

NHẬP MÔN MẬT MÃ HỌC

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 1

GIỚI THIỆU HỌC PHẦN

ĐẢM BẢO TÍNH BÍ MẬT
Thông tin chỉ được phép truy cập bởi đối tượng được cấp phép

ĐẢM BẢO TÍNH TOÀN VẸN
Dữ liệu, thông tin không bị thay đổi, mất mát khi truyền tin

TÍCH HỢP CÁC DỊCH VỤ
Khả năng vận dụng kết hợp giữa các thuật toán mật mã để giải quyết các bài toán đảm bảo an toàn thông tin cơ bản

XÁC THỰC
Đảm bảo thông tin đến từ một nguồn đáng tin cậy

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 1

GIỚI THIỆU HỌC PHẦN

THỜI LƯỢNG: 3tc

- 54 tiết lý thuyết (3 tiết/1 buổi x 18 buổi)
- 18 tiết bài tập

ĐÁNH GIÁ KẾT QUẢ HỌC TẬP

- Điểm chuyên cần
 - Đi học đầy đủ, đúng giờ
 - Tham gia xây dựng bài
- Kiểm tra giữa kỳ: thi viết/BTL
- Thi kết thúc học phần: thi viết

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 1

GIỚI THIỆU HỌC PHẦN

Cơ sở lý thuyết mật mã, Học viện KTMM
Nguyễn Bình, Hoàng Thu Phương, 2013

Mật mã ứng dụng trong an toàn thông tin
Nguyễn Ngọc Cường, Trần Thị Lương, 2013

Và tài liệu khác
Google

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 1

GIỚI THIỆU VỀ PHÂN LOẠI MẬT MÃ

Thuật toán mật mã

```

graph TD
    A[Thuật toán mật mã] --> B[Mật mã đối xứng/ Mật mã khóa bí mật]
    A --> C[Hàm băm]
    A --> D[Chữ kí số]
    A --> E[Sinh số ngẫu nhiên]

    B --> B1[Mã dòng]
    B --> B2[Mã khóa]
    C --> C1[Hàm băm không khóa]
    C --> C2[Hàm băm có khóa]
  
```

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 1

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NỘI DUNG

- TỔNG QUAN VỀ MẬT MÃ HỌC**
Tổng quan về mật mã học
- CÁC HỆ MẬT KHÓA BÍ MẬT**
Các hệ mật khóa bí mật
- CÁC HỆ MẬT KHÓA CÔNG KHAI**
Các hệ mật khóa công khai
- HÀM BĂM, XÁC THỰC VÀ CHỮ KÍ SỐ**
Hàm băm, toàn vẹn và chữ kí số
- VẤN ĐỀ PHÂN PHỐI & THỎA THUẬN KHÓA**
Vấn đề phân phối & thỏa thuận khóa

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 6

CHƯƠNG 01

TỔNG QUAN VỀ MẬT MÃ HỌC

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 7

BÀI 01 - MỤC TIÊU

- An toàn thông tin là gì?
- Các tính chất (dịch vụ) cơ bản của an toàn thông tin?
- Mối quan hệ giữa các dịch vụ an toàn thông tin cơ bản và các loại thuật toán mật mã cơ bản như thế nào?
- Định nghĩa hình thức toán học của một Hệ mật là gì?
- Hệ mật đối xứng/bất đối xứng? Hệ mật mã khóa/mã đóng?
- Có những ứng dụng cụ thể điển hình nào của mật mã trong thực tế?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 8

TỔNG QUAN VỀ MẬT MÃ HỌC

- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 9

KN An toàn thông tin

An toàn thông tin là gì?

- An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bí mật và tính khả dụng của thông tin

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Một số vấn đề cơ bản trong ATTT

- Tránh bị truy nhập
- Tránh bị sử dụng
- Tránh bị tiết lộ
- Tránh bị gián đoạn
- Tránh bị sửa đổi
- Tránh bị phá hoại trái phép

DATA PROTECTION

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 11

Một số vấn đề trong bảo vệ thông tin

```

graph TD
    A[Đối tượng bảo vệ thông tin] --> B[Phân tích hệ quả của việc thực hiện các mối đe dọa]
    B --> C[Phân tích các mối đe dọa]
    C --> D[Phân tích các mối đe dọa]
    D --> E[Phân tích các mối đe dọa]
    E --> F[Phân tích các mối đe dọa]
    F --> G[Phân tích các mối đe dọa]
    G --> H[Phân tích các mối đe dọa]
    H --> I[Phân tích các mối đe dọa]
    I --> J[Phân tích các mối đe dọa]
    J --> K[Phân tích các mối đe dọa]
    K --> L[Phân tích các mối đe dọa]
    L --> M[Phân tích các mối đe dọa]
    M --> N[Phân tích các mối đe dọa]
    N --> O[Phân tích các mối đe dọa]
    O --> P[Phân tích các mối đe dọa]
    P --> Q[Phân tích các mối đe dọa]
    Q --> R[Phân tích các mối đe dọa]
    R --> S[Phân tích các mối đe dọa]
    S --> T[Phân tích các mối đe dọa]
    T --> U[Phân tích các mối đe dọa]
    U --> V[Phân tích các mối đe dọa]
    V --> W[Phân tích các mối đe dọa]
    W --> X[Phân tích các mối đe dọa]
    X --> Y[Phân tích các mối đe dọa]
    Y --> Z[Phân tích các mối đe dọa]
    Z --> AA[Phân tích các mối đe dọa]
    AA --> BB[Phân tích các mối đe dọa]
    BB --> CC[Phân tích các mối đe dọa]
    CC --> DD[Phân tích các mối đe dọa]
    DD --> EE[Phân tích các mối đe dọa]
    EE --> FF[Phân tích các mối đe dọa]
    FF --> GG[Phân tích các mối đe dọa]
    GG --> HH[Phân tích các mối đe dọa]
    HH --> II[Phân tích các mối đe dọa]
    II --> JJ[Phân tích các mối đe dọa]
    JJ --> KK[Phân tích các mối đe dọa]
    KK --> LL[Phân tích các mối đe dọa]
    LL --> MM[Phân tích các mối đe dọa]
    MM --> NN[Phân tích các mối đe dọa]
    NN --> OO[Phân tích các mối đe dọa]
    OO --> PP[Phân tích các mối đe dọa]
    PP --> QQ[Phân tích các mối đe dọa]
    QQ --> RR[Phân tích các mối đe dọa]
    RR --> SS[Phân tích các mối đe dọa]
    SS --> TT[Phân tích các mối đe dọa]
    TT --> UU[Phân tích các mối đe dọa]
    UU --> VV[Phân tích các mối đe dọa]
    VV --> WW[Phân tích các mối đe dọa]
    WW --> XX[Phân tích các mối đe dọa]
    XX --> YY[Phân tích các mối đe dọa]
    YY --> ZZ[Phân tích các mối đe dọa]
    ZZ --> AA
  
```

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 12

 Một số vấn đề trong bảo vệ thông tin



BÍ MẬT THÔNG TIN (CONFIDENTIALITY) Đảm bảo chỉ những đối tượng đã được cấp quyền mới biết được nội dung thông tin	TOÀN VEN THÔNG TIN (INTEGRITY) Bảo đảm thông tin không bị sửa đổi, xuyên tạc bởi những người không có thẩm quyền hoặc đối tượng trái phép (hoặc giúp phát hiện rằng thông tin đã bị sửa đổi)
CHỐNG THOÁI THẮC TRÁCH NHIỆM (NON-REPUDIATION) Đảm bảo một đối tác bất kỳ trong hệ thống không thể từ chối trách nhiệm về hành động mà mình đã thực hiện	XÁC THỰC (AUTHENTICATION) Xác thực các đối tác trong liên lạc, xác thực nguồn gốc của một thông báo

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 15

 Thuật toán mật mã cơ bản
Có những loại thuật toán mật mã cơ bản nào?

- Mã hóa
- Hàm băm, mã xác thực thông điệp (MAC)
- Chữ ký số

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 15

 Quan hệ giữa Dịch vụ ATTT & Thuật toán
Mỗi quan hệ giữa các dịch vụ an toàn thông tin và các kỹ thuật (thuật toán) mật mã cơ bản?

	Dịch vụ	Kỹ thuật
	Đảm bảo tính bí mật	Mã hóa
	Đảm bảo tính toàn vẹn	Chữ ký số, hàm băm, MAC
	Xác thực	Chữ ký số, MAC
	Chống chối bỏ	Chữ ký số

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 15

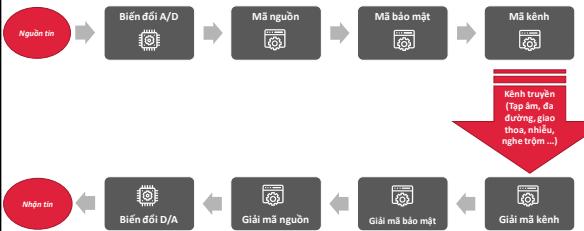
 TỔNG QUAN VỀ MẬT MÃ HỌC



- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 15

 Sơ đồ hệ thống truyền tin số



Nguồn tin → Biến đổi A/D → Mã nguồn → Mã bảo mật → Mã kênh
Nhận tin ← Giải mã kênh ← Giải mã bảo mật ← Giải mã nguồn ← Biến đổi D/A

Kênh truyền (Tập âm, đà dường, giao thoa, nhiễu, nghe trộm...)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 17

 TỔNG QUAN VỀ MẬT MÃ HỌC



- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 15

 **Một số ứng dụng của mật mã trong thực tế**

-  **Ứng dụng trong thực tiễn**
 - Ứng dụng trong đời sống thông tin, KT-XH
 - Ứng dụng trong an ninh, quốc phòng
-  **Ứng dụng của một số thành phần mật mã**
-  **Ứng dụng trong các giao thức bảo mật**
 - Mã hóa mật khẩu và xác thực đăng nhập trên Linux
 - SSH, SSL, SET, ...

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 19

 **TỔNG QUAN VỀ MẬT MÃ HỌC**



-  Một số vấn đề cơ bản trong bảo vệ thông tin
-  Sơ đồ hệ thống truyền tin số
-  Một số ứng dụng của mật mã trong thực tế
-  Các hệ thống mật mã

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 20

 **Định nghĩa hình thức của hệ mật**
Một số khái niệm/ký hiệu liên quan

- P là tập hữu hạn các bản rõ có thể
- C là tập hữu hạn các bản mã có thể
- K là tập hữu hạn các khóa có thể
- $E_k: P \rightarrow C$ - là quy tắc mã hóa với khóa $k \in K$. Tập $\{E_k: k \in K\}$ ký hiệu là E , còn tập $\{E_k(x): x \in P\}$ ký hiệu là $E_k(P)$.
- $D_k: C \rightarrow P$ - là quy tắc giải mã với khóa $k \in K$. Tập $\{D_k: k \in K\}$ ký hiệu là D .
- Với mỗi $k \in K$ sẽ được mô tả dưới dạng $k = (k_e, k_d)$, trong đó: k_e - là khóa dùng cho mã hóa, k_d - là khóa dùng cho giải mã. Khi đó E_k được hiểu là hàm E_{k_e} , D_k được hiểu là hàm D_{k_d}

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 21

 **Định nghĩa hình thức của hệ mật**
Một số khái niệm/ký hiệu liên quan

- Định nghĩa hệ mật:** Một hệ mật là bộ 5 (P, C, K, E, D) thoả mãn các điều kiện sau:
 - $\forall x \in P, k \in K$ ta có:
$$D_k(E_k(x)) = x;$$

$$C = \bigcup_{k \in K} E_k(P)$$
- Ghi chú:**
 - Mã hóa: $y = E_{k_e}(x)$
 - Giải mã: $x = D_{k_d}(y)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 22

 **Các hệ thống mật mã**

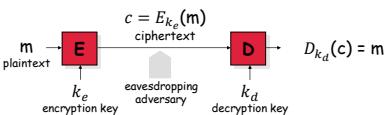


Quá trình chung của hệ mật

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 23

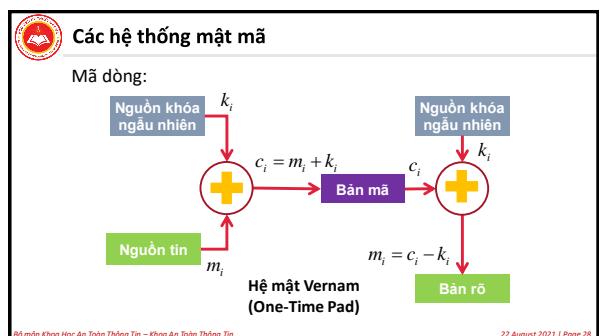
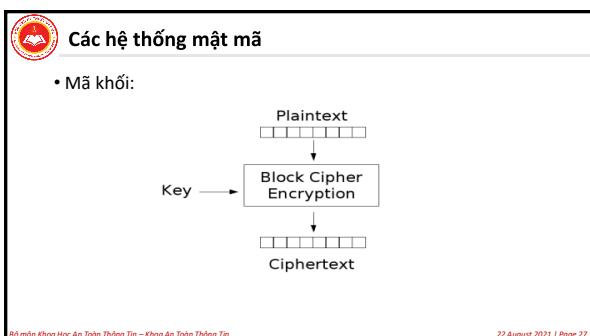
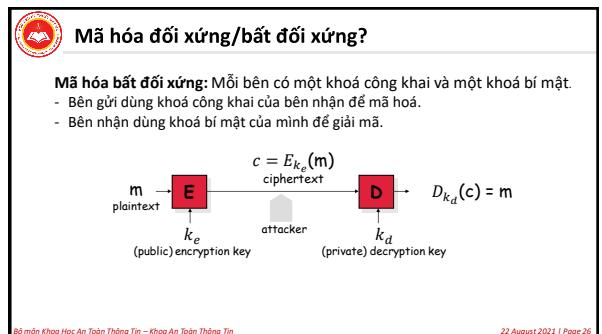
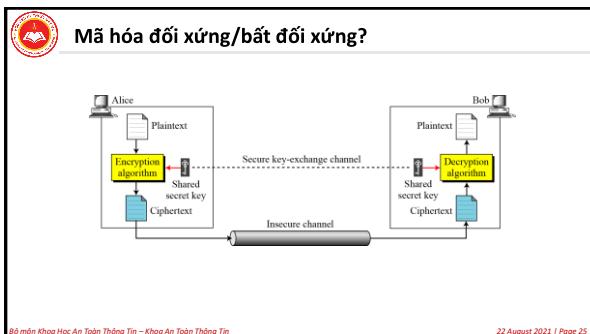
 **Mã hóa đối xứng/bất đối xứng?**

Mã hóa đối xứng: biết được khóa mã hóa dễ dàng suy ra được khóa giải mã (thông thường $k_e = k_d$)



$m \xrightarrow{k_e} E \xrightarrow{\text{ciphertext}} c \xrightarrow{k_d} D \xrightarrow{\text{decryption key}} m$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 24



Ví dụ: Hệ mật Vernam

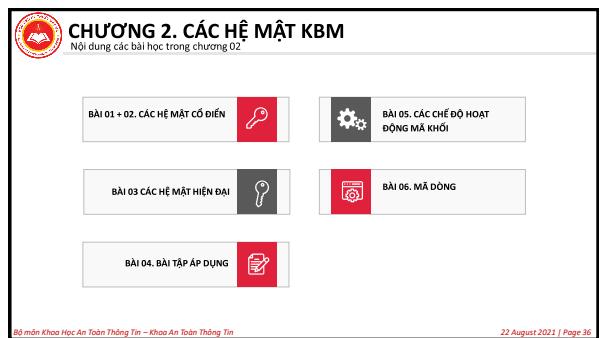
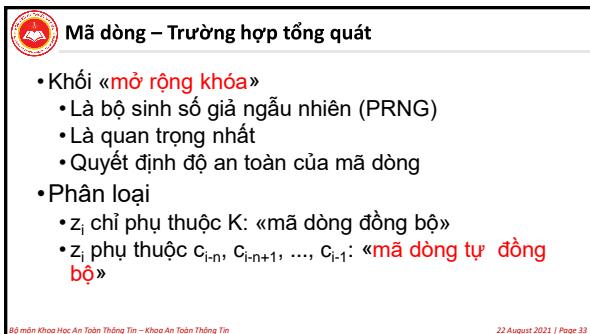
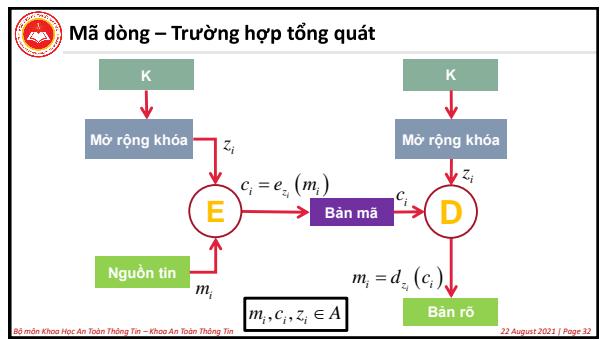
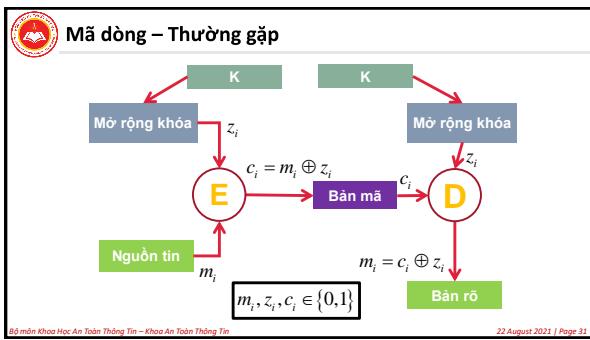
MÃ HÓA					
Bộ kí tự: chữ cái latin Khóa ngẫu nhiên: PWKAX Thông điệp: HELLO					
Rõ	H (7)	E (4)	L (11)	L (11)	O (14)
Khóa	P (15)	W (22)	K (10)	A (0)	X (23)
Mã	W (22)	A (0)	V (21)	?	?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 29

Ví dụ: Hệ mật Vernam

GIẢI MÃ					
Bộ kí tự: chữ cái latin Khóa ngẫu nhiên: PWKAX Bản mã: WAVLL					
Mã	W (22)	A (0)	V (21)	L (11)	L (11)
Khóa	P (15)	W (22)	K (10)	A (0)	X (23)
Rõ	H (7)	E (4)	L (11)	L (11)	O (14)

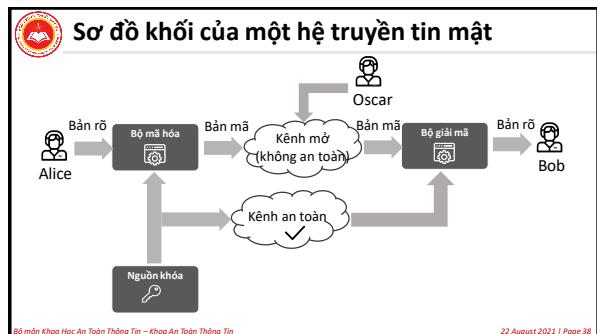
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 30



BÀI 01. CÁC HỆ CỔ ĐIỂN
Mục tiêu bài học, SV trả lời được các câu hỏi sau

- Sơ đồ khối của một hệ truyền tin mật sử dụng hệ mật KBM?
- Các phương pháp chính của hệ mật KBM?
- Yếu điểm của mã đơn biểu vs mã đa biểu?
- Hệ mật tích?
- Thám mã một số hệ mã cổ điển dựa trên phương pháp thống kê?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 37



Các hệ mật cổ điển

- Các hệ mật thay thế đơn biểu**
 - Khi khóa đã được chọn thì **mỗi kí tự của bản rõ được ánh xạ đến một kí tự duy nhất của bản mã**.
 - Như vậy độ dài của khóa ở đây là 26 và số khóa có thể có là 26!.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 39

Các hệ mật cổ điển

- Mã dịch vòng (MDV – Shift cipher):**
 - Bản rõ: **HOC TAP TOT LAO DONG TOT**
 - Khóa **k = 5**

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

 - Tìm bản mã
 - Từ bản mã thu được giải mã để thu bản rõ ban đầu.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 40

Các hệ mật cổ điển

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

Bản rõ	H	O	C	T	A	P	T	O	T	L	A	O	D	O	N	G	T	O	T
Mã tương ứng (x)	19	0	15	19	14	19	11	0	14	3	14	13	6	19	14	19			
(x + 5) mod 26	12	19	7	24	5	20	24	19	24	5	19	8	19	18	11	24	19	24	
Bản mã	M	T	H	Y	F	U	Y	T	Y	Q	F	T	I	T	S	L	Y	T	

Bản mã thu được: **MTHFYUYTYQFTITSLYTY**

Giải mã: **SV tự làm!**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 41

Các hệ mật cổ điển

- Mã Affine:**
 - Cho $P = C = \mathbb{Z}_{26}$, $K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}$. Giả sử:
 $K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{UCLN}(a, 26) = 1\}$
Với $k = (a, b) \in K$ ta định nghĩa:

$$y = e_k(x) = ax + b \pmod{26}$$

$$x = d_k(y) = a^{-1}(y - b) \pmod{26}$$
- Ví dụ:**
 - Cho $k = (7, 3)$. Bản rõ: **It is nice today**
 - Tìm bản mã.
 - Giải mã bản mã thu được

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 42



Các hệ mật cổ điển

Giải:

- Tìm bản mã của bản rõ: **It is nice today**

▪ Ta có hàm mã: $e_k(x) = 7x + 3 \bmod 26$

Ký tự	I	T	I	S	N	I	C	E	T	O	D	A	Y
Mã (x)	8	9	8	18	13	8	2	4	19	14	3	0	24
$7x + 3 \bmod 26$	7	6	7	25	16	7	17	5	6	23	24	3	15
Bản mã	H	G	H	Z	Q	H	R	F	G	X	Y	D	P

- Bản mã thu được là: **HGHZQHRCFGXYDP**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

Giải:

- Tìm bản rõ của bản mã: **HGHZQHRCFGXYDP**

▪ Ta có hàm giải mã:

$$d_k(y) = 7^{-1} \cdot (y - 3) \bmod 26 = 15 \cdot (y - 3) \bmod 26$$

Bản mã	H	G	H	Z	Q	H	R	F	G	X	Y	D	P
Mã (y)	7	6	7	25	16	7	17	5	6	23	24	3	15
$15(y - 3) \bmod 26$	8	19	8	18	13	8	2	4	19	14	3	0	24
Bản rõ	I	T	I	S	N	I	C	E	T	O	D	A	Y

- Bản rõ thu được là: **It is nice today**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

Nhận xét về các hệ mật thay thế đơn biểu:

- Mỗi ký tự của bản rõ được ánh xạ đến một ký tự duy nhất của bản mã.
- Các đặc trưng về ngôn ngữ, tần suất xuất hiện của các chữ trong bản rõ và chữ tương ứng trong bản mã là như nhau

⇒ **Phương pháp thám mã bằng thống kê tần suất!**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

Các hệ mật thay thế đa biểu

- Yếu điểm của các mã pháp đơn biểu
- Một hướng khác làm tăng độ an toàn cho mã trên bảng chữ là sử dụng **nhiều bảng chữ để mã**.
- Mỗi chữ sẽ được mã bằng bất kì chữ nào trong bản mã tùy thuộc vào ngữ cảnh khi mã hóa. Là như vậy để trái bằng tần suất các chữ xuất hiện trong bản mã. Do đó làm **mất bớt cấu trúc của bản rõ** được thể hiện trên bản mã và làm cho mã thám đa bằng khó hơn.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

Hệ mật thay thế đa biểu:



Hệ Vigenere:

- Blaise de Vigenere (1523 – 1596)
- Tự tường:**
 - Sử dụng một loạt mã Caesar khác nhau dựa trên các ký tự của một từ khóa
 - Để hiểu và dễ thực hiện

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

Biến đổi bảng chữ cái A, B, ..., Z thành các ký tự 0, 1, ..., 25

Khóa (từ khóa) là một chuỗi các ký tự có độ dài m

Thông điệp được chia thành các khối độ dài m. Mỗi lần mã hóa sẽ thực hiện biến đổi đồng thời m ký tự

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 43



Các hệ mật cổ điển

• Mô tả hệ mã Vigenere:

Cho m là số nguyên dương. Ta định nghĩa $P = C = K = (\mathbb{Z}_{26})^m$. Với khóa $k = (k_1, k_2, \dots, k_m)$ ta xác định:
 $e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
Và $d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$
(Các phép toán đều thực hiện trên \mathbb{Z}_{26})

• Nhận xét:

- Số khoá: 26^m
- ⇒ Tấn công tìm khoá vét cạn là không khả thi



Các hệ mật cổ điển

• Ví dụ minh họa:

- $m = 6$, $k = \text{cipher}$
- Bản rõ: **Information security**
 - Hay mã hoá bản rõ trên
 - Giải mã bản mã vừa thu được



Các hệ mật cổ điển

• Giải:

- Ta có từ khoá **CIPHER**, tương ứng với dãy số: $k = (2, 8, 15, 7, 4, 17)$
- Chuyển các ký tự rõ thành mã trên \mathbb{Z}_{26} rồi cộng với từ khoá

Bản rõ	I	N	F	O	R	M	A	T	I	O	N	S	E	C	U	R	I	T	Y
Mã	8	13	5	14	17	12	0	19	8	14	13	18	4	2	20	17	8	19	24
Khoá	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2
Bản mã	10	21	20	21	21	3	2	1	23	21	17	9	6	10	9	24	12	10	0

- Chuyển các ký tự số thành chữ cái tương ứng. Ta có bản mã:

KVUVVDCBXVRJGKJYMK



Các hệ mật cổ điển

• Nhận xét?

- Nhu vậy có chữ mã khác nhau cho cùng một chữ của bản rõ.
 - Ví dụ: Chữ I được mã bởi các chữ: K, X, M; chữ N được mã bởi các chữ V, R; ...
- ⇒ Tần suất của các chữ bị là phẳng, nghĩa là tần suất xuất hiện các chữ trên bản mã tương đối đều nhau.
- Tuy nhiên chưa mất hoàn toàn, do độ dài của khoá có hạn, nên có thể tạo nên chu kỳ lặp lặp, hoặc việc lặp do ngẫu nhiên



Các hệ mật cổ điển

Baconian Cypher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z			
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z				
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z					
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z						
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z							
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z								
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z									
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z										
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z											
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z												
N	O	P	Q	R	S	T	U	V	W	X	Y	Z													
O	P	Q	R	S	T	U	V	W	X	Y	Z														
P	Q	R	S	T	U	V	W	X	Y	Z															
Q	R	S	T	U	V	W	X	Y	Z																
R	S	T	U	V	W	X	Y	Z																	
S	T	U	V	W	X	Y	Z																		
T	U	V	W	X	Y	Z																			
U	V	W	X	Y	Z																				
V	W	X	Y	Z																					
W	X	Y	Z																						
X	Y	Z																							
Y	Z																								
Z																									



Các hệ mật cổ điển

• Mô tả:

Cho m là số nguyên dương cố định. Cho $P = C = K = (\mathbb{Z}_{26})^m$: k (các ma trận khai nghịch cấp $m \times m$ trên \mathbb{Z}_{26}):

Với $k \in K$, ta xác định:

$$e_k(x) = xk$$

$$d_k(y) = yk^{-1}$$

(Các phép toán đều thực hiện trên \mathbb{Z}_{26} .)

 **Các hệ mật cổ điển**

- Cho ma trận:
$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$
- Định thức $\text{det}A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$
- Ma trận là khả nghịch $\Leftrightarrow \det A \neq 0$
- Vì các phép toán tính theo modulo 26 nên phải có điều kiện: $\text{UCLN}(\det A, 26) = 1$.
- Ma trận nghịch đảo:
$$A^{-1} = \det A^{-1} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 55

 **Các hệ mật cổ điển**

- Ví dụ minh họa:**
 - Bản rõ: "july"
 - Ma trận khoá:
$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$
 - Tìm bản mã của bản rõ trên
 - Từ bản mã thu được tìm bản rõ ban đầu.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 56

 **Các hệ mật cổ điển**

- Các hệ mật thay thế không tuần hoàn**
 - Phép thế lý tưởng là dùng nhiều bảng chữ cái để không nhận diện được phân bố tần suất
 - Điều gì xảy ra nếu văn bản được mã bằng số bảng chữ cái không hạn chế?
 - Vigenere đề xuất hệ mật khoá tự sinh (hệ mật khoá chạy)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 57

 **Các hệ mật cổ điển**

- Hệ mật khoá chạy:**
 - Ý tưởng:**
 - Từ khoá được nối tiếp bằng chính bản rõ, sau đó sử dụng mã Vigenere để mã
 - Khi biết từ khoá, giải được một số chữ của bản rõ rồi dùng chúng giải nốt phần còn lại
 - Sự cải tiến này gây mất khái niệm chu kỳ.
 - Ví dụ:**
 - Key = **deceptive**
 - Bản rõ: **we are discovered save yourself**
 - Hay mã hoá bản rõ trên.
 - Giải mã bản mã thu được

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 58

 **Các hệ mật cổ điển**

Mã hoá bản rõ

Khoá	D	E	C	E	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	V			
Bản rõ	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	V	Y	O	U	R	S	E	L
Bản mã	Z	I	C	V	T	W	Q	N	G	K	Z	E	I	I	G	A	S	X	S	T	S	L	V	V	L

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 59

 **Các hệ mật cổ điển**

O V E R E D S A V																									
Khoá	D	E	C	E	P	T	I	V	E																
Bản rõ	Z	I	C	V	T	W	Q	N	G	K	Z	E	I	I	G	A	S	X	S	T	S	L	V	V	L
Bản rõ	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	V	Y	O	U	R	S	E	L

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 60



Các hệ mật cổ điển

• Hệ mật OTP

- Do Gilbert Vernam đưa ra 1971

- Mô tả:

$P = C = K = (Z_2)^n$, $n \geq 1$ là số nguyên, $K \in (Z_2)^n$,
với $x = (x_1, \dots, x_n)$ và $K = (K_1, \dots, K_n)$, ta có hàm mã hóa:
 $e_K(x) = (x_1 \oplus K_1, \dots, x_n \oplus K_n)$
Phép mã đồng nhất với phép giải. Nếu $y = (y_1, \dots, y_n)$
ta có:
 $d_K(y) = (y_1 \oplus K_1, \dots, y_n \oplus K_n)$



Các hệ mật cổ điển

• Hệ mật hoán vị (MHV):

• Ý tưởng:

- Các chữ trong bản rõ không được thay thế bằng các chữ khác mà chỉ thay đổi vị trí giữa các chữ trong bản rõ.

• Nhận xét?

- Bản mã có cùng tần suất xuất hiện các chữ như trong bản gốc
- Dễ thám mã



Các hệ mật cổ điển

• MHV:

Cho m là số nguyên dương xác định. Cho $P = C = (Z_{26})^m$

k là tất cả hoán vị có thể có của $\{1, 2, \dots, m\}$:

Với khoá π , ta xác định:

$$e_{\pi}: (x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)})$$

$$d_{\pi^{-1}}: (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)}) = (x_1, \dots, x_m)$$

(Trong đó π^{-1} là hoán vị ngược của π)



Các hệ mật cổ điển

• Ví dụ 1:

- $m = 6$; khóa là phép hoán vị π sau:

1	2	3	4	5	6
3	5	1	6	4	2

- Khi đó phép HV ngược π^{-1} :

1	2	3	4	5	6
3	6	1	5	2	4

- Bản rõ: **asecondclasscarriageontherain**



Các hệ mật cổ điển

• Mã hóa:

- B1:** Nhóm bản rõ thành các nhóm 6 ký tự

asecon dclass carria geonth etrain

- B2:** Mỗi nhóm 6 ký tự sẽ được sắp xếp lại theo phép HV π (3, 5, 1, 6, 4, 2), ta có:

EOANCS LSDSAC RICARA OTGHNE RIENAT

- Khi đó ta có bản mã:

EOANCSLSDSACRICARAOTGHNERIENAT



Các hệ mật cổ điển

• Giải mã:

- B1:** Nhóm bản mã thành các nhóm 6 ký tự

EOANCS LSDSAC RICARA OTGHNE RIENAT

- B2:** Mỗi nhóm 6 ký tự sẽ được sắp xếp lại theo phép HV π^{-1} (3, 6, 1, 5, 2, 4), ta có:

asecon dclass carria geonth etrain

- Khi đó ta có bản rõ tương ứng:

asecondclasscarriageontherain



Các hệ mật cổ điển

Hệ mật tích:

- Ý tưởng: kết hợp các hệ mật bằng cách tạo tích của chúng.
- Xét các hệ mật có $C = P$ (các hệ mật loại này được gọi là tự đồng cấu)

Giả sử $S_1 = (P, P, K_1, E_1, D_1)$ và $S_2 = (P, P, K_2, E_2, D_2)$ là hai hệ mật tự đồng cấu có cùng không gian bản mã, rõ. Khi đó tích S_1 và S_2 (KH: $S_1 \times S_2$) được xác định là hệ mật $(P, P, K_1 \times K_2, E, D)$

Với khoá k = (k_1, k_2) trong đó $k_1 \in K_1, k_2 \in K_2$ ta xác định:

$$e_{(k_1, k_2)}(x) = e_{k_2}(e_{k_1}(x))$$

Và quy tắc giải mã:

$$d_{(k_1, k_2)}(x) = d_{k_2}(d_{k_1}(x))$$



Các hệ mật cổ điển

Thám mã một số hệ mật cổ điển:

- Nhận xét về các hệ mật thay thế đơn biểu:
 - Mỗi ký tự của bản rõ được ánh xạ đến một ký tự duy nhất của bản mã.
 - Các đặc trưng về ngôn ngữ, tần suất xuất hiện của các chữ trong bản rõ và chữ tương ứng trong bản mã là như nhau

⇒ Phương pháp thám mã bằng thống kê tần suất!



Các hệ mật cổ điển

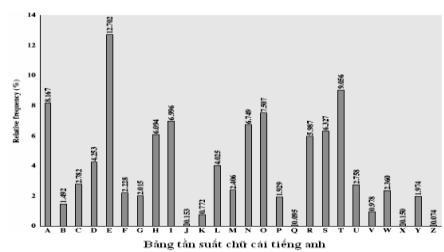
Phương pháp thám mã bằng thống kê tần suất:

- Ngôn ngữ có tính duy thừa
 - Ví dụ: tiếng Anh, chữ E được sử dụng nhiều nhất; sau đó đến các chữ T, R, N, I, O, A, S. Một số chữ rất ít dùng như: Z, J, K, Q, X
 - Các bộ chữ thường xuất hiện: th, nt, lrd, shll, ...
- Bằng phương pháp thống kê, ta có thể xây dựng các bảng các tần suất các chữ đơn, cặp hay bộ ba các chữ



Các hệ mật cổ điển

Bảng tần suất chữ cái tiếng Anh



Các hệ mật cổ điển

Ví dụ: Giả sử ta có bản mã

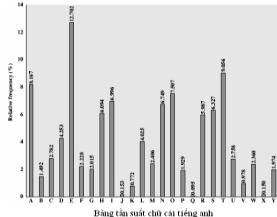
```
GWNB GRQB AGNBH WNDJD ORGGR ANBR OGWNJ ZFNIZ
WRRKR QGVNN ONLVD ORGHR LZOTE JGROR JARPO ANBKZ
ONDDG RANHN ZMNWZ LORGR OGWNH WBOHN RQWZD ORGBG
GBHFZ OTEIG ARGVN AROGW NOBHG GWBGP NWBKL BKNRJ
AURDZ GZROJ OBDBB ZIBEI
```

Thám mã Affine bằng phương pháp thống kê tần suất.



Các hệ mật cổ điển

Bước 1: xác định tần suất



Kí tự	Tần suất xuất hiện	Kí tự	Tần suất xuất hiện
G	22	I	5
N	21	K	4
R	21	L	4
B	16	Q	4
O	16	E	3
W	13	P	3
Z	11	F	2
A	9	T	2
D	9	M	1
H	7	U	1
J	6	V	1

 **Các hệ mật cổ điển**

- Bước 2:** Tách nhóm
 - Từ bảng tần suất, giả sử
 - G (6)** là mã hóa của **E (4)**
 - N (13)** là mã hóa của **T (19)**
 - Thiết lập hệ phương trình

$$\begin{cases} 4a + b = 6 \\ 19a + b = 13 \end{cases}$$
 - Giải hệ được $a = 23$, $b = -8 = 18$. Ta có hàm mã:
 $e_k(x) = 23x + 18 \bmod 26$
 - Hàm giải mã tương ứng:
 $d_k(y) = 17(y - 18) = (17y + 6) \bmod 26$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

 **Các hệ mật cổ điển**

- Bước 3:** Tìm bản rõ
 - Từ hàm giải mã, ta có bản rõ tương ứng:

aefps atwzp safpx ejfijj cyaat sfuht caefu vdfluv
 ettot waefl cflhj claxt lvng ractc rstdc sfpo
 cfija tafxf vifev lctat caefx epcxr twevj ctapa
 apxdv cngra apaef atcae fwpxa aepaz fepol poft
 aktiv avter cpjjp vupgu

- Nhận xét gì về bản rõ?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

 **Các hệ mật cổ điển**

- Quay lại bước 2**
 - Giả sử **G** là mã hóa của **T**
 - N** là mã hóa của **E**
 - Ta lại có hệ:

$$\begin{cases} 19a + b = 6 \\ 4a + b = 13 \end{cases}$$
 - Giải hệ được $a = 3$, $b = 1$. Ta có hàm mã:
 $e_k(x) = 3x + 1 \bmod 26$
 - Hàm giải mã tương ứng:
 $d_k(y) = 9(y - 1) = 9y + 17 \bmod 26$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

 **Các hệ mật cổ điển**

- Bước 3:** Bản rõ tương ứng



"The art of war teaches us to rely not on the likelihood of the enemy's not coming but on our own readiness to receive him not on the chance of his not attacking but rather on the fact that we have made our position unassailable"

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

 **Các hệ mật cổ điển**

- Ví dụ minh họa:**
 - Giả sử ta dùng hệ mật Hill với bản rõ: "**Friday**", bản mã tương ứng "**ZIQVSO**".
 - Hãy tìm ma trận khoá.
 - Giải:
 - Ta có FR (5; 17), ID (8;3), AY (0; 24)
 - ZI (25; 8) QV(16; 21); SO (18; 14)
 - PT: $\begin{pmatrix} 25 & 8 \\ 16 & 21 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} \cdot K$
 - $K = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 25 & 8 \\ 16 & 21 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \cdot \begin{pmatrix} 25 & 8 \\ 16 & 21 \end{pmatrix} = \begin{pmatrix} 7 & 15 \\ 4 & 19 \end{pmatrix}$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

 **Các hệ mật cổ điển**

- Thám mã hệ mã Vigerner: đọc thêm tài liệu [4, 1.2 chapter 1]

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 73

Bài 02. Các hệ mật KBM



Mục tiêu:

- Thực hiện làm thành thạo các bài tập minh họa phần lí thuyết về các hệ mật cổ điển học trong Bài 01

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 79

Bài tập áp dụng



Bài 1.

- Bản rõ P được mã bằng mã Affine với $k = (7, 11)$, đầu ra tiếp tục được mã bằng hệ mã Vigenere với từ khóa là **CIPHER** thu bản mã **BNNIECQDZSSGHG**. Hãy tìm P ban đầu

Bài 2.

- Giải mã bản mã **QQCD** thu được khi mã bản rõ bằng hệ mã Hill. Cho khóa $k = \begin{pmatrix} 5 & 8 \\ 12 & 7 \end{pmatrix}$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 80

Bài tập áp dụng



Bài 3.

- Ta có phương thức mã hoán vị như sau : Giả sử m , n là các số nguyên dương. Ta viết bản rõ theo từng hàng thành một ma trận $n \times m$. Sau đó tạo ra bản mã bằng cách lấy các cột của ma trận này. Cho $n = 3$, $m = 5$ em hãy mô tả cách giải mã bản mã "**WAT ORW REI DBN SUD**" thu được bằng phương pháp đã nêu ở trên

Bài 4.

- Hãy giải mã bản mã "**ZFFPXNZXXQ**" thu được từ mã Affine. Biết rằng "**P**" là mã hóa của "**y**", "**Z**" là mã hóa của "**s**".

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 81

CHƯƠNG 2. CÁC HỆ MẬT KBM



Nội dung các bài học trong chương 02

BÀI 01 + 02. CÁC HỆ MẬT CỔ ĐIỂN		BÀI 05. CÁC CHẾ ĐỘ HOẠT ĐỘNG MÃ KHỐI
BÀI 03 CÁC HỆ MẬT HIỆN ĐẠI		BÀI 06. MÃ DỘNG
BÀI 04. BÀI TẬP ÁP DỤNG		

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 82

Bài 03. Các hệ mật hiện đại

Mục tiêu bài học, SV trả lời được các câu hỏi sau



- Nguyên lí thiết kế mã khối?
- Thuật toán mã khối DES
 - Các bước thực hiện thuật toán DES
 - Vấn đề liên quan tới DES?
 - Biến thể của DES?
- Nắm vững cơ sở toán học của hệ mã AES, cấu trúc SPN, thuật toán AES

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 83

Mã khối



Nguyên lí thiết kế mã khối:

- Theo Shannon có 2 nguyên tắc cơ sở để độ bảo mật cao đó là việc tạo **tính xáo trộn** (confusion) và **tính khuếch tán** (diffusion)
- **Tính xáo trộn:** sự phụ thuộc vào bản mã đối với bản rõ phải thực sự phức tạp để gây rắc rối, cảm giác xáo trộn đối với kẻ thảm mã có ý định phân tích tìm quy luật để phá mã. Quan hệ của mã – tin là phi tuyến
- **Khuếch tán:** làm khuếch tán những mẫu văn bản mang đặc tính thống kê (gây ra do dư thừa ngôn ngữ) lẫn vào toàn bộ văn bản. Nhờ đó gây khó khăn cho kẻ phá hoại trong việc dò mã trên cơ sở thống kê các mẫu lặp lại cao. Sự thay đổi 1 bit trong 1 khối bản rõ phải dẫn tới sự thay đổi hoàn toàn trong khối mã tạo ra
- Một cách đơn giản, xáo trộn được thực hiện bằng phép thay thế, khuếch tán được thực hiện bằng phép đổi chỗ hay hoán vị

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 84

Mã khối

- Chuẩn mã dữ liệu DES
 - Giới thiệu về DES
 - Thuật toán DES
 - Double DES và Triple DES

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 85

Mã khối

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 hóa 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).

