

# Nội dung

- Mã khối lý tưởng
- Chế độ ECB
- Mã hoá xác suất
- Chế độ CBC
- Một số chế độ mã khối dựa trên mã dòng

# Mã khối lý tưởng

- Trên thực tế, người ta xem AES hoặc 3DES như hệ mã khối lý tưởng  $E(k, x)$ .
- Tức là, với mỗi khoá  $k$ , ánh xạ  
$$F_k(x) = E(k, x)$$
là một hoán vị ngẫu nhiên độc lập.

# Nội dung

- **Mã khối lý tưởng**
- Chế độ ECB
- Mã hoá xác suất
- Chế độ CBC
- Một số chế độ mã khối dựa trên mã dòng

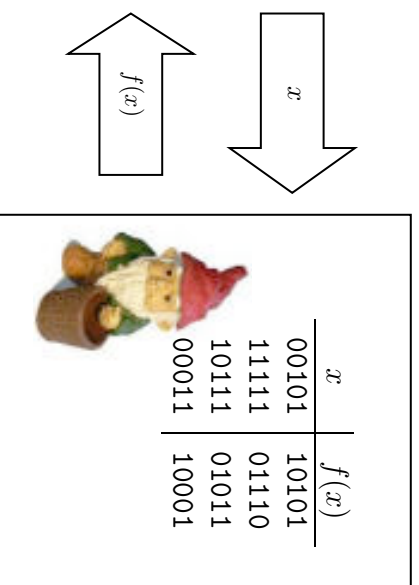
## Nhập môn An Toàn Thông Tin

### Các chế độ mã khối

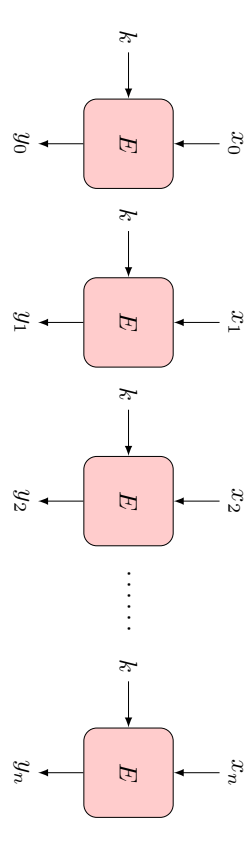
# Các chế độ sử dụng

- **Câu hỏi:** Làm thế nào để mã hoá thông điệp với độ dài bất kỳ? (dùng AES hoặc 3DES)
- **Trả lời:** Dùng một trong các chế độ sau:
  - “ECB” = “Electronic code book”
  - “CTR” = “Counter mode”
  - “CBC” = “Cipher Block Chaining”
  - “OFB” = “Output Feedback” • V.V.

# Hoàn vị ngẫu nhiên



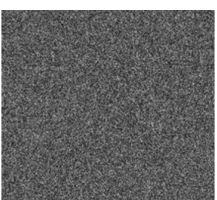
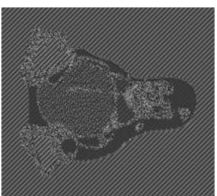
# ECB (Electronic code book)

- 
- The diagram shows a sequence of input blocks  $x_0, x_1, x_2, \dots, x_n$  being encrypted using a function  $E$  with a key  $k$  to produce output blocks  $y_0, y_1, y_2, \dots, y_n$ . Each block is encrypted independently.
- Dữ liệu được chia thành các khối khối  $b$  bit, với  $b$  = kích thước khối.
  - Với dữ liệu không chia hết cho  $b$  bit: Thêm dãy “10..0” để độ dài thông điệp chia hết cho  $b$ .
  - Phép toán padding này cho có tính khả nghịch. Nó cho phép giải mã.

