

Sử dụng mã khối

Trần Vĩnh Đức

HUST

Ngày 2 tháng 4 năm 2020

Mã khối lý tưởng

- Trên thực tế, người ta xem AES hoặc 3DES như một hệ **mã khối lý tưởng**;
- Tức là, với mỗi khóa k , ánh xạ

$$F_k(x) = e(k, x)$$

là một hoán vị ngẫu nhiên độc lập từ $\{0, 1\}^{128}$ lên chính nó.

Các chế độ và mode sử dụng

Câu hỏi: Làm thế nào để mã hóa thông điệp với độ dài bất kỳ? (dùng AES)

Trả lời: Dùng một trong các mode sau:

- “ECB” = “Electronic code book”
- “CTR” = “Counter mode”
- “CBC” = “Cipher Block Chaining”
- “OFB” = “Output Feedback”
- ...

Chế độ sử dụng: Khoá chỉ sử dụng một lần và **khoá dùng nhiều lần**.

Ứng dụng của khoá dùng nhiều lần

Mã hóa hệ thống file

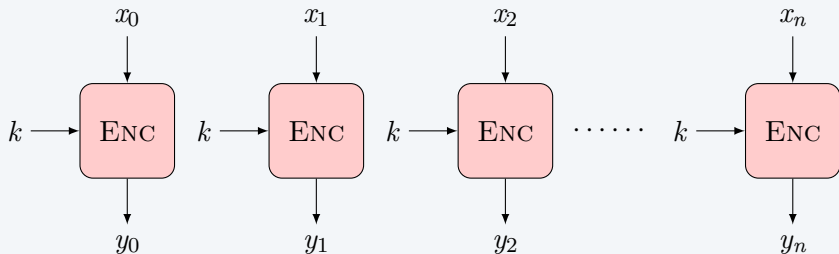
- Mã hóa nhiều file dùng AES với cùng khóa

IPSec

- Nhiều gói tin cùng được mã hóa bằng AES với cùng một khóa

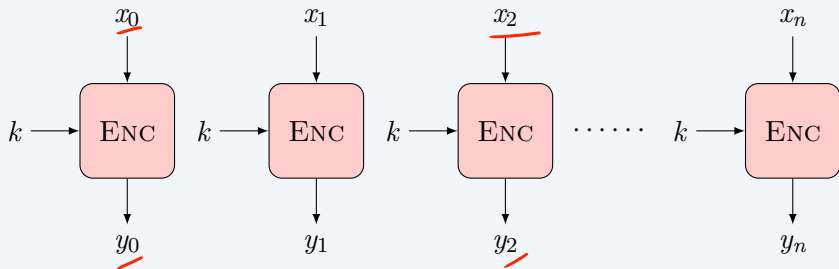
- 1 Electronic Codebook Mode (ECB)
- 2 Cipher Block Chaining Mode (CBC)
- 3 Mã dòng

ECB (Electronic code book)



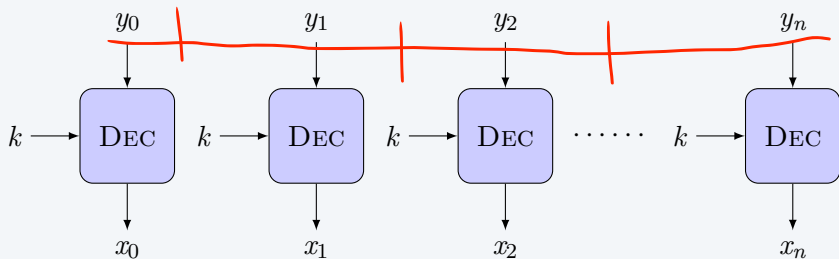
- Dữ liệu được chia thành các khối khối b bit, với $b =$ kích thước khối.
- Với dữ liệu không chia hết cho b bit: Thêm dãy "10..0" để độ dài thông điệp chia hết cho b .

