
## Chuẩn mã dữ liệu DES

- Giới thiệu về DES
- Thuật toán DES
- Các chế độ hoạt động của DES
- Double DES và Triple DES

2

## Chuẩn mã dữ liệu DES

- Giới thiệu về DES
  - Năm 1972, Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ (National Institute of Standards and Technology-NIST) đặt ra yêu cầu xây dựng một thuật toán mã hoá bảo mật thông tin với yêu cầu là dễ thực hiện, sử dụng được rộng rãi trong nhiều lĩnh vực và mức độ bảo mật cao.
  - Năm 1974, IBM giới thiệu thuật toán Lucifer, thuật toán này đáp ứng hầu hết các yêu cầu của NIST.
  - Sau một số sửa đổi, năm 1976, Lucifer được NIST công nhận là chuẩn quốc gia Hoa kỳ và được đổi tên thành Data Encryption Standard (DES).

3

## Chuẩn mã dữ liệu DES

- Sự xuất hiện của DES đã tạo nên một làn sóng nghiên cứu trong giới khoa học về lĩnh vực mật mã học, đặc biệt là các phương pháp thám mã mã khối. Về điều này, Bruce Schneier viết:
- "*NSA coi DES là một trong những sai lầm lớn nhất. Nếu họ biết trước rằng chi tiết của thuật toán sẽ được công bố để mọi người có thể viết chương trình phần mềm, họ sẽ không bao giờ đồng ý. DES đã tạo nên nguồn cảm hứng nghiên cứu trong lĩnh vực thám mã hơn bất kỳ điều gì khác: Giới khoa học đã có một thuật toán để nghiên cứu - thuật toán mà NSA khẳng định là an toàn.*"

4

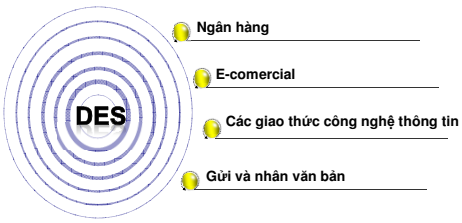
## Chuẩn mã dữ liệu DES

- DES là thuật toán mã hoá bảo mật được sử dụng rộng rãi nhất trên thế giới
- Ở thời điểm DES ra đời người ta đã tính toán rằng việc phá được khoá mã DES là rất khó khăn, nó đòi hỏi chi phí hàng chục triệu USD và tiêu tốn khoảng thời gian rất nhiều năm.
- Cùng với sự phát triển của các loại máy tính và mạng máy tính có tốc độ tính toán rất cao, khoá mã DES có thể bị phá trong khoảng thời gian ngày càng ngắn với chi phí ngày càng thấp. Dù vậy việc này vẫn vượt xa khả năng của các hacker thông thường và mã hoá DES vẫn tiếp tục tồn tại trong nhiều lĩnh vực

5

## Chuẩn mã dữ liệu DES

- Ứng dụng của DES:



## Chuẩn mã dữ liệu DES

- Mô tả DES:

Input: Xâu bit x có độ dài 64 bit, khoá độ dài 56 bit

Output: xâu bit mã hoá y độ dài 64 bit

- Thuật toán gồm 3 bước

7

## Chuẩn mã dữ liệu DES

Bước 1:

- Với bản rõ cho trước x
- Tạo xâu $x_0$ theo hoán vị cố định ban đầu IP.
- Ta có: $x_0 = IP(x) = L_0R_0$
- Trong đó $L_0$ gồm 32 bit đầu và $R_0$ là 32 bit cuối.

8

## Chuẩn mã dữ liệu DES

Bước 2:

Ta sẽ tính $L_iR_i$, $1 \le i \le 16$ theo quy tắc sau:

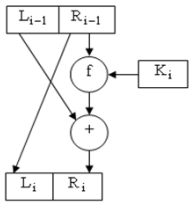
$$L_i = R_{i-1}; R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

Trong đó:
- $\oplus$ là phép loại trừ của hai xâu bit
- f là hàm Fiestel
- $k_1, k_2, \ldots, k_{16}$ là các xâu bit có độ dài 48 được tính như 1 hàm của khóa k

9

## Chuẩn mã dữ liệu DES

- Một vòng của phép mã hóa được mô tả như sau:




10

## Chuẩn mã dữ liệu DES

Bước 3:

Áp dụng phép hoán vị ngược $IP^{-1}$ cho xâu bit $R_{16}L_{16}$, ta thu được bản mã y. Tức là $y = IP^{-1}(R_{16}L_{16})$ .

(Hãy chú ý thứ tự đã đảo của $L_{16}$ và $R_{16}$)

11

## Chuẩn mã dữ liệu DES

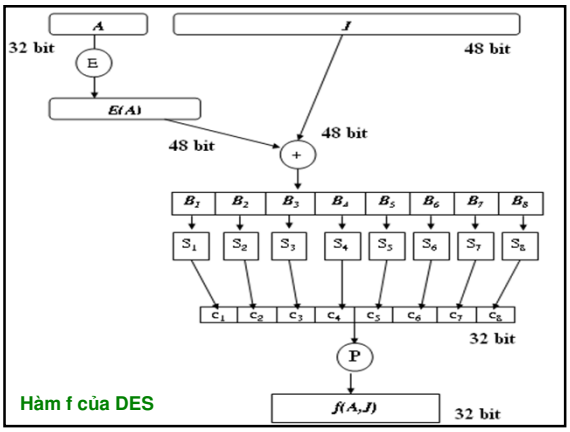
- Mô tả hàm f:

Input: Xâu bit A có độ dài 32
Xâu bit J có độ dài 48

Output: xâu bit có độ dài 32 bit

- Các bước thực hiện

12




Hàm f của DES

## Chuẩn mã dữ liệu DES

- **Bước 1:** Biến thứ nhất A được mở rộng thành một xâu bit độ dài 48 theo một hàm mở rộng cố định E. E(A) gồm 32 bit của A (được hoán vị theo cách cố định) với 16 bit xuất hiện hai lần.
- **Bước 2:** Tính E(A) ⊕ J và viết kết quả thành một chuỗi 8 xâu 6 bit là $B_1B_2B_3B_4B_5B_6B_7B_8$

14

## Chuẩn mã dữ liệu DES

- **Bước 3:** Bước tiếp theo dùng 8 bảng $S_1S_2,\ldots,S_8$ ( được gọi là các hộp $S$ ). Với mỗi $S_i$ là một bảng 4×16 cố định có các hàng là các số nguyên từ 0 đến 15. Với xâu bit có độ dài 6 (kí hiệu $B_i = b_1\, b_2\, b_3\, b_4\, b_5\, b_6$), ta tính $S_i(B_i)$ như sau:
  - Hai bit $b_1b_6$ xác định biểu diễn nhị phân hàng $r$ của $S_i$ ($0 \le r \le 3$)
  - Bốn bit ($b_2\, b_3\, b_4\, b_5$) xác định biểu diễn nhị phân của cột $c$ của $S_i$ ($0 \le c \le 15$).
  - Khi đó $S_i(B_i)$ sẽ xác định phần tử $S_i(r, c)$ ; phần tử này viết dưới dạng nhị phân là một xâu bit có độ dài 4
  - Bằng cách tương tự tính các $C_i = S_i(B_i)$ , ($1 \le i \le 8$).

15

## Chuẩn mã dữ liệu DES

- **Bước 4:** Xâu bit $C = C_1\, C_2 \ldots C_8$ có độ dài 32 được hoán vị theo phép hoán vị cố định P. Xâu kết quả là P(C) được xác định là f(A, J).

16

## Chuẩn mã dữ liệu DES

- Phép hoán vị ban đầu IP:

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

- Bảng này có ý nghĩa là bit thứ 58 của x là bit đầu tiên của IP(x); bit thứ 50 của x là bit thứ 2 của IP(x)

17

## Chuẩn mã dữ liệu DES

- Phép hoán vị ngược $IP^{-1}$:

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

18

## Chuẩn mã dữ liệu DES

- Hàm mở rộng E được xác định theo bảng sau:

| Bảng chọn E bit | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

19

## Chuẩn mã dữ liệu DES

- Tám hộp S:

| $S_1$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

| $S_2$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

20

## Chuẩn mã dữ liệu DES

| $S_3$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

| $S_4$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

| $S_5$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

21

## Chuẩn mã dữ liệu DES

| $S_6$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 15 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

| $S_7$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

| $S_8$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

22

## Chuẩn mã dữ liệu DES

- Phép hoán vị P:

| P | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

23

## Chuẩn mã dữ liệu DES

- Mô tả tính bảng khóa từ khóa k.
  - Trên thực tế k là một xâu bit độ dài 64, trong đó có 56 bit khóa và 8 bit kiểm tra tính chẵn lẻ nhằm phát hiện sai.
  - Các bit ở các vị trí 8, 16, …, 64 được xác định sao cho mỗi byte chứa một số lẻ các số "1". Bởi vậy, một sai sót đơn lẻ có thể phát hiện được trong mỗi nhóm 8 bit.
  - Các bit kiểm tra bị bỏ qua trong quá trình tính bảng khóa.

24

## Chuẩn mã dữ liệu DES

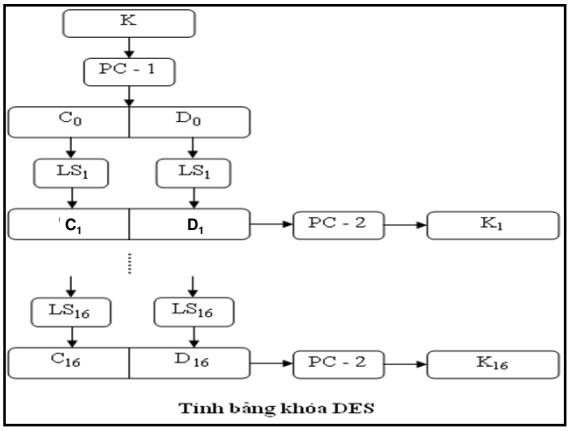
- Các bước tính bảng khóa DES:
  - Với một khoá k 64 bit cho trước, ta loại bỏ các bit kiểm tra tính chẵn lẻ và hoán vị các bit còn lại của k theo phép hoán vị cố định PC-1. Ta viết: PC-1(k) = $C_0D_0$
  - Với i thay đổi từ 1 đến 16:

$$C_i = LS_i(C_{i-1}); \qquad D_i = LS_i(D_{i-1})$$

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

  - Hoán vị các bít của $C_iD_i$ theo HV cố định PC-2 ta được khóa $K_i$: $K_i$ = PC-2($C_iD_i$)

25



Tính bảng khóa DES

## Chuẩn mã dữ liệu DES

- Các hoán vị PC-1 và PC-2:

| PC-1 | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

| PC-2 | | | | | |
|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

27

## Chuẩn mã dữ liệu DES

- Giải mã
  - Phép giải mã được thực hiện nhờ dùng cùng thuật toán như phép mã hóa với đầu vào là bản mã y nhưng dùng bảng khoá theo thứ tự ngược lại $K_{16}$,...$K_1$.
  - Đầu ra của thuật toán sẽ là bản rõ x.

