

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

16 September 2021 | Page 1

NỘI DUNG

- 01. TỔNG QUAN VỀ MẬT MÃ HỌC**
Tổng quan về mật mã học
- 02. CÁC HỆ MẬT KHÓA BÍ MẬT**
Các hệ mật khóa bí mật
- 03. CÁC HỆ MẬT KHÓA CÔNG KHAI**
Các hệ mật khóa công khai
- 04. HÀM BẤM, XÁC THỰC VÀ CHỮ KÍ SỐ**
Hàm băm, toán ven và chữ kí số
- 05. 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

16 September 2021 | Page 2

CHƯƠNG 03
CÁC HỆ MẬT KHÓA CÔNG KHAI

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

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

16 September 2021 | Page 3

CHƯƠNG 3. CÁC HỆ MẬT KCK
Nội dung các bài học trong chương 03

BÀI 01 + 02. BỔ TÚC CƠ SỞ TOÁN HỌC CỦA LÝ THUYẾT MÃ		BÀI 04 + 05. GIỚI THIỆU MỘT SỐ HỆ MẬT KHÓA CÔNG KHAI	
BÀI 03. BÀI TẬP ÁP DỤNG		BÀI 06. BÀI TẬP ÁP DỤNG	

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

16 September 2021 | Page 4

Bài 01. Bổ túc cơ sở toán học

Mục tiêu bài học

- SV nắm được một số kiến thức cơ bản về lí thuyết số (số học modulo), cấu trúc đại số được ứng dụng trong mật mã cũng như một số thuật toán cơ bản liên quan đến tính nghịch đảo theo modulo, tính các kí hiệu Legendre và Jacobi.

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

16 September 2021 | Page 5

Bài 01. Bổ túc cơ sở toán học

- ❖ **Cấu trúc toán học**
- ❖ **Số học modulo**

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

16 September 2021 | Page 6

Một số kiến thức toán học

- Cấu trúc đại số:**
 - Định nghĩa nhóm:** Tập hợp G đó với phép toán $(.)$ đã cho được gọi là **nhóm**, nếu nó thỏa mãn các tính chất sau với mọi phần tử a, b, c thuộc G :

1. Tính kết hợp: $a.b.c = (a.b).c = a.(b.c)$
2. Có phần tử đơn vị e : $e.a = a.e = a$
3. Có nghịch đảo a^{-1} : $a.a^{-1} = a^{-1}.a = e$

Nếu có thêm tính giao hoán: $a.b = b.a$, thì gọi là **nhóm Aben** hay **nhóm giao hoán**.

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

16 September 2021 | Page 7

Một số kiến thức toán học

- Cấp của nhóm G chính là số phần tử của G**
- Cấp của phần tử a trong nhóm G chính là số nguyên dương nhỏ nhất m thỏa mãn: $a^m = e$, trong đó e là phần tử đơn vị của G**
- Kí hiệu cấp của nhóm G là $\text{ord}(G)$ hoặc $|G|$; cấp của phần tử a là $\text{ord}(a)$ hoặc $|a|$.**

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

16 September 2021 | Page 8

Một số kiến thức toán học

- Định nghĩa nhóm xyclic:**
 - G được gọi là **nhóm xyclic** nếu nó chứa một phần tử a sao cho mọi phần tử của G đều là lũy thừa nguyên nào đó của a
 - a được gọi là **phần tử sinh** (hay phần tử nguyên thuỷ của nhóm G)

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

16 September 2021 | Page 9

Một số kiến thức toán học

- Vành:** Cho một tập $R \neq \emptyset$ phép toán hai ngôi $(+, *)$ được gọi là 1 **vành** nếu:
 - Với phép cộng, R là nhóm Aben
 - Với phép nhân, có:
 - tính kết hợp: $a * b * c = a * (b * c) = (a * b) * c$
 - tính phân phối đối với phép cộng:
 - $a * (b + c) = a * b + a * c$
 - $(b + c) * a = b * a + c * a$
 - Nếu phép nhân có tính giao hoán thì tạo thành **vành giao hoán**.
 - Nếu phép nhân có nghịch đảo và không có thương 0 (tức là không có hai phần khác 0 mà tích của chúng lại bằng 0), thì nó tạo thành **miền nguyên**

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

16 September 2021 | Page 10

Một số kiến thức toán học

- Trường** là một tập hợp F với hai phép toán cộng và nhân, thỏa mãn tính chất sau:
 - F là một **vành**
 - Với phép nhân $F \setminus \{0\}$ là nhóm Aben.
- Có thể nói là có các phép toán cộng, trừ, nhân, chia số khác 0. Phép trừ được coi như là cộng với số đối của phép cộng và phép chia là nhân với số đối của phép nhân:
 - $a - b = a + (-b)$
 - $a / b = a \cdot b^{-1}$

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

16 September 2021 | Page 11

Một số kiến thức toán học

- Số học modulo**
 - Tính chia hết:** Chia số nguyên a cho n được thương là số nguyên q , $a = n.q$.
 - a chia hết cho n , n chia hết a hay a là bội số của n , n là ước số của a và ký hiệu là $n | a$
 - Cho 2 số nguyên a và n , $n > 1$. Thực hiện phép chia a cho n ta sẽ được 2 số nguyên q và r sao cho:

$$a = n.q + r, 0 \leq r < n$$
 - q được gọi là thương, ký hiệu là $a \text{ div } n$
 - r được gọi là số dư, ký hiệu là $a \text{ mod } n$
 - Định nghĩa quan hệ đồng dư trên tập số nguyên:** $a \equiv b \pmod{n}$ khi và chỉ khi a và b có phần dư như nhau khi chia cho n .

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

16 September 2021 | Page 12



Một số kiến thức toán học

▪ Ví dụ:

- $100 \bmod 11 = 1$;
- $34 \bmod 11 = 1$,
- $\Rightarrow 100 \equiv 34 \bmod 11$

▪ **Đại diện của $a \bmod n$:** Số b được gọi là đại diện của a theo mod n, nếu

- $a \equiv b \bmod n$ (hay $a = qn + b$) và $0 \leq b < n$.

- **Ví dụ:** $-12 \bmod 7 \equiv -5 \bmod 7 \equiv 2 \bmod 7 \equiv 9 \bmod 7$.
 $\Rightarrow 2$ là đại diện của $-12, -5, 2$ và 9 .



Một số kiến thức toán học

▪ Ví dụ:

- Trong Modulo 7 ta có các lớp tương đương viết trên các hàng như bảng bên
- Các phần tử cùng cột là có quan hệ đồng dư với nhau.
- Tập các đại diện của các số nguyên theo Modulo n gồm n phần tử ký hiệu như sau: $Z_n = \{ 0, 1, 2, 3, \dots, n-1 \}$.

...	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

Các phần tử trong cùng một hàng có cùng đồng dư với $3 \bmod 7$



Một số kiến thức toán học

▪ Ước số

- Số b không âm được gọi là ước số của a, nếu có số m sao cho: $a = m.b$ trong đó a, b, m đều nguyên (tức là a chia hết cho b).
- b là ước của a ta ký hiệu: $b|a$
- **Ví dụ:**
 - 1, 2, 3, 4, 6, 8, 12, 24 là các ước số của 24



Một số kiến thức toán học

▫ Các phép toán số học trên Modulo:

- Cho trước số n, thực hiện các phép toán theo modulo n như thế nào?

Thực hiện các phép toán trên các số nguyên như các phép cộng, nhân các số nguyên thông thường sau đó rút gọn lại bằng phép lấy Modulo



Hoặc có thể vừa tính toán, kết hợp với rút gọn tại bất cứ thời điểm nào



Một số kiến thức toán học

$$(a+b) \bmod n = [a \bmod n + b \bmod n] \bmod n \quad (*)$$

$$(a.b) \bmod n = [a \bmod n . b \bmod n] \bmod n \quad (**)$$

- Như vậy khi thực hiện các phép toán ta có thể thay các số bằng các số tương đương theo Modulo n đó hoặc đơn giản hơn có thể thực hiện các phép toán trên các đại diện của nó: $Z_n = \{ 0, 1, 2, 3, \dots, n-1 \}$.



Một số kiến thức toán học

- Z_n với các phép toán theo Modulo tạo thành ván giao hoán có đơn vị. Các tính chất kết hợp, giao hoán và nghịch đảo được suy ra từ các tính chất tương ứng của các số nguyên.

▫ Các chú ý về tính chất rút gọn:

- Nếu $(a+b) \equiv (a+c) \bmod n$, thì $b \equiv c \bmod n$
- Nhưng $(ab) \equiv (ac) \bmod n$, thì $b \equiv c \bmod n$ chỉ khi a là nguyên tố cùng nhau với n

- **Ví dụ:** Tính $(11*19 + 10^{17}) \bmod 7 = ?$

Một số kiến thức toán học

- Giải:**
 - Áp dụng các tính chất của modulo, ta có:

$$\begin{aligned} & (11 * 19 + 10^{17}) \bmod 7 \\ & = ((11 * 19) \bmod 7 + 10^{17} \bmod 7) \bmod 7 \\ & = ((11 \bmod 7 * 19 \bmod 7) \bmod 7 + (10 \bmod 7)^{17}) \bmod 7 \\ & = ((4 * 5) \bmod 7 + ((3^2)^2)^2 * 3 \bmod 7) \bmod 7 \\ & = (6 + (2^2)^2 * 3 \bmod 7) \bmod 7 \\ & = (6 + 4 * 3) \bmod 7 = 4 \end{aligned}$$
- Bài tập: Tính $11^{207} \bmod 13 = ?$**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 19

Một số kiến thức toán học

- Ước số chung của hai số nguyên a và b**
 - d được gọi là ước số chung của hai số nguyên a và b nếu $d|a$ và $d|b$.
- Ước số chung lớn nhất:**
 - Số nguyên d được gọi là ước số chung lớn nhất của a và b nếu $d > 0$, d là ước chung của a và b và mọi ước chung của a và b đều là ước số của d .
 - Ký hiệu $\text{gcd}(a,b)$ là ước số chung lớn nhất của a và b
 - Ví dụ: $\text{gcd}(12, 18) = 6$, $\text{gcd}(-18, 27) = 9$, $\text{gcd}(7,15) = 1$
 - Với mọi a ta có $\text{gcd}(a, 0) = a$
 - Ta cũng quy ước $\text{gcd}(0, 0) = 0$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 20

Một số kiến thức toán học

- Số nguyên tố:**
 - Số nguyên $a > 1$ được gọi là **số nguyên tố**, nếu a không có ước số nào khác ngoài 1 và chính a.
- Nguyên tố cùng nhau:**
 - Hai số a và b được gọi là **nguyên tố cùng nhau** nếu chúng không có ước chung nào khác 1, tức là $\text{gcd}(a,b)=1$.
 - Ví dụ:** $\text{gcd}(8,15) = 1$, tức là 8 và 15 là hai số nguyên tố cùng nhau

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 21

Một số kiến thức toán học

- Định lý:**
 - Nếu $b > 0$ và $b|a$ thì $\text{gcd}(a,b) = b$.
 - Nếu $a = b.q + r$ thì $\text{gcd}(a,b) = \text{gcd}(b,r)$
- Thuật toán Euclid tìm UCLN:**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 22

Một số kiến thức toán học

- Thuật toán Euclidean tìm GCD(a, b):**
 - $A=a$, $B=b$
 - while $B>0$
 - $R = A \bmod B$
 - $A = B$, $B = R$
 - Return A
- Tính GCD(1970, 1066)?**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 23

Một số kiến thức toán học

- Giải:**

$$\begin{aligned} 1970 &= 1 \times 1066 + 904 & \text{gcd}(1066, 904) \\ 1066 &= 1 \times 904 + 162 & \text{gcd}(904, 162) \\ 904 &= 5 \times 162 + 94 & \text{gcd}(162, 94) \\ 162 &= 1 \times 94 + 68 & \text{gcd}(94, 68) \\ 94 &= 1 \times 68 + 26 & \text{gcd}(68, 26) \\ 68 &= 2 \times 26 + 16 & \text{gcd}(26, 16) \\ 26 &= 1 \times 16 + 10 & \text{gcd}(16, 10) \\ 16 &= 1 \times 10 + 6 & \text{gcd}(10, 6) \\ 10 &= 1 \times 6 + 4 & \text{gcd}(6, 4) \\ 6 &= 1 \times 4 + 2 & \text{gcd}(4, 2) \\ 4 &= 2 \times 2 + 0 & \end{aligned}$$

$$\text{gcd}(1970, 1066) = 2$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 24



Một số kiến thức toán học

Thuật toán Euclidean mở rộng:

- Nếu $\text{gcd}(a,b) = d$ thì phương trình bất định $ax + by = d$ có nghiệm nguyên (x,y) và một nghiệm nguyên (x,y) như vậy có thể được tính bằng thuật toán Euclidean mở rộng.
- Điều cần và đủ để có nghịch đảo là $d = 1$ và khi đó x là nghịch đảo của $a \text{ mod } b$ và y là nghịch đảo của $b \text{ mod } a$.
- Ta mở rộng thuật toán Euclidean:
 - Tìm ước chung lớn nhất của a và b ,
 - Tính nghịch đảo trong trường hợp $\text{GCD}(a, b) = 1$.