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

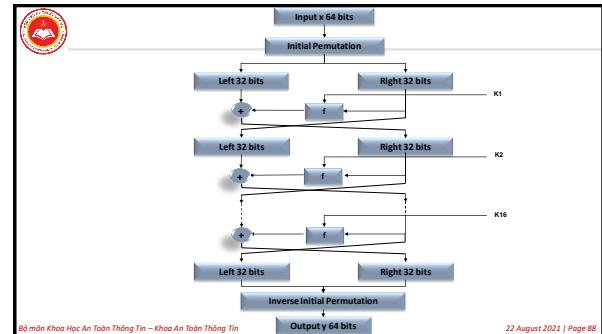
22 August 2021 | Page 85

Mã khối



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 87



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 85

Mã khối

Mô tả thuật toán:

Với bản rõ cho trước x
Tạo xâu x_0 theo hoán vị
cố định ban đầu IP.

Ta có: $x_0 = IP(x) = L_0 R_0$
Trong đó L_0 gồm 32 bit
đầu và R_0 là 32 bit cuối.

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})

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								
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								

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 89

Mã khối

Xâu bit A có độ dài 32 bit,
J độ dài 48 bit.

Input

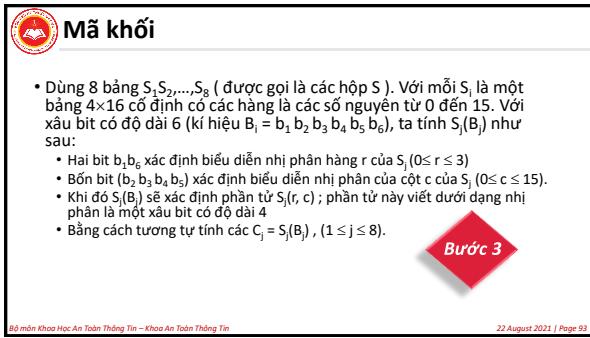
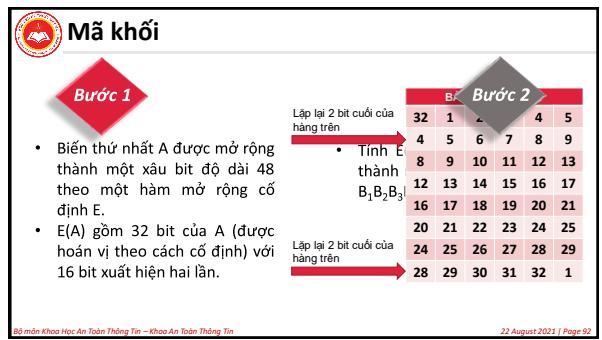
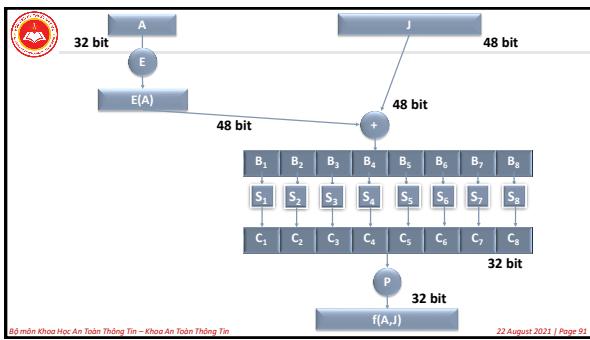
Hàm f

Output

Xâu bit độ dài 32 bit

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 90



Mã khối

Các hộp thế:

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

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 51

Mã khối

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

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 51

Mã khối

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

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 51

Mã khối

- 3 tính chất của S-box được NSA công bố
 - Các bit vào luôn phụ thuộc không tuyến tính vào các bit ra
 - Sửa đổi ở một bit vào làm thay đổi ít nhất là hai bit ra.
 - Khi một bit vào được giữ cố định và 5 bit con lại cho thay đổi thì S-boxes thể hiện một tính chất được gọi là 'phân bố đồng nhất' (uniform distribution): so sánh số lượng bit số 0 và 1 ở các đầu ra luôn ở mức cân bằng. Tính chất này khiến cho việc áp dụng phân tích theo lý thuyết thông kê để tìm cách phá S-boxes là vô ích.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 57

Mã khối

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

Bước 4

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

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 58

Mã khối

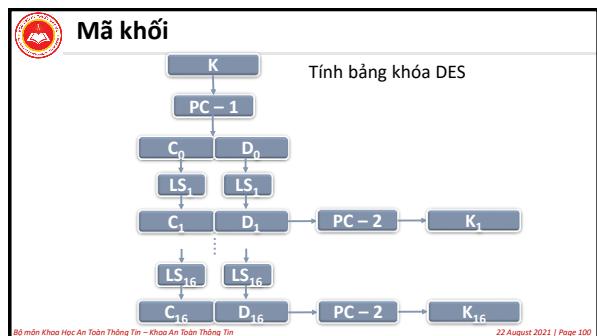
- Các bước tính bảng khóa DES:**
 - Với một khoá k 64 bit cho trước, ta loại bỏ các bit kiểm tra tính chẵn lẻ và hoán vị các bit còn lại của k theo phép hoán vị cố định PC-1. Ta viết: $PC-1(k) = C_0 D_0$
 - Với i thay đổi từ 1 đến 16:

$$C_i = LS_i(C_{i-1})$$

$$D_i = LS_i(D_{i-1})$$

- Dịch trái 1 bit tương ứng với các vòng 1, 2, 9, 16
- Dịch trái 2 bit tương ứng với các vòng 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 59



Mã khối

- 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		

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 101

Mã khối

- 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 bit đầu vào hoặc khoá sẽ kéo theo thay đổi một nửa số bit đầu ra. Do đó không thể đoán khoá được. Co thể nói rằng DES thể hiện tác động đồng loạt mạnh.
 - Tính chất bù:** Ký hiệu \bar{x} là bù của x theo từng bit, $E_k(x) = y \Leftrightarrow E_k(\bar{x}) = \bar{y}$
 - Khóa yếu:** DES có 4 khóa yếu
 - k được gọi là khóa yếu nếu $E_k(E_k(x)) = x; \forall x$
 - 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

Khóa yếu
1) 0101 0101 0101 0101
2) FEEF FEEF FEEF FEEF
3) 1F1F 1F1F 0E0E 0E0E
4) E0E0 E0E0 F1F1 F1F1

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 102

Mã khối

Tính chất của DES

- ...
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

Cặp khóa bán yếu	
1)	01FE 01FE 01FE 01FE FE01 FE01 FE01 FE01
2)	1FE0 0EF1 0EF1 0EF1 E01F E01F F10E F10E
3)	01E0 01E0 01F1 01F1 E001 E001 F101 F101
4)	1FFE 1FFE 0EFE 0EFE FE1F FE1F FE0E FE0E
5)	011F 011F 010E 010E 1F01 1E01 0E01 0E01
6)	EOF0 EOF0 F1FE F1FE FE00 FE00 FEF1 FEF1

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Mã khối

Các biến thể của DES

- DES bội hai

- Mã hóa:
 $C = DES_{K_2}[DES_{K_1}(M)]$
- Giải mã:
 $M = DES_{K_1}^{-1}[DES_{K_2}^{-1}(C)]$
- 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)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

DES bội ba

Mã hóa TDES với 2 khóa $C = DES_{K_1}\{DES_{K_2}^{-1}[DES_{K_1}(M)]\}$

Giải mã TDES với 2 khóa $M = DES_{K_1}^{-1}\{DES_{K_2}[DES_{K_1}^{-1}(C)]\}$

- Với TDES việc tìm khóa vét cạn yêu cầu khoảng: 2^{112} phép tính TDES, bởi vậy thực tế khó có thể thám mã thành công.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Mã khối

Thuật toán AES:

- Nguyên gốc:
 - Rõ ràng 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.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Mã khối

Yêu cầu của AES

- Là mã khối đối xứng khóa riêng.
- Kích thước khối dữ liệu 128 bit và độ dài khóa là tùy biến: 128, 192 hoặc 256 bit.
- Chuẩn mã mới phải mạnh và nhanh hơn Triple DES. Mã mới có cơ sở lý 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.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Mã khối

Cơ sở toán học của thuật toán 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: $c_i = a_i + b_i \text{ mod } 2, 1 \leq i \leq 8$.
 - 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: $(x^6 + x^5 + x^4 + x + 1) + (x^6 + x^3 + x^2 + x) = (x^5 + x^4 + x^3 + x^2 + 1)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 10

Mã khối

❖ **Phép nhân:** được thực hiện trên GF(2⁸) 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

$$a(x) = x^7 + x^6 + x + 1 \text{ và } b(x) = x^7 + x^6 + 1. \text{ Khi đó: } C = A \cdot B$$

$$c(x) = a(x) \cdot b(x) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$c(x) = x^7 + x^5 + x^3 + x^2 + x \text{ hay } C = AE_H = 10101110$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 109

Mã khối

❖ **Phép xtime()**

- Là phép nhân với x (hay là $(02)_H$)
- Giả sử $A(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0$
- Khi đó $x \cdot A(x)$

$$= a_7x^8 + a_6x^7 + a_5x^6 + a_4x^5 + a_3x^4 + a_2x^3 + a_1x^2 + a_0x \bmod m(x)$$

$$= \begin{cases} x \cdot A(x), & \text{nếu } a_7 = 0 \\ x \cdot A(x) - m(x), & \text{nếu } a_7 = 1 \\ & \text{dịch trái 1 bit, nếu } a_7 = 1 \\ & \text{dịch trái 1 bit rồi XOR với } (1B)_H, & \text{nếu } a_7 = 1 \end{cases}$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 110

Mã khối

❖ **Phép xtime()**

- VD: Tính $xtime(57)$
 - $(57)=0101\ 0111$
 - $a_7=0 \Rightarrow xtime(57)=1010\ 1110=(AE)$
- VD: Tính $xtime(92)$
 - $(92)=1001\ 0010$
 - $a_7=1 \Rightarrow xtime(92)=0010\ 0100 \oplus 0001\ 1011 = 0011\ 1111=(3F)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 111

Mã khối

❖ **Phép xtime()**

- $1=0000\ 0001=(01) \Rightarrow 1 \cdot x = ???$
- $x=0000\ 0010=(02) \Rightarrow x \cdot x = ???$
- $x^2=x \cdot x=xtime(x)=0000\ 0100 = (04) \Rightarrow x^2 \cdot x = ???$
- $x^3=x \cdot x^2=xtime(x^2)=0000\ 1000 = (08) \Rightarrow x^3 \cdot x = ???$
- $x^4=x \cdot x^3=xtime(x^3)=0001\ 0000 = (10) \Rightarrow x^4 \cdot x = ???$
- $x^5=x \cdot x^4=xtime(x^4)=0010\ 0000 = (20) \Rightarrow x^5 \cdot x = ???$
- ...
- \Rightarrow Đây là các lũy thừa của (02)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 112

Mã khối

❖ **Phép xtime()**

- VD: Tính $(57)\bullet(13)$
 - Phân tích (13) thành các lũy thừa của (02)
 - $Có (13)=0001\ 0011 = x^4 + x + 1 = (10) + (02) + (01)$
 - $\Rightarrow (57)\bullet(13) = (57)\bullet((01) \oplus (02) \oplus (10)) = (57)\bullet(01) \oplus (57)\bullet(02) \oplus (57)\bullet(10)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 113

