

Bài 8. Mã hóa

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

Mục tiêu của bài học

Giới thiệu



Nắm được lý thuyết về một số mô hình mã hóa thông tin.

Khái niệm, phân loại

Đánh giá được các phương pháp mã hóa khác nhau (mã hóa cổ điển, một số mã hóa theo tiêu chuẩn và hàm băm)

Mã hóa cổ điển

Một số mã hóa tiêu chuẩn

Sử dụng được một số thư viện mã hóa trong mã hóa (thư viện SSL, một số thư viện mã hóa trong trên C#, QT)

Hàm băm

Bài tập

Nội dung bài học

Giới thiệu



Khái niệm, phân loại mã hóa và một số thuật toán mã hóa cổ điển (60')

Một số thuật toán mã hóa tiêu chuẩn (45')

Hàm băm (30')

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

1. Khái niệm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Hệ thống mã hóa (cryptosystem) là một bộ năm thành phần (P, C, K, E, D) thỏa mãn các điều kiện sau:

1. Tập nguồn P là tập hữu hạn tất cả các bản tin nguồn cần mã hóa có thể có
2. Tập đích C là tập hữu hạn tất cả các bản tin có thể có sau khi mã hóa

1. Khái niệm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Hệ thống mã hóa (cryptosystem) là một bộ năm thành phần (P, C, K, E, D) thỏa mãn các điều kiện sau:

3. Tập khóa K là tập hữu hạn các khóa có thể được sử dụng

4. E, D là tập luật mã hóa và giải mã.

Với mỗi khóa $k \in K$ tồn tại:

- ✓ Luật mã hóa $e_k \in E$
- ✓ Luật giải mã tương ứng $d_k \in D$.
thỏa mãn: $d_k(e_k(x)) = x, \forall x \in P$.

2. Phân loại mã hóa

Giới thiệu

Khái niệm,
phân loại



Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Phân loại thông thường

- ✓ Mã hóa cổ điển (classical cryptography)
- ✓ Mã hóa đối xứng (symetric cryptography)
- ✓ Mã hóa bất đối xứng (asymetric cryptography)
- ✓ Hàm băm (hash function)

2. Phân loại mã hóa

Giới thiệu

Khái niệm,
phân loại



Phân loại theo tính chất của khóa

- ✓ Mã hóa khóa bí mật (private-key cryptography)
- ✓ Mã hóa khóa công khai (public-key cryptography)

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

3. Mã hóa cổ điển

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

3.1 Mã hóa dịch vòng

3.2 Mã hóa thay thế

3.3 Mã hóa Affine

3.4 Mã hóa Vigenere

3.5 Mã hóa Hill

3.6 Mã hóa hoán vị

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Định nghĩa:

Mã hóa dịch vòng là một bộ năm (P, C, K, E, D) thỏa mãn:

- $P = C = K = \mathbb{Z}_n$
- $E = \{e_k, k \in K\}$ trong đó: $e_k(x) = (x + k) \bmod n$ với $x \in \mathbb{Z}_n$
- $D = \{d_k, k \in K\}$ trong đó: $d_k(y) = (y - k) \bmod n$ với $y \in \mathbb{Z}_n$

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Ví dụ: Mã hóa và giải mã hóa đoạn text: $p = \text{"abcde"}$ với $k = 3$ bằng phương pháp mã hóa dịch vòng (p chỉ gồm các ký tự thường trong bảng chữ cái tiếng anh)

Bài toán 1: mã hóa

Input

- $p = \text{"abcde"}$
- $k = 3$
- $n = 26$

Output

- Xác định bản mã c

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: $a = 0, b = 1, \dots, z = 25$

Bước 1: đổi các ký tự trong p sang thứ tự của chúng trong bảng chữ cái.

a	b	c	d	e
0	1	2	3	4

Bước 2: tiến hành mã hóa bản rõ p với khóa $k = 3$

p	0	1	2	3	4
$(p + k) \bmod 26$	3	4	5	6	7

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: $a = 0, b = 1, \dots, z = 25$

Bước 3: xác định bản mã c

$(p + k) \bmod 26$	3	4	5	6	7
c	d	e	f	g	h

$c = \text{"defgh"}$

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Bài toán 2: Giải mã

Input

- $c = \text{"defgh"}$
- $k = 3$
- $n = 26$

Output

- Xác định bản rõ p

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: $a = 0, b = 1, \dots, z = 25$

Bước 1: đổi các ký tự trong c sang thứ tự của chúng trong bảng chữ cái.

d e f g h

Bước 2: tiến hành giải mã bản mã c với khóa $k = 3$

c 3 4 5 6 7

$(c - 3) \bmod 26$ 0 1 2 3 4

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Quy ước: Số thứ tự của các chữ cái trong bảng chữ cái tiếng anh như sau: $a = 0, b = 1, \dots, z = 25$