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

16 September 2021 | Page 25



Một số kiến thức toán học

Thuật toán Euclidean mở rộng

Input: Hai số nguyên dương a, b ($a \geq b$)

Output: $d = \text{gcd}(a, b)$ và số nguyên x, y thỏa mãn $ax + by = d$

1. If $b = 0$ then $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$ and Return(d, x, y).
2. $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$
3. While $b > 0$ do
 - 3.1. $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$
 - 3.2. $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$
4. $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$
5. Return(d, x, y)

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

16 September 2021 | Page 25



Một số kiến thức toán học

Áp dụng thuật toán trên với các đầu vào:

- 1) $a = 1759$, $b = 550$
- 2) $a = 3458$, $b = 4864$

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

16 September 2021 | Page 26



Một số kiến thức toán học

▫ $a = 1759$, $b = 550$

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	1759	550	1	0	0	1
3	109	1	-3	550	109	0	1	1	-3
5	5	-5	16	109	5	1	-5	-3	16
21	4	106	-339	5	4	-5	106	16	-339
1	1	-111	335	4	1	106	-111	-339	355
4	0	550	-1759	1	0	-111	550	355	-1759

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

16 September 2021 | Page 26



Một số kiến thức toán học

Bài tập áp dụng:

- Tim các nghịch đảo sau (nếu có)
 - $127^{-1} \text{ mod } 319 = ?$
 - $254^{-1} \text{ mod } 1028 = ?$
 - $1031^{-1} \text{ mod } 3713 = ?$
 - $508^{-1} \text{ mod } 819 = ?$
 - $9773^{-1} \text{ mod } 7079 = ?$

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

16 September 2021 | Page 26



Một số kiến thức toán học

Các số nguyên tố

- Như chúng ta đã biết số nguyên tố là các số nguyên dương chỉ có ước số là 1 và chính nó. Chúng không thể được viết dưới dạng tích của các số khác.
- Các số nguyên tố là trung tâm của lý thuyết số. Số các số nguyên tố là vô hạn.

Số nguyên tố < 200

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179
181 191 193 197 199

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

16 September 2021 | Page 26

 **Một số kiến thức toán học**

- ❖ Một trong những bài toán cơ bản của số học là **phân tích ra thừa số nguyên tố**, tức là viết nó dưới dạng tích của các số nguyên tố.
- ❖ Lưu ý rằng phân tích là bài toán khó hơn rất nhiều so với bài toán nhân các số để nhận được tích.
- ❖ Người ta đã chứng minh được rằng: mọi số nguyên dương đều có phân tích **đơn nhất** thành tích các lũy thừa của các số nguyên tố.
- **Ví dụ:** $51 = 3 \times 17$; $3600 = 2^4 \times 3^2 \times 5^2$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

 **Một số kiến thức toán học**

- ❖ Ta có thể xác định ước chung lớn nhất bằng cách trong các phân tích ra thừa số của chúng, tìm các thừa số nguyên tố chung và lấy bậc lũy thừa nhỏ nhất trong hai phân tích của hai số đó.
- **Ví dụ:**
 - Ta có phân tích: $300 = 2^2 \times 3^1 \times 5^2$ và $18 = 2^1 \times 3^2$.
 - Vậy $\text{GCD}(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

 **Một số kiến thức toán học**

- ❖ **Định lý Fermat (Định lý Fermat nhỏ)**
- **$a^{p-1} \text{ mod } p = 1$** trong đó p là số nguyên tố và a là số nguyên bất kỳ khác bội của p : $\text{GCD}(a, p) = 1$.
 - Hay $\forall p$ và a không là bội của p , ta luôn có **$a^p \equiv a \pmod p$**
 - Công thức trên luôn đúng, nếu p là số nguyên tố, còn a là số nguyên dương nhỏ hơn p .
 - **Ví dụ?**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

 **Một số kiến thức toán học**

- ❖ **Ví dụ:**
 - Vì 5 và 7 là các số nguyên tố, 2 và 3 không là bội tương ứng của 7 và 5 , nên theo định lý Fermat ta có:
 - $2^{7-1} \pmod 7 = 1$ ($= 2^6 \pmod 7 = 64 \pmod 7 = 1$)
 - $3^{5-1} \pmod 5 = 1$ ($= 3^4 \pmod 5 = 81 \pmod 5 = 1$)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

 **Một số kiến thức toán học**

- ❖ **Hàm $\phi(n)$**
 - Tập $Z_n = \{0, 1, 2, \dots, n-1\}$ thường được gọi là **thặng dư đầy đủ theo mod n**.
 - Xét tập $Z_n^* = \{a \in Z_n : \text{gcd}(a, n) = 1\}$. Tập này được gọi là **tập các thặng dư thu gọn theo mod n**
 - Nếu p là số nguyên tố thì $Z_p^* = \{1, 2, \dots, p-1\}$
 - Kí hiệu $\phi(n)$ (hàm Euler) là số phần tử lớn hơn 0, nhỏ hơn n và nguyên tố cùng nhau với n

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

 **Một số kiến thức toán học**

- ❖ **Các tính chất của hàm $\phi(n)$:**
 - Dễ dàng thấy, nếu p là số nguyên tố $\Phi(p) = p-1$
 - Nếu $\text{gcd}(m, n) = 1$, thì: $\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$
 - Nếu $n = p_1^{e_1} \cdots p_k^{e_k}$ là phân tích ra thừa số nguyên tố của n thì:

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 31

Một số kiến thức toán học

Ví dụ:

- Tính $\phi(37)$; $\phi(25)$; $\phi(18)$; $\phi(21)$?

$\phi(37) = 37 - 1 = 36$
 $\phi(25) = \phi(5^2) = 20$
 $\phi(18) = \phi(2) \cdot \phi(9) = 1 \cdot \phi(3^2) = 6$
 $\phi(21) = \phi(3) \cdot \phi(7) = 2 \cdot 6 = 12$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 37

Một số kiến thức toán học

Định lý Ole: Định lý Ole là tổng quát hóa của Định lý Ferma

$a^{\Phi(n)} \bmod n = 1$

với mọi cặp số nguyên dương nguyên tố cùng nhau a và n : $\gcd(a,n)=1$.

Ví dụ:

- $a = 3; n = 10; \Phi(10)=4$; Vì vậy $3^4 = 81 = 1 \bmod 10$
- $a = 2; n = 11; \Phi(11)=10$; Do đó $2^{10} = 1024 = 1 \bmod 11$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 38

Một số kiến thức toán học

Định nghĩa:

- Nhóm nhân của Z_n là $Z_n^* = \{a \in Z_n \mid (a, n) = 1\}$
- Cấp của Z_n^* là số các phần tử trong Z_n^* . KH: $|Z_n^*| = \phi(n)$
- Theo định nghĩa hàm phi Euler ta có: $|Z_n^*| = \phi(n)$

Định lý Euler:

- Nếu $a \in Z_n^*$ thì $a^{\phi(n)} \equiv 1 \bmod n$
- Nếu n là tích các số nguyên khác nhau và nếu $r \equiv s \pmod{\phi(n)}$ thì $a^r \equiv a^s \pmod{n}; \forall a$

Định nghĩa cấp của phần tử:

- Cho $a \in Z_n^*$. Cấp a kí hiệu $\text{ord}(a)$ là số nguyên dương **nhỏ nhất** t sao cho: $a^t \equiv 1 \pmod{n} (t>0)$
- Lưu ý:** Cho $a \in Z_n^*$, $\text{ord}(a) = t$ và $a^s \equiv 1 \pmod{n}$ khi đó t là ước của s . Đặc biệt $t \mid \phi(n)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 39

Một số kiến thức toán học

Ví dụ:

- Tính cấp của các phần tử trong Z_{20}^* ?

- Ta có $n = 20 = 2^2 \cdot 5$; $\phi(20) = 8 = |Z_{20}^*|$
- $Z_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$a \in Z_{20}^*$	1	3	7	9	11	13	17	19
$\text{Ord}(a)$	1	4	4	2	2	4	4	2

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 40

Một số kiến thức toán học

Định nghĩa phần tử sinh:

- $\alpha \in Z_n^*$ được gọi là phần tử sinh của Z_n^* nếu: $Z_n^* = \{\alpha^i \pmod{n} \mid 0 \leq i \leq \phi(n)-1\}$
- Cho $\alpha \in Z_n^*$. Nếu cấp của $\alpha = \phi(n)$ thì α được gọi là phần tử sinh của Z_n^* (hay còn được gọi là phần tử nguyên thuỷ).
- Nếu Z_n^* có phần tử sinh thì Z_n^* được gọi là nhóm xylic
- Z_{20}^* có phần tử sinh không?

 - Z_{20}^* không có phần tử sinh vì $\phi(20) = |Z_{20}^*| = 8$ nhưng $\max(\text{ord}(a)) = 4 \neq 8$, với $a \in Z_{20}^*$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 41

Một số kiến thức toán học

1 Z_n^* có phần tử sinh nếu và chỉ nếu $n = 2, 4, p^k$ hoặc $2 \cdot p^k$. Trong đó p là số nguyên tố lẻ và $k \geq 1$.

2 Nếu α là một phần tử sinh của Z_n^* thì: $Z_n^* = \{\alpha^i \pmod{n} \mid 1 \leq i \leq \phi(n)-1\}$

Giả sử α là một phần tử sinh của Z_n^* . Khi đó: $b = \alpha^i \pmod{n}$ cũng là phần tử sinh của Z_n^* nếu và chỉ nếu $\gcd(i, \phi(n)) = 1$. Nếu Z_n^* là xylic thì số phần tử sinh là $\phi(\phi(n))$

3 $\alpha \in Z_n^*$ là phần tử sinh Z_n^* nếu và chỉ nếu $\alpha^{\frac{\phi(n)}{\text{lcm}(\phi(n), p)}} \not\equiv 1 \pmod{n}$ đối với mỗi nguyên tố p của $\phi(n)$

4 $\alpha \in Z_n^*$ là phần tử sinh Z_n^* nếu và chỉ nếu $\alpha^{\frac{\phi(n)}{\text{lcm}(\phi(n), p)}} \not\equiv 1 \pmod{n}$ đối với mỗi nguyên tố p của $\phi(n)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2022 | Page 42



Một số kiến thức toán học

❖ Ví dụ:

- (1) Z_{25}^* là nhóm cyclic và có phần tử sinh $\alpha = 2$. Tìm các phần tử sinh còn lại của Z_{25}^* .
- (2) Tìm phần tử sinh của Z_{37}^* . Từ phần tử sinh vừa tìm được tìm tất cả các phần tử sinh còn lại của Z_{37}^* .

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

16 September 2021 | Page 43



Một số kiến thức toán học

❖ Giải:

- (1) Tập các phần tử sinh của $Z_{25}^* = \{2, 3, 8, 12, 13, 17, 22, 23\}$
- (2)
 - Ta có $\phi(37) = 36$; $p - 1 = 36 = 2^2 \cdot 3^2$
 - Tìm phần tử sinh nhỏ nhất thoả mãn:

$$\begin{cases} x^{36/2} \bmod 37 \neq 1 \\ x^{36/3} \bmod 37 \neq 1 \end{cases}$$
 với $x \in Z_{37}^*$ (*)
 - Xét $x = 2$ thấy $2^{18} \bmod 37 = 36 \neq 1$ và $2^{12} \bmod 37 = 26 \neq 1$. Thoả mãn (*). Vậy 2 là phần tử sinh của Z_{37}^* .
 - Các giá trị i thoả mãn ($i, \phi(37)\right) = 1$ là $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$. Ta lần lượt tính các giá trị $2^i \bmod 37$ ta thu được tập các giá trị phần tử sinh của Z_{37}^* là $\{2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35\}$

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

16 September 2021 | Page 43



Một số kiến thức toán học

❖ BTVN:

- Tim tất cả các phần tử sinh của Z_{59}^*, Z_{41}^* .

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

16 September 2021 | Page 43



Một số kiến thức toán học

❖ Định lí phần dư Trung Hoa

n_1, \dots, n_k nguyên tố cùng nhau từng đôi một thì hệ sau có nghiệm duy nhất theo modulo $n = n_1 \dots n_k$

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

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

16 September 2021 | Page 43



Một số kiến thức toán học

❖ Giải hệ phương trình modulo:

- Cho:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$
- Với $\text{GCD}(n_i, n_j) = 1, \forall i \neq j$. Khi đó ta cũng áp dụng Định lý phần dư Trung Hoa để tìm x.
- Nghiệm x của hệ phương trình được tính như sau:

$$x = \left(\sum_{i=1}^k a_i N_i M_i \right) \pmod{N}$$
- Trong đó: $N = n_1 \dots n_k$, $N_i = N/n_i$, $M_i = N_i^{-1} \pmod{n_i}$.

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

16 September 2021 | Page 43



Một số kiến thức toán học

❖ Ví dụ giải hệ phương trình:

- $x \equiv 10 \pmod{11}$
- $x \equiv 19 \pmod{21}$
- $x \equiv 20 \pmod{26}$
- $x \equiv 7 \pmod{9}$
- $x \equiv 4 \pmod{10}$
- $x \equiv 15 \pmod{23}$

$$X \equiv 670 \pmod{6006}$$

$$X \equiv 1924 \pmod{2070}$$

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

16 September 2021 | Page 43



Một số kiến thức toán học

Định lý:

- Nếu $(n_1, n_2) = 1$ thì cấp phương trình đồng dư:

$$x \equiv a \pmod{n_1}$$

$$x \equiv a \pmod{n_2}$$

Có nghiệm duy nhất $x \equiv a \pmod{n_1 \cdot n_2}$



Một số kiến thức toán học

Định nghĩa thặng dư bậc hai và bất thặng dư bậc hai:

- Cho $a \in \mathbb{Z}_n^*$, a được gọi là thặng dư bậc hai theo modulo n (hay bình phương modulo n) nếu $\exists x \in \mathbb{Z}_n^*$: $x^2 \equiv a \pmod{n}$. Nếu không tồn tại x như vậy thì a được gọi là bất thặng dư bậc hai mod n.
- Tập tất cả các thặng dư bậc hai modulo n được KH: Q_n .
- Tập tất cả các bất thặng dư bậc hai modulo n được KH: \bar{Q}_n



Một số kiến thức toán học

Định lý:

- Cho p là nguyên tố lẻ và α là phần tử sinh của \mathbb{Z}_p^* . Khi đó a $\in \mathbb{Z}_p^*$ là một thặng dư bậc hai modulo p nếu và chỉ nếu $a = \alpha^i \pmod{p}$ với i là số nguyên chẵn

$$\text{Hệ quả: } |Q_p| = \frac{(p-1)}{2}; |\bar{Q}_p| = \frac{(p-1)}{2}$$

Ví dụ:

- Cho $\alpha = 3$ là phần tử sinh của \mathbb{Z}_{17}^* .
- Tìm Q_{17}, \bar{Q}_{17}



Một số kiến thức toán học

Định lý:

- Cho $n = p \cdot q$, với p, q là hai số nguyên tố, $p \neq q$. Khi đó a $\in \mathbb{Z}_n^*$ là thặng dư bậc hai theo modulo n nếu và chỉ nếu $a \in Q_p$ và $a \in Q_q$.

Hệ quả:

$$|Q_n| = \frac{(p-1)(q-1)}{4}; |\bar{Q}_p| = \frac{3(p-1)(q-1)}{4}$$



Một số kiến thức toán học

Định nghĩa căn bậc hai của một số modulo n:

- Cho $a \in Q_n$. Nếu $x \in \mathbb{Z}_n^*$, thỏa mãn $x^2 = a \pmod{n}$ thì x được gọi là căn bậc hai của a mod n.

Định lý về số căn bậc hai của một số modulo n:

- Cho $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_k^{e_k}$, trong đó p_i là các số nguyên tố lẻ phân biệt và $e_i \geq 1$. Nếu $a \in Q_n$ thì có đúng 2^k căn bậc hai khác nhau theo modulo n

Ví dụ: Tìm các căn bậc hai của $4 \pmod{15}$?

- Căn bậc hai của $4 \pmod{15}$ là: 2, 13, 7, 8
- Căn bậc hai của $4 \pmod{15}$ là: 1, 14, 4, 11



Một số kiến thức toán học

Ký hiệu Legendre và Jacobi:

- Định nghĩa: p là số nguyên tố lẻ, a là số nguyên. KH Legendre $\left(\frac{a}{p}\right)$ được xác định như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & a \in Q_p \\ -1 & a \in \bar{Q}_p \end{cases}$$

- Các tính chất ký hiệu Legendre: SGK (T112)

 **Một số kiến thức toán học**

❖ **Định nghĩa:**

- Cho $n \geq 3$ là các số nguyên lẻ có phân tích:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Khi đó KH Jacobi $\left(\frac{a}{n}\right)$ được định nghĩa là:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

Ta thấy rằng nếu n là số nguyên tố thì KH Jacobi chính là kí hiệu Legendre.

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

16 September 2022 | Page 55

 **1** Nếu n là số nguyên lẻ và $m_1 \equiv m_2 \pmod{n}$ thì: $\left(\frac{m_1}{n}\right) \equiv \left(\frac{m_2}{n}\right)$

2 Nếu n là số nguyên lẻ thì: $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{nếu } n \equiv \pm 1 \pmod{8} \\ -1 & \text{nếu } n \equiv \pm 3 \pmod{8} \end{cases}$

3 Nếu n là số nguyên lẻ thì: $\left(\frac{m_1 \cdot m_2}{n}\right) \equiv \left(\frac{m_1}{n}\right) \left(\frac{m_2}{n}\right)$
Đặc biệt nếu $m = 2^k \cdot t$ (t là số lẻ) thì: $\left(\frac{m}{n}\right) \equiv \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right)$

4 Giả sử m và n là $\left(\frac{m}{n}\right)$ số nguyên lẻ thì $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{nếu } m, n \equiv 3 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{khác} \end{cases}$

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

16 September 2022 | Page 56

 **Một số kiến thức toán học**

❖ **Bài tập áp dụng:**

- Tính kí hiệu Jacobi:
 - A) $\left(\frac{7411}{9283}\right)$
 - B) $\left(\frac{6278}{9975}\right)$

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

16 September 2022 | Page 57

 **Một số kiến thức toán học**

❖ **Giải:**

- A) $\left(\frac{7411}{9283}\right)^{(4)} = -\left(\frac{9283}{7411}\right)^{(1)} = -\left(\frac{1872}{7411}\right)^{(3)} = -\left(\frac{2}{7411}\right)^4 \cdot \left(\frac{117}{7411}\right)$
 $\stackrel{(2)}{=} -(1)^4 \cdot \left(\frac{117}{7411}\right)^{(4)} = -\left(\frac{7411}{117}\right)^{(1)} = -\left(\frac{40}{117}\right)^{(3)} = -\left(\frac{2}{117}\right)^3 \cdot \left(\frac{5}{117}\right)$
 $= -(-1)^3 \cdot \left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1$

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

16 September 2022 | Page 58

 **Một số kiến thức toán học**

❖ B) Ta có: $\left(\frac{a}{m \cdot n}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$

$$\Rightarrow \left(\frac{6278}{9975}\right) = \left(\frac{6278}{3}\right) \cdot \left(\frac{6278}{5}\right)^2 \cdot \left(\frac{6278}{7}\right) \cdot \left(\frac{6278}{19}\right)$$

$$= \left(\frac{2}{3}\right) \cdot \left(\frac{3}{5}\right)^2 \cdot \left(\frac{6}{7}\right) \cdot \left(\frac{8}{19}\right)^2 = -(1) \cdot \left(\frac{5}{3}\right)^2 \cdot \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{2}{19}\right)^3$$

$$= -(1)$$

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

16 September 2022 | Page 59

 **Bài 02. Một số kiến thức toán học**

❖ **Số nguyên Blum:**

- Là một hợp số có dạng $n = p \cdot q$ trong đó p, q là các số nguyên tố khác nhau thỏa mãn: $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$.

❖ **Định lý:**

- Cho $n = p \cdot q$ là một số nguyên Blum và cho $a \in Q_n$. Khi đó a có đúng 4 căn bậc hai modulo và chỉ có một số nằm trong Q_n .

❖ **Căn bậc hai chính:**

- n là số nguyên Blum và $a \in Q_n$. Căn bậc hai duy nhất của a nằm trong Q_n được gọi là căn bậc hai chính của $a \pmod{n}$

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

16 September 2022 | Page 60

Một số kiến thức toán học

- Ví dụ: $n = 21$; $Q_{21} = \{1, 4, 16\}$**
- 4 căn bậc hai của $4 \bmod 21$ là: 2; 5; 16; 19. Trong đó $16 \in Q_{21}$. Do vậy 16 là căn bậc hai chính của $4 \bmod 21$
- 4 căn bậc hai của $1 \bmod 21$ là: 1; 8; 13; 20. Trong đó $1 \in Q_{21}$. Do vậy 1 là căn bậc hai chính của $1 \bmod 21$
- 4 căn bậc hai của $16 \bmod 21$ là: 4; 10; 11; 17. Trong đó $4 \in Q_{21}$. Do vậy 4 là căn bậc hai chính của $16 \bmod 21$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 61

Một số kiến thức toán học

- Một số thuật toán tìm căn bậc hai theo modulo n:**

Thuật toán 1: Input: Số nguyên tố lẻ p ; $p \equiv 3 \pmod 4$ và $a \in Q_p$.
Output: 2 căn bậc hai của $a \bmod p$

1. Tính $r = a^{(p+1)/4} \bmod p$
2. Return $(r, -r)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 62

Một số kiến thức toán học

Thuật toán 2: Tìm căn bậc hai của $a \bmod p$ ($p \equiv 5 \pmod 8$)
Input: Số nguyên tố lẻ p ; $p \equiv 5 \pmod 8$ và $a \in Q_p$.
Output: 2 căn bậc hai của $a \bmod p$

1. Tính $d = a^{(p-1)/4} \bmod p$
- Nếu $d = 1$ thì tính $r = a^{(p+3)/8} \bmod p$
- Nếu $d = p - 1$ thì tính $r = 2a \cdot (4a)^{(p-5)/8} \bmod p$
- Return $(r, -r)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 63

Một số kiến thức toán học

Thuật toán 3: Tìm căn bậc hai của $c \bmod n$ ($n = p \cdot q$ và $p \equiv 3 \pmod 4$;
 $p \equiv 3 \pmod 4$).
Input: Số nguyên n ; p, q và $c \in Q_n$.
Output: 4 căn bậc hai của $c \bmod n$

1. Dùng thuật toán Euclidean mở rộng tìm a, b : $ap + bq = 1$
- Tính:
 $r = c^{(p+1)/4} \bmod p$
 $s = c^{(q+1)/4} \bmod q$
 $x = (aps + bqr) \bmod n$
 $y = (aps - bqr) \bmod n$
- Return $(\pm x, \pm y)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 64

Một số kiến thức toán học

Thuật toán 4: Input: Số nguyên tố lẻ, số nguyên a , $1 \leq a \leq p - 1$.
Output: 2 căn bậc hai của $a \bmod p$ nếu $a \in Q_p$

1. Tính kí hiệu $\left(\frac{a}{p}\right)$ nếu $\left(\frac{a}{p}\right) = -1$ thì Return "a không có căn bậc hai theo mod p"
- Chọn số nguyên b : $1 \leq b \leq p - 1$ sao cho: $\left(\frac{b}{p}\right) = -1$ (tức $b \notin Q_p$)
- Phân tích: $p - 1 = 2^s \cdot t$ (t là số lẻ)
- Tính $a^{-1} \bmod p$
- Đặt $c \leftarrow b^t \bmod p$; $r \leftarrow a^{(t+1)/2} \bmod p$
- For i from 1 to $s - 1$ do
 - 6.1. Tính $d = (r^2, a^{-1})^{2^{s-i-1}} \bmod p$
 - 6.2. Nếu $d \equiv -1 \pmod p$ thì đặt $r \leftarrow r \cdot c \bmod p$
 - 6.3. $c \leftarrow c^2 \bmod p$
- Return $(r, -r)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 65

Một số kiến thức toán học

- Thuật toán nhân bình phương có lặp**

$a \in Z_n$ và số nguyên k , $0 \leq k < n$ có biểu diễn nhị phân:

$$k = \sum_{i=0}^t k_i 2^i$$

Input

$a \in Z_n$

Output

$a^k \bmod n$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 66

Một số kiến thức toán học

Bài tập áp dụng:

- $5^{96} \bmod 1234 = ?$
- $25^{705} \bmod 3542 = ?$

```

    graph TD
        A["(1). Đặt b ← 1  
Nếu k = 0 thì  
Return (b)"] --> B["(2). Đặt A ← a"]
        B --> C["(3). Nếu k₀ = 1  
thì đặt b ← a"]
        C --> D["(4). For i from 1 to t do  
    4.1. Đặt A ← A² mod n  
    4.2. Nếu kᵢ = 1 thì b ← A.b mod n"]
        D --> E["(5). Return (b)"]
    
```

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin | 16 September 2022 | Page 67

Giới thiệu một số hệ mật KCK

Bài toán logarit rời rạc:

- Giả sử cho g là phần tử sinh của nhóm nhân Z_p^* tức là với $a \neq 0$ bất kỳ thuộc Z_p^* ta có thể tìm được một số nguyên x duy nhất thỏa mãn: $a = g^x$.
- Ta có thể viết $x = \log_g a$
- Bài toán logarit rời rạc chính là bài toán tìm x khi biết a .