# Nội dung

- Mã khối lý tưởng
- **Chế độ ECB**
- Mã hoá xác suất
- Chế độ CBC
- Một số chế độ mã khối dựa trên mã dòng

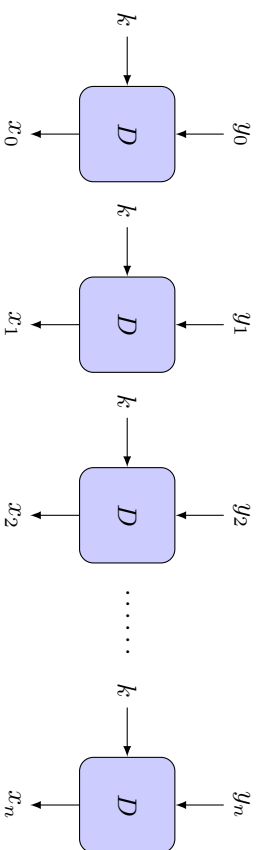
# ECB không an toàn



Hình: Bên trái là Bản rõ. Ở giữa là chế độ ECB. Bên phải là Mã hoá an toàn

- **Vấn đề:** Nếu  $x_i = x_j$  thì  $y_i = y_j$
- ECB chỉ an toàn khi mã hoá dữ liệu ngẫu nhiên (Ví dụ, mã hoá các khoá).

# ECB: giải mã



# Oscar tấn công

Block # 1 2 3 4 5

Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount \$
----------------	-------------------	------------------	---------------------	-----------

1. Oscar mở một tài khoản tại ngân hàng A và một tài khoản tại ngân hàng B
2. Oscar chuyển nhiều lần 1\$ từ tài khoản của anh ta ở ngân hàng A sang tài khoản ở ngân hàng B
3. Oscar bắt gói tin trên đường truyền và nhận được các bản mã giống nhau và anh ta giữ lại bản mã  $B_4$   
 $B_1 || B_2 || B_3 || B_4 || B_5$
4. Trong tương lai, mỗi khi thấy lệnh chuyển tiền từ  $B_1$  tới  $B_3$ , thay block thứ 4 bởi  $B_4$

# Ví dụ: Chuyển tiền giữa hai ngân hàng

Block # 1 2 3 4 5

Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount \$
----------------	-------------------	------------------	---------------------	-----------

1. Giả sử: kích thước mỗi trường là n-bit (ví dụ 128 bit)
2. Giả sử: khoá  $k_{AB}$  để trao đổi thông tin giữa hai ngân hàng không thay đổi thường xuyên

# Mã hoá xác suất

- Mã hóa hai lần của cùng một thông điệp sẽ cho hai bản mã khác nhau
- Bản mã phải dài hơn bản rõ
- Nói một cách nôm na:

**Kích thước bản mã =  
Kích thước bản rõ + “dãy bit ngẫu nhiên”**



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

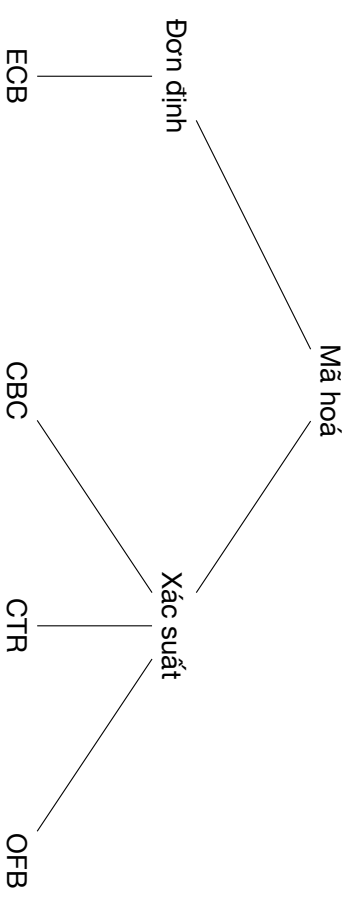
## Nội dung

- Mã khối lý tưởng
- Chế độ ECB
- **Mã hoá xác suất**
- Chế độ CBC
- Một số chế độ mã khối dựa trên mã dòng