Bước 3: xác định bản rõ p

$(c - 3) \bmod 26$	0	1	2	3	4
p	a	b	c	d	e

$p = \text{"abcde"}$

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

■ Ví dụ: Tấn công bản mã sau:

jbcrc1qrwcrvnbjenbwrwn

■ Tấn công bằng cách lần lượt thử các khóa $k = 0, 1, 2, \dots, 25$

jbcrc1qrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlfklqlwlpvhdyhvqlqh
cuvkvej kpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine ← $k=9$

3.1 Mã hóa dịch vòng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

Ưu điểm:

- ✓ Thực hiện đơn giản
- ✓ Thời gian chạy thuật toán ngắn

Nhược điểm:

- ✓ Không gian khóa bé (Z_n)
- ✓ Dễ tấn công
 - Vết cặn
 - Thống kê ký tự

3.2 Mã hóa thay thế

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Định nghĩa:

Mã hóa thay thế là một bộ năm thành phần (P, C, K, E, D) thỏa mãn:

- $P = C = Z_n$
- K là tập tất cả các hoán vị của n phần tử $\{0, 1, 2, \dots, n-1\}$
Vậy mỗi khóa $\pi \in K$ là một hoán vị của n phần tử $\{0, 1, 2, \dots, n-1\}$
- $E = \{e_\pi, \pi \in K\}$ trong đó: $e_\pi(x) = \pi(x)$ với $x \in Z_n$
- $D = \{d_\pi, \pi \in K\}$ trong đó: $d_\pi(y) = \pi^{-1}(y)$ với $y \in Z_n$

3.2 Mã hóa thay thế

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Ví dụ: mã hóa

Input:

- $p = \text{"abcde"}$
- π được mô tả trên bảng

Output:

- xác định bản mã c

Xác định c

p	a	b	c	d	e
c	y	u	d	h	k

$c = \text{"yudhk"}$

a	y	n	w
b	u	o	z
c	d	p	t
d	h	q	q
e	k	r	v
f	e	s	x
g	m	t	c
h	i	u	o
i	l	v	r
j	j	w	b
k	f	x	s
l	p	y	g
m	n	z	a

3.2 Mã hóa thay thế

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Ví dụ: giải mã

Input:

- $c = \text{"yudhk"}$
- π^{-1} được mô tả trên bảng

Output:

- xác định bản rõ p

Xác định p

c	y	u	d	h	k
p	a	b	c	d	e

- $p = \text{"abcde"}$

y	a	w	n
u	b	z	o
d	c	t	p
h	d	q	q
k	e	v	r
e	f	x	s
m	g	c	t
i	h	o	u
l	i	r	v
j	j	b	w
f	k	s	x
p	l	g	y
n	m	a	z

3.2 Mã hóa thay thế

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

Ưu điểm:

- ✓ Thời gian thực hiện ngắn
- ✓ Không gian khóa là $n!$

Nhược điểm:

- ✓ Tấn công theo phương pháp thống kê

3.3 Mã hóa Affine

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Định nghĩa:

Mã hóa Affine là một bộ năm (P, C, K, E, D) thỏa mãn:

- $P = C = \mathbb{Z}_n$
- $K = \{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n\} : \gcd(a, n) = 1\}$
- $E = \{e_k, k \in K\}$ trong đó: $e_k(x) = (ax + b) \bmod n$ với $x \in \mathbb{Z}_n$
- $D = \{d_k, k \in K\}$ trong đó: $d_k(y) = (a^{-1}(y - b)) \bmod n$ với $y \in \mathbb{Z}_n$

3.3 Mã hóa Affine

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Ví dụ: Mã hóa

Input:

- $p = \text{"affinecipher"}$
- $k = (a, b) = (5, 8); n = 26$

Output:

- tính c

p	a	f	f	i	n	e	c	i	p	h	e	r
x	0	5	5	8	13	4	2	8	15	7	4	17
$(5x + 8) \bmod 26$	8	7	7	22	21	2	18	22	5	17	2	15
c	i	h	h	w	v	c	s	w	f	r	c	p

3.3 Mã hóa Affine

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Bài toán 2: Giải mã

Input:

- $c = \text{"ihhwvcswfrcp"}$
- $k = (a, b) = (5, 8)$; $n = 26$; tính được $a^{-1} = 21$

Output:

- tính p

c	i	h	h	w	v	c	s	w	f	r	c	p
y	8	7	7	22	21	2	18	22	5	17	2	15
$(21(y - 8)) \bmod 26$	0	5	5	8	13	4	2	8	15	7	4	17
p	a	f	f	i	n	e	c	i	p	h	e	r

3.3 Mã hóa Affine

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

- Ưu điểm:
 - ✓ Trường hợp riêng của thay thế
 - ✓ Tính toán đơn giản
- Nhược điểm
 - ✓ Số lượng khóa không lớn
 - ✓ Tấn công bằng phương pháp vét cạn
 - ✓ Tấn công bằng phương pháp thống kê ký tự

3.4 Mã hóa Vigenere

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Định nghĩa:

Mã hóa Vigenere là một bộ năm (P, C, K, E, D) thỏa mãn:

- Cho $m \in \mathbb{Z}^+$
- $P = C = (\mathbb{Z}_n)^m$
- $K = \{(k_0, k_1, \dots, k_{m-1}) \in (\mathbb{Z}_n)^m\}$
- $E = \{e_k, k \in K\}$ trong đó: $e_k(x_1, x_2, \dots, x_m) = ((x_0 + k_0) \bmod n, (x_1 + k_1) \bmod n, \dots, (x_{m-1} + k_{m-1}) \bmod n)$ với $(x_1, x_2, \dots, x_m) \in (\mathbb{Z}_n)^m$
- $D = \{d_k, k \in K\}$ trong đó: $d_k(y_1, y_2, \dots, y_m) = ((y_0 - k_0) \bmod n, (y_1 - k_1) \bmod n, \dots, (y_{m-1} - k_{m-1}) \bmod n)$ với $(y_1, y_2, \dots, y_m) \in (\mathbb{Z}_n)^m$

3.4 Mã hóa Vigenere

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

- Ưu điểm:
 - ✓ Thuật toán này là mở rộng thuật toán dịch vòng với khóa là bộ nhiều khóa dịch vòng
 - ✓ Thực hiện đơn giản
- Nhược điểm:
 - ✓ Có thể tấn công bằng phương pháp thống kê ký tự

3.5 Mã hóa Hill

Chọn số nguyên dương m . Định nghĩa:

$P = C = (\mathbb{Z}_n)^m$ và K là tập hợp các ma trận $m \times m$ khả nghịch

Với mỗi khóa $k = \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & \cdots & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \in K$, định nghĩa:

$$e_k(x) = xk = (x_1, x_2, \dots, x_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & \cdots & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \text{ với } x = (x_1, x_2, \dots, x_m) \in P$$

và $d_k(y) = yk^{-1}$ với $y \in C$.

Mọi phép toán số học đều được thực hiện trên \mathbb{Z}_n .

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

3.5 Mã hóa Hill

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

- Ưu điểm:
 - ✓ Thực hiện đơn giản với phép nhân ma trận
 - ✓ Không gian khóa là nm^2
- Nhược điểm:
 - ✓ Có thể tấn công bằng phương pháp thống kê ký tự

3.6 Mã hóa Hoán vị

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Định nghĩa:

Mã hóa Hoán vị là một bộ năm (P, C, K, E, D) thỏa mãn:

- $P = C = \mathbb{Z}_n$
- Cho $m \in \mathbb{Z}^+$
- K là tập hợp các hoán vị của m phần tử $(1, 2, \dots, m)$
- $E = \{e_\pi, \pi \in K\}$ trong đó: $e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$
- $D = \{d_\pi, \pi \in K\}$ trong đó: $d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}^{-1}, y_{\pi^{-1}(2)}^{-1}, \dots, y_{\pi^{-1}(m)}^{-1})$
- Với π^{-1} là hoán vị ngược của π

3.6 Mã hóa Hoán vị

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển



Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Nhận xét:

- Ưu điểm:
 - ✓ Thực hiện đơn giản
 - ✓ Không gian khóa là $n!$
- Nhược điểm:
 - ✓ Có thể tấn công bằng phương pháp thống kê ký tự

