ĐẠI HỌC
BÁCH KHOA

25 YEARS ANNIVERSARY
SOICT

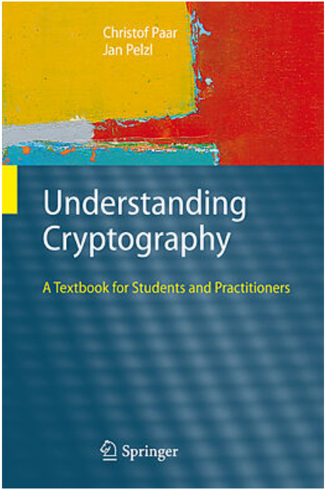
HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

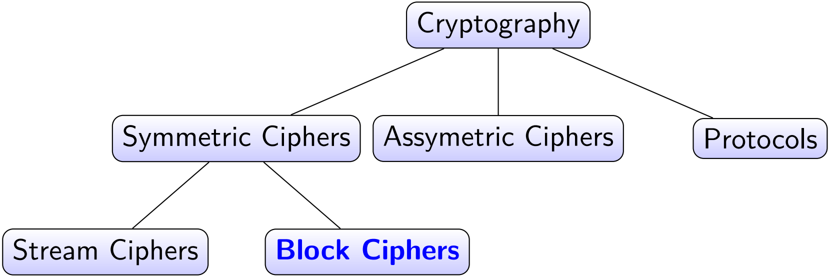
Modes of Operation

Textbook

https://www.crypto-textbook.com


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

Cryptography



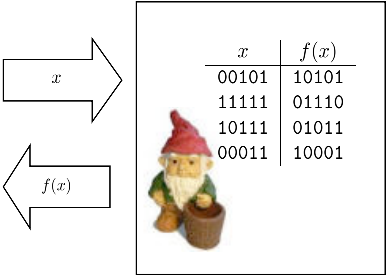
Ideal block cipher

- In fact, we consider AES or 3DES as an **ideal block cipher**
- That is, for each key k, the mapping

$$F_k(x) = \mathrm{Enc}(k, x)$$

is an independent random permutation from X onto itself.

Random Permutation



x	$f(x)$
00101	10101
11111	01110
10111	01011
00011	10001

```
upon receiving the $i$th query $x_i \in \mathcal{X}$ from $\mathcal{A}$ do:
    if $x_i = x_j$ for some $j < i$
        then $y_i \leftarrow y_j$
        else $y_i \overset{R}{\leftarrow} \mathcal{X} \setminus \{y_1, \ldots, y_{i-1}\}$
    send $y_i$ to $\mathcal{A}$
```

Modes of Operations

Question: How to encrypt long messages? (using AES)

Answer: There are several ways of encrypting long messages with a block cipher:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Output Feedback ()
- Output Feedback (OFB)
- Counter Mode (CTR)

Modes of Operation: One-time key and many-time key.

Example applications

Many-time key

File systems

- Same AES key used to encrypt many files.

IPSec

- Same AES key used to encrypt many packets.

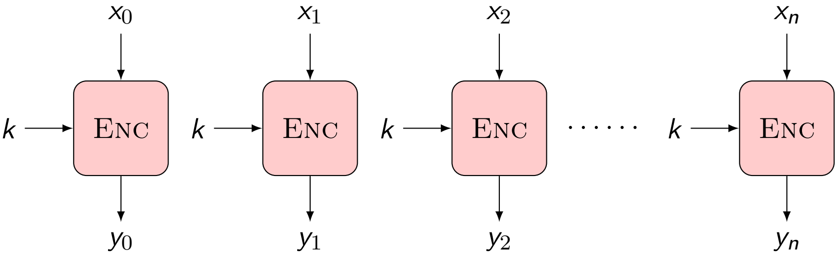
Outline

1. Electronic Codebook Mode (ECB)

2. Cipher Block Chaining Mode (CBC)

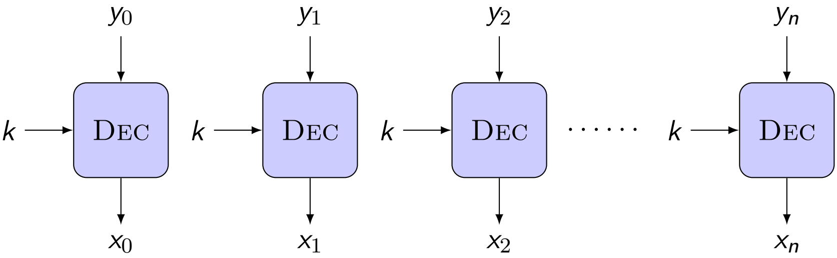
3. Stream cipher

ECB (Electronic code book)



- The messages are partitioned into b-bit blocks, where b is the block size.
- If the length of the message is not a multiple of b bits, it must be padded $10..0$ to a multiple of b bits prior to encryption.
- The padding operation is invertible.