28

## Chuẩn mã dữ liệu DES

- Tính chất của DES
  - Tác dụng đồng loạt: Khi ta thay đổi 1 bit trong khoá sẽ gây ra tác động đồng loạt làm thay đổi nhiều bit trên bản mã. Đây là tính chất mong muốn của khoá trong thuật toán mã hoá. Nếu thay đổi 1 bít đầu vào hoặc khoá sẽ kéo theo thay đổi một nửa số bít đầu ra. Do đó không thể đoán khoá được. Co thể nói rằng DES thể hiện tác động đồng loạt mạnh

29

## Chuẩn mã dữ liệu DES

- Tính chất của DES
  - Tính chất bù: Ký hiệu $\bar{x}$ là bù của $x$ theo từng bít, ta có

$$e_k(x) = y \Leftrightarrow e_{\bar{k}}(\bar{x}) = \bar{y}$$

  - Khóa yếu: DES có 4 khóa yếu
    - $k$ được gọi là khóa yếu nếu $e_k(e_k(x)) = x$ với mọi $x$
  - Khóa nửa yếu: Có 6 cặp khóa nửa yếu
    - Là cặp ($k_1$, $k_2$) sao cho $e_{k_1}(e_{k_2}(x)) = x$ với mọi $x$
  - DES không là nhóm dưới phép hợp hàm

30

## Chuẩn mã dữ liệu DES

- Sức mạnh của DES – tấn công thời gian:
  - Đây là dạng tấn công vào cài đặt thực tế của mã. Ở đây sử dụng hiểu biết về quá trình cài đặt thuật toán mà suy ra thông tin về một số khoá con hoặc mọi khoá con. Đặc biệt sử dụng kết luận là các tính toán chiếm khoảng thời gian khác nhau phụ thuộc vào giá trị đầu vào của nó. Do đó kẻ thám mã theo dõi thời gian thực hiện mà phán đoán về khoá. Có thể kẻ thám mã sáng tạo ra các loại card thông minh phán đoán khoá, mà còn phải bàn bạc thêm về chúng.
- Sức mạnh của DES – tấn công thám mã:
  - Có một số phân tích thám mã trên DES, từ đó đề xuất xây dựng một số cấu trúc sâu về mã DES. Rồi bằng cách thu thập thông tin về mã, có thể đoán biết được tất cả hoặc một số khoá con đang dùng. Nếu cần thiết sẽ tìm duyệt những khoá còn lại. Nói chung, đó là những tấn công dựa trên phương pháp thống kê bao gồm: thám mã sai phân, thám mã tuyến tính và tấn công khoá liên kết.

31

## Chuẩn mã dữ liệu DES

- Sự khác biệt ở đầu vào cho sự khác biệt ở đầu ra với một xác suất cho trước.
  - Nếu tìm được một thể hiện đầu vào - đầu ra với xác suất cao. Thì có thể luận ra khoá con được sử dụng trong vòng đó
  - Sau đó có thể lặp lại cho nhiều vòng (với xác suất giảm dần)
  - Cặp đúng cho bít khoá như nhau
  - Cặp sai cho giá trị ngẫu nhiên
  - Đối với số vòng lớn, xác suất để có nhiều cặp đầu vào 64 bít thoả mãn yêu cầu là rất nhỏ.

32

## Chuẩn mã dữ liệu DES

- Thám mã sai phân: đây là phương pháp mạnh để phân tích mã khối
  - Thám mã sai phân so sánh hai cặp mã có liên quan với nhau
    - Với sự khác biệt đã biết ở đầu vào
    - Khảo sát sự khác biệt ở đầu ra
    - Khi với cùng khoá con được dùng
    - Trong công thức sau với hai đầu vào khác nhau, vế trái là sự khác biệt mã ở cùng vòng thứ i được biểu diễn qua sự khác biệt mã ở vòng trước đó i-1 và sự khác biệt của hàm f trong ngoặc vuông.

$$\begin{aligned}\Delta m_{i+1} &= m_{i+1} \oplus m'_{i+1} \\ &= \left[m_{i-1} \oplus f(m_i, K_i)\right] \oplus \left[m'_{i-1} \oplus f(m'_i, K_i)\right] \\ &= \Delta m_{i-1} \oplus \left[f(m_i, K_i) \oplus f(m'_i, K_i)\right]\end{aligned}$$

33

## Chuẩn mã dữ liệu DES

- Qui trình thám mã như sau: thực hiện mã hoá lặp lại với cặp bản rõ có XOR đầu vào biết trước cho đến khi nhận được XOR đầu ra mong muốn
- Khi đó có thể tìm được
  - Nếu vòng trung gian thỏa mãn XOR yêu cầu thì có cặp đúng
  - Nếu không thì có cặp sai, tỷ lệ sai tương đối cho tấn công đã biết trước dựa vào thống kê.