II. Một số mã hóa tiêu chuẩn

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

A. Một số mô hình mã hóa đối xứng (mã hóa mật)

4.1 DES (Data Encryption Standard)

4.2 AES (Advanced Encryption Standard)

B. Một số mô hình mã hóa bất đối xứng (mã hóa công khai)

4.3 RSA

4.4 ECC

A. Mô hình mã hóa đối xứng

Giới thiệu

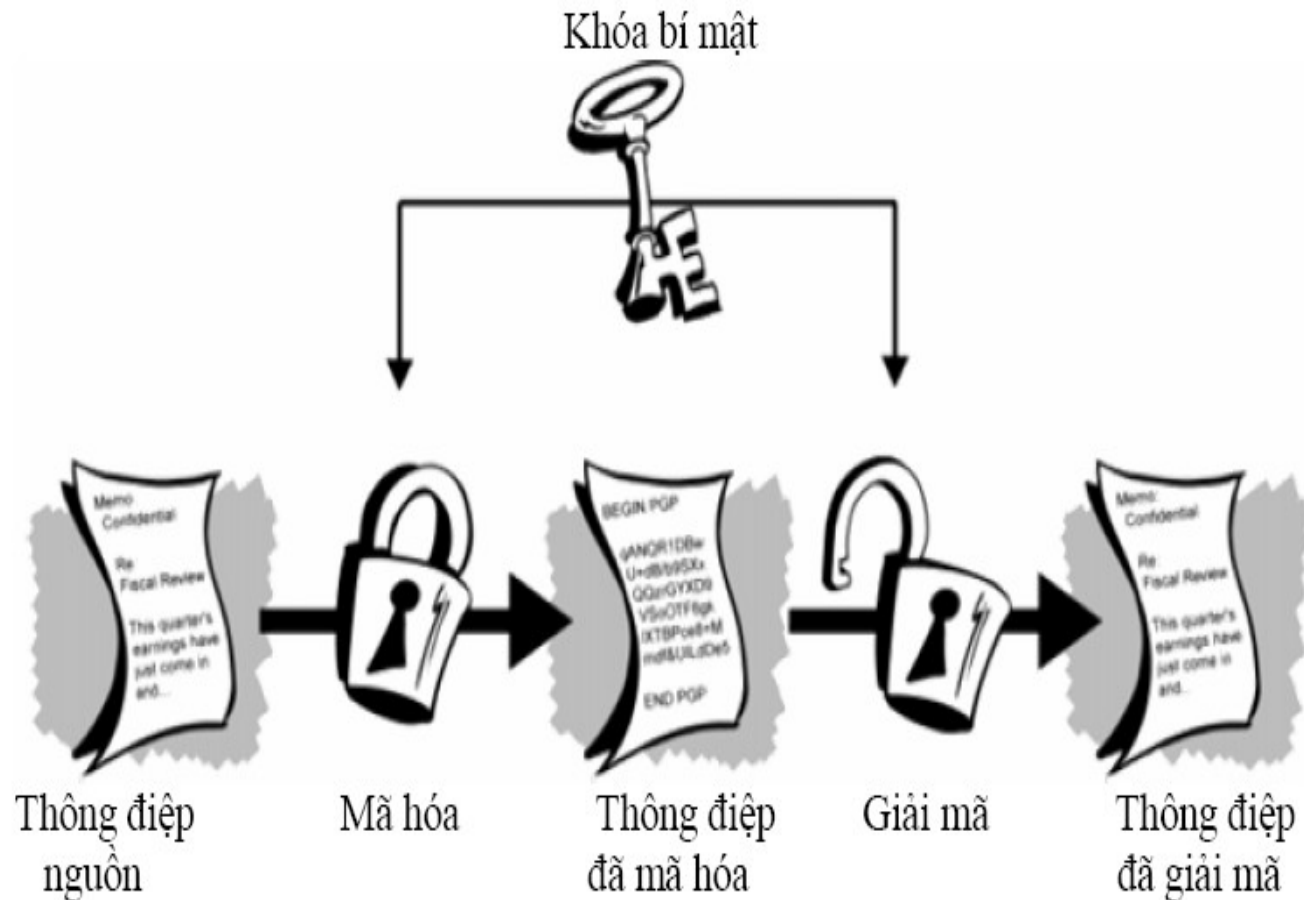
Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập



A. Mô hình mã hóa đối xứng

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

4.1 DES (Data Encryption Standard)

4.2 AES (Advanced Encryption Standard)

4.1 DES

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Input:

- ✓ Thông điệp nguồn $x \in P$ được biểu diễn bằng dãy 64 bit
- ✓ Khóa $k \in K$ được biểu diễn bằng dãy 56 bit

Output:

- ✓ Bản mã c có độ dài 64 bit

4.1 DES

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Đánh giá:

- Không thể tấn công bằng phương pháp thống kê
- Có thể tấn công bằng mạng máy tính gồm 100.000 máy tính. Thời gian tấn công là 24h
- Sử dụng tripple DES để tăng tính an toàn cho DES

4.2 AES

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Input:

- Đầu vào là một khối n bit
- Khóa k là một khối n bit

Output:

- Bản mã c là một khối n bit

4.2 AES

- Giới thiệu
- Khái niệm, phân loại
- Mã hóa cổ điển
- Một số mã hóa tiêu chuẩn
- Hàm băm
- Bài tập

Đánh giá:

- Thiết kế đơn giản, cài đặt dễ dàng
- Không thể tấn công bằng phương pháp vét cạn hoặc phương pháp thống kê
- Có thể xem là an toàn ở thời điểm hiện tại