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin | 16 September 2022 | Page 68

Giới thiệu một số hệ mật KCK

Ví dụ: Z_{19}^* có phần tử sinh là 2. Hãy tính $\log_2 x$ với mọi $x \in Z_{19}^*$.

- Ta có bảng tính:

$2^1 \bmod 19 = 2$	$2^7 \bmod 19 = 14$	$2^{13} \bmod 19 = 3$
$2^2 \bmod 19 = 4$	$2^8 \bmod 19 = 9$	$2^{14} \bmod 19 = 6$
$2^3 \bmod 19 = 8$	$2^9 \bmod 19 = 18$	$2^{15} \bmod 19 = 12$
$2^4 \bmod 19 = 16$	$2^{10} \bmod 19 = 17$	$2^{16} \bmod 19 = 5$
$2^5 \bmod 19 = 13$	$2^{11} \bmod 19 = 15$	$2^{17} \bmod 19 = 10$
$2^6 \bmod 19 = 7$	$2^{12} \bmod 19 = 11$	$2^{18} \bmod 19 = 1$

Log₂7 = log₂2⁶ = 6, log₂15 = log₂2¹¹ = 11.log₂2 = 11;

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin | 16 September 2022 | Page 69

Giới thiệu một số hệ mật KCK

Log₂x với mọi $x \in Z_{19}^*$.

x	1	2	3	4	5	6	7	8	9
log ₂ x	18	1	13	2	16	14	6	3	8

x	10	11	12	13	14	15	16	17	18
log ₂ x	17	12	15	5	7	11	4	10	9

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin | 16 September 2022 | Page 70

Thuật toán: Tìm $\log_\alpha \beta$ trên Z_n^* , với α là phần tử sinh của Z_n^*

Input: β, α, n

Output: $\log_\alpha \beta$ trên Z_n^*

1. Tính $m = \lceil \sqrt{\text{ord}(\alpha)} \rceil$

2. Lập bảng $(j, \alpha^j \bmod n)$ với $j = \overline{0 \rightarrow m - 1}$

3. Tính $\beta \cdot (\alpha^m)^i \bmod n$ với $i = \overline{0 \rightarrow m - 1}$

4. Tra bảng (j, α^j) cho tới khi thỏa mãn $\beta \cdot (\alpha^m)^i = \alpha^j$

5. Khi đó: $\log_\alpha \beta = m.i + j$

Giới thiệu một số hệ mật KCK

Bài tập áp dụng:

- Cho $\alpha = 31$ là phần tử sinh của Z_{61}^* . Hãy tìm $\log_{31} 45$ trên Z_{61}^* .
- Cho $\alpha = 17$ là phần tử sinh của Z_{97}^* . Hãy tìm $\log_{17} 15$ trên Z_{97}^* .

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin | 16 September 2022 | Page 72

 **Giới thiệu một số hệ mật KCK**

❖ Giải: Tim $\log_{31} 45$ trên Z_{61}^*

- Ta có: $m = \lceil \sqrt{\text{ord}(31)} \rceil = \lceil \sqrt{60} \rceil = 8$
- Ta lập bảng (j, 31^j) với $j = 0 \rightarrow 7$

j	0	1	2	3	4	5	6	7
$31^j \bmod 61$	1	31	46	23	42	21	41	51

$$\begin{aligned} \text{Log}_{31} 45 &= mi + j \\ &= 8 \cdot 3 + 2 = \boxed{26} \end{aligned}$$

▫ Ta có $31^{-1} \bmod 61 = 2 \Rightarrow 31^8 \bmod 61 = 2^8 \bmod 61 = 12$. Lập bảng tính $\beta \cdot (\alpha^m)^i \bmod n = 45$. $31^i \bmod 61$ với $i = 0 \rightarrow 7$

i	0	1	2	3	4	5	6	7
$45 \cdot 31^i \bmod 61$	45	52	14	46	3	36	5	60

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **Giới thiệu một số hệ mật KCK**

❖ Giải: Tim $\log_{17} 15$ trên Z_{97}^*

- Ta có: $m = \lceil \sqrt{\text{ord}(17)} \rceil = \lceil \sqrt{96} \rceil = 10$
- Ta lập bảng (j, 17^j) với $j = 0 \rightarrow 9$

j	0	1	2	3	4	5	6	7	8	9
$17^j \bmod 97$	1	17	95	63	4	68	89	58	16	78

$$\begin{aligned} \text{Log}_{17} 15 &= mi + j \\ &= 10 \cdot 3 + 1 = \boxed{31} \end{aligned}$$

▫ Ta có $17^{-1} \bmod 97 = 40 \Rightarrow 17^{10} \bmod 97 = 40^{10} \bmod 97 = 3$. Lập bảng tính $\beta \cdot (\alpha^m)^i \bmod n = 15$. $3^i \bmod 97$ với $i = 0 \rightarrow 9$

i	0	1	2	3	4	5	6	7	8	9
$15 \cdot 3^i \bmod 97$	15	45	38	17	51	56	71	19	57	74

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **CHƯƠNG 3. CÁC HỆ MẬT KCK**
Nội dung các bài học trong chương 3:

BÀI 01 + 02. BỔ TỰC CƠ SỞ TOÁN HỌC CỦA LÝ THUYẾT MÃ		BÀI 04 + 05. GIỚI THIỆU MỘT SỐ HỆ MẬT KHÓA CÔNG KHAI
BÀI 03. BÀI TẬP ÁP DỤNG		BÀI 06. BÀI TẬP ÁP DỤNG

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **Bài 03. Bài tập áp dụng**

❖ 1) Dùng thuật toán Euclide tìm phần tử nghịch đảo:

- $357^{-1} \bmod 1137$
- $213^{-1} \bmod 1577$

❖ 2) Giải hệ phương trình:

- $5x \equiv 13 \pmod{17}$
- $4x \equiv 39 \pmod{53}$
- $7x \equiv 9 \pmod{19}$

❖ 3) Tính $\phi(490)$; $\phi(768)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **Bài 03. Bài tập áp dụng**

❖ 4) Dùng thuật toán Euclide mở rộng tìm UCLN của 1573, 308.
Tim cặp x, y thỏa mãn: $1573x+308y = \text{UCLN}(1573, 308)$

❖ 5) Tính KH Jacobi: $\left(\frac{29}{199}\right); \left(\frac{21}{211}\right); \left(\frac{47}{97}\right); \left(\frac{5}{97}\right)$

❖ 6) Áp dụng thuật toán tính căn bậc 2 ở phần trước tính:

- Căn bậc hai của 47 mod 97
- Căn bậc hai của 43 mod 57
- Căn bậc hai của 184 mod 211; 44 mod 211
- Căn bậc hai của 40 mod 53; 29 mod 53

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **Bài 03. Bài tập áp dụng**

❖ Chữa bài tập

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2022 | Page 73

 **CHƯƠNG 3. CÁC HỆ MẬT KCK**
Nội dung các bài học trong chương 03

BÀI 01 + 02. BỔ TỰC CƠ SỞ TOÁN HỌC CỦA LÝ THUYẾT MÃ		BÀI 04 + 05. GIỚI THIỆU MỘT SỐ HỆ MẬT KHÓA CÔNG KHAI
BÀI 03. BÀI TẬP ÁP DỤNG		BÀI 06. BÀI TẬP ÁP DỤNG

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 79

 **Bài 04. Giới thiệu một số hệ mật KCK**
Mục tiêu bài học, SV trả lời được các câu hỏi

- ❖ Sự khác biệt hệ mật KBM so với KCK?
- ❖ KCK giải quyết được những vấn đề nào mà KBM không làm được?
- ❖ Phân tích đánh giá độ an toàn của các hệ mật KCK theo lớp các bài toán như phân tích thừa số, logarit rời rạc, bài toán xếp ba lô?
- ❖ Các hệ mật KCK: RSA, Rabin, ElGamal, Merkle – Hellman?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 80

 **Giới thiệu một số hệ mật KCK**

❖ **Giới thiệu:**

- Trong hệ mật khóa đối xứng thì khóa phải được chia sẻ giữa hai bên trên một kênh an toàn trước khi gửi một bản mã bắt kí. Trên thực tế điều này rất khó đảm bảo.
- Ý tưởng về một hệ mật khóa công khai được Diffie và Hellman đưa ra vào năm 1976
- Rivesrt, Shamir và Adleman hiện thực hóa ý tưởng trên vào năm 1977, họ đã tạo nên hệ mật nổi tiếng RSA...

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 81

 **Giới thiệu một số hệ mật KCK**

❖ **Hệ mật RSA:**

- Độ an toàn của hệ RSA dựa trên độ khó của việc phân tích ra thừa số nguyên lớn

❖ **Hệ mật xếp ba lô Merkle - Hellman:**

- Hệ này và các hệ liên quan dựa trên tính khó giải của bài toán tổng các tập con (bài toán này là bài toán NP đầy đủ).

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 82

 **Giới thiệu một số hệ mật KCK**

❖ **Hệ mật ElGamal:**

- Hệ mật ElGamal dựa trên tính khó giải của bài toán logarithm rời rạc trên các trường hữu hạn

❖ **Hệ mật trên các đường cong Elliptic:**

- Các hệ mật này là biến thể của các hệ mật khác (chẳng hạn như hệ mật ElGamal), chúng làm việc trên các đường cong Elliptic chứ không phải là trên các trường hữu hạn. Hệ mật này đảm bảo độ mật với số khoá nhỏ hơn các hệ mật khoá công khai khác.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 83

 **Giới thiệu một số hệ mật KCK**

❖ Một chú ý quan trọng là một hệ mật khóa công khai không bao giờ có thể đảm bảo được độ mật tuyệt đối (an toàn vô điều kiện).

❖ Ta chỉ nghiên cứu độ mật về mặt tính toán của các hệ mật này

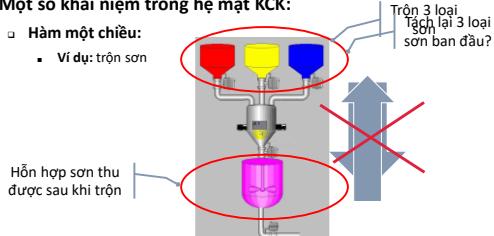
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin 16 September 2021 | Page 84



Giới thiệu một số hệ mật KCK

- ❖ Một số khái niệm trong hệ mật KCK:

- Hàm một chiều:
 - Ví dụ: trộn sơn



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

16 September 2022 | Page 85



Giới thiệu một số hệ mật KCK

- ❖ Một số khái niệm trong hệ mật KCK:

- Đặc tính một chiều: Hàm mã khóa công khai e_k của Bob phải là một hàm dễ tính toán. Song việc tìm hàm ngược (hàm giải mã) rất khó khăn (đối với bất kỳ ai không phải là Bob)
 - Ví dụ:
 - Giả sử $n = p \cdot q$, trong đó p, q là các số nguyên tố lớn, giả sử b là một số nguyên dương.
 - Khi đó hàm $f(x) = x^b \text{ mod } n$ là một hàm một chiều.
- Hàm cửa sổ một chiều: thông tin bí mật cho phép Bob dễ dàng tìm hàm của e_k .

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

16 September 2022 | Page 85



Giới thiệu một số hệ mật KCK

- ❖ Bài toán phân tích thừa số:

- Cho trước một số N , tìm p, q là các số nguyên tố: $N = p \times q$
- Ta thấy rằng tính xuôi: $p \times q = N$ rất dễ dàng, tính ngược tìm p, q từ N là rất khó khăn

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

16 September 2022 | Page 87



Giới thiệu một số hệ mật KCK

- ❖ Ví dụ: Cho $N = 408.508.091$, tìm số nguyên tố p, q : $p \times q = 408.508.091$

- Với máy tính cầm tay \Rightarrow mất bao lâu để có được p, q ?
 - Kiểm tra mỗi số nguyên tố xem có là ước của N hay không? Ví dụ: 3, 5, ... , cho tới $p = 18.313$ (số nguyên tố thứ 2000) thì thấy 18.313 thực sự là thừa số của 408.508.091, như vậy dễ dàng xác định được số $q = 22.307$.
 - Một máy tính kiểm tra 4 số nguyên tố/1 phút \Rightarrow mất 500 phút \Leftrightarrow **hơn 8 giờ** để tìm ra p, q
- Nếu biết trước giá trị $p = 18.313$ và $q = 22.307$ \Rightarrow mất chưa tới **10s** để tính ra N

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

16 September 2022 | Page 87



Giới thiệu một số hệ mật KCK

- ❖ Thời gian cần thiết để phân tích số nguyên n ra thừa số nguyên tố bằng thuật toán nhanh nhất hiện nay:

Số chữ số thập phân	Số phép tính bit	Thời gian
50	$1.4 \cdot 10^{10}$	3.9 giờ
75	$9 \cdot 10^{12}$	104 ngày
100	$2.3 \cdot 10^{15}$	74 năm
200	$1.2 \cdot 10^{23}$	$3.8 \cdot 10^9$ năm
300	$1.5 \cdot 10^{29}$	$4.9 \cdot 10^{15}$ năm
500	$1.3 \cdot 10^{39}$	$4.2 \cdot 10^{25}$ năm

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

16 September 2022 | Page 88



Giới thiệu một số hệ mật KCK

- ❖ Hệ mật RSA:

- RSA là mã công khai được sáng tạo bởi Rivest, Shamir & Adleman ở MIT (Trường Đại học Công nghệ Massachusetts) vào năm 1977.



- RSA là mã công khai được biết đến nhiều nhất và sử dụng rộng rãi nhất hiện nay.

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

16 September 2022 | Page 89



Giới thiệu một số hệ mật KCK

- ❖ **Sơ đồ chung của hệ mật khóa công khai được cho bởi**
 (P, C, K, E, D) (1)
 - Mỗi khóa $k \in K$ gồm có 2 thành phần $k = (k_e, k_d)$, k_e là khóa công khai dành cho việc mã hóa, còn k_d là khóa bí mật dành cho việc giải mã.
- ❖ **Để xây dựng hệ mật RSA**
 - Chọn trước 2 số nguyên tố lớn p và q, tính $n = p \cdot q$
 - Chọn một số e sao cho $\gcd(e, \phi(n)) = 1$ và tính số d sao cho: $e \cdot d \equiv 1 \pmod{\phi(n)}$
 - Mỗi cặp khóa $k = (k_e, k_d)$, với $k_e = (n, e)$, $k_d = d$ là một cặp khóa cho mỗi người dùng cụ thể



Giới thiệu một số hệ mật KCK

- ❖ **Sơ đồ chung của hệ mật RSA theo danh sách (1):**

$P = C = Z_n$, trong đó n là tích của 2 số nguyên tố

$K = \{k_e, k_d\}$ với $k_e = (n, e)$; $k_d = d$ sao cho $\text{gcd}(e, \phi(n)) = 1$, $e \cdot d \equiv 1 \pmod{\phi(n)}$

Hàm mã hóa E và giải mã D được xác định bởi:

$$y = E_{k_e}(x) = x^e \pmod{n} \quad \forall x \in P$$
$$x = D_{k_d}(y) = y^d \pmod{n} \quad \forall y \in C$$

Giới thiệu một số hệ mật KCK

Lưu ý:

- KCK: $K_E = (n, e)$
- KBM: $K_D = d$

Bản rõ

Bản mã

Bản rõ

The logo of the University of Technology, Ho Chi Minh City, featuring a red circular emblem with a white book and a pencil inside, surrounded by the university's name in Vietnamese and English.

Giới thiệu một số hệ m^át KCK

- ❖ **Ví dụ: Cho hệ m^át RSA với $p = 37$, $q = 41$ và số m^áu m^á hoá $e = 211$.**
 - ❑ Hãy tính số m^áu giải m^áa d.
 - ❑ Hãy m^á hoá b^{án} tin $m = 47$ và giải m^áa b^{án} m^áa v^ùa thu đ^é được.

Bộ môn Khoa Học Áp Án Trí Tuệ T^{ín} – Khoa Áp Án Trí Tuệ T^{ín}

16 September 2021 | Page 84

The diagram illustrates the components of RSA encryption:

- Dữ liệu** (Data) leads to **Bản mã** (Encryption) and **Bản rõ** (Decryption). It is associated with the use of a specific key.
- Phép mã** (Key) leads to **Mã hóa** (Encryption) and **Giải mã** (Decryption). It is associated with the use of the modulus n , the public key e , and the private key $\Phi(n)$.
- Khóa** (Key) leads to **Tạo số p, q** (Generating primes p, q) and **Tạo cặp khóa** (Generating keys). It is associated with the use of the Chinese Remainder Theorem and prime factorization.

Giới thiệu một số hệ mật KCK

- ❖ Một số vấn đề khác của RSA:
 - Điểm bất động:
 - **Định lí:** Nếu các thông báo được mã bằng hệ mật RSA với cặp khóa công khai (e, n) với $n = p \cdot q$ thì số các thông báo không thể che giấu được là

$$N = (1 + UCLN(e - 1, p - 1))(1 + UCLN(d - 1, q - 1))$$



Giới thiệu một số hệ mật KCK

- Độ dài khóa:

Năm	Độ dài nên sử dụng
2010	1024 bits
2030	2048 bits
2031	3072 bits

- Ứng dụng của RSA: ngân hàng, TMĐT, các giao thức công nghệ thông tin, chính phủ điện tử, gửi nhận văn bản,...



Giới thiệu một số hệ mật KCK

- Hệ mật Rabin:

- Sơ đồ chung của hệ mật Rabin
 - $P = \mathbb{Z}_n ; C = \mathbb{Z}_n$
 - $K = \{k=(k_e, k_d); k_e = n, k_d = (p, q), n = p \cdot q\}$
 - Hàm mã hóa e và giải mã d được xác định như sau:
 - Với mỗi $x \in P$, để lập mã cho x ta tính $y = e_{k_e}(x, k) = x^2 \bmod n$
 - Hàm giải mã $x = d_{k_d}(y)$ trong đó $d_{k_d}(y)$ là hàm tính căn bậc hai của $y \bmod n$ với các đầu vào (y, p, q)



Giới thiệu một số hệ mật KCK

- Ví dụ:

- Tạo khóa:
 - Chọn các số nguyên tố $p = 19; q = 23$
 - Tính $n = p \cdot q = 437$
 - \Rightarrow Khóa công khai là 437 , khóa bí mật là $(19, 23)$
- Ta có bản tin $x = 101001001$ (lặp 3 bit cuối).
- Thực hiện mã hóa bản tin x và giải mã bản mã thu được.



Giới thiệu một số hệ mật KCK

- Đánh giá hiệu quả

- Thuật toán mã hóa Rabin là một thuật toán cực nhanh vì nó chỉ cần thực hiện một phép bình phương modulo đơn giản.
- Trong khi đó, chẳng hạn với thuật toán RSA có $e = 3$ phải cần tới một phép nhân modulo và một phép bình phương modulo.
- Thuật toán giải mã Rabin có chậm hơn thuật toán mã hóa, tuy nhiên về mặt tốc độ nó cung tương đương với thuật toán giải mã RSA.



Giới thiệu một số hệ mật KCK

- Độ an toàn của hệ mật Rabin:

- Tấn công bắn rỗ có lựa chọn: an toàn
- Không hoàn toàn an toàn với tấn công bắn mã có lựa chọn.



Giới thiệu một số hệ mật KCK

- Hệ mật ElGamal:

- Sơ đồ chung của hệ mật Elgamal:
 - $P = \mathbb{Z}_p^*, C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ với p là số nguyên tố
 - $K = \{k=(k_e, k_d); k_e = (p, \alpha, \beta), k_d = a \in [1, p-2], \beta = \alpha^a \bmod p\}$ ở đây α là một phần tử nguyên thủy của \mathbb{Z}_p^*
 - Hàm mã hóa e và giải mã d được xác định như sau:
 - Với mỗi $x \in P$, để lập mã cho x ta chọn thêm một số ngẫu nhiên $k \in \mathbb{Z}_{p-1}$ rồi tính $e_{k_e}(x, k) = (y_1, y_2)$ với $y_1 = \alpha^k \bmod p, y_2 = x \cdot \beta^k \bmod p$
 - Hàm giải mã: $x = d_{k_d}(y) = d_{k_d}(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$

Giới thiệu một số hệ mật KCK

- Ví dụ:** Sử dụng hệ mật Elgamal với số nguyên tố $p = 211$, phần tử sinh $\alpha = 39$ của Z^{*}_{211} . Giả sử người dùng A chọn khóa bí mật $a = 113$.
 - Hãy tìm khoá công khai của A?
 - Giả sử chọn số ngẫu nhiên $k = 23$, hãy thực hiện mã hoá bản tin $x = 34$ với khoá công khai của A, và giả mã bản mã vừa thu được.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Giới thiệu một số hệ mật KCK

- Bài toán xếp ba lô và hệ mật Merkle – Hellman:**
 - Bài toán ba lô tổng quát:**

Cho tập giá trị a_1, a_2, \dots, a_n và một tổng S. Tính giá trị v_i để cho:

$$S = v_1 a_1 + v_2 a_2 + \dots + v_n a_n \text{ với } v_i \in \{0,1\}$$

Ví dụ:

- Cho $S = 53$, dãy số nguyên $(17, 38, 73, 4, 11, 1)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Giới thiệu một số hệ mật KCK

- Với $S = 53$, dãy số nguyên $(17, 38, 73, 4, 11, 1)$
 - Loại 73, vì $73 > 53$
 - Thứ 17, $S = 53 - 17 = 36$, Loại 38, nhưng $4 + 11 + 1 < 36$. Vậy 17 không có trong lời giải
 - Thứ 38, $S = 53 - 38 = 15$, thấy tổng số hạng còn lại $4 + 11 = 15$. Vậy lời giải: $S = 53 - 38 + 4 + 11$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Cách giải bài toán:

Lời giải của bài toán được tiến hành theo thứ tự, ta xét mỗi số nguyên có thể góp phần vào tổng và đã rút gọn bài toán tương ứng.

Khi một lời giải không đưa ra tổng mong muốn, ta quay lại, loại bỏ các phỏng đoán gần và thử lần lượt.

Với dãy nhiều số nguyên, rất khó tìm lời giải đặc biệt khi tất cả chúng đều lớn như nhau đến mức ta không thể loại trực tiếp được số nào.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Giới thiệu một số hệ mật KCK

- Dãy siêu tăng:**
 - Cho dãy số nguyên dương (a_1, \dots, a_n) , dãy này được gọi là dãy siêu tăng nếu:

$$a_i > \sum_{j=1}^{i-1} a_j \quad \forall i; i = \overline{2, n}$$

Ví dụ: $\{1, 4, 11, 17, 38, 73\}$ là một dãy siêu tăng

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Giới thiệu một số hệ mật KCK

- Nếu ta hạn chế bài toán ba lô thành các **dãy siêu tăng**, ta có thể dễ dàng nói một số hạng có trong tổng không.
- Nếu tổng nằm giữa a_k và a_{k+1} thì nó phải bao hàm a_k như một số hạng. Ngược lại nếu tổng nhỏ hơn a_k thì nó không thể bao hàm a_k như một số hạng.
- Ví dụ:**
 - Cho dãy $\{1, 4, 11, 17, 38, 73\}$.
 - Giải bài toán với các tổng đích $S = 96, S = 95$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 10

Giới thiệu một số hệ mật KCK

- Thuật giải bài toán xếp ba lô trong trường hợp dãy siêu tăng:**

Thuật giải Ba lô siêu tăng

Input: Dãy siêu tăng (M_1, \dots, M_n)
Output: Số nguyên S là tổng một tập con trong dãy siêu tăng
Dãy nhị phân: $v = (v_1, \dots, v_n)$
 $v \in \{0,1\}$

$$\sum_{i=1}^n v_i M_i = S$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 109

Giới thiệu một số hệ mật KCK

- Chứng minh:** $i \leftarrow n$ **Chứng nào $i \geq 1$ thực hiện:**
 - Nếu $S \geq M_i$
 $v_i \leftarrow 1; S \leftarrow S - M_i$
 ngược lại $v_i \leftarrow 0$
 - $i \leftarrow i - 1$
- Ví dụ: tìm dãy nhị phân v**
 - (1) Cho dãy siêu tăng (12, 17, 33, 74, 157, 316, 620, 1230, 2460); tổng $S = 4401$
 - (2) Cho dãy siêu tăng (5, 7, 13, 30, 57, 116, 230, 460, 920); tổng $S = 1508$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 110

Giới thiệu một số hệ mật KCK

- Hệ mật Merkle – Hellman:**
 - Kỹ thuật mã hóa:**
 - Các nguyên tắc của số học modulo:
 - Trong số học thông thường, việc cộng hay nhân một dãy siêu tăng vẫn duy trì bản chất siêu tăng của nó, nên kết quả vẫn là một dãy siêu tăng.
 - Trong số học modulo n , tính chất siêu tăng của một dãy có thể bị phá.
 - Với những kết quả rút ra từ số học modulo, Diffie Hellman đã tìm ra cách phá bản chất siêu tăng của dãy số nguyên, bằng cách nhân tất cả các số nguyên với một hằng số w và lấy kết quả mod n , trong đó $\gcd(n, w) = 1$.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 111