ECB (Electronic code book)

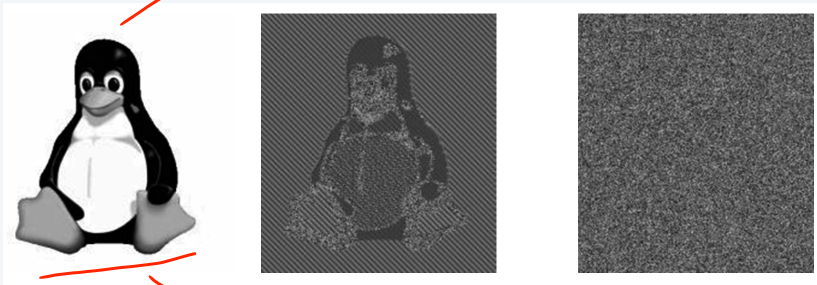


- Dữ liệu được chia thành các khối khối b bit, với $b =$ kích thước khối.
- Với dữ liệu không chia hết cho b bit: Thêm dãy "10..0" để độ dài thông điệp chia hết cho b .
- Phép toán **padding** này cho có tính **khả nghịch**. Nó cho phép giải mã.

ECB: Làm thế nào để giải mã?



ECB là không an toàn



Hình: Ảnh ở giữa là ECB mode, ảnh bên phải là mã hóa an toàn

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

Ví dụ: Chuyển tiền giữa hai ngân hàng dùng ECB

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

Hình: Giao thức trao đổi giữa các ngân hàng:

- Giả sử:** Mỗi trường đều là n -bit (ví dụ 128 bit)
- Giả sử:** Khoá k_{AB} để trao đổi thông tin giữa hai ngân hàng A và B là cố định.

Oscar tấn công

Block #	1	2	3	4	5
	<u>Sending Bank A</u>	Sending Account #	<u>Receiving Bank B</u>	<u>Receiving Account #</u>	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

$$B_1 || B_2 || B_3 || B_4 || B_5$$

và anh ta giữ lại bản mã B_4 .

- 4 Trong tương lai, mỗi khi thấy lệnh chuyển tiền từ B_1 tới B_3 , thay block thứ 4 bởi B_4 .

Nội dung

- 1 Electronic Codebook Mode (ECB)
- 2 Cipher Block Chaining Mode (CBC)
- 3 Mã dòng

Bài toán

Ta cần giải quyết hai vấn đề:

- Làm cho hệ mã trở thành hệ mã xác suất;
- Ảnh hưởng của việc mã hoá trên mọi khối.



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 + "số bit ngẫu nhiên"

Bài tập

Hãy viết hàm giải mã D cho hàm mã hoá E được định nghĩa bởi:

$E(k, m)$:

$r = \text{random}()$

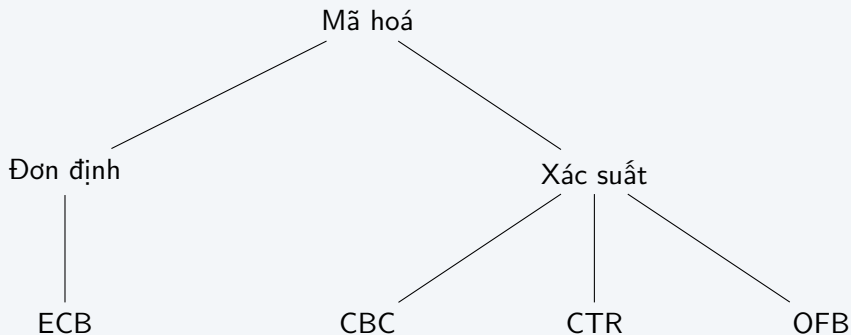
$c = \text{AES}(k, r) \oplus m$

return (r, c)

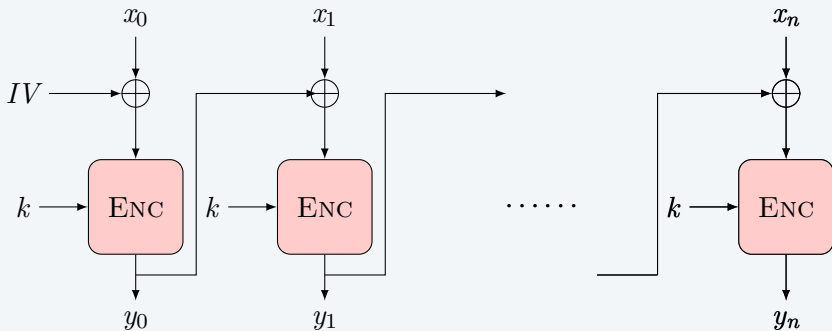
$D(k, (r, c))$:

$m = \text{AES}^{-1}(k, r) \oplus c$

Dạng mã hoá



CBC (Cipher Block Chaining mode)



Thuật toán. Chọn IV (“initialization value”) một cách ngẫu nhiên, sau đó dùng y_i như “IV” cho M_{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

- 1 Là ngẫu nhiên “thật”
- 2 Là bộ đếm “counter” (phải được lưu trữ bởi Alice)
- 3 $ID_A || ID_B || \text{time}$

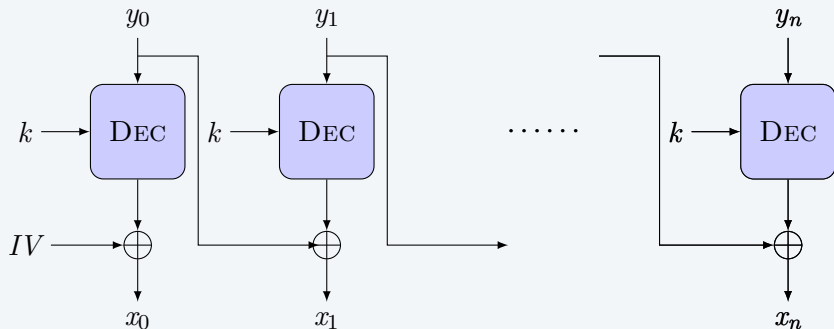
Một kỹ thuật padding cho CBC

- Padding theo từng byte;
- Giá trị mỗi byte được thêm là số byte cần được thêm.
Ví dụ, nếu kích thước block là 8 và ta cần padding 4 byte:

... | DD DD DD DD 04 04 04 04 |

- nếu không cần padding, ta thêm một block giả.

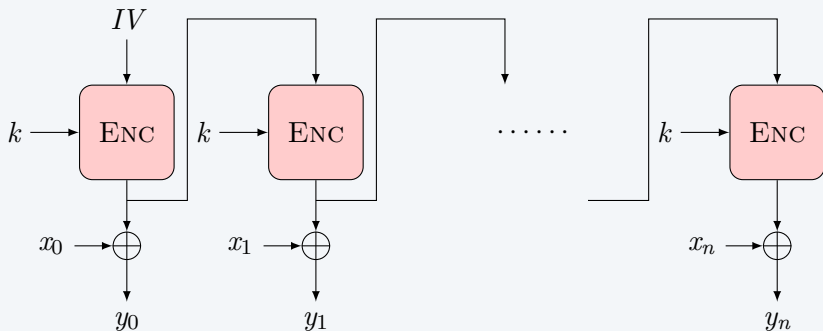
CBC: Giải mã



Nội dung

- 1 Electronic Codebook Mode (ECB)
- 2 Cipher Block Chaining Mode (CBC)
- 3 Mã dòng

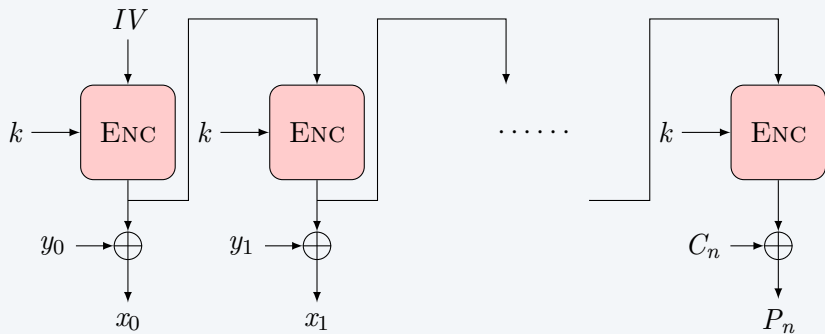
Output Feedback Mode (OFB)