B. Mô hình mã hóa bất đối xứng

Giới thiệu

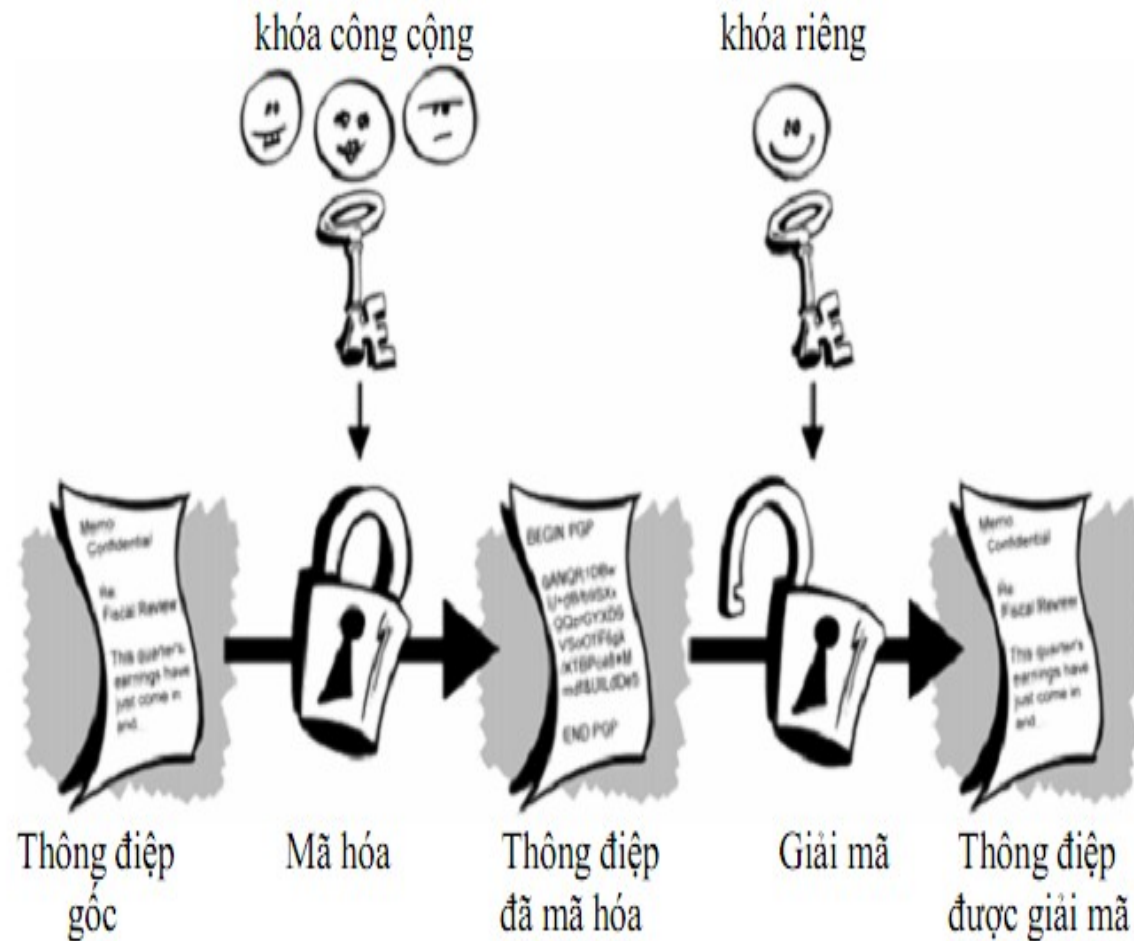
Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập



B. Mô hình mã hóa bất đối xứng

Giới thiệu

4.3 RSA

Khái niệm,
phân loại

4.4 ECC

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

4.3 RSA

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Định nghĩa:

Mã hóa RSA là một bộ năm (P, C, K, E, D) thỏa mãn:

$$P = C = Z_n$$

$$K = \{(n, p, q, a, b) : n = pq, \text{ với } p, q \text{ là các số nguyên tố, } \phi(n) = (p-1)(q-1), ab \equiv 1 \pmod{\phi(n)}\}$$

$$E = \{e_k, k \in K: e_k(x) = x^b \pmod{n} \text{ với } x \in Z_n\}$$

$$D = \{d_k, k \in K: d_k(y) = y^a \pmod{n} \text{ với } y \in Z_n\}$$

4.3 RSA

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Xác định khóa:

Phát sinh 2 số nguyên tố lớn p và q

Tính $n = pq$ và $\phi(n) = (p-1)(q-1)$

Chọn ngẫu nhiên số nguyên tố b ($1 < b < \phi(n)$) : $\gcd(b, \phi(n)) = 1$

Tính $a = b^{-1} \pmod{\phi(n)}$

Trong đó (n, b) được công bố và (p, q, a) được giữ bí mật

4.3 RSA

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Nhận xét:

- Ưu điểm:
 - Việc tấn công RSA là không thể thực hiện được với RSA 512 hoặc RSA 1024 bit.
 - An toàn hơn so với mã hóa khối
- Nhược điểm
 - Để đảm bảo tính an toàn của RSA thì $n = pq$ phải đủ lớn
 - Thời gian thực hiện lớn hơn so với mã hóa khối

4.4 ECC

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn



Hàm băm

Bài tập

Mã hóa dựa trên các đường cong elliptic

- Tìm được đường cong
- Tìm được nghiệm trên đường cong thỏa mãn số bậc của nghiệm lớn