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# Dạng mã hoá



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

## Bài tập

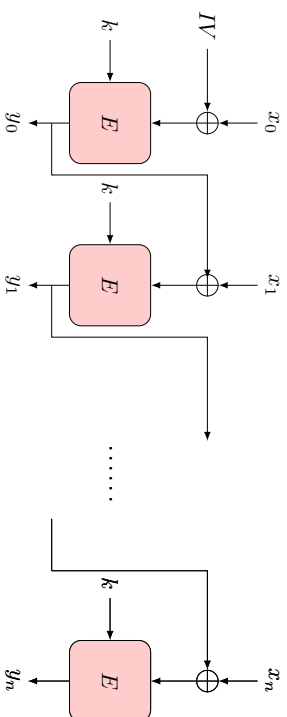
- Hãy viết hàm giải mã cho hàm mã hoá Enc được định nghĩa bởi

$Enc(k, m)$  :  
 $r = \text{random}()$   
 $c = \text{AES}(k, r) \oplus m$   
 $\text{return } (r, c)$



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# Chế độ CBC



**Thuật toán.** Chọn IV (“initialization value”) một cách ngẫu nhiên, sau đó dùng  $y_i$  như “IV” cho  $x_{i+1}$ . Gửi IV cùng với bản mã

$$IV \parallel y_0 \parallel y_1 \parallel \dots \parallel y_n$$

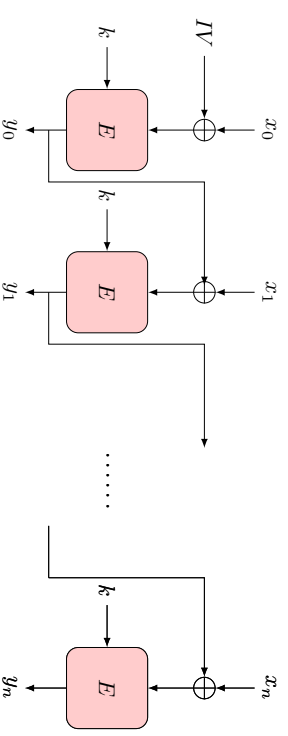
# Sử dụng IV như thế nào?

- IV không cần giữ bí mật
- Nhưng phải là “nonce” = “number used only once”
- **Ví dụ:** IV có thể là
  - ngẫu nhiên “thật”
  - bộ đếm “counter” (phải được lưu trữ bởi Alice)
  - $ID_A \parallel ID_B \parallel \text{time}$

# Nội dung

- Mã khối lý tưởng
- Chế độ ECB
- Mã hoá xác suất
- **Chế độ CBC**
- Một số chế độ mã khối dựa trên mã dòng

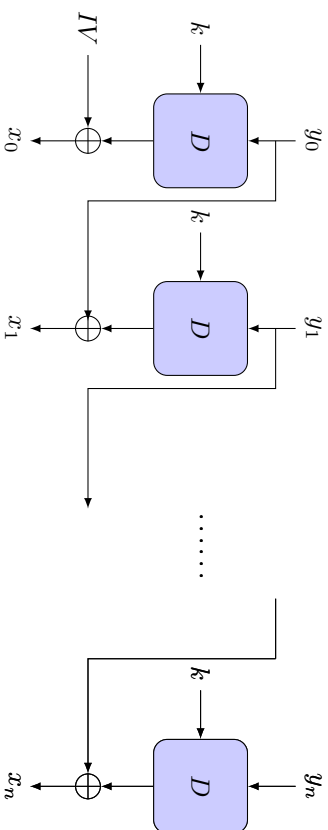
# CBC: công thức đại số



$$y_{-1} = IV \quad // \text{ Khởi tạo}$$

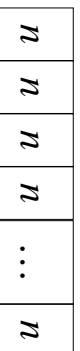
$$y_i = E_k(y_{i-1} \oplus x_i) \quad \text{với } i = 0, 1, \dots$$