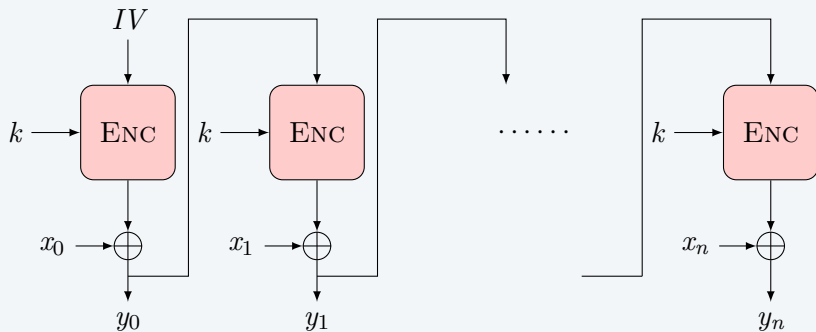
Thuật toán. Tương tự như CBC mode. Sử dụng IV ngẫu nhiên truyền cùng bản mã.

Nếu kích thước của bản rõ M không chia hết cho b , ta chỉ cần truyền bản mã rút gọn (không cần padding).

OFB: Giải mã

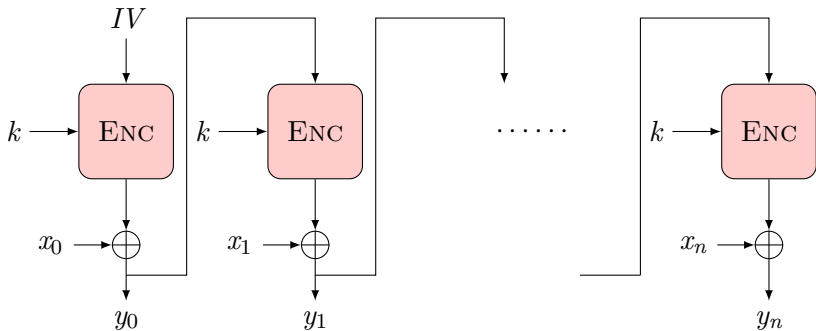


Cipher Feedback Mode (CFB)

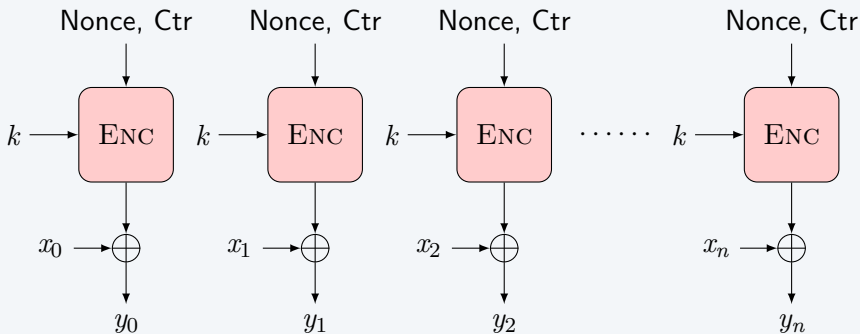


Bài tập

Hãy mô tả mạch giải mã CFB



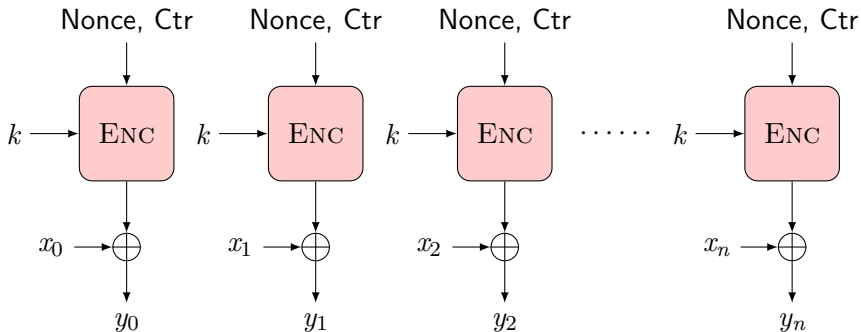
Counter Mode (CTR)



- Đảm bảo cặp Nonce||Ctr cặp không bao giờ lặp lại.
- Ctr được bắt đầu từ 0 cho mọi thông điệp.

Bài tập

Hãy mô tả mạch giải mã CTR



Bài tập

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