So sánh RSA và ECC

Giới thiệu

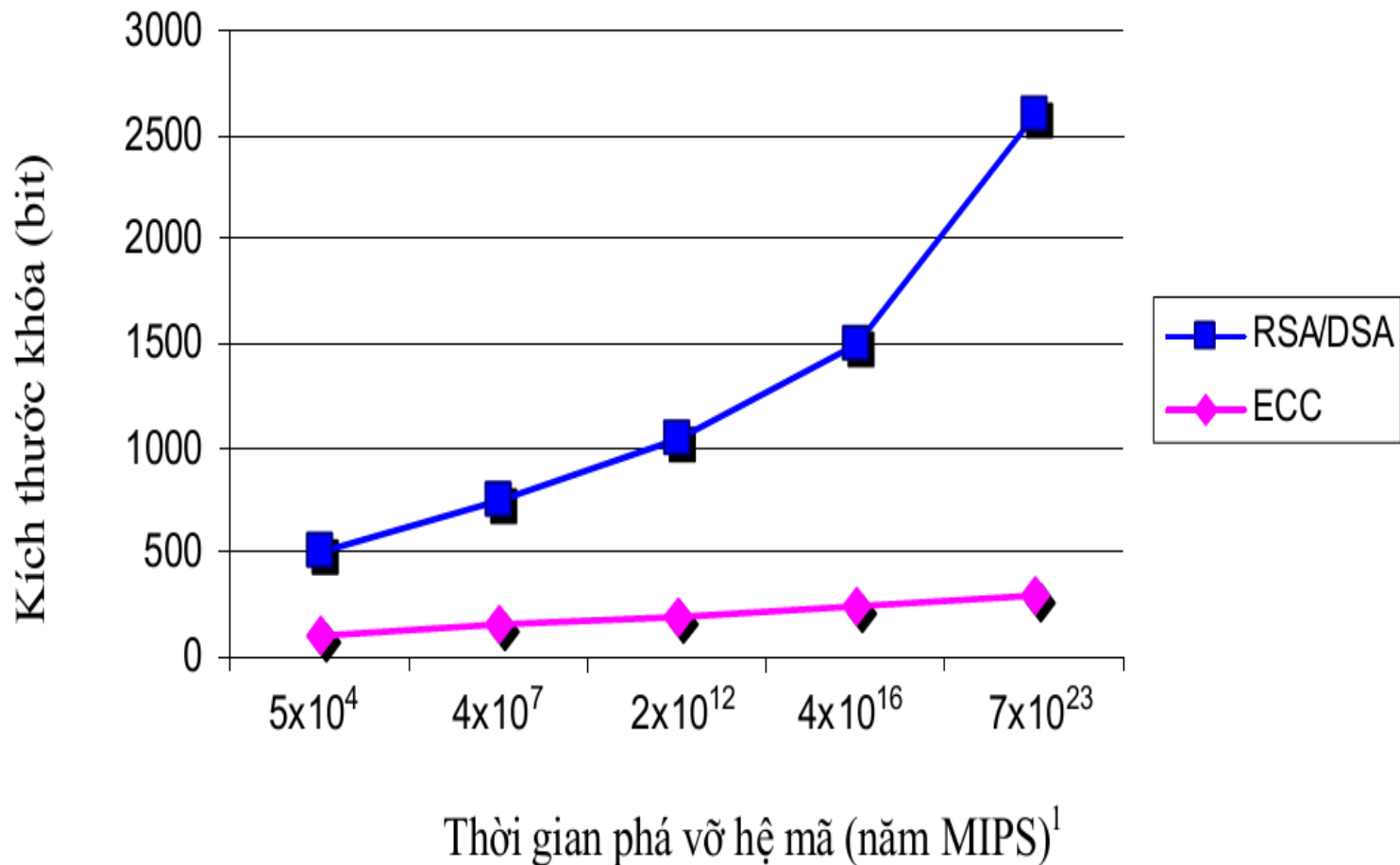
Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập



Hàm băm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm



Bài tập

Mục đích:

- ✓ Sử dụng để kiểm tra tính toàn vẹn cho dữ liệu
- ✓ Sử dụng để đại diện cho phần chữ ký
- ✓ Sử dụng lưu trữ thông tin kiểm chứng (mật khẩu, ...)

Hàm băm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

■ Hàm băm (hash function)

- **Hàm băm** là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán ***h*** một chiều nào đó, rồi đưa ra một bản băm – văn bản đại diện – có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.
- Giá trị của hàm băm là duy nhất, và **không thể suy ngược** lại được nội dung thông điệp từ giá trị băm này.