ECB: Decryption



ECB is not secure

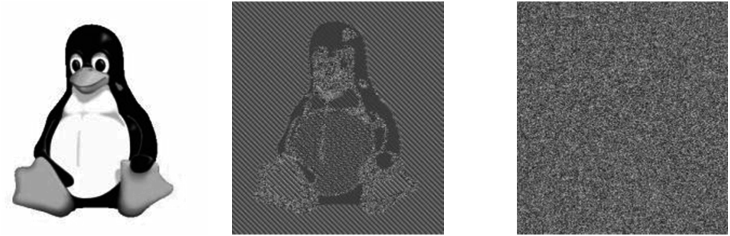


Figure: The middle figure is an encryption using ECB mode; the figure on the right is an encryption using a secure mode.

- Problem: If $x_i = x_j$ then $y_i = y_j$.
- ECB is secure if the message is random (eg., the keys).

Example: Electronic Bank Transfer

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

1. Assumption: Each of the fields has exactly the size of the block cipher width (for example 128 bits)
2. Assumption: The encryption key k_{AB} between the two banks A and B does not change too frequently.

Attacker Oscar

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

1. He opens one account at bank A and one at bank B.
2. He sends \$1.00 transfers from his account at bank A to his account at bank B repeatedly.
3. He observes the ciphertexts going through the communication network

   $$B_1 \parallel B_2 \parallel B_3 \parallel B_4 \parallel B_5$$

   and he stores blocks $B_1,\ B_3,\ B_4$.
4. For all transfers that are made from B_1 to B_3, he replaces block 4 with B_4.

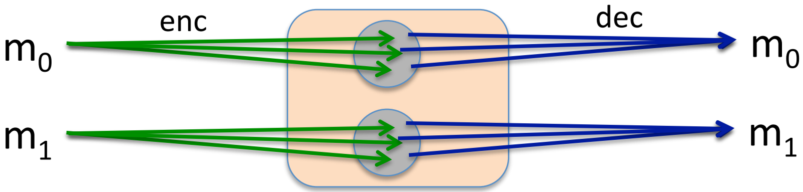
Outline

1. Electronic Codebook Mode (ECB)

2. Cipher Block Chaining Mode (CBC)

3. Stream cipher

Randomized encryption



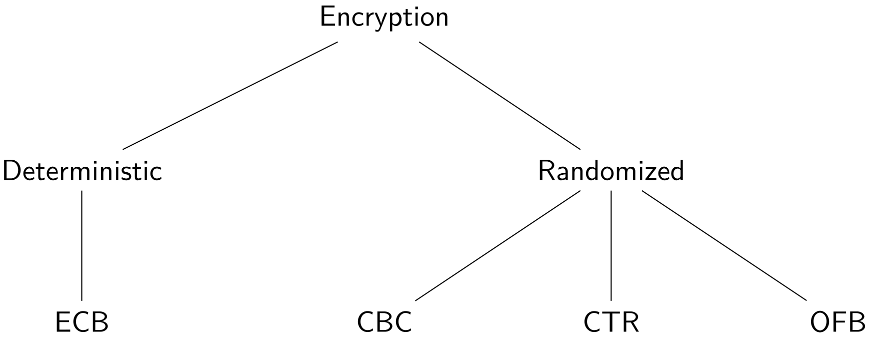
- Enc(k, m) is a randomized algorithm.
- Given the same plaintext message twice, encryption must produce different outputs.
- Ciphertext must be longer than plaintext
- Roughly speaking: CT-size = PT-size + "# random bits"

Exercise

Write the Dec() function for the following Enc().

$$\text{Enc}(k, m) := \begin{cases} r = \texttt{random}() \\ c = \texttt{AES}(k, r) \oplus m \\ \text{output } (r, c) \end{cases}$$