34

## Chuẩn mã dữ liệu DES

- **Thám mã tuyến tính:** nó cũng dùng phương pháp thống kê. Cơ sở của phương pháp dựa trên tìm xấp xỉ tuyến tính
  - Tìm xấp xỉ tuyến tính với xác suất p= ½
    $P[i_1, i_2, \ldots, i_a] (+) C[j_1, j_2, \ldots, i_b] = K[k_1, k_2, \ldots, k_c]$
    trong đó $i_a$, $j_b$, $k_c$ là các vị trí bit trong bản rõ, mã, khoá.
  - Điều kiện trên cho phương trình tuyến tính của các bít khoá.
  - Để nhận được 1 bít khoá sử dụng thuật toán lân cận tuyến tính
    - Sử dụng một số lớn các phương trình thử nghiệm. Hiệu quả cho bởi |p – 1/2|
  - Trong quá trình tìm hiểu DES người ta đã hệ thống lại các tiêu chuẩn thiết kế DES. Như báo cáo bởi Copperscmith trong [COPP94]:
    - Có 7 tiêu chuẩn đối với S box được cung cấp để đảm bảo
      - » tính phi tuyến tính
      - » chống tham mã sai phân
      - » Xáo trộn tốt
    - Có 3 tiêu chuẩn cho hoán vị P để tăng độ khuếch tán

35

## Chuẩn mã dữ liệu DES

- Có 4 chế độ làm việc đã được phát triển cho DES:
  - Chế độ quyển mã điện tử (ECB – Electronic CodeBook)
  - Chế độ phản hồi mã (CFB – Cipher FeedBack)
  - Chế độ liên kết khối mã (CBC – Cipher Block Chaining)
  - Chế độ phản hồi đầu ra (OFB – Output FeedBack)

36

## Chuẩn mã dữ liệu DES

- Chế độ quyển mã điện tử (ECB):
  - Là cách sử dụng thông thường và đơn giản của DES
  - Bản rõ được chia thành từng khối 64 bit $x=x_1x_2\ldots x_n$ và dùng khóa k để mã từng khối độc lập rồi ghép lại để được bản mã $y=y_1y_2\ldots y_n$, trong đó $y_i = e_k(x_i)$

37

## Chuẩn mã dữ liệu DES

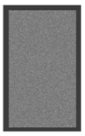
- Ưu và nhược của ECB:
  - Lặp trên bản mã được chỉ rõ lặp trên bản tin nếu dóng đúng khối, đặc biệt với hình ảnh, hoặc với bản tin có rất ít sự thay đổi thì sẽ trở thành đối tượng dễ thám mã
  - Được sử dụng chủ yếu khi gửi một ít dữ liệu


38

## Chuẩn mã dữ liệu DES

- Chế độ liên kết khối mã(CBC):
  - Để được khối mã $y_i$ ta dùng DES cho không phải $x_i$ mà là $x_i \oplus y_{i-1}$, tức là ta có

    $y_i=e_k(x_i \oplus y_{i-1})$ với mọi $i>1$
  - $y_0$ là một vector khởi tạo 64 bit

39

## Chuẩn mã dữ liệu DES

- Chế độ CFB và OFB:
  - Dùng DES để tạo ra dòng khóa $z_1, z_2,\ldots$ rồi sau đó lập mã $y_i = x_i \oplus z_i$ $(i \geq 1)$
  - Với OFB, $z_1, z_2,\ldots$ được tạo bởi
    - $z_0 = y_0$ (là vector khởi tạo 64)
    - $z_i = e_k(z_{i-1})$
  - Với CFB, $z_1, z_2,\ldots$ được tạo bởi
    - $y_0$ là một vector khởi tạo 64 bit
    - $z_i = e_k(y_{i-1})$ $(i \geq 1)$

40

## Chuẩn mã dữ liệu DES

- Ưu và nhược điểm của CFB
  - Được dùng khi dữ liệu đến theo byte/bit. Đây là chế độ dòng thường gặp nhất
  - Lỗi sẽ lan ra một vài block sau lỗi
- Ưu điểm và nhược điểm của OFB
  - Được dùng khi lỗi phản hồi ngược lại hoặc ở nơi cần mã trước khi mẩu tin sẵn sàng
  - Rất giống CFB, nhưng phản hồi là từ đầu ra của mã và độc lập với mẩu tin
  - Người gửi và người nhận phải đồng bộ, có phương pháp khôi phục nào đó là cần thiết để đảm bảo việc đó.

41

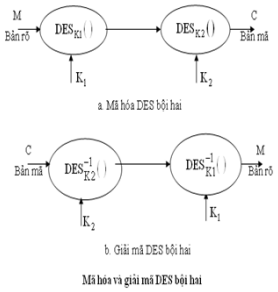
## Chuẩn mã dữ liệu DES

- **Ưu điểm và nhược điểm của OFB**
  - Được dùng khi lỗi phản hồi ngược lại hoặc ở nơi cần mã trước khi mẩu tin sẵn sàng
  - Rất giống CFB, nhưng phản hồi là từ đầu ra của mã và độc lập với mẩu tin
  - Người gửi và người nhận phải đồng bộ, có phương pháp khôi phục nào đó là cần thiết để đảm bảo việc đó.