Hàm băm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

■ Đặc trưng:

- Hàm băm h là hàm một chiều (one-way hash) với các đặc tính:
 - Với thông điệp đầu vào x thu được bản băm $z = h(x)$ là duy nhất.
 - Nếu dữ liệu trong thông điệp x thay đổi để thành thông điệp x' thì $h(x') \neq h(x)$
=> Hai thông điệp hoàn toàn khác nhau thì giá trị hàm băm cũng khác nhau.
 - Nội dung của thông điệp gốc không thể bị suy ra từ giá trị hàm băm

Hàm băm

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

■ **Vai trò** hàm băm trong mật mã hiện đại:

- Được dùng để xác thực tính nguyên vẹn dữ liệu
- Được dùng trong quá trình tạo chữ kí số trong giao dịch điện tử.

■ Các hàm băm lấy một thông báo đầu vào và tạo một đầu ra được xem như là:

- Mã băm (hash code),
- Kết quả băm (hash result),
- Hoặc giá trị băm (hash value).

Hàm băm

Giới thiệu

Khái niệm,
phân loại

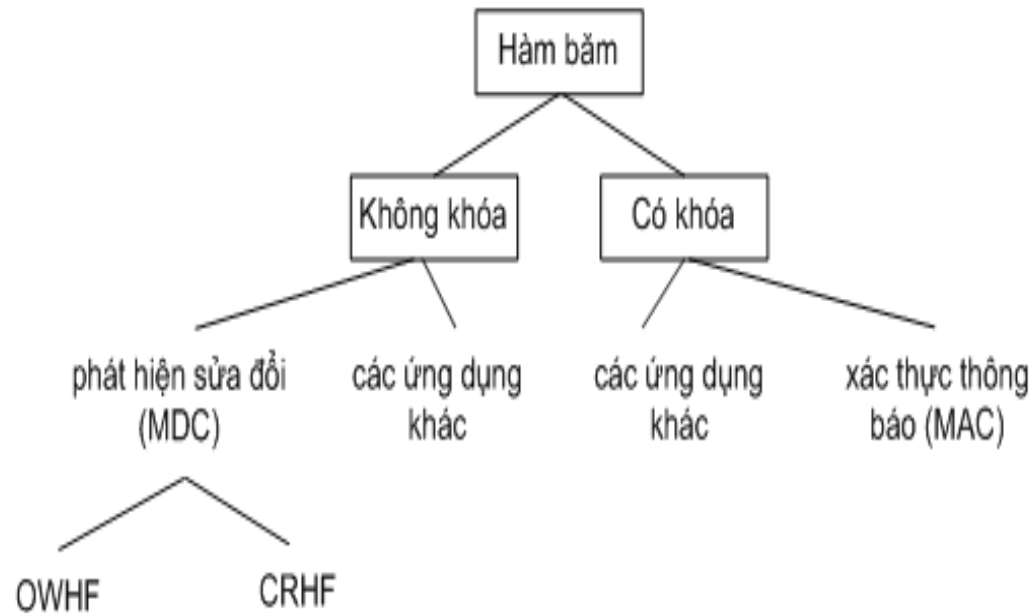
Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Phân loại



Phân loại các hàm băm mật mã và ứng dụng

Một số hàm băm phổ biến

Giới thiệu

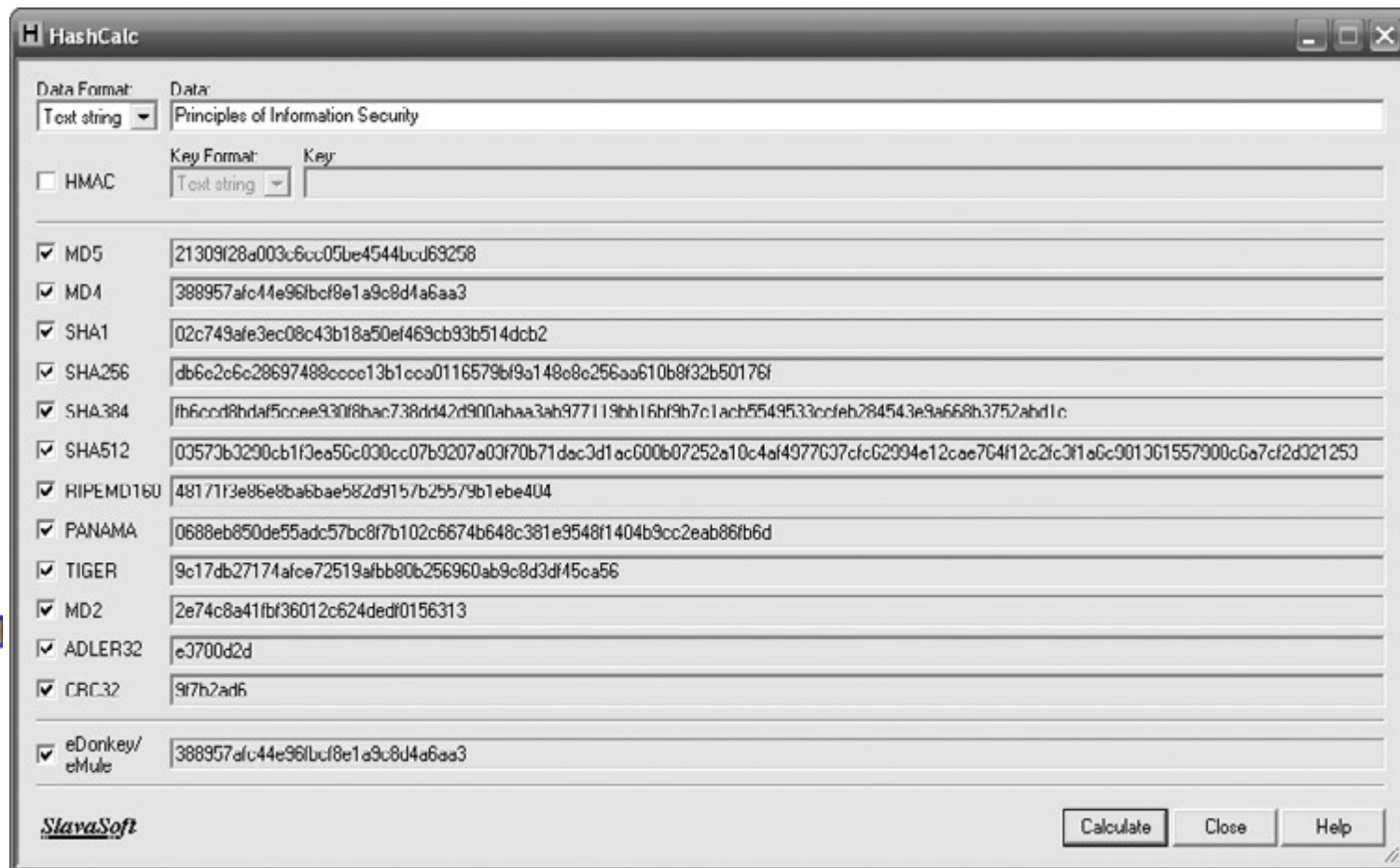
Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập



The screenshot shows the HashCalc application window. The 'Data Format' is set to 'Text string' and the 'Data' field contains 'Principles of Information Security'. The 'Key Format' is also 'Text string' and the 'Key' field is empty. The 'HMAC' checkbox is unchecked. A list of hash functions is shown with checkboxes and their corresponding hash values:

Hash Function	Hash Value
<input checked="" type="checkbox"/> MD5	21309f28a003c6cc05be4544bcd69258
<input checked="" type="checkbox"/> MD4	388957afc44e96/bcf8e1a9c8d4a6aa3
<input checked="" type="checkbox"/> SHA1	02c749afe3ec08c43b18a50ef469cb93b514dcb2
<input checked="" type="checkbox"/> SHA256	db6e2c6c28697488cccc13b1cca0116579bf9a148c8c256aa610b8f32b50176f
<input checked="" type="checkbox"/> SHA384	fb6cccd8bdaf5ccce930f8bac738dd42d900ahaa3ab977119bb16bf9b7c1acb5549533ccfeh284543e9a668b3752abd1c
<input checked="" type="checkbox"/> SHA512	03573b3290cb1f3ea56c030cc07b9207a03f70b71dac3d1ac600b07252a10c4af4977637cfc62994e12cae764f12c2fc3f1a6c901361557900c6a7cf2d321253
<input checked="" type="checkbox"/> RIPEMD160	48171f3e86e8ba6bae582d9157b25579b1ebe404
<input checked="" type="checkbox"/> PANAMA	0688eb850de55adc57bc8f7b102c6674b648c381e9548f1404b9cc2eab86fb6d
<input checked="" type="checkbox"/> TIGER	9c17db27174afce72519afbb80b256960ab9c8d3df45ca56
<input checked="" type="checkbox"/> MD2	2e74c8a41fbf36012c624dedf0156313
<input checked="" type="checkbox"/> ADLER32	e3700d2d
<input checked="" type="checkbox"/> CRC32	9f7b2ad6
<input checked="" type="checkbox"/> eDonkey/ eMule	388957afc44e96/bcf8e1a9c8d4a6aa3

At the bottom, there are buttons for 'Calculate', 'Close', and 'Help'. The 'SlavaSoft' logo is visible in the bottom left corner.

Bài tập

Giới thiệu

Khái niệm,
phân loại

Mã hóa cổ
điển

Một số mã
hóa tiêu
chuẩn

Hàm băm

Bài tập

Bài 1: Thực hiện mã hóa và giải mã thông điệp p = “hoc vien ky thuat quan su” với các thuật toán sau:

1. Mã hóa dịch vòng với $k = 12$
2. Mã hóa affine với $(a,b) = (17,20)$

Bài 2: thực hiện mã hóa và giải mã dãy số $\{11,2,2,323\}$ với $p=61$, $q=53$, $a=17$ và $b=2753$ theo thuật toán RSA

HỎI VÀ ĐÁP