Types of Encryption



Encryption

Deterministic

Randomized

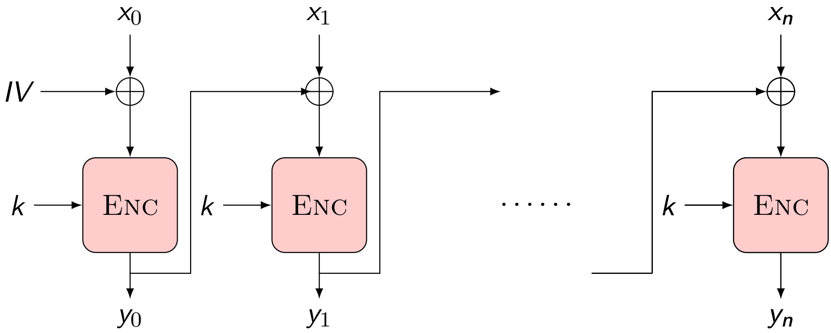
ECB

CBC

CTR

OFB

Cipher Block Chaining mode (CBC)



Algorithm. Choose IV ("initialization value") randomly, use each y_i is "IV" for M_{i+1}. Transmit IV with ciphertext:

$$IV \| y_0 \| y_1 \| \ldots \| y_n$$

How to use the *IV*?

- *IV* does not need to be kept a secret
- But it must be “nonce” = “number used only once”

Example

1. True random number
2. Counter value (must be stored by Alice)
3. $\mathrm{ID}_A \| \mathrm{ID}_B \| \mathrm{time}$

A CBC technicality: PKCS5 padding

- The value is the number of bytes that need to be added.
- Padding n byte, for $n > 0$

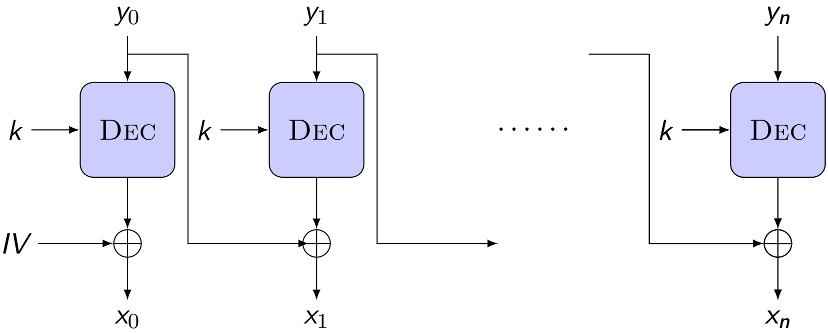
n	n	n	n	$\cdots$	n

- if no padding is needed, we add a dummy block:

b	b	b	b	b	$\cdots$	b

where b is block size (in bytes).

CBC: Decryption



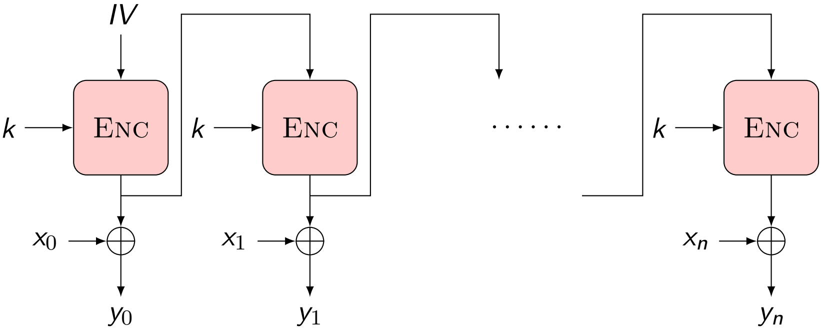
Outline

1. Electronic Codebook Mode (ECB)

2. Cipher Block Chaining Mode (CBC)

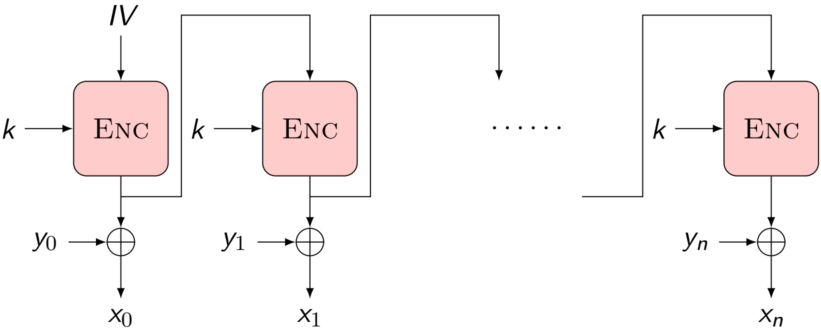
3. Stream cipher

Output Feedback Mode (OFB)