42

## Chuẩn mã dữ liệu DES

- DES bội hai
  - **Mã hóa:**
    $C = DES_{K2}[DES_{K1}(M)]$
  - **Giải mã:**
    $M = DES_{K1}^{-1}[DES_{K2}^{-1}(C)]$
    - Có $2^{56}$ sự lựa chọn cho khóa $K_1$ và $2^{56}$ sự lựa chọn cho khóa $K_2$. Bởi vậy có $2^{112}$ sự lựa chọn cho cặp khóa ($K_1$, $K_2$)

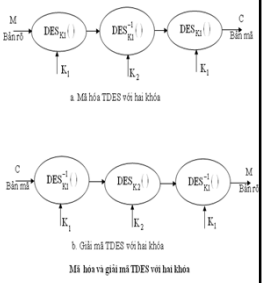


Mã hóa và giải mã DES bội hai



## Chuẩn mã dữ liệu DES

- DES bội ba
  - **Mã hóa:**
    $C = DES_{K1}\{DES_{K2}^{-1}[DES_{K1}(M)]\}$
  - **Giải mã:**
    $M = DES_{K1}^{-1}\{DES_{K2}[DES_{K1}^{-1}(C)]\}$
  - Với TDES việc tìm khóa vét cạn yêu cầu khoảng:
    $2^{112} = 5{,}1923.1023$ phép tính TDES, bởi vậy thực tế khó có thể thám mã thành công.



Mã hóa và giải mã TDES với hai khóa



## Nội dung

1. Giới thiệu về hệ mật khóa bí mật
2. Các hệ mật thay thế đơn biểu
3. Các hệ mật thay thế đa biểu
4. Các hệ mật thay thế không tuần hoàn
5. Các hệ mật chuyển vị
6. Chuẩn mã dữ liệu DES
7. Chuẩn mã dữ liệu tiên tiến AES



## Chuẩn mã dữ liệu AES

- **Nguồn gốc:**
  - Cần phải thay thế DES, vì có những tấn công về mặt lý thuyết có thể bẻ được nó.
  - Do đó Viện chuẩn quốc gia Hoa kỳ US NIST ra lời kêu gọi tìm kiếm chuẩn mã mới vào năm 1997. Sau đó có 15 đề cử được chấp nhận vào tháng 6 năm 1998. Và được rút gọn còn 5 ứng cử viên vào tháng 6 năm 1999. Đến tháng 10 năm 2000, mã Rijndael được chọn làm chuẩn mã nâng cao và được xuất bản là chuẩn FIPS PUB 197 vào 11/2001.
- **Yêu cầu của AES**
  - Là mã khối đối xứng khoá riêng.
  - Kích thước khối dữ liệu 128 bit và độ dài khoá là tùy biến: 128, 192 hoặc 256 bit.
  - Chuẩn mã mới phải mạnh và nhanh hơn Triple DES. Mã mới có cơ sở lí thuyết mạnh để thời gian sống của chuẩn khoảng 20-30 năm (cộng thêm thời gian lưu trữ).
  - Khi đưa ra thành chuẩn yêu cầu cung cấp chi tiết thiết kế và đặc tả đầy đủ. Đảm bảo rằng chuẩn mã mới cài đặt hiệu quả trên cả C và Java.



## Chuẩn mã dữ liệu AES

- Cơ sở toán học của AES: trong AES các phép toán cộng và nhân được thực hiện trên các byte trong trường hữu hạn GF($2^8$)
  - **Phép cộng:**
    - $A = (a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8)$; $B = (b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8)$
    - $C = A + B = (c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8)$
    - Trong đó: $C_i = a_i + b_i \bmod 2$, $1 \le i \le 8$.
    - **Ví dụ:** tổng của $A = 73_H$; $B = 4E_H$ là:
      - Dạng cơ số Hexa: $73_H + 4E_H = 3D_H$
      - Dạng nhị phân: 01110011 + 01001110 = 00111101
      - Dạng đa thức:
        $(x^6 + x^5 + x^4 + x + 1) + (x^6 + x^3 + x^2 + x) = (x^5 + x^4 + x^3 + x^2 + 1)$



## Chuẩn mã dữ liệu AES

- **Phép nhân:** Phép nhân được thực hiện trên GF($2^8$) bằng cách nhân hai đa thức rút gọn theo modulo của một đa thức bất khả quy m(x). Trong AES đa thức bất khả quy này là:

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$

- Ví dụ: $A = C3_H$, $B = 85_H$ tương ứng với
  $a(x) = x^7 + x^6 + x + 1$ và $b(x) = x^7 + x^2 + 1$. Khi đó: C= A.B
  $c(x) = a(x).b(x) \bmod (x^8 + x^4 + x^3 + x + 1)$
  $c(x) = x^7 + x^5 + x^3 + x^2 + x$ hay $C = AE_H = 10101110$

# Chuẩn mã dữ liệu AES

- **Chuẩn mã nâng cao AES – Rijndael**: có các đặc trưng sau:
  - Có 128/192/256 bit khoá và 128 bit khối dữ liệu.
  - Lặp hơi khác với Fiestel
    - Chia dữ liệu thành 4 nhóm – 4 byte
    - Thao tác trên cả khối mỗi vòng
    - Thiết kế để:
      - chống lại các tấn công đã biết
      - tốc độ nhanh và nén mã trên nhiều CPU
      - Đơn giản trong thiết kế

49

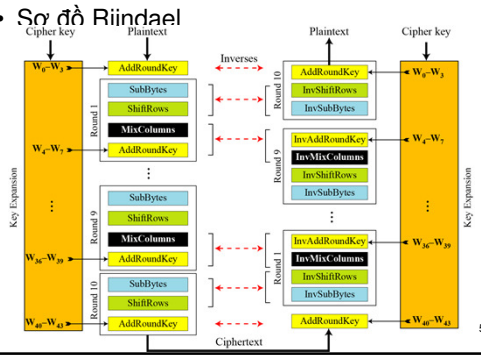
# Chuẩn mã dữ liệu AES

- Xử lý khối dữ liệu 128 bit như 4 nhóm của 4 byte: 128 = 4*4*8 bit. Mỗi nhóm nằm trên một hàng. Ma trận 4 hàng, 4 cột với mỗi phần tử là 1 byte coi như trạng thái được xử lý qua các vòng mã hoá và giải mã.
- Khoá mở rộng thành mảng gồm 44 từ 32 bit w[i].
- Có tùy chọn 9/11/13 vòng, trong đó mỗi vòng bao gồm
  - Phép thế byte (dùng một S box cho 1 byte)
  - Dịch hàng (hoán vị byte giữa nhóm/cột)
  - Trộn cột (sử dụng nhân ma trận của các cột)
  - Cộng khoá vòng (XOR trạng thái dữ liệu với khoá vòng).
  - Mọi phép toán được thực hiện với XOR và bảng tra, nên rất nhanh và hiệu quả.

50

# Chuẩn mã dữ liệu AES

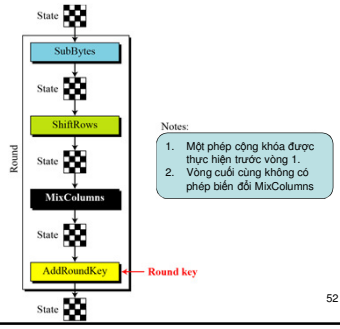
- Sơ đồ Rijndael




51

# Chuẩn mã dữ liệu AES

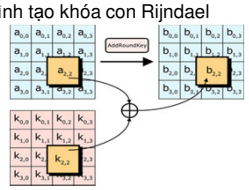
- Một vòng của AES:




52

# Chuẩn mã dữ liệu AES

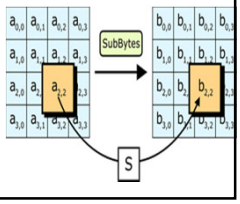
- **Sau đây ta xét chi tiết hơn các quá trình mã hoá, sinh khoá và giải mã AES:**
  - Quá trình mã gồm 4 bước sau:
    - 1. AddRoundKey - mỗi byte của khối được kết hợp với khóa con, các khóa con này được tạo ra từ quá trình tạo khóa con Rijndael



53

# Chuẩn mã dữ liệu AES

- 2. SubBytes - đây là quá trình thay thế (phi tuyến) trong đó mỗi byte sẽ được thay thế bằng một byte khác theo bảng tra
  - Phép thê byte đơn giản
  - Sử dụng một bảng 16 x 16 byte chứa hoán vị của tất cả 256 giá trị 8 bit
  - Mỗi byte trạng thái được thay bởi byte trên hàng xác định bởi 4 bit trái và cột xác định bởi 4 bit phải.
    - –Chẳng hạn {95} được thay bởi hàng 9, cột 5, mà giá trị sẽ là {2A}.
    - –S box được xây dựng sử dụng hoán vị các giá trị trong GF(28) đã được xác định trong chương trước.
    - –Thiết kế để chống mọi tấn công đã biết



# Chuẩn mã dữ liệu AES

- 2. SubBytes

**Table** *SubBytes transformation table*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |



# Chuẩn mã dữ liệu AES

- 2. SubBytes

**Table** *SubBytes transformation table (continued)*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |



# Chuẩn mã dữ liệu AES

- InvSubBytes

**Table** *InvSubBytes transformation table*

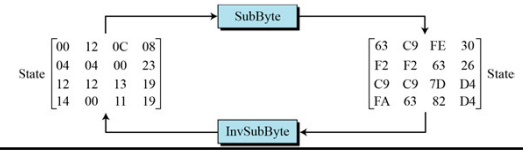
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 52 | 09 | 6A | D5 | 30 | 36 | A5 | 38 | BF | 40 | A3 | 9E | 81 | F3 | D7 | FB |
| 1 | 7C | E3 | 39 | 82 | 9B | 2F | FF | 87 | 34 | 8E | 43 | 44 | C4 | DE | E9 | CB |
| 2 | 54 | 7B | 94 | 32 | A6 | C2 | 23 | 3D | EE | 4C | 95 | 0B | 42 | FA | C3 | 4E |
| 3 | 08 | 2E | A1 | 66 | 28 | D9 | 24 | B2 | 76 | 5B | A2 | 49 | 6D | 8B | D1 | 25 |
| 4 | 72 | F8 | F6 | 64 | 86 | 68 | 98 | 16 | D4 | A4 | 5C | CC | 5D | 65 | B6 | 92 |
| 5 | 6C | 70 | 48 | 50 | FD | ED | B9 | DA | 5E | 15 | 46 | 57 | A7 | 8D | 9D | 84 |
| 6 | 90 | D8 | AB | 00 | 8C | BC | D3 | 0A | F7 | E4 | 58 | 05 | B8 | B3 | 45 | 06 |
| 7 | D0 | 2C | 1E | 8F | CA | 3F | 0F | 02 | C1 | AF | BD | 03 | 01 | 13 | 8A | 6B |



