographic checksum is computed for a message





Galois Counter Mode (GCM)

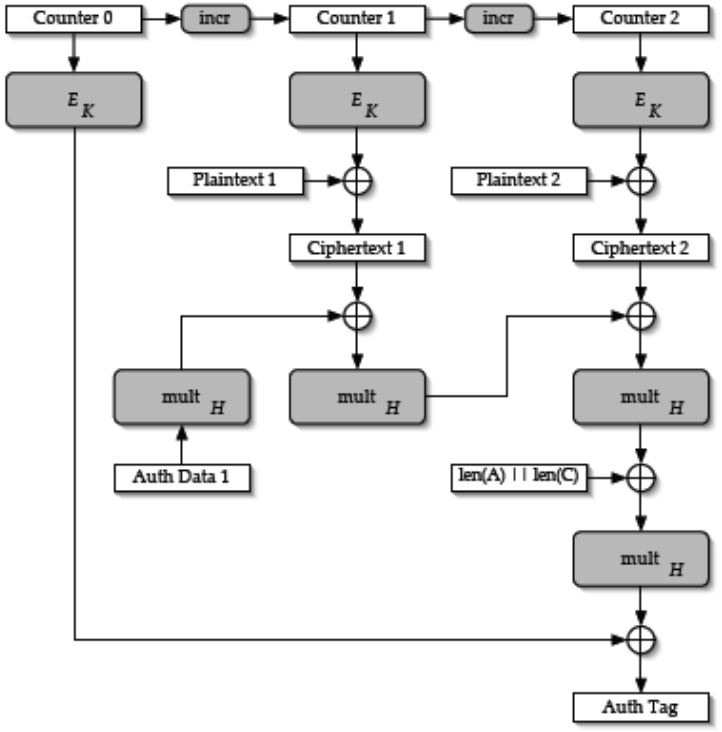
- By making use of GCM, two additional services are provided:

1. Message Authentication

The receiver can make sure that the message was really created by the original sender.

2. Message Integrity

The receiver can make sure that nobody tampered with the ciphertext during transmission.



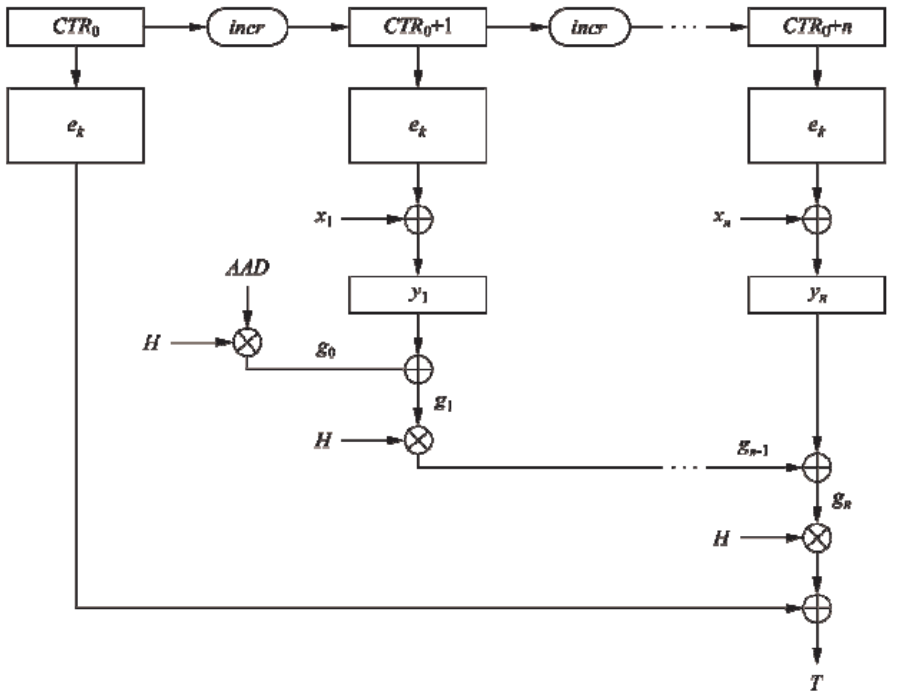
Galois Counter Mode (GCM)

➢ For encryption

- An initial counter is derived from an IV and a serial number
- The initial counter value is incremented then encrypted and XORed with the first plaintext block.
- For subsequent plaintexts, the counter is incremented and then encrypted.

➢ For authentication

- A chained Galois field multiplication is performed
- For every plaintext an intermediate authentication parameter *gi* is derived
- *gi* is computed as the XOR of the current ciphertext and the last *gi*-1, and multiplied by the constant *H*
- *H* is generated by encryption of the zero input with the block cipher
- All multiplications are in the 128-bit Galois field GF(2^{128})



Encryption:

a. Derive a counter value CTR_0 from the IV and compute $\mathrm{CTR}_1 = \mathrm{CTR}_0 + 1$

b. Compute ciphertext: $y_i = e_k(\mathrm{CTR}_i) \oplus x_i, \quad i \geq 1$

Authentication:

a. Generate authentication subkey $H = e_k(0)$

b. Compute $g_0 = AAD \times H$ (Galois field multiplication)

c. Compute $g_i = (g_{i-1} \oplus y_i) \times H, \ 1 \leq i \leq n$ (Galois field multiplication)

d. Final authentication tag: $T = (g_n \times H) \oplus e_k(\mathrm{CTR}_0)$

Modes of Operation for Block Ciphers Summary

Choice of encryption mode affects

- Encryption/decryption speed
- Security against active adversaries (bit flips)
- Security against passive adversaries (ECB)
- Error propagation

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?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt
Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451
Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg