MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

Bài 03. Chuẩn mã khối tiên tiến và chuẩn đệm

1. Giới thiệu AES
2. Cấu trúc của AES
3. Cài đặt AES
4. Đệm cho mã khối

1. Giới thiệu AES
2. Cấu trúc của AES
3. Cài đặt AES
4. Đệm cho mã khối

Giới thiệu chung về AES

❑**Lịch sử ra đời (1/2)**

- DES không còn an toàn
- Năm 1997: NIST phát động cuộc thi tìm kiếm hệ mật làm chuẩn mới
- Yêu cầu đối với thuật toán ứng viên:
  - –được mô tả công khai
  - –là mã khối
  - –hỗ trợ nhiều kích thước khóa khác nhau
  - –cài đặt tốt trên phần cứng và phần mềm
  - –miễn phí cho mọi mục đích sử dụng

4

Giới thiệu chung về AES

❑**Lịch sử ra đời (2/2)**

- Tổng cộng có 21 ứng viên
- Sau vòng 1 (1998): có 15 đạt yêu cầu
- Sau vòng 2 (1999): còn 5 thuật toán, gồm MARC (IBM), RC6 (RSA), Rijndael (Daemon và Rijmen), Serpent (Anderson) và Twofish (Schneier)
- S
- N

MARC, RC6, Serpent, Twofish có thể coi là tốt ngang ngửa với AES!

5

Giới thiệu chung về AES

❑**Đặc điểm của thuật toán**

- Rijndael
  - –Kích thước khối: 128, 160, 192, 224, 256
  - –Kích thước khóa: 128, 160, 192, 224, 256
  - –Số vòng lặp: 10, 11, 12, 13, 14
- AES
  - –Kích thước khối: 128
  - –Kích thước khóa: 128, 192, 256
  - –Số vòng lặp: 10, 12, 14

6

Giới thiệu chung về AES

❑**Độ an toàn của AES**

- Chưa có tấn công hiệu quả lên **thuật toán** AES
- Chỉ có tấn công kênh kề (side channel) lên **cài đặt** thuật toán.

7

Giới thiệu chung về AES

❑**Phần mềm sử dụng AES**

- 7z, WinRAR, WinZIP
- NTFS (EFS)
- BitLocker, VeraCrypt, DiskCryptor
- IPsec, KeePass
- WPA

8

Giới thiệu chung về AES

❑**Thư viện lập trình mật mã**

- C: OpenSSL, CryptoAPI
- C++: Bortan, Crypto++
- C#/.NET: .NET Framework, Bouncy Castle
- Java: JCE, Bouncy Castle
- Python: PyCrypto
- JavaScript: SJCL, AES-JS

9

1. Giới thiệu AES
2. **Cấu trúc của AES**
3. Cài đặt AES
4. Đệm cho mã khối

Cấu trúc của AES

- Tiêu chuẩn FIPS 197: Advanced Encryption Standard
- Tiêu chuẩn TCVN 7816-2007: Kỹ thuật mật mã – Các thuật toán mật mã – Thuật toán mã hóa dữ liệu AES

11

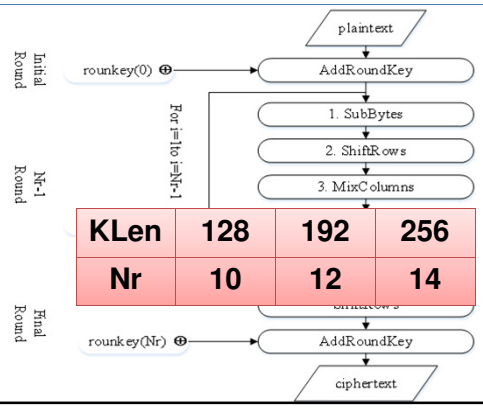
Cấu trúc của AES

- Dữ liệu (input, intermediate state, output, round keys) trong AES là ma trận kích thước 4xNb = 4x4
- Nạp dữ liệu $x_0x_1x_2...x_{15}$ vào ma trận:

x_0	x_4	x_8	x_{12}
x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}

12

Cấu trúc của AES

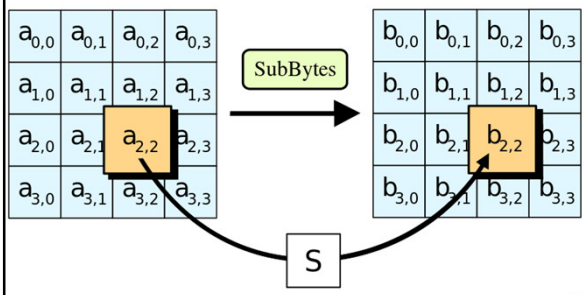


KLen	128	192	256
Nr	10	12	14

13

Cấu trúc của AES

- SubBytes



14

Cấu trúc của AES

$$y = Ax^{-1} + b$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

15

Cấu trúc của AES

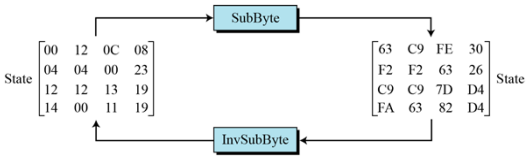
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	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
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

SubBytes(0x53) = ?
SubBytes(0xFA) = ?

16

Cấu trúc của AES

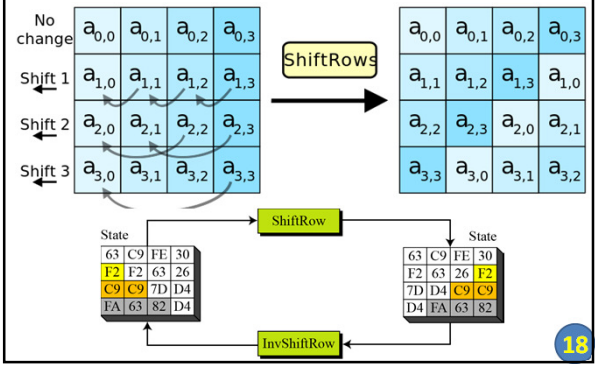
- SubBytes



17

Cấu trúc của AES

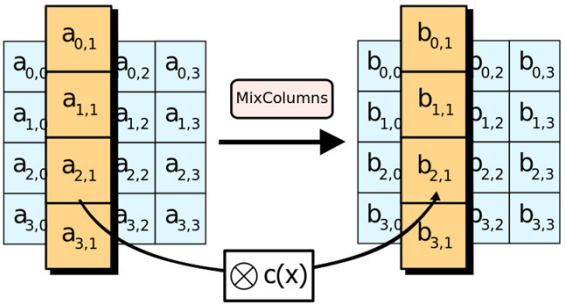
- ShiftRows



18

Cấu trúc của AES

- MixColumns



19

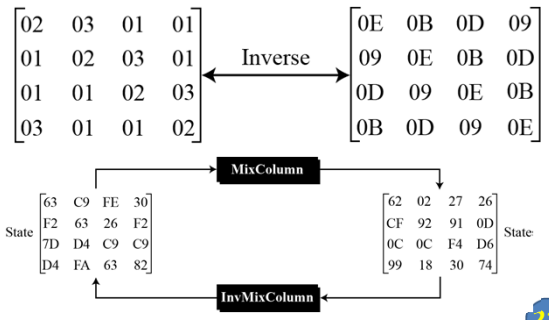
Cấu trúc của AES

$$s'_c = C \cdot s_c$$

$$\begin{pmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \bullet \begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix}$$