Giới thiệu một số hệ mật KCK

- Biến đổi một ba lô siêu tăng**
 - Để thực hiện thuật toán mã Merkle – Hellman, ta cần một ba lô siêu tăng. Cách làm như sau:

Chọn số nguyên ban đầu a_1 2 Chọn số nguyên thứ 2: $a_2 > a_1$ 3 Chọn số nguyên thứ 3 $a_3 > a_1 + a_2$... Số nguyên n: $a_n > \sum_{i=1}^{n-1} a_i$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 112

Giới thiệu một số hệ mật KCK

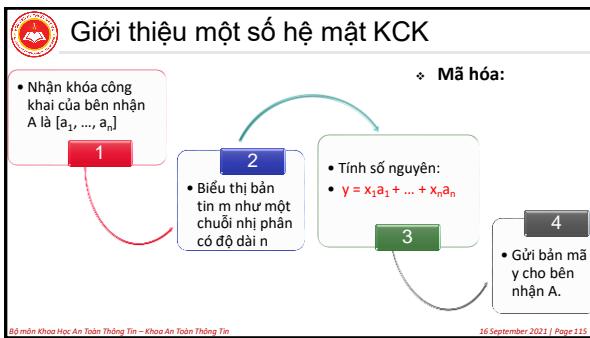
- Để xây dựng hệ mật Merkle – Hellman**
 - Chọn n là tham số chung
 - Chọn dãy siêu tăng: M_1, \dots, M_n
 - Chọn số modulo $M: M > M_1, \dots, M_n$
 - Chọn số nguyên ngẫu nhiên $W: 1 \leq W \leq M - 1$ và $(W, M) = 1$
 - Chọn phép hoán vị π của các số nguyên $\{1, 2, \dots, n\}$
 - Tính $a_i = W \cdot M_{\pi(i)} \bmod M$ với $i = 1, 2, \dots, n$
 - Một cặp khóa $k = (k_e, k_d)$ trong đó $k_e = (a_1, \dots, a_n)$; $k_d = (\pi, M, W(M_1, \dots, M_n))$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 113

Giới thiệu một số hệ mật KCK

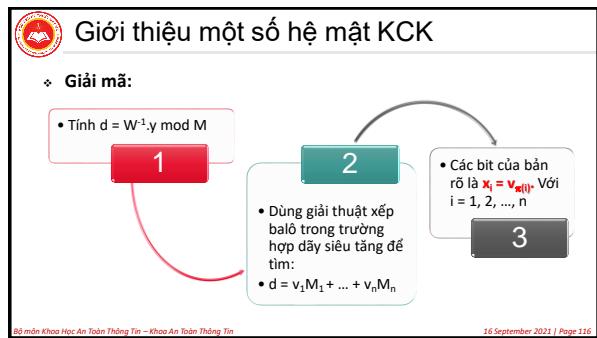
- Sơ đồ chung của hệ mật Merkle – Hellman:**
 - $P = (Z_2)^n$, $C = Z_M$
 - $K = \{k = (k_e, k_d)\}$ với $k_e = (a_1, \dots, a_n)$; $k_d = (\pi, M, W(M_1, \dots, M_n))$
 - Hàm mã hóa e và giải mã d được xác định như sau:
 - Với mỗi $x = (x_1, x_2, \dots, x_n) \in P$, để lập mã cho x ta tính
 $y = e_{k_e}(x) = x_1 a_1 + x_2 a_2 + \dots + x_n a_n$
 - Hàm giải $x = d_{k_d}(y) = (v_{\pi(1)}, \dots, v_{\pi(n)}) = (x_1, x_2, \dots, x_n)$. Trong đó $v_{\pi(i)}$ thu được khi giải bài toán xếp ba lô cho dãy siêu tăng: $d = v_1 M_1 + v_2 M_2 + \dots + v_n M_n$ với $d = W^{-1} \cdot y \bmod M$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 114



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

16 September 2021 | Page 115



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

16 September 2021 | Page 115

Giới thiệu một số hệ mật KCK

Bài tập:

- Cho $n = 6$, dây siêu tăng $(12, 17, 33, 74, 157, 316)$, $M = 737$, $W = 635$, thỏa mãn $(W, M) = 1$.
- Phép hoán vị π của $\{1, 2, 3, 4, 5, 6\}$ được xác định như sau: $\pi(1) = 3$, $\pi(2) = 6$, $\pi(3) = 1$, $\pi(4) = 2$, $\pi(5) = 5$, $\pi(6) = 4$
- Thực hiện mã hóa bản tin $m = 101101$, và giải mã ngược lại từ bản mã vừa thu được.

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

16 September 2021 | Page 116

Giới thiệu một số hệ mật KCK

Đánh giá:

- Thông thường ta thường chọn giá trị mỗi số hạng M_i của ba lô dễ dàng khoảng từ 200 – 400 chữ số. Chính xác hơn các M_i được chọn như sau:
 - $1 \leq M_1 < 2^{200}$
 - $2^{200} \leq M_2 < 2^{201}$
 - $2^{201} \leq M_3 < 2^{202}$
 - ...
- Như vậy có xấp xỉ 2^{200} lựa chọn cho mỗi M_i .
- Có thể dùng dây các số ngẫu nhiên để tạo một ba lô dễ dàng n số ngẫu nhiên r_1, \dots, r_n . Mỗi r_i phải trong khoảng từ 0 đến 2^{200} . Khi đó mỗi giá trị M_i được tính như sau:
 - $M_i = 2^{200+i-1} + r_i$, với $i = 1, 2, \dots, n$

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

16 September 2021 | Page 116

Giới thiệu một số hệ mật KCK

- Với các số hạng lớn như vậy, không thể thử tất cả các giá trị có thể có của M_i khi biết khóa công khai (a_1, \dots, a_n) và bản mã c.
- Ngay cả khi giả thiết một máy có thể thực hiện một phép tính trên một micro giây thì cũng mất 10^{47} năm để thử một trong 2^{200} lựa chọn cho mỗi của M_i . Một máy song song cực lớn với 1000 hay thậm chí 1.000.000 phần tử song song thì cũng không đủ để làm yếu phép mã!
- Phương pháp Merkle – Hellman đường như rất an toàn. Với các giá trị lớn thích hợp cho M, n thì các cơ hội phá được phương pháp bằng tấn công theo kiểu vét cạn là rất mong manh.

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

16 September 2021 | Page 119

Giới thiệu một số hệ mật KCK

Hệ mật đường cong Elliptic

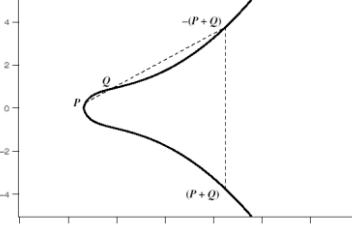
Các đường cong Elliptic:

- Đường cong Elliptic:**
 - Đường cong Ellip được định nghĩa bởi phương trình với 2 biến x, y và hệ số thực
 - Xét đường cong Ellip bậc 3 dạng:
 $y^2 = x^3 + ax + b$; trong đó x, y, a, b là các số thực và định nghĩa thêm điểm O.
 - Có phép cộng đối với đường cong Ellip
 - Về hình học tổng của P và Q là điểm đối xứng của giao điểm R
 - Điểm O đóng vai trò là đơn vị đối với phép cộng và nó là điểm vô cực.

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

16 September 2021 | Page 120

 Giới thiệu một số hệ mật KCK



(b) $y^2 \approx x^3 + x + 1$

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

16 September 2021 | Page 121

 Giới thiệu một số hệ mật KCK

- ❖ **Đường cong Elip hữu hạn**
 - Mã đường cong Elip sử dụng đường cong Elip mà các biến và hệ số là hữu hạn.
 - Có hai họ được sử dụng nói chung:
 - Đường cong nguyên tố $E_p(a,b)$ được xác định trên Z_p
 - Sử dụng các số nguyên modulo số nguyên tố
 - Tốt nhất trong phần mềm
 - Đường cong nhị phân $E_{2^n}(a,b)$ xác định trên $GF(2^n)$
 - Sử dụng đa thức với hệ số nhị phân
 - Tốt nhất trong phần cứng

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

16 September 2021 | Page 122

 Giới thiệu một số hệ mật KCK

- ❖ **Đường cong Elliptic**
 - **Định nghĩa đường cong Elliptic:** Cho $p > 3$ là số nguyên tố, đường cong elliptic $y^2 = x^3 + ax + b$ trên Z_p là tập các nghiệm $(x, y) \in Z_p \times Z_p$ của phương trình đồng dư: $y^2 \equiv x^3 + ax + b \pmod{p}$, trong đó $a, b \in Z_p$ là các hằng số thỏa mãn $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ cùng với một điểm đặc biệt O được gọi là điểm vô cực.

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

16 September 2021 | Page 123

 Giới thiệu một số hệ mật KCK

- ❖ **Ta định nghĩa phép toán trên E là phép cộng**
- ❖ **Giả sử $P = (x_1, y_1), Q = (x_2, y_2)$ là hai điểm thuộc $E_p(a, b)$, phép cộng được định nghĩa như sau:**
 - Nếu $x_2 = x_1, y_2 = -y_1$ thì $P + Q = O$,
 - Ngược lại $P + Q = (x_3, y_3)$ trong đó:
 - $x_3 = \lambda^2 - x_1 - x_2$
 - $y_3 = \lambda(x_1 - x_3) - y_1$
 - Với $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{nếu } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{nếu } P = Q \end{cases}$

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

16 September 2021 | Page 124

 Giới thiệu một số hệ mật KCK

- ...
- $P + O = O + P = P, \forall P \in E$
- Phép lấy nghịch đảo được tính toán khá dễ dàng, nghịch đảo của (x, y) là $-(x, y)$ và là $(x, -y)$
- Do đó đường cong Elliptic E tạo thành một nhóm Abel (các phép toán thực hiện trên Z_p)

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

16 September 2021 | Page 125

 Giới thiệu một số hệ mật KCK

- ❖ **Ví dụ: Cho E là đường cong Elliptic $y^2 = x^3 + x + 6$ trên Z_{11} , ta cần xác định các điểm trên E.**
 - B1. Với mỗi $x \in Z_{11}$ ta xác định được $z = y^2 = x^3 + x + 6 \pmod{11}$
 - B2. Kiểm tra xem z có phải là thặng dư bậc hai trên Z_{11} không
 - B3. Nếu z là một thặng dư bậc hai trên Z_{11} thì tính các căn bậc hai của z trên Z_{11} , đó chính là các giá trị của y ứng với x

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

16 September 2021 | Page 126



Giới thiệu một số hệ mật KCK

♦ BTVN:

- Cho đường cong elliptic trên Z_{19} :
 $y^2 = x^3 + x + 1 \text{ mod } 19$.
- Tìm tất cả các điểm nằm trên đường cong elliptic này.

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

16 September 2021 | Page 127



Giới thiệu một số hệ mật KCK

♦ Hệ mật đường cong Elliptic:

- Để xây dựng hệ mật ECC:
 - Chọn $E_p(a,b)$
 - Chọn G là phần tử với bậc lớn, tức là n lớn sao cho $nG = O$
 - Người dùng A chọn khóa riêng $k_d = n_A < n$
 - Tính $P_A = n_A \times G$
 - Khóa công khai $k_e = (E_p(a,b), G, P_A)$

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

16 September 2021 | Page 128



Giới thiệu một số hệ mật KCK

♦ Sơ đồ chung của hệ mật ECC:

- Gọi $E^* = E_p(a, b) \setminus \{O\}$
- $P = E^*$; $C = (E^* \times E^*)$
- $K = \{k = (k_e, k_d)\}$ với $k_e = (E_p(a,b), G, P_A); k_d = n_A$
- Hàm mã hóa e và giải mã d được xác định như sau:
 - Người B gửi tin cho A, thực hiện mã hóa $P_M \in E^*$, B chọn thêm một số ngẫu nhiên k và tính bản mã: $P_c = e_{k_e}(P_M, k) = [P_1, P_2]$ trong đó $P_1 = kG; P_2 = (P_M + kP_A)$
 - Hàm giải mã, A tính: $P_M = e_{k_d}(P_c) = P_2 - n_A P_1$

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

16 September 2021 | Page 129



Giới thiệu một số hệ mật KCK

♦ Độ an toàn:

- Phụ thuộc độ khó của việc xác định số nguyên ngẫu nhiên bí mật k khi biết 2 điểm P và kP
- Chính là bài toán logarit rời rạc trên ECC.
- So với RSA cùng mức an toàn thì hệ mật ECC có độ dài khóa nhỏ hơn.