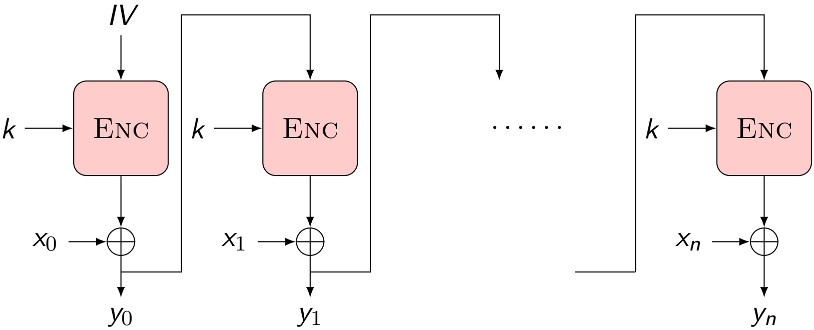


Algorithm. Similar to CBC mode. Use a random IV transmitted with the ciphertext.

OFB: Decryption

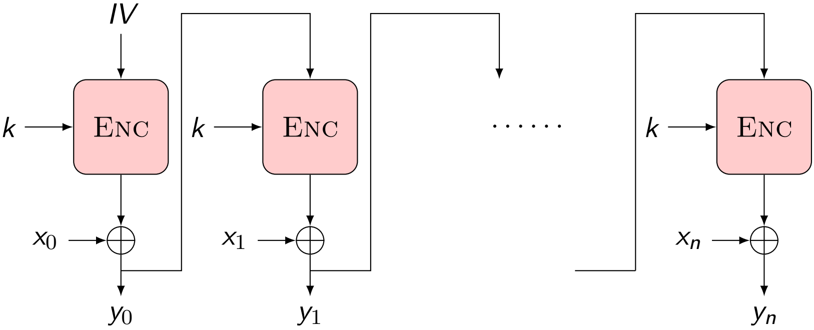


Cipher Feedback Mode (CFB)



Exercise

What is the decryption for CFB mode?



Counter Mode (CTR)

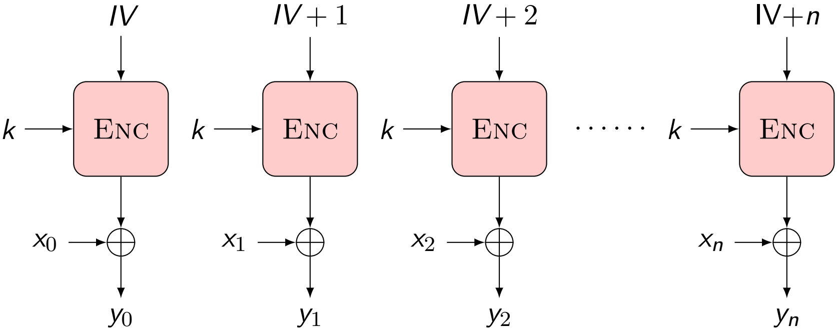
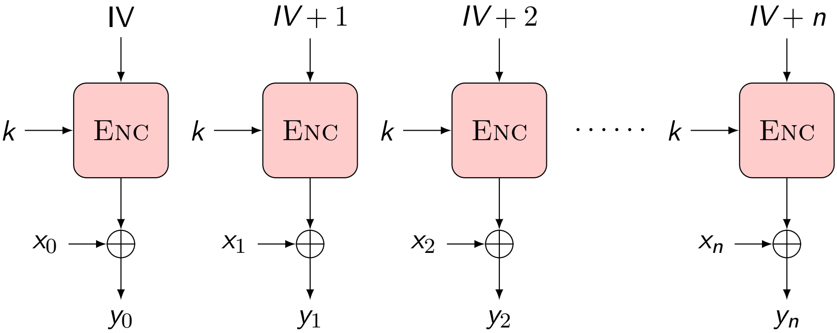


Figure: Use a random IV transmitted with the ciphertext.

Exercise

What is the decryption for CTR mode?



Exercise

- Let m be a message consisting of ℓ AES blocks (say $\ell = 100$).
- Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob.
- Due to a network error, ciphertext block number $\ell/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly.
- Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

Exercise

- Let m be a message consisting of ℓ AES blocks (say $\ell = 100$).
- Alice encrypts m using randomized counter mode and transmits the resulting ciphertext to Bob.
- Due to a network error, ciphertext block number $\ell/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly.
- Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you!

soict.hust.edu.vn/ fb.com/groups/soict