# Chuẩn mã dữ liệu AES

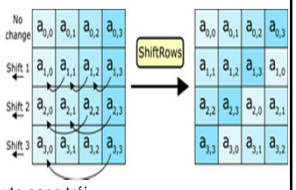
- InvSubBytes (tiếp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 3A | 91 | 11 | 41 | 4F | 67 | DC | EA | 97 | F2 | CF | CE | F0 | B4 | E6 | 73 |
| 9 | 96 | AC | 74 | 22 | E7 | AD | 35 | 85 | E2 | F9 | 37 | E8 | 1C | 75 | DF | 6E |
| A | 47 | F1 | 1A | 71 | 1D | 29 | C5 | 89 | 6F | B7 | 62 | 0E | AA | 18 | BE | 1B |
| B | FC | 56 | 3E | 4B | C6 | D2 | 79 | 20 | 9A | DB | C0 | FE | 78 | CD | 5A | F4 |
| C | 1F | DD | A8 | 33 | 88 | 07 | C7 | 31 | B1 | 12 | 10 | 59 | 27 | 80 | EC | 5F |
| D | 60 | 51 | 7F | A9 | 19 | B5 | 4A | 0D | 2D | E5 | 7A | 9F | 93 | C9 | 9C | EF |
| E | A0 | E0 | 3B | 4D | AE | 2A | F5 | B0 | C8 | EB | BB | 3C | 83 | 53 | 99 | 61 |
| F | 17 | 2B | 04 | 7E | BA | 77 | D6 | 26 | E1 | 69 | 14 | 63 | 55 | 21 | 0C | 7D |




# Chuẩn mã dữ liệu AES

- 3. ShiftRows - đổi chỗ, các hàng trong khối được dịch vòng
  - Dịch hàng vòng quanh trên mỗi hàng
  - Hàng 1 không đổi
  - Hàng 2 dịch vòng quanh 1 byte sang trái

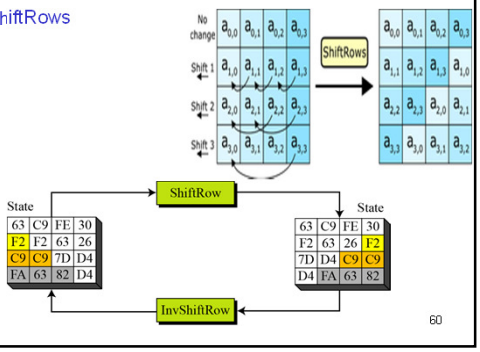



  - Hàng 3 dịch vòng quanh 2 byte sang trái
  - Hàng 4 dịch vòng quanh 3 byte sang trái
  - Giải mã thực hiện dịch ngược lại sang phải
  - Vì trạng thái được xử lý bởi cột, bước này thực chất là hoán vị byte giữa các cột.



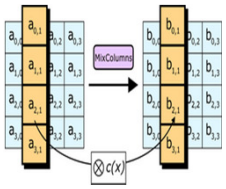
# Chuẩn mã dữ liệu AES

- 3. ShiftRows



## Chuẩn mã dữ liệu AES

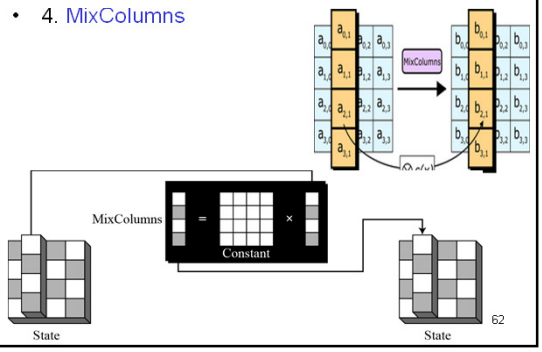
- 4. MixColumns - quá trình trộn làm việc theo các cột trong khối theo một chuyển đổi tuyến tính.
  - Có thể biểu diễn mỗi cột mới là nghiệm của 4 phương trình để tìm ra byte mới trong mỗi cột
  - Mã yêu cầu sử dụng ma trận nghịch đảo, với hệ số lớn thì tính toán khó khăn hơn
  - Có các đặc trưng khác của cột như sau:
    - » Mỗi cột là một đa thức bậc 3 gồm 4 số hạng
    - » Với mỗi phần tử là một byte tương ứng với phần tử trong GF(28).
    - » Các đa thức nhân tính theo Modulo ($x^4+1$).