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

16 September 2021 | Page 130



Tổng kết

- Hệ mật khoá công khai ra đời hỗ trợ thêm để giải quyết một số bài toán an toàn, chứ không phải thay thế khoá riêng. Cả hai khoá cùng tồn tại, phát triển và bổ sung cho nhau
- Khoá công khai/không đối xứng bao gồm việc sử dụng 2 khoá:
 - **Khoá công khai:** mà mọi người đều biết, được dùng để mã hoá mẫu tin và kiểm chứng chữ ký.
 - **Khoá riêng:** chỉ người nhận biết, để giải mã bản tin hoặc để tạo chữ ký.
 - Là không đối xứng vì những người mã hoá và kiểm chứng chữ ký không thể giải mã hoặc tạo chữ ký.

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

16 September 2021 | Page 131



Tổng kết

♦ Tại sao lại phải dùng mã khoá công khai?

- Người ta muốn giải quyết các vấn đề sau về khoá này sinh trong thực tế:
 - Số lượng khoá lớn, khó khăn trong việc thiết lập quản lý khoá chia sẻ trước khi dùng hệ mật khoá đối xứng
 - Phân phối khoá - làm sao có thể phân phối khoá an toàn mà không cần trung tâm phân phối khoá tin cậy.
 - Chữ ký điện tử - làm sao có thể kiểm chứng được rằng mẫu tin gửi đến nguyên vẹn từ đúng người đứng tên gửi.

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

16 September 2021 | Page 132

Tổng kết

- Ứng dụng khoá công khai**
 - Có thể phân loại các ứng dụng của khoá công khai thành 3 loại khác nhau:
 - Mã giải mã – cung cấp bảo mật. Đây là ứng dụng bảo mật truyền thống giống như ta vẫn thường dùng với khoá đối xứng.
 - Chữ ký điện tử – cung cấp xác thực. Một trong các ứng dụng mới của khoá công khai mà khoá đối xứng không thể thực hiện được, đó là khoá công khai có đủ cơ sở để xác nhận người gửi và có thể là một lựa chọn để tạo chữ ký điện tử của người gửi.
 - Một số thuật toán mã công khai phù hợp với mọi ứng dụng, còn một số khác chuyên dùng cho ứng dụng cụ thể.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 134

NỘI DUNG

01. TỔNG QUAN VỀ MẬT MÃ HỌC
Tổng quan về mật mã học

02. CÁC HỆ MẬT KHÓA BÍ MẬT
Các hệ mật khóa bí mật

03. CÁC HỆ MẬT KHÓA CÔNG KHAI
Các hệ mật khóa công khai

04. HÀM BĂM, XÁC THỰC VÀ CHỮ KÍ SỐ
Hàm băm, toàn vẹn và chữ kí số

05. 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
16 September 2021 | Page 134

CHƯƠNG 04

HÀM BĂM, XÁC THỰC VÀ CHỮ KÍ SỐ

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 135

Bài 01. Vấn đề xác thực, hàm băm, chữ kí số

- Bài toán xác thực liên quan tới bảo vệ tính toàn vẹn, kiểm chứng danh tính, nguồn gốc, chống chối từ bản gốc?
- Hàm băm, mã xác thực, chữ kí số?
- Các ứng dụng trong việc xác thực và đảm bảo tính toàn vẹn dữ liệu?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 135

Vấn đề xác thực

- Xác thực mẫu tin liên quan đến các khóa cạnh sau khi truyền tin trên mạng:**
 - Bảo vệ tính toàn vẹn của mẫu tin:** bảo vệ mẫu tin không bị thay đổi hoặc có các biện pháp phát hiện nếu mẫu tin bị thay đổi trên đường truyền.
 - Kiểm chứng danh tính và nguồn gốc:** xem xét mẫu tin có đúng do người xưng tên gửi không hay một kẻ mạo danh nào khác gửi.
 - Không chối từ bản gốc:** trong trường hợp cần thiết, bản thân mẫu tin chứa các thông tin chứng tỏ chỉ có người xưng danh gửi, không một ai khác có thể làm điều đó. Như vậy người gửi không thể từ chối hành động gửi, thời gian gửi và nội dung của mẫu tin.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 137

Hàm băm

- Giá trị băm “đại diện” cho một thông báo (văn bản) rất dài**
 - Có thể gọi là “bản tóm lược” của thông báo (message digest)
- Một bản tóm lược thông báo như là một “dấu vân tay số - digital fingerprint” của tài liệu gốc**

Tóm lược thông báo M có độ dài tùy ý thành bản tóm lược có độ dài cố định $h = H(M)$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 139

Hàm nghiền

- Hàm băm như hàm “nghiền” hay “tóm lược”**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 139

Băm và mã hóa

Xin chào.
Đây là một ví dụ về mã hóa.
NhbxBsZSzBzZW50ZW5jZS
B0byBzaG93IEVuY3JScHR
pb24KsZSzBz

Xin chào.
Đây là một ví dụ về mã hóa.
NhbxBsZSzBzZW50ZW5jZS
B0byBzaG93IEVuY3JScHR
pb24KsZSzBz

Mã hóa là hai chiều, và yêu cầu khóa để mã hóa/giải mã

Bây giờ rõ ràng đây không cần dùng khóa. Các câu dài hơn vẫn bản trên rất nhiều.

Băm là một chiều. Không có khả năng tính ngược lại (no ‘de-hashing’)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 140

Các ứng dụng của hàm băm

- Ứng dụng đơn**
 - “Đầu vân tay” – xác minh tính toàn vẹn của file, “đầu vân tay” cho khóa công khai
 - Lưu trữ mật khẩu (mã hóa một chiều)
- Kết hợp với các hàm mã hóa**
 - Mã xác thực thông điệp (Message Authentication Code - MAC)
 - Bảo vệ cả tính toàn vẹn cũng như tính xác thực của thông báo
 - Chữ ký số
 - Mã hóa giá trị băm với khóa riêng (khóa ký) và xác minh bằng khóa công khai (khóa xác minh - verification)

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 141

Tính toàn vẹn

Current Message → Hash function → Current digest

Previous digest

Message is changed (discard)
N
Same
Y
Message is not changed

- Để tạo một file mật khẩu một chiều**
 - Lưu giá trị băm của mật khẩu, không phải là mật khẩu thực
- Dùng cho phát hiện tấn công và phát hiện virus**
 - Duy trì và kiểm tra giá trị băm của các file trên hệ thống

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 142

Xác minh mật khẩu

Lưu giá trị băm của mật khẩu

Xác minh một mật khẩu nhập vào với giá trị băm đã lưu

Grant
Deny

Giá trị băm bằng nhau?

Yes
No

MESSAGE
Key (K) → MAC Algorithm → MAC

MESSAGE
Key (K) → MAC Algorithm → MAC

MAC: Message Authentication Code

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 143

Xác thực

SENDER

RECEIVER

MESSAGE
Key (K) → MAC Algorithm → MAC

MESSAGE
Key (K) → MAC Algorithm → MAC

Decision: If same then authentic and integrity checked else something is wrong!

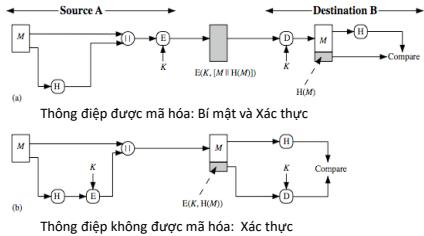
MAC: Message Authentication Code

- Bảo đảm cả tính toàn vẹn và xác thực của thông báo bằng cách kiểm tra (ai là người sở hữu khóa mật) để phát hiện bất kỳ thay đổi nào trong nội dung của thông báo**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 144



Sử dụng hàm băm

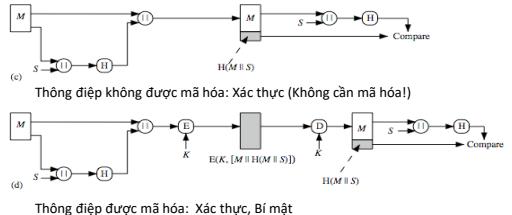


Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

16 September 2021 | Page 145



Sử dụng hàm băm

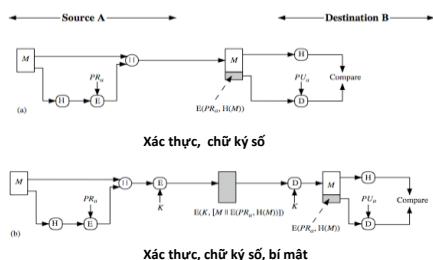


Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

16 September 2021 | Page 145



Sử dụng hàm băm



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

16 September 2021 | Page 146



Các tính chất của hàm băm

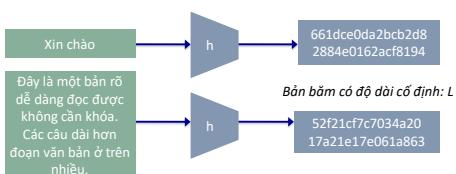
- ❖ Thông điệp có độ dài tùy ý thành bản tóm lược có độ dài cố định
- ❖ Kháng tiền ảnh (tính một chiều) {Preimage resistant (One-way property)}
 - Đầu ra được xác định trước không có khả năng tính toán để tìm 1 đầu vào bất kì mà khi băm sẽ cho ra đầu ra tương ứng (tim x : $h(x) = y$, với y cho trước và không biết đầu vào tương ứng)
- ❖ Kháng tiền ảnh thứ 2 (kháng va chạm yếu) {Second preimage resistant (Weak collision resistant) }
 - Không có khả năng tính toán để tìm một đầu vào đã cho trước (tức là với x cho trước phải tìm $x' \neq x$ sao cho $h(x) = h(x')$)
- ❖ Kháng va chạm mạnh (Strong collision resistance)
 - Không có khả năng về mặt tính toán để tìm 2 đầu vào khác nhau bất kì x và x' để $h(x) = h(x')$

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

16 September 2021 | Page 146



Sử dụng hàm băm



- ❖ Thông điệp có độ dài tùy ý, bản băm có độ dài cố định

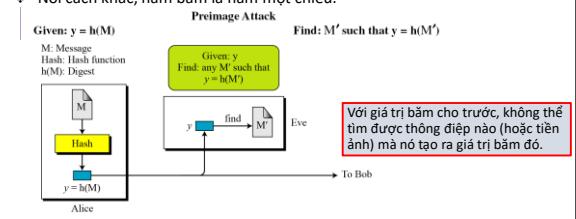
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

16 September 2021 | Page 146



Kháng tiền ảnh (tính chất một chiều)

- ❖ Nghĩa là cho M tính $y = h(M)$ là dễ, nhưng ngược lại, biết y tính ra M là việc cực kỳ khó
- ❖ Nói cách khác, hàm băm là hàm một chiều.



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

16 September 2021 | Page 150

- Đối với thông báo M, rất khó tìm được M' khác M mà $h(M) = h(M')$

Second Preimage Attack

Given: M and $h(M)$

Find: $M' \neq M$ such that $h(M) = h(M')$

M: Message
Hash: Hash function
HMD: Digest

Eve

To Bob

- Chưa trước một thông báo, không thể tìm được thông báo khác mà có giá trị băm giống nhau. Tần cống tìm một thông báo thứ 2 có cùng giá trị băm được gọi là tần công tiền ảnh thứ 2 (*second pre-image attack*).
- Sẽ dễ dàng để giả mạo chữ ký mới từ chữ ký cũ nếu hàm băm được dùng không có tính chất kháng tiền ảnh thứ 2

Kháng va chạm (kháng va chạm mạnh)

Given: none

Collision Attack
Find: $M' \neq M$ such that $h(M) = h(M')$

M: Message
Hash: Hash function
 $h(M)$: Digest

Find: M and M' such that $M \neq M'$, but $h(M) = h(M')$

Eve

M

M'

$h(M) = h(M')$

- ❖ Không thể tìm được 2 thông điệp khác nhau mà có giá trị băm giống nhau
 - ❑ Kháng va chạm hàm ý đến kháng kháng tiền ảnh thứ 2
 - ❑ Nếu tìm thấy các va chạm, thì các bên ký kết dễ dàng phủ nhận chữ ký của mình.

```

graph TD
    A[Hàm băm] --> B[Không khóa]
    A --> C[Có khóa]
    B --> D[Mã phát hiện sửa đổi (MDC)]
    B --> E[Các ứng dụng khác]
    C --> F[Hàm băm một chiều (OWHF)]
    C --> G[Hàm băm kháng va chạm (CRHF)]
    E --> H[Các ứng dụng khác]
    E --> I[Mã xác thực thông điệp (MAC)]

```

Sơ đồ phân loại hàm băm mật mã và ứng dụng

Hàm băm

- Không khóa
 - Mã phát hiện sửa đổi (MDC)
 - Các ứng dụng khác
- Có khóa
 - Các ứng dụng khác
 - Mã xác thực thông điệp (MAC)