20

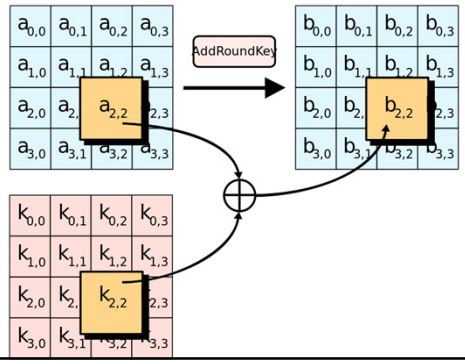
Cấu trúc của AES



21

Cấu trúc của AES

- AddRoundKey

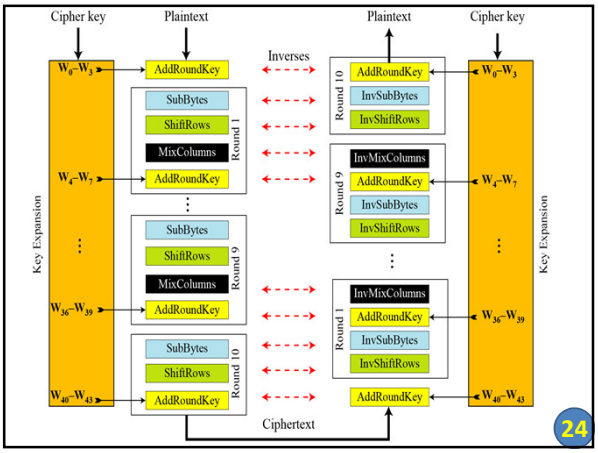


22

Cấu trúc của AES

- Mỗi phép biến đổi trong AES đều có phép biến đổi ngược: InvSubBytes, InvShiftRows, InvMixColumns, AddRoundKey
- Pha giải mã giống như pha mã hóa, nhưng sử dụng các phép biến đổi ngược và trật tự đảo ngược các khóa vòng
- Có hai cấu trúc giải mã: giải mã xuôi và giải mã ngược

23



24

Cấu trúc của AES

- **Mã hóa**

Add → (Nr-1)x{Sub,Shift,Mix,Add} → {Sub,Shift, Add}

- **Giải mã xuôi**

Add→(Nr-1)x{IShift,ISub,Add,IMix}→{IShift,ISub,Add}

- **Giải mã ngược**

Add→(Nr-1)x{ISub,IShift,IMix,Add}→{ISub,IShift,Add}

RoundKey' = Inv (RoundKey)

25

1. Giới thiệu AES
2. Cấu trúc của AES
3. **Cài đặt AES**
4. Đệm cho mã khối

Cài đặt AES

❑**Test vector**

- Khi cài đặt một thuật toán mật mã, chương trình mã hóa được, giải mã được chưa hẳn đã là cài đặt đúng!
- Cần kiểm tra tính đúng đắn bằng việc sử dụng các test vector.
- Ví dụ với AES-128

K = 2b7e151628aed2a6abf7158809cf4f3c

p = 6bc1bee22e409f96e93d7e117393172a

c = 3ad77bb40d7a3660a89ecaf32466ef97

27

Cài đặt AES

❑**Cài đặt theo mô tả trong chuẩn**

- Đa phần các phép tính thực hiện trên số 8 bít, không khai thác được tính năng của vi xử lý 32 bít
- Tốn ít bộ nhớ
- Phù hợp cho vi xử lý 8 bít, như trong các hệ thống nhúng (embeded systems)
- Đối với hệ thống 32 bít thì cần có cài cách cài đặt hiệu quả hơn

28

Cài đặt AES

❑**Cài đặt cho hệ thống 32 bít**

- Xét một vòng của AES, ký hiệu
  - **a** – giá trị đầu vào của vòng (round) đó
  - **b** – trạng thái sau SubBytes
  - **c** – trạng thái sau ShiftRows
  - **d** – trạng thái sau MixColumns
  - **e** – trạng thái sau AddRoundKey, tức là đầu ra
  - **k** – khóa vòng
- Ký hiệu $\mathbf{s}_j$ là cột thứ **j** của ma trận **s**.