# CBC: giải mã



# Padding cho CBC

- Padding  $n$  byte, với  $n > 0$ ,

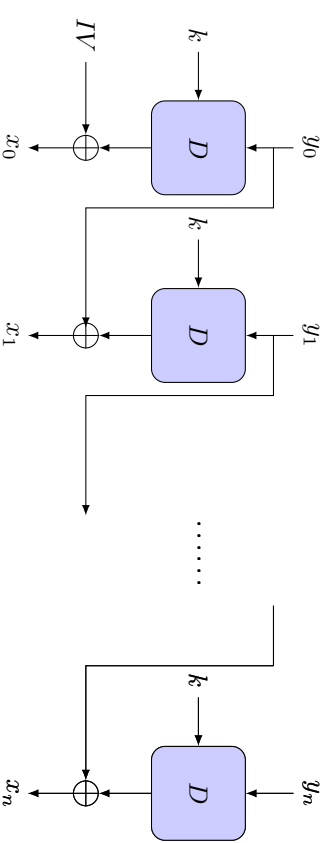


- Nếu không cần pad, thêm một khối giả
- Khi giải mã, loại bỏ pad.

# Nội dung

- Mã khối lý tưởng
- Chế độ ECB
- Mã hoá xác suất
- Chế độ CBC
- **Một số chế độ mã khối dựa trên mã dòng**

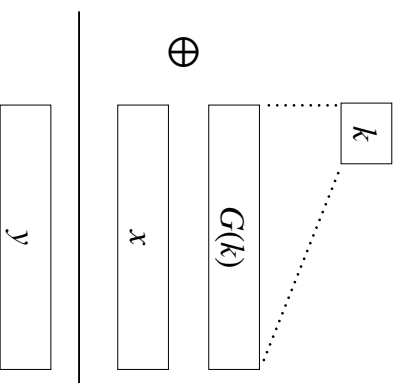
# Bài tập



- Hãy viết công thức đại số cho mạch giải mã của chế độ CBC.

# Mã dòng

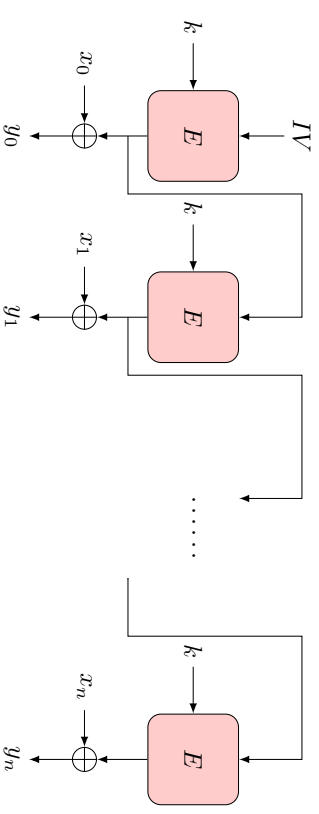
- Mã hoá  
 $y = E_k(x) = G(k) \oplus x$
- Giải mã  
 $x = D_k(y) = G(k) \oplus y$



# Mã dòng

- Sử dụng một hàm sinh số giả ngẫu nhiên  
 $G : \mathcal{K} \rightarrow \{0,1\}^n$ ,  
là hàm đơn định từ không gian khoá đến dãy bit độ dài  $n$
- Mã hoá  $y = E_k(x) = G(k) \oplus x$
- Giải mã  $x = D_k(y) = G(k) \oplus y$

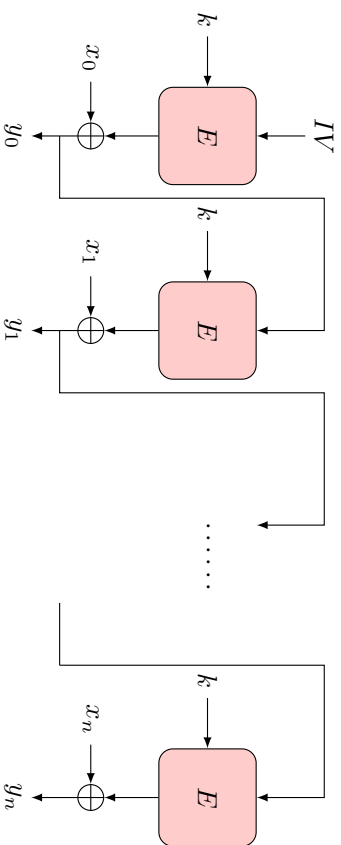
# Chế độ Output Feedback (OFB)