61

## Chuẩn mã dữ liệu AES

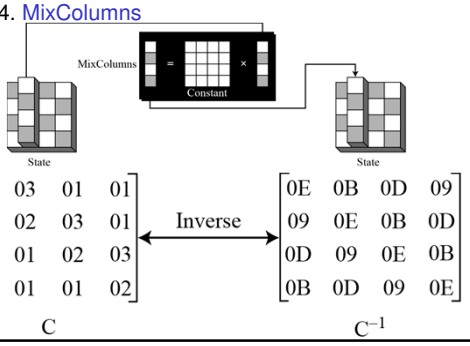
- 4. MixColumns




62

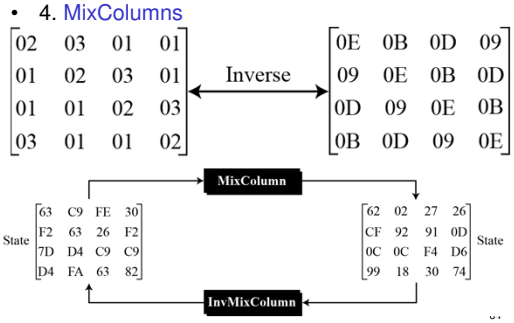
## Chuẩn mã dữ liệu AES

- 4. MixColumns




## Chuẩn mã dữ liệu AES

- 4. MixColumns




## Chuẩn mã dữ liệu AES

- Bốn byte trong từng cột được kết hợp lại theo một phép biến đổi tuyến tính khả nghịch. Mỗi khối 4 byte đầu vào sẽ cho một khối 4 byte ở đầu ra với tính chất là mỗi byte ở đầu vào đều ảnh hưởng tới cả 4 byte đầu ra.
- Cùng với bước ShiftRows, MixColumns đã tạo ra tính chất khuếch tán cho thuật toán. Mỗi cột được xem như một đa thức trong trường hữu hạn và được nhân với đa thức

$$c(x) = 3x^3 + x^2 + x + 2 \text{ (modulo } x^4 + 1)$$

Vì thế, bước này có thể được xem là phép nhân ma trận trong trường hữu hạn.

65

## Chuẩn mã dữ liệu AES

- **Mở rộng khoá AES**
  - Dùng khoá 128 bit (16 byte) và mở rộng thành mảng gồm 44/52/60 từ 32 bit.
  - Bắt đầu bằng việc copy khoá vào 4 từ đầu
  - Sau đó tạo quay vòng các từ mà phụ thuộc vào giá trị ở các vị trí trước và 4 vị trí sau
    - 3 trong 4 trường hợp chỉ là XOR chúng cùng nhau
    - Mỗi cái thứ 4 có S box kết hợp quay và XOR với hằng số trước đó, trước khi XOR cùng nhau
    - Thiết kế chống các tấn công đã biết

66

## Chuẩn mã dữ liệu AES

- Giải mã AES
  - Giải mã ngược lại không duy nhất vì các bước thực hiện theo thứ tự ngược lại.
  - Nhưng có thể xác định mã ngược tương đương với các bước đã làm đối với mã
    - Nhưng sử dụng ngược lại với từng bước
    - Với khoá con khác nhau
  - Thực hiện được vì kết quả không thay đổi khi
    - Đổi lại phép thế byte và dịch các hàng
    - Đổi lại việc trộn các cột và bổ sung khoá vòng
  - Lý do mở rộng khoá: các tiêu chuẩn thiết kế bao gồm
    - Giả sử biết một phần khoá, khi đó không đủ để biết nhiều hơn, tức là các khoá con khác hoặc khoá nói chung.
    - Phép biến đổi nghịch đảo được.
    - Nhanh đối với nhiều kiểu CPU.

67

## Chuẩn mã dữ liệu AES

- Sử dụng hằng số vòng để làm mất tính đối xứng
- Khuếch tán bit khoá thành khoá con cho các vòng
- Có đủ tính phi đối xứng để chống thám mã
- Đơn giản trong việc giải mã

- Các khía cạnh cài đặt:
  - Có thể cài đặt hiệu quả trên CPU 8 bit
  - Phép thế byte làm việc trên các byte sử dụng bảng với 256 đầu vào.
  - Dịch hàng là phép dịch byte đơn giản
  - Cộng khoá vòng làm việc trên byte XOR
  - Các cột hỗn hợp yêu cầu nhân ma trận trong GF($2^8$) mà làm việc trên giá trị các byte, có thể đơn giản bằng cách tra bảng

68

## Chuẩn mã dữ liệu AES

- Có thể cài đặt hiệu quả trên CPU 32 bit
- Xác định lại các bước để sử dụng từ 32 bit
- Có thể tính trước 4 bảng với 256 đầu vào
- Sau đó mỗi cột trong mỗi vòng có thể tính bằng cách tra 4 bảng và 4 XOR
- Cần 16 Kb để lưu các bảng
- Những nhà thiết kế tin tưởng rằng việc cài đặt rất hiệu quả này là yếu tố cơ bản trong việc chọn nó là mã AES

69

## Chuẩn mã dữ liệu AES

- Độ an toàn của AES:
  - Thiết kế và độ dài khóa của thuật toán AES (128, 192 và 256 bít) là đủ an toàn để bảo vệ các thông tin được xếp vào loại MẬT (secret). Các thông tin TUYỆT MẬT (top secret) sẽ phải dùng khóa 192 hoặc 256 bít.
  - Một vấn đề khác nữa là cấu trúc toán học của AES. Không giống với các thuật toán mã hóa khác, AES có mô tả toán học khá đơn giản. Tuy điều này chưa dẫn đến mối nguy hiểm nào nhưng một số nhà nghiên cứu sợ rằng sẽ có người lợi dụng được cấu trúc này trong tương lai.

70

## Chuẩn mã dữ liệu AES

- Vào thời điểm năm 2006, dạng tấn công lên AES duy nhất thành công là tấn công kênh bên (side channel attack).
- Tấn công kênh bên không tấn công trực tiếp vào thuật toán mã hóa mà thay vào đó, tấn công lên các hệ thống thực hiện thuật toán có sơ hở làm lộ dữ liệu

71