Mã khối

❖ **Phép xtime()**

- VD: Tính $(57)\bullet(13)$
- $(57)=(0101\ 0111)$
- $(57)\bullet(02) = xtime(57) = (10101110) = (ae)$
- $(57)\bullet(04) = xtime(ae) = (01011100) \oplus (00011011) = (01000111) = (47)$
- $(57)\bullet(08) = xtime(47) = (10001110) = (8e)$
- $(57)\bullet(10) = xtime(8e) = (00011100) \oplus (00011011) = (07)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 114

Mã khối

- Phép xtime()
 - VD: Tính $(57) \bullet (13)$
 - $(57) = (0101\ 0111)$
 - $(57) \bullet (02) = xtime(57) = (10101110) = (ae)$
 - $(57) \bullet (04) = xtime(ae) = (01011100) \oplus (00011011) = (01000111) = (47)$
 - $(57) \bullet (08) = xtime(47) = (10001110) = (8e)$
 - $(57) \bullet (10) = xtime(8e) = (00011100) \oplus (00011011) = (0000\ 0111) = (07)$
 - Từ đó $(57) \bullet (13) = 57 \bullet ((01) \oplus (02) \oplus (10))$
 - $= (57) \oplus (57) \bullet (02) \oplus (57) \bullet (10) = (57) \oplus (ae) \oplus (07)$
 - $= (01010111) \oplus (10101110) \oplus (00000111) = (11111110) = (fe)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 115

Mã khối

- 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

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 115

Mã khối

- Có 10/12/14 vòng lặp tương ứng với kích thước khóa (128, 192 và 256 bit), trong đó mỗi vòng bao gồm
 - Phép thế byte (dùng một S box cho từng 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).

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 116

Mã khối

- SubBytes:
 - Là quá trình thay thế (phi tuyến) trong đó mỗi byte sẽ được thay thế bằng một byte khác theo bảng tra
 - Sử dụng một bảng 16×16 byte chứa vị trí 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.
 - Ví dụ:** Chẳng hạn $\{8d\}$ được thay bởi hàng 8, cột d, mà giá trị sẽ là $\{5d\}$.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 117

Mã khối

- Hộp thế S-Box được xây dựng dựa trên phép biến đổi phi tuyến: $y = Ax^{-1} + c$ (1)
- trên trường hữu hạn $GF(2^8)$.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad c = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

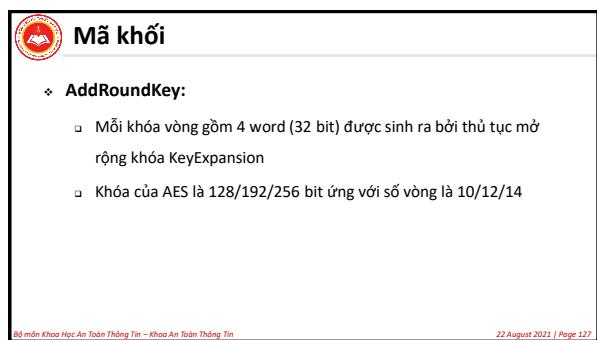
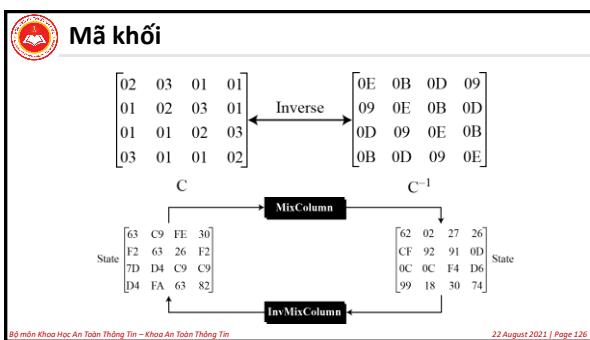
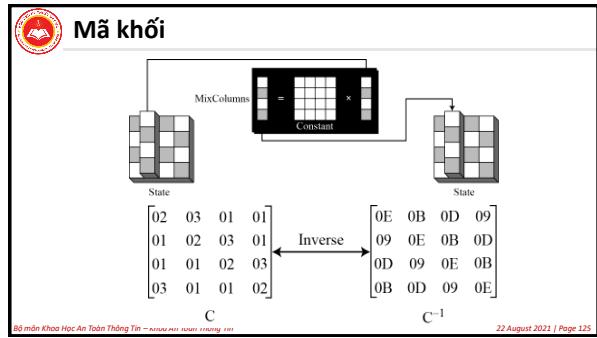
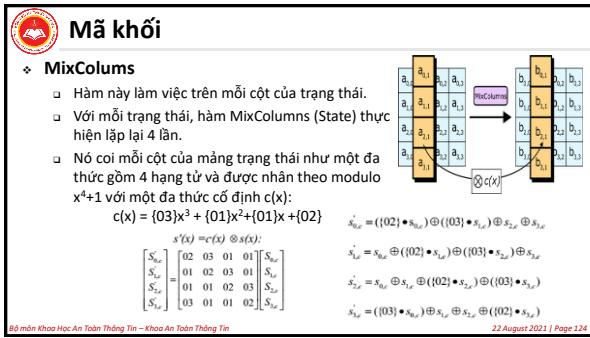
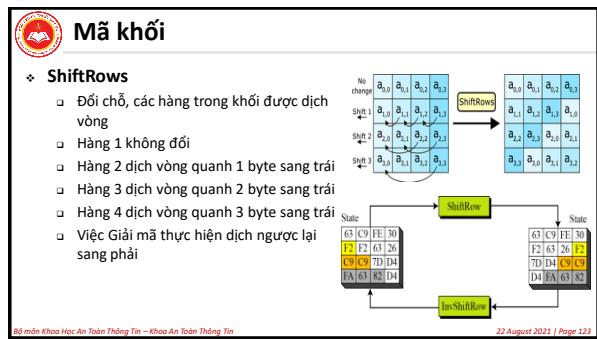
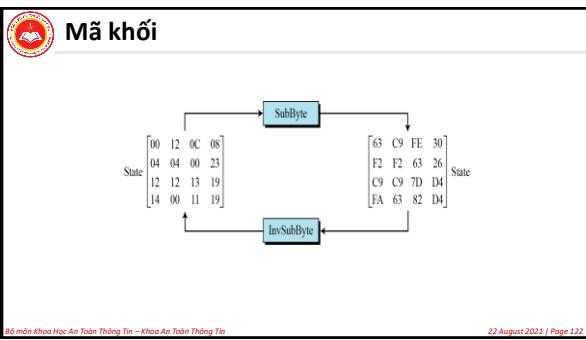
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 120

Mã khối

- Hộp thế S-Box
- Hộp thế ngược InvS-Box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	52	09	63	82	91	40	48	51	16	35	30	47	15	58	24
1	92	c9	37	79	12	60	05	09	46	54	18	55	21	42	76
2	33	93	25	16	39	77	04	34	57	11	72	36	31	15	64
3	03	96	73	49	92	94	53	62	01	45	48	14	39	17	27
4	93	59	42	79	94	08	03	24	76	52	29	47	12	56	94
5	00	80	92	41	58	39	17	06	43	35	30	49	10	38	57
6	92	00	57	19	81	95	48	03	65	67	12	15	39	17	73
7	99	19	04	11	70	54	71	51	22	10	93	91	04	92	05
8	99	37	79	61	62	01	49	99	05	07	12	15	39	17	73
9	99	57	37	95	06	24	99	05	07	12	15	39	17	73	05
10	99	79	12	10	14	04	99	05	07	12	15	39	17	73	05
11	99	99	37	79	61	62	01	49	99	05	07	12	15	39	05
12	99	99	57	37	95	06	24	99	05	07	12	15	39	17	73
13	99	99	79	12	10	14	04	99	05	07	12	15	39	17	73
14	99	99	99	37	79	61	62	01	49	99	05	07	12	15	05
15	99	99	99	57	37	95	06	24	99	05	07	12	15	39	17

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 121



Mã khối

- KeyExpansion (128 bit khóa và 10 vòng mã hóa)**
 - Khóa đầu vào là 128 bit (16 byte/4 word) mở rộng thành một mảng w gồm 44 word
 - 4 word đầu tiên là 4 word đầu vào
 - 40 word được mở rộng thêm để dùng cho 10 vòng mã hóa

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 128

Mã khối

- KeyExpansion (128 bit khóa và 10 vòng mã hóa)**

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 129

Mã khối

- KeyExpansion**
 - Cách mở rộng:
 - $w[i] = w[i - 1] \oplus w[i - 4]$, với $4 < i < 44$ và i không là bội của 4
 - Nếu i là bội của 4: $w[i] = g(w[i - 1]) \oplus w[i - 4]$
 - Trong đó g gồm các bước:
 - Dịch vòng trái một byte trên $w[i - 1]$: $\text{RotWord}(w[i - 1])$
 - Thay thế một byte dùng hộp S: $\text{SubWord}(\text{RotWord}(w[i - 1]))$
 - XOR với hàng số vòng $Rcon[j]$: $\text{SubWord}(\text{RotWord}(w[i - 1])) \oplus Rcon[j], j = i/4$

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 130

Mã khối

- KeyExpansion**
 - Cách mở rộng:
 - $Rcon[j] = (RC[j], 00, 00, 00)$, với $RC[1] = (01), RC[j] = (02) \cdot RC[j - 1]$, phép nhân ở đây được xác định trên $GF(2^8)$
 - = Giá trị của $RC[j]$ ở dạng hexa như sau

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 131

Mã khối

- Độ an toàn:**
 - Tính chất phức tạp của biểu thức S – box trên $GF(2^8)$ cùng với hiệu ứng khuếch tán giúp cho thuật toán không bị phân tích bằng phương pháp nội suy.
 - Rcon khác nhau hạn chế tính đối xứng
 - Tính chất phi tuyến cùng khả năng khuếch tán thông tin trong việc tạo bảng mã khóa mở rộng làm cho việc phân tích mật mã dựa vào các khóa tương đương hay các khóa có liên quan trở nên không khả thi.
 - Cấu trúc mã hóa giải mã khác nhau hạn chế được khóa yếu
 - Năm 2006, dạng tấn công lên AES duy nhất thành công là tấn công kénh bên.
 - Tháng 6 năm 2003, chính phủ Hoa Kỳ tuyên bố AES có thể được sử dụng cho thông tin mật.
 - Cấu trúc toán học của AES có mô tả khá đơn giản. Tuy nhiên nay chưa dẫn đến mối nguy hiểm nào những một số nhà khoa học sợ rằng điều này sẽ bị lợi dụng trong tương lai.