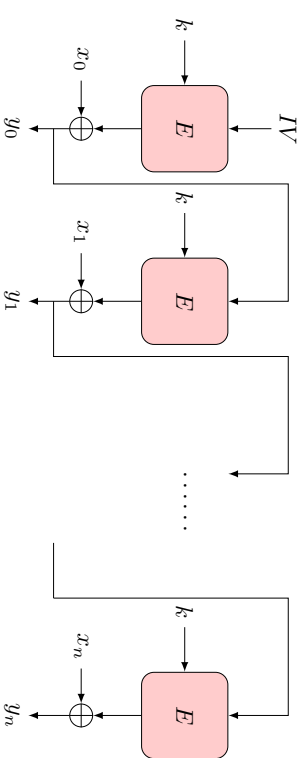
# Mã dòng và mã khối

- Các chế độ mã khối trong mục này đều dựa trên nguyên lý của hệ mã dòng: **mã khối an toàn được dùng xây dựng các hàm sinh số giả ngẫu nhiên**
- Ví dụ:  
 $G(k) = E_k(0) \| E_k(1) \| \dots \| E_k(n)$
- Hàm mã hoá và giải mã của mã dòng đều giống nhau  
 $D_k(z) = E_k(z) = G(k) \oplus z$

# Chế độ Cipher Feedback (CFB)

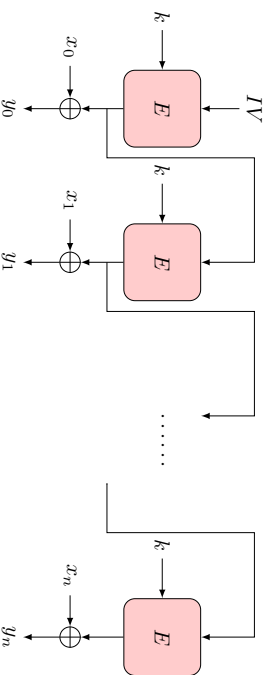


# Bài tập



- Hãy mô tả mạch giải mã ở dạng công thức đại số cho chế độ CFB.

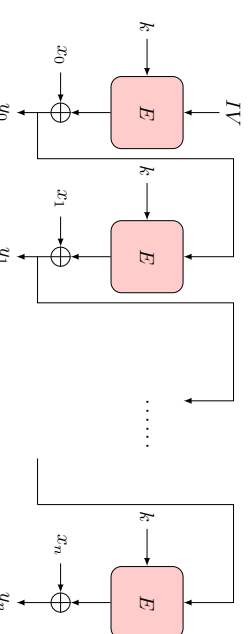
# OFB: công thức đại số



- $s_{-1} := IV$  // Khởi tạo
- $s_i := E_k(s_{i-1})$  // Khối bit giả ngẫu nhiên

$$y_i := s_i \oplus x_i \quad \text{với } i = 0, 1, 2, \dots$$

# CFB: công thức đại số

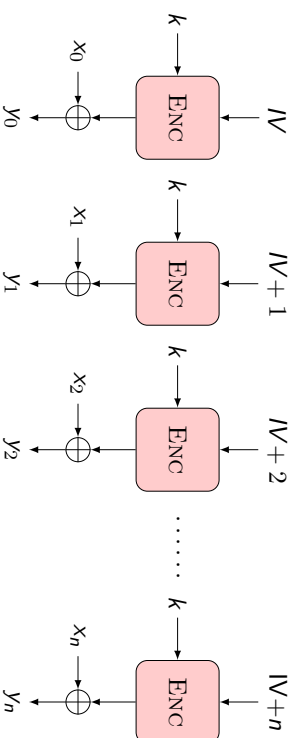


- $y_{-1} := IV$  // Khởi tạo
- $s_i := E_k(y_{i-1})$  // Khối bit giả ngẫu nhiên