29

Cài đặt AES

- Xét $\mathbf{e}_j$ là kết quả mã hóa cột thứ **j**

$$e_j = \left(e_{0,j}, e_{1,j}, e_{2,j}, e_{3,j}\right)^T$$

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} + \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

30

Cài đặt AES

$$\begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j+1 \bmod Nb} \\ b_{2,j+2 \bmod Nb} \\ b_{3,j+3 \bmod Nb} \end{bmatrix} = \begin{bmatrix} S[a_{0,j}] \\ S[a_{1,j+1}] \\ S[a_{2,j+2}] \\ S[a_{3,j+3}] \end{bmatrix}; \quad j+k \bmod Nb \neq j+k$$

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S[a_{0,j}] \\ S[a_{1,j+1}] \\ S[a_{2,j+2}] \\ S[a_{3,j+3}] \end{bmatrix} + \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

31

Cài đặt AES

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} S[a_{0,j}] \bullet 02 \\ S[a_{0,j}] \\ S[a_{0,j}] \\ S[a_{0,j}] \bullet 03 \end{bmatrix} \oplus \begin{bmatrix} S[a_{0,j+1}] \bullet 03 \\ S[a_{0,j+1}] \bullet 2 \\ S[a_{0,j+1}] \\ S[a_{0,j+1}] \end{bmatrix} \oplus \begin{bmatrix} S[a_{0,j+2}] \\ S[a_{0,j+2}] \bullet 03 \\ S[a_{0,j+2}] \bullet 02 \\ S[a_{0,j+2}] \end{bmatrix} \oplus \begin{bmatrix} S[a_{0,j+3}] \\ S[a_{0,j+3}] \\ S[a_{0,j+3}] \bullet 03 \\ S[a_{0,j+3}] \bullet 02 \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Xây dựng 4 bảng tra T_0, T_1, T_2, T_3

32

Cài đặt AES

$$T_0[x] = \begin{bmatrix} S[x] \bullet 02 \\ S[x] \\ S[x] \\ S[x] \bullet 03 \end{bmatrix}; \quad T_1[x] = \begin{bmatrix} S[x] \bullet 03 \\ S[x] \bullet 2 \\ S[x] \\ S[x] \end{bmatrix};$$

$$T_2[x] = \begin{bmatrix} S[x] \\ S[x] \bullet 03 \\ S[x] \bullet 02 \\ S[x] \end{bmatrix}; \quad T_3[x] = \begin{bmatrix} S[x] \\ S[x] \\ S[x] \bullet 03 \\ S[x] \bullet 02 \end{bmatrix}; \quad x = 0x00..0xFF$$

Mỗi bảng T_i có 256 phần tử 32 bít ứng với 256 giá trị 8 bít của x

33

Cài đặt AES

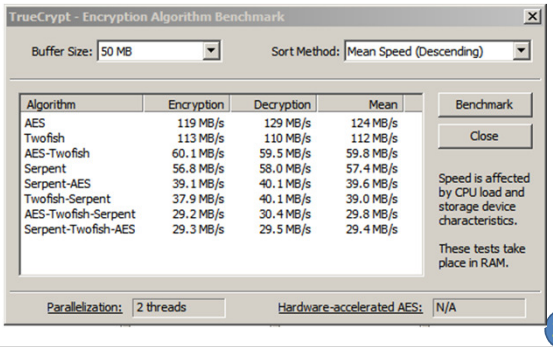
$$e_j = T_0[a_{0,j}] \oplus T_1[a_{1,j+1}] \oplus T_2[a_{2,j+2}] \oplus T_3[a_{3,j+3}] \oplus k_j$$

Toàn bộ phép mã hóa đã chuyển thành phép tra bảng và XOR trên số 32 bít!