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 132

CHƯƠNG 2. CÁC HỆ MẬT KBM

Nội dung các bài học trong chương 02

BÀI 01 + 02. CÁC HỆ MẬT CỔ ĐIỂN	BÀI 05. CÁC CHẾ ĐỘ HOẠT ĐỘNG MÃ KHỐI
BÀI 03 CÁC HỆ MẬT HIỆN ĐẠI	BÀI 06. MÃ DỘNG
BÀI 04. BÀI TẬP ÁP DỤNG	

Bài môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
22 August 2021 | Page 133



Bài 04. Bài tập áp dụng

- ❖ SV tự thực hiện làm các bài tập để hiểu được quy trình thực hiện của thuật toán mã DES
- ❖ Tìm hiểu thuật toán DES qua mô đun thực hành về DES được giáo viên cung cấp.
- ❖ Hiểu rõ các bước sinh khóa, mã, giả mã DES được thực hiện như thế nào.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 134



Mã khối

- ❖ Ví dụ minh họa cách thực hiện 1 vòng của DES

- Với xâu x 64 bit:

1	0	0	0	0	1	0	1
1	0	0	1	1	0	1	0
0	0	1	0	1	0	0	0
1	1	0	1	1	1	1	1
0	1	1	0	1	1	0	0
0	0	0	1	0	0	1	0
0	0	0	0	0	1	0	0
0	0	1	0	1	0	0	0

- Với 48 bit khóa k_1 :

1	1	0	1	0	1
0	0	0	1	0	1
0	0	1	1	1	0
1	1	1	1	1	0
1	0	0	1	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	1	0	1	0	0

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 135



Mã khối

- ❖ Demo các bước thực hiện mã và giải mã, sinh khóa của thuật toán DES qua môđun thực hành DES

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 136



CHƯƠNG 2. CÁC HỆ MẬT KBM

Nội dung các bài học trong chương 02

BÀI 01 + 02. CÁC HỆ MẬT CỔ ĐIỂN



BÀI 05. CÁC CHẾ ĐỘ HOẠT ĐỘNG MÃ KHỐI



BÀI 03 CÁC HỆ MẬT HIỆN ĐẠI



BÀI 06. MÃ DỘNG



BÀI 04. BÀI TẬP ÁP DỤNG



22 August 2021 | Page 137



Bài 05. Các chế độ hoạt động của mã khối

Mục tiêu bài học, SV trả lời được các câu hỏi sau:

- ❖ SV nắm được một số chế độ hoạt động cơ bản của mã khối (ECB, CFB, CBC, OFB, CTR).

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 138



Các chế độ hoạt động của mã khối

- ❖ Có 4 chế độ làm việc đã được phát triển cho mã khối:
 - Chế độ quyền mã điện tử (ECB)
 - Chế độ liên kết khối mã (CBC)
 - Chế độ phản hồi mã (CFB)
 - Chế độ phản hồi đầu ra (OFB)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

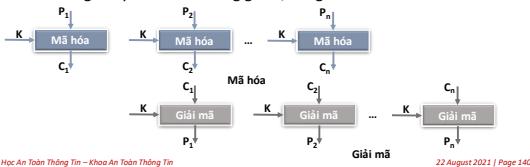
22 August 2021 | Page 139



Các chế độ hoạt động của mã khối

Chế độ quyền mã điện tử (ECB):

- Mẫu tin được chia thành các khối độc lập, sau đó mã từng khối
- Mỗi khối là giá trị cần thay thế như dùng sách mã, do đó có tên như vậy
- Mỗi khối được mã độc lập với các mã khác $C_i = E_K(P_i)$
- Khi dùng: truyền an toàn từng giá trị riêng lẻ



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 140



Các chế độ hoạt động của mã khối

Tính chất chế độ ECB:

- Các khối như nhau (dưới cùng một khóa) sẽ cho các khối mã giống nhau
- Sự phụ thuộc mộc xích: Các khối được mã hóa độc lập với các khối khác, việc sắp xếp lại thứ tự các khối mã cũng sẽ tương ứng với việc phải sắp xếp lại các khối rõ
- Tính lan sai: một hoặc nhiều bit sai trong một khối đơn lẻ chỉ ảnh hưởng tới chính việc giải mã khối đó
- Khả năng xử lý song song: Có thể xử lý các khối song song



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

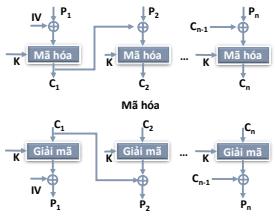
22 August 2021 | Page 141



Các chế độ hoạt động của mã khối

Chế độ liên kết khối mã (CBC)

- Các mẫu tin được chia thành các khối
- Nhưng chúng được liên kết với nhau trong quá trình mã hóa
- Các block được sáp thành dây, vì vậy có tên như vậy
- Sử dụng véc-tơ ban đầu IV để bắt đầu quá trình
 $C_1 = E_K(P_1 \text{ XOR } C_{-1}); C_1 = IV$
- Dùng khi: mã dữ liệu lớn, xác thực



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 140



Các chế độ hoạt động của mã khối

Tính chất chế độ CBC:

- Các bản rõ giống nhau: kết quả các khối mã sẽ như nhau khi cùng bản rõ được mã hóa dưới cùng một khóa và IV. Thay đổi IV, khóa hoặc khối rõ đầu tiên thì bản mã kết quả sẽ khác nhau
- Sự phụ thuộc mộc xích: cơ chế mộc xích làm cho bản mã y_j phụ thuộc vào x_i và toàn bộ các khối rõ trước đó. Hết quả là việc xắp xếp lại các khối mã sẽ là ảnh hưởng đến việc giải mã. Việc giải mã đúng một khối mã đòi hỏi phải giải mã đúng khối trước đó
- Tính lan sai: sai một bit trong khối mã c_j sẽ ảnh hưởng việc giải mã các khối y_j và y_{j+1} (từ chỗ y_j phụ thuộc vào y_j và y_{j+1}).
- Khắc phục sai: chế độ CBC là kiểu tự đồng bộ theo nghĩa nếu một số sô (bao gồm cả việc mất một hoặc nhiều hơn các khối đầu vào) xuất hiện trong khối y_j nhưng không có ở trong y_{j+1} và y_{j+2} thì sẽ được giải mã chính xác tới khôi x_{j+2}



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 141



Các chế độ hoạt động của mã khối

Chế độ phản hồi mã (CFB)

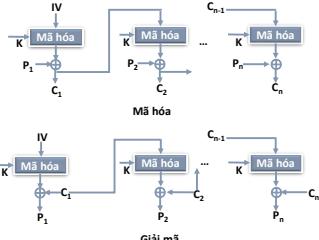
- Bản tin coi như dòng các bit
- Bổ sung vào đầu râu của mã khối
- Kết quả phản hồi trả lại cho giai đoạn tiếp theo, vì vậy có tên như vậy.
- Nói chung cho phép số bit phản hồi là 1, 8, 64, hoặc tùy ý: ký hiệu tương ứng là CFB1, CFB8, CFB64,...
- Thường hiệu quả sử dụng cả 64 bit $C_i = P_i \text{ XOR } E_K(C_{i-1}); C_{-1} = IV$
- Được dùng cho mã dữ liệu dòng, xác thực

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 140



Các chế độ hoạt động của mã khối



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 141



Các chế độ hoạt động của mã khối

Tính chất chế độ CFB:

- Các bản rõ giống nhau: cũng giống như chế độ CBC, sự thay đổi IV làm cho cùng một bản rõ đầu vào như nhau sẽ được mã hóa thành các bản mã khác nhau. Véc tơ IV không cần phải giữ bí mật (mặc dù trong ứng dụng thì cũng nên dùng IV khô đoán được để an toàn)
- **Sự phụ thuộc mộc xích:** tương tự như chế độ CBC, cơ chế mộc xích làm cho khối mã y_i phụ thuộc vào cả x_j và các khối rõ trước đó, hệ quả là việc thay đổi thứ tự của các khối mã sẽ ảnh hưởng tới việc giải mã.
- **Tính lan sai:** một hoặc nhiều hơn bit sai trong một khối mã đơn lẻ sẽ ảnh hưởng việc giải mã ngay tại đó và ảnh hưởng tới việc giải mã các khối tiếp theo. Thám mã đối phương cũng có thể dự đoán sự thay đổi bit trong x_j bằng cách thay đổi các bit tương ứng của y_j .
- **Khắc phục sai:** chế độ CFB là tự đồng bộ tương tự như CBC, nhưng đòi hỏi phải có các khối mã để khắc phục.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 146



Các chế độ hoạt động của mã khối

Chế độ phản hồi đầu ra (OFB)

- Mẫu tin xem như dòng bit
 - Đầu ra của mã được bổ sung cho mẫu tin
 - Đầu ra do đó là phản hồi, do đó có tên như vậy
 - Phản hồi ngược là độc lập đối với bản tin
 - Có thể được tính trước
- $$C_i = P_i \oplus O_i; O_i = E_K(O_{i-1});$$
- $$O_1 = IV$$

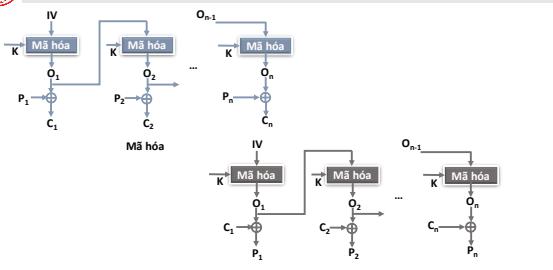
- Được dùng cho mã dòng trên các kênh âm thanh

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 147



Các chế độ hoạt động của mã khối



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 148



Các chế độ hoạt động của mã khối

Tính chất chế độ OFB:

- Các bản rõ giống nhau: cũng giống như CBC, CFB sự thay đổi IV làm cho 1 bản rõ đầu vào như nhau sẽ được mã hóa thành các bản mã khác nhau
- **Sự phụ thuộc mộc xích:** Dòng khóa là độc lập với bản rõ
- **Tính lan sai:** một hay nhiều hơn bit sai trong ký tự mã bắt kí c_i sẽ chỉ ảnh hưởng việc giải mã ngay tại kí tự đó, chính xác là ảnh hưởng tới vị trí bit sai làm cho bit bản rõ được giải ra sẽ là bit phần bù của bit rõ đúng.
- **Khắc phục sai:** chế độ OFB khắc phục các bit mã sai, nhưng không thể tự đồng bộ sau khi đã mất các bit mã, chúng làm lệch đi dòng khóa để giải mã

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 149



Các chế độ hoạt động của mã khối

Chế độ CRT:

- Một bộ đếm bằng với khối văn bản gốc
 - Mỗi khối nhận được 1 bộ đếm và 1 khóa để tạo khối đầu ra
 - Đầu ra được XOR với khối bản rõ tương ứng để tạo bản mã
- $$C_i = E_K(CTR_i) \oplus P_i$$
- $$P_i = E_K(CTR_i) \oplus C_i$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 150



Các chế độ hoạt động của mã khối

Đánh giá CTR:

- Hiệu quả cao:
 - Có thể thực hiện mã hóa (hoặc giải mã) song song
 - Có thể thực hiện giải thuật mã hóa trước nếu cần
- Có thể xử lý bất kí khối nào trước các khối khác
- An ninh không kém gì các phương thức khác
- Đơn giản, chỉ cần cài đặt giải thuật mã hóa, không cần đến giải thuật giải mã
- Không sử dụng lại cùng giá trị khóa và biến đếm (tương tự OFB)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 151

 **CHƯƠNG 2. CÁC HỆ MẬT KBM**
Nội dung các bài học trong chương 02

BÀI 01 + 02. CÁC HỆ MẬT CỔ ĐIỂN		BÀI 05. CÁC CHẾ ĐỘ HOẠT ĐỘNG MÃ KHỐI
BÀI 03 CÁC HỆ MẬT HIỆN ĐẠI		BÀI 06. MÃ DÒNG
BÀI 04. BÀI TẬP ÁP DỤNG		

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

 **Bài 06. Mã dòng**
Mục tiêu bài học, SV trả lời được các câu hỏi sau

- ❖ Ý tưởng cơ bản và vấn đề bảo mật của mã dòng?
- ❖ Các đặc trưng của mã dòng?
- ❖ Nguyên lí thiết kế mã dòng?
- ❖ Nắm được hệ mã dòng tiêu biểu RC4
- ❖ Ưu nhược điểm của hệ mật KBM

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

 **Mã dòng**

- ❖ **Khái niệm mã dòng:**
 - Ý tưởng cơ bản của mã dòng là sinh dòng khóa z_1, z_2, \dots, z_n theo một thuật toán nào đó và mã một dòng các đặc trưng rõ rệt theo cách $Y = y_1 y_2 \dots = e_{z_1}(x_1) e_{z_2}(x_2) \dots$ (1)
 - Việc sinh dòng khóa được thực hiện như sau:
 - Giả sử K là một khóa nào đó (thường là một dãy có l bit). Các hàm f_i được sử dụng để sinh ra dãy khóa z_i như sau:

$$z_1 = f_1(K)$$

$$z_i = f_i(K, x_1, \dots, x_{i-1}, y_{i-h}, \dots, y_i), i = 2, 3, \dots \quad (2)$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

 **Mã dòng**

- ❖ **Quá trình mã hóa:**
 - Tính z_1 , sau đó tính $y_1 = e_{z_1}(x_1)$
 - Tính z_2 , sau đó tính $y_2 = e_{z_2}(x_2)$
 - Cứ như vậy cho đến hết các bit rõ
- ❖ **Quá trình giải mã:**
 - Tính liên tiếp $z_1, x_1 = d_{z_1}(y_1), \dots$
 - Mã dòng gọi là đồng bộ nếu $z_i = f_i(K), \forall i = 1, 2, \dots$
 - Mã dòng được gọi là tự đồng bộ nếu $z_i = f_i(K, y_{i-h}, \dots, y_i), \forall i = h+1, h+2, \dots, s$
 - Mã dòng là tuần hoàn với chu kỳ d nếu $z_{i+d} = z_i, \forall i \geq h$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

 **Mã dòng**

- ❖ Thông thường (và phổ biến nhất) là dùng loại mã dòng có quy tắc mã hóa và giải mã như sau:

$$e_z(x) = x + z \bmod 2; \quad d_z(y) = y + z \bmod 2.$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

 **Mã dòng**

- ❖ **Các đặc trưng của mã dòng:**
 - Độ phức tạp tuyến tính
 - Độ phức tạp tuyến tính của một dãy nhị phân hữu hạn s^n , ký hiệu là $L(s^n)$, là độ dài của LFSR ngắn nhất sinh ra dãy s^n như n số hạng đầu của nó.
 - Độ phức tạp tuyến tính của một dãy nhị phân vô hạn s , ký hiệu là $L(s)$, được xác định như sau:
 - Nếu s là dãy zero ($s = 0, 0, \dots$) thì $L(s) = 0$;
 - Nếu không có LFSR nào sinh ra s , thì $L(s) = \infty$;
 - Ngược lại, $L(s)$ là độ dài của LFSR ngắn nhất sinh ra s .

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 154

Mã dòng

- Chu kỳ:**
 - Dãy $s = s_0, s_1, s_2 \dots$ là tuần hoàn bậc N nếu $s_i = s_{i+N}$ với mọi $i \geq 0$.
 - Chu kỳ của một dãy tuần hoàn là số nguyên dương nhỏ nhất N mà s là tuần hoàn bậc N.
- Tự tương quan:**
 - Trong dòng khóa gồm các biến ngẫu nhiên độc lập, đồng xác suất thì quan hệ giữa các phần tử bất kỳ là độc lập và do đó có hệ số tương quan bằng 0. Đây là một tính chất tốt của khóa.
 - Tuy nhiên, khi dòng khóa được tạo ra nhờ thuật toán xác định thì quan hệ giữa các phần tử bất kỳ là không độc lập vì vậy người ta mong muốn làm sao dòng khóa đạt được hệ số tương quan gần bằng 0

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 158

Mã dòng

- Lực lượng 1 loại dãy:**
 - Lực lượng của một loại dãy là số tất cả các dãy mà thuật toán xác định có thể sinh ra với tất cả các tham số khác nhau của nó.
- Các tính chất thống kê:**
 - Kiểm tra tần số đơn
 - Kiểm tra seri
 - Kiểm tra Poker
 - Kiểm tra loạt
 - Kiểm tra tự tương quan

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 159

Mã dòng

- Các nguyên lí thiết kế mã dòng:**
 - Thiết kế mật mã dòng dựa trên các LFSR.
 - Thiết kế mật mã dòng dựa trên mã khối;
 - Những mã dòng không thực tế
 - Thiết kế mật mã dòng dựa trên hàm hash.
- Cần lưu ý rằng, khi nói thiết kế mã dòng thì nội dung chủ yếu là nói về thiết kế thuật toán sinh dòng khóa.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 160

Mã dòng

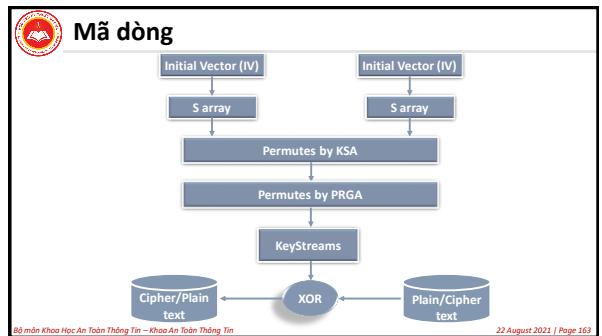
- Hệ mật RC4:**
 - RC4 được thiết kế bởi Ron Rivest của hãng bảo mật RSA Security vào năm 1987.
 - RC4 là mã dòng được sử dụng rộng rãi nhất và được dùng trong các giao thức như: SSL, TLS (để bảo vệ lưu lượng Internet) và WEP, WPA (để đảm bảo an toàn mạng không dây).
 - RC4 hỗ trợ kích cỡ khóa từ 40 tới 2048 bit, sau đó từ khóa này, tạo ra một dòng khóa để XOR với bản rõ.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 161

Mã dòng

- Thuật toán mã RC4:**
 - Mảng hoàn vị S gồm các số 0, ..., N - 1, với N = 256
 - Thuật toán Key Scheduling Algorithm (KSA): dùng 1 khóa mật như là 1 mầm khóa để tạo trạng thái giả ngẫu nhiên
 - Thuật toán Pseudo Random Generation Algorithm (PRGA): tạo dòng số giả ngẫu nhiên

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 22 August 2021 | Page 162



Mã dòng

Bước 1:

- Khởi tạo mảng S được sắp theo thứ tự tăng dần: $S[0] = 0, S[1] = 1, \dots, S[255] = 255$
- Khởi tạo 1 vecto tạm T
- Nếu độ dài khóa k là 256 bit thì k được chuyển sang T
- Nếu độ dài khóa k là l bit, phần tử đầu tiên được copy lần lượt sang T cho đến khi hết l bit, sau đó tiếp tục copy lặp lại k cho đến khi lấp đầy T

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 164

Mã dòng

Bước 2: Thuật toán KSA

Algorithm 1. A key scheduling algorithm (KSA)

Input: S // Before permutation
T // A temporary vector of secret key k as a seed
Output: Array S // After permutation

1. For i = 0 to 255 do
2. $S[i] = i$
3. End for
4. j = 0
5. For i = 0 to 255 do
6. $j = (j + S[i] + T[i]) \text{ mod } 256$
7. Swap ($S[i], S[j]$)
8. End for
9. Return (S)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 165

Mã dòng

Bước 3: Thuật toán PRGA

Algorithm 2. Pseudo-random generation algorithm (PRGA)

Input: S // State of array S
u // A temporary vector
Output: K // Sequence of keystreams

1. i = 0
2. j = 0
3. While not end of sequence do
4. $i = (i + 1) \text{ mod } 256$
5. $j = (j + S[i]) \text{ mod } 256$
6. Swap ($S[i], S[j]$)
7. $u = S[S[i] + S[j]] \text{ mod } 256$
8. $K = S[u]$
9. End while
10. Return (K)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 166

Mã dòng

Bước 4. Mã/giải mã:

- Khi luồng khóa cuối cùng đã được tạo, quá trình mã hóa và giải mã cũng giống nhau, chuỗi văn bản được XOR với luồng khóa được tạo. Nếu đầu vào là bản rõ thì sẽ tạo ra bản mã hóa và ngược lại nếu đầu vào là bản mã thì sẽ cho đầu ra là bản rõ

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 167

Ưu nhược điểm của các hệ mật khẩu bí mật

Ưu nhược điểm của các hệ mật khẩu bí mật:

Ưu điểm:

- Hệ mật KBM có khả năng cung cấp mức độ bảo mật khá cao, vừa có khả năng cho phép mã hóa và giải mã tin nhắn rất nhanh.
- Mức độ đơn giản về tương quan của các hệ mật KBM là một ưu điểm về mặt logic bởi nó sử dụng ít năng lượng tính toán hơn so với các hệ thống KCK.
- Thêm vào đó, cấp độ bảo mật mà mã hóa đối xứng mang lại có thể được nhân rộng lên một cách đơn giản chỉ bằng việc tăng độ dài của các khóa. Với mỗi bit được thêm vào trong độ dài 1 khóa đối xứng, thì độ khó của việc phá vỡ mã hóa đó bằng tấn công brute force sẽ tăng lên theo cấp số mũ.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 168

Ưu nhược điểm của các hệ mật khẩu bí mật

Nhược điểm:

- Vấn đề trong việc truyền tải các khóa dùng để mã hóa và giải mã dữ liệu. Nếu các khóa này được chia sẻ lên các kết nối không an toàn thì nguy cơ bị can thiệp bởi một bên thứ 3 là rất lớn.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

22 August 2021 | Page 169