$$y_i := s_i \oplus x_i \quad \text{với } i = 0, 1, 2, \dots$$

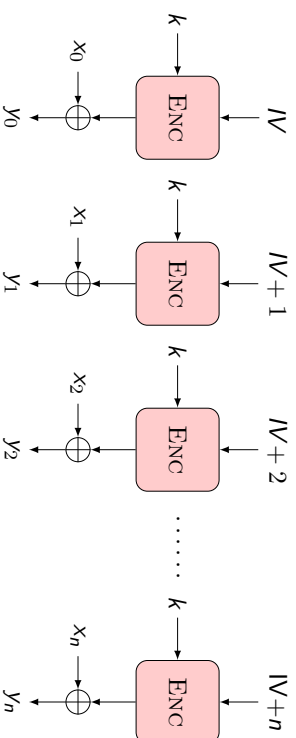


## Bài tập



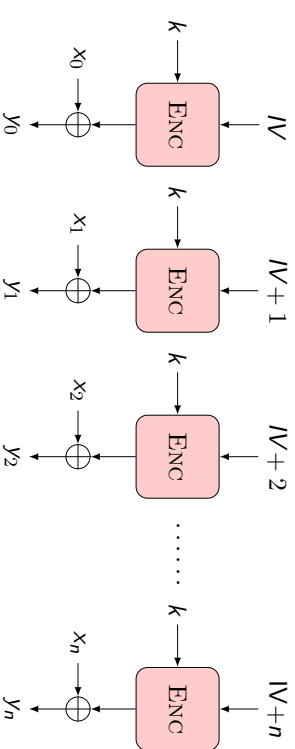
- Hãy mô tả mạch giải mã cho chế độ CTR.

## Chế độ Counter (CTR)



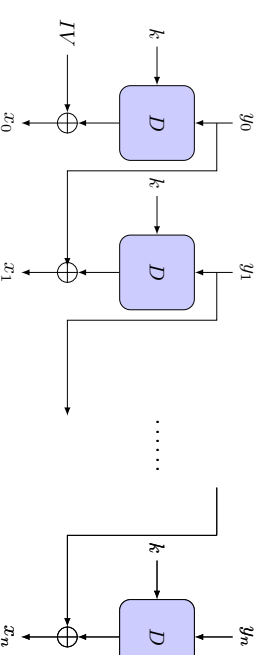
- Đảm bảo **IV** + **Ctr** không bao giờ lặp lại.
- Ctr được bắt đầu từ 0 cho mỗi thông điệp; và tăng (**Ctr**=**Ctr**+1) sau mỗi khối của thông điệp.

## Bài tập



- Xét thông điệp  $x$  gồm  $\ell$  khối AES (ví dụ  $\ell = 100$ ). Alice mã hóa  $x$  dùng chế độ **CTR** (với **Nonce ngẫu nhiên**) và truyền bản mã kết quả tới Bob.
- Do mạng lỗi, khối bản mã số  $\ell/2$  bị mất trong khi truyền. Mọi bản mã khác được truyền và nhận đúng.
- Khi Bob giải mã bản mã nhận được, bao nhiêu khối bản rõ sẽ bị mất?

## Bài tập



- Xét thông điệp  $x$  gồm  $\ell$  khối AES (ví dụ  $\ell = 100$ ). Alice mã hóa  $x$  dùng chế độ **CBC** và truyền bản mã kết quả tới Bob.
- Do mạng lỗi, khối bản mã số  $\ell/2$  bị mất trong khi truyền. Mọi bản mã khác được truyền và nhận đúng.
- Khi Bob giải mã bản mã nhận được, bao nhiêu khối bản rõ sẽ bị mất?