34

Cài đặt AES

- Tốc độ cài đặt mềm



35

Cài đặt AES

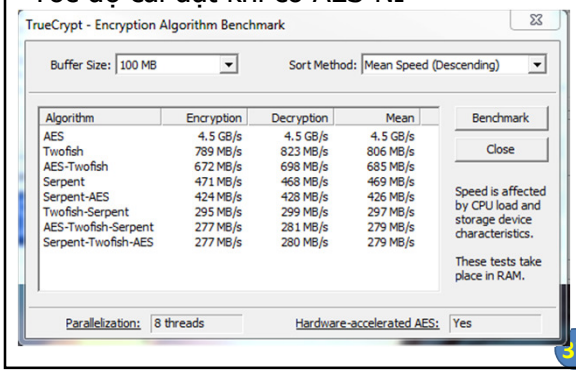
❑Tập lệnh AES-NI

- Các vi xử lý đời mới của Intel (Core i5 trở lên) và AMD hỗ trợ tập lệnh đặc biệt để cài đặt AES, gọi là AES-NI
- AES-NI gồm 6 lệnh
  - AESENC và AESENCLAST: mã hóa 1 vòng
  - AESDEC và AESDECLAST: giải mã 1 vòng
  - AESKEYGENASSIST: tạo khóa vòng
  - AESIMC: tạo khóa vòng giải mã

36

Cài đặt AES

- Tốc độ cài đặt khi có AES-NI



37

Cài đặt AES

Kết luận

Việc cài đặt một thuật toán mật mã đòi hỏi phải nghiên cứu kỹ lưỡng để đảm bảo an toàn và đạt được hiệu năng thực thi cao!

38

1. Giới thiệu AES
2. Cấu trúc của AES
3. Cài đặt AES
4. **Đệm cho mã khối**

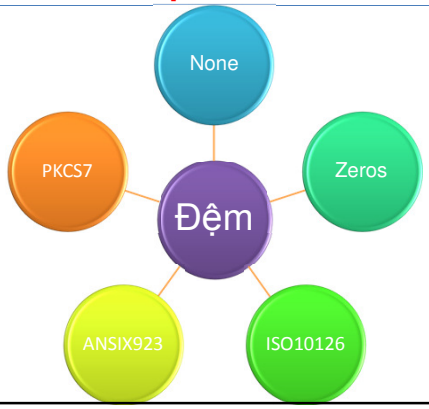
Chuẩn đệm cho mã khối

Đệm (padding) là gì?

Tại sao cần đệm?

40

Chuẩn đệm cho mã khối



41

Chuẩn đệm cho mã khối

None padding
and
Zero padding
Why are they possible?

42

Chuẩn đệm cho mã khối

ANSIX923 Padding
- byte cuối: tổng số byte đệm
- các byte còn lại: 0

11	22	33	44	55	66	77	88	99	AA						
11	22	33	44	55	66	77	88	99	AA	00	00	00	00	00	06

11	22	33	44	55	66	77	88								
11	22	33	44	55	66	77	88	00	00	00	00	00	00	00	08

43

Chuẩn đệm cho mã khối

ISO10126 Padding
- byte cuối: tổng số byte đệm
- các byte còn lại: ngẫu nhiên

11	22	33	44	55	66	77	88	99	AA						
11	22	33	44	55	66	77	88	99	AA	4B	1F	A2	11	2E	06

11	22	33	44	55	66	77	88								
11	22	33	44	55	66	77	88	69	32	0A	B9	F1	16	EA	08

44

Chuẩn đệm cho mã khối

PKCS7 Padding
Mỗi byte đệm: tổng số byte đệm

11	22	33	44	55	66	77	88	99	AA						
11	22	33	44	55	66	77	88	99	AA	06	06	06	06	06	06

11	22	33	44	55	66	77	88								
11	22	33	44	55	66	77	88	08	08	08	08	08	08	08	08

45

1. Giới thiệu AES
2. Cấu trúc của AES
3. Cài đặt AES
4. Đệm cho mã khối