Hàm băm một chiều (OWHF)

Hàm băm kháng va chạm (CRHF)

Lược đồ Merkle - Damgard

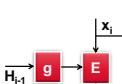
Original message	Padding/length
M_1	n bits
M_2	n bits
...	...
M_i	n bits
H_1	m bits
H_2	m bits
...	...
H_{i-1}	m bits
f	Compression function
H_i	m bits
f	Compression function
Message digest	Message digest

Một thông điệp có độ dài bất kỳ được chia thành các khối

- Độ dài phu thuộc vào hàm nén f
- Đem vào để kích thước thông điệp là bộ số của kích thước khối.
- Xử lý tựa tựa các khối, dùng kết quả băm của mỗi khối và khối hiện tại như là đầu vào của quá trình băm tiếp theo, cuối cùng là đầu ra có độ dài cố định

Matyas – Mayer – Oseas Davies – Mayer Miyaguchi - Preneel

 Thuật toán Matyas – Mayer – Oseas



Cấu trúc thuật toán

- ❖ **Input:** Xâu bit x
- ❖ **Output:** Mã băm n bit của x

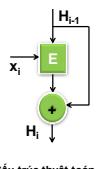
(1) Đầu vào x được phân chia thành các khối n bit và được độn nêu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được t khối n bit: $x_1, x_2 \dots x_t$. Xác định trước một giá trị ban đầu n bit (**kí hiệu IV**)

(2) Đầu ra là H_t được xác định như sau:

$$H_0 = IV, H_i = E_{g(H_{i-1})}(x_i) \oplus x_i, 1 \leq i \leq t$$



Thuật toán băm Davies - Mayer



- ❖ **Input:** Xâu bit x

- ❖ **Output:** Mã băm n bit của x

(1) Đầu vào x được phân chia thành các khối n bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được **t** **khối n bit:** x_1, x_2, \dots, x_t . Xác định trước một giá trị ban đầu n bit (ki hiệu IV)

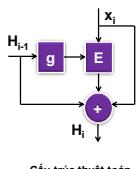
(2) Đầu ra là H_t được xác định như sau:

$$H_0 = IV, H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1}, 1 \leq i \leq t$$

Cấu trúc thuật toán



Thuật toán băm Miyaguchi - Preneel



Cấu trúc thuật toán

- ❖ Sơ đồ này tương tự như ở thuật toán M-M-O ngoại trừ H_{i-1} đầu ra ở giai đoạn trước) được cộng mod 2 với tín hiệu ra ở giai đoạn hiện thời. Như vậy:

$$H_0 = IV, H_i = E_{g(H_{i-1})}(x_i) \oplus x_i \oplus H_{i-1}; 1 \leq i \leq t$$



Họ hàm băm

- ❖ **MD (Message Digest)**

- Designed by Ron Rivest
 - Family: MD2, MD4, MD5

- ❖ **SHA (Secure Hash Algorithm)**

- Designed by NIST
 - Family: SHA-0, SHA-1, and SHA-2
 - SHA-2: SHA-224, SHA-256, SHA-384, SHA-512
 - SHA-3: New standard in competition

- ❖ ...



Các tấn công lên hàm băm

- ❖ **Tấn công kiểu vét cạn**

- ❖ **Tấn công vào tính chất kháng tiền ánh, kháng tiền ánh thứ 2**

- Tìm m sao cho $H(m)$ bằng một giá trị băm y đã cho

- ❖ **Kháng va chạm**

- Tìm hai thông điệp $x \neq y$ mà $H(x) = H(y)$



Tấn công ngày sinh nhật

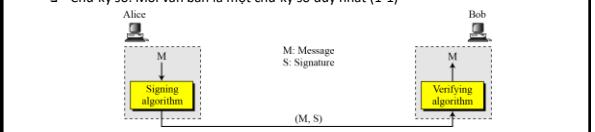
- ❖ Cần có bao nhiêu người để xác suất 2 người trong số đó trùng ngày sinh > 50% ?
- ❖ Trong 23 người được chọn 1 cách ngẫu nhiên thì ít nhất có 2 người trùng ngày sinh (tức có va chạm mạnh)
- ❖ Người ta chứng minh được rằng: Nếu có tất cả n bản tóm lược, và $k \approx \sqrt{2n \ln \frac{1}{1-\epsilon}}$ thì trong k văn bản được chọn ngẫu nhiên có ít nhất một va chạm mạnh (tức là có $x \neq y$ mà $h(x) = h(y)$) với xác suất là ϵ
- ❖ Khi $\epsilon = 0.5$ thì $k \approx 1.17\sqrt{n}$, trong trường hợp ngày sinh n = 365, nên $k \approx 23$
- ❖ Với văn đề chọn độ dài cho đầu ra của hàm băm. Nếu là 40 bit, thi $n = 2^{40}$, do đó $k \approx 2^{20}$ (khoảng 1 triệu văn bản) sẽ có một va chạm mạnh, như vậy là không an toàn!



Xác thực và chữ ký số

- ❖ **Chữ ký số:**

- Chữ ký thông thường được bao gồm trong tài liệu, là một phần không tách rời của tài liệu
 - Nhưng khi ký tài liệu số, chữ ký số là phần tách riêng, được gửi kèm cùng tài liệu
 - Chữ ký tay thường "giống nhau" trên nhiều văn bản
 - Chữ ký số: Mỗi văn bản là một chữ ký số duy nhất (1-1)



Xác thực và chữ kí số

❖ Phương pháp kiểm tra chữ kí:

- Đối với một chữ ký thông thường, khi người nhận nhận được một tài liệu, họ so sánh chữ ký trên văn bản với chữ ký trong hồ sơ.
- Đối với một chữ kí số, người nhận nhận được tài liệu số và chữ ký. Người nhận cần phải áp dụng một kỹ thuật **kiểm tra sự kết hợp** của thông điệp và chữ ký để **xác minh tính xác thực**.
- Chữ ký viết tay thường rất ngắn. Một chữ ký số phải mang được chút gắn bó nào đó với từng bit của thông tin
 - ⇒ theo hình dung ban đầu, độ dài chữ ký số cũng phải theo độ dài của văn bản
 - Cần có được chữ ký ngắn ⇒ Phải dùng thêm một kỹ thuật riêng

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16

Xác thực và chữ kí số

❖ Định nghĩa:

- Một sơ đồ hệ thống chữ ký số là bộ 5 (P, A, K, S, V), trong đó
 - P là một tập hữu hạn các thông báo có thể.
 - A là một tập hữu hạn các chữ ký có thể.
 - K là một tập hữu hạn các khóa, mỗi khóa $k \in K$ gồm có 2 thành phần $k = (k_s, k_p)$, k_s là khóa bí mật dùng để ký, k_p là khóa công khai dùng để kiểm tra chữ ký.
 - Với mỗi $k = (k_s, k_p)$ trong K có một thuật toán ký $\text{sig}_k: P \rightarrow A$, và trong V có một thuật toán kiểm tra chữ ký.

$\text{ver}_k: P \times A \rightarrow \{\text{đúng}, \text{sai}\}$

thỏa mãn điều kiện sau với mọi thông báo $x \in P$ và chữ ký $y \in A$

$$\text{ver}_{k_y}(x, y) = \text{đúng} \Leftrightarrow y = \text{sig}_{k_x}(x)$$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16

Xác thực và chữ kí số

❖ Chú ý:

- Một hệ thống sử dụng khóa riêng và khóa công khai của **người nhận**
- Hệ thống chữ ký số sử dụng khóa riêng và khóa công khai của **người gửi**

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16

Xác thực và chữ kí số

❖ Chữ kí số và hàm băm

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16

Xác thực và chữ kí số

❖ Chữ kí số và đảm bảo tính bí mật

❖ Chữ kí số không đảm bảo tính bí mật, nếu cần đảm bảo tính bí mật, kỹ thuật mã hóa/giải mã phải được áp dụng

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16

Bài 02. Vấn đề xác thực, hàm băm, chữ kí số (tiếp)

❖ Lược đồ kí RSA?

❖ Các tấn công đối với chữ kí RSA, và chữ kí RSA trong thực tế?

❖ Chữ kí số ElGamal cơ bản, hệ chữ kí ElGamal tổng quát sử dụng các đường cong elliptic?

❖ Vấn đề xác thực khóa công khai?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin
16 September 2021 | Page 16



Xác thực và chữ kí số

Chữ kí số RSA:

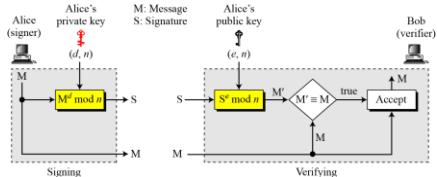
- Sơ đồ hệ thống chữ kí số RSA là bộ 5 (P, A, K, S, V), trong đó
 - $P = A = \mathbb{Z}_n$ với $n = p \cdot q$ là tích của 2 số nguyên tố lớn p và q
 - $K = \{(k_s, k_v), k_s = d, k_v = (n, e)\}$; và $e \cdot d \equiv 1 \pmod{\phi(n)}$
 - Hàm ký $\text{sig}_k: P \rightarrow A$ và hàm kiểm tra chữ kí $\text{ver}_k: P \times A \rightarrow \{\text{đúng}, \text{sai}\}$ được định nghĩa như sau:

$$\begin{aligned} s &= \text{sig}_{k_s}(m) = m^d \pmod{n} \\ \text{ver}_{k_v}(m, s) &= \text{đúng} \Leftrightarrow m = s^e \pmod{n} \end{aligned}$$



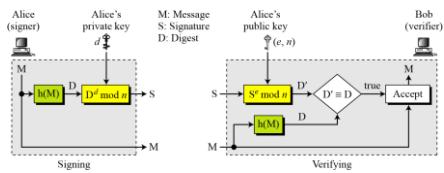
Xác thực và chữ kí số

Sơ đồ hệ thống chữ kí số RSA:



Xác thực và chữ kí số

Chữ kí số RSA và hàm băm



Xác thực và chữ kí số

Ví dụ

- $p = 31, q = 23$
- $n = 31 * 23 = 713$
- $\Phi(n) = 30 * 22 = 660$
- $\rightarrow d = 223$ với $\text{gdc}(223, 660) = 1$
- $\rightarrow e = 223^{-1} \pmod{660} = 367$
- Thông điệp cần ký: 439
- Ký:**
 $s = 439^{223} \pmod{713}$
 $= 284$
 - Công khai: $(713, 367)$
Bí mật: (223)
- Kiểm tra chữ kí:**
 $439 = 284^{367} \pmod{713}$
 $\Leftrightarrow \text{đúng}$



Xác thực và chữ kí số

Sơ đồ chữ kí ElGamal (1985)

- Được thiết kế với mục đích dành riêng cho chữ kí số, khác với RSA được dùng cho cả hệ thống mã khóa công khai lẫn chữ kí số.
- Sơ đồ El Gamal không tắt định giống như hệ thống mã KCK Elgamal. Điều này có nghĩa là **có nhiều chữ kí hợp lệ** trên bức điện cho trước bất kì
- Thuật toán xác minh phải có khả năng chấp nhận bất kì chữ kí hợp lệ khi xác thực.



Xác thực và chữ kí số

Mô tả sơ đồ E:

- Cho số nguyên tố p : bài toán logarit rời rạc trên \mathbb{Z}_p là khó và giả sử $\alpha \in \mathbb{Z}_p$ là phần tử nguyên thủy
- Chọn số $a \in \mathbb{Z}_p$ và tính $\beta = \alpha^a \pmod{p}$
- Giá trị p, α, β là công khai, còn a là mật
- Chọn số ngẫu nhiên (mật) $k \in \mathbb{Z}_{p-1}$. Định nghĩa:
 $\text{sig}_k(x) = (\gamma, \delta)$
- Trong đó: $\gamma = \alpha^k \pmod{p}$; $\delta = (x - a \cdot \gamma) \cdot \beta^k \pmod{p}$, với $x, \gamma \in \mathbb{Z}_p$ và $\delta \in \mathbb{Z}_{p-1}$, ta định nghĩa: $\text{Ver}(x, \gamma, \delta) = \text{true} \Leftrightarrow \beta^\gamma \delta^k \equiv \alpha^x \pmod{p}$



Xác thực và chữ kí số

Ví dụ:

- Cho $p = 467$, $\alpha = 2$, $a = 127$.
- Hãy kí lên bức điện $x = 100$, với số ngẫu nhiên $k = 213$ và xác minh chữ kí thu được

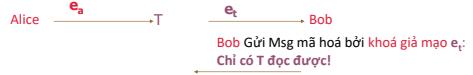


Xác thực và chữ kí số

Vấn đề chứng thực khóa công khai

- Trước hết, ta hãy xem xét một số vấn đề trong sử dụng mật mã khóa công khai:

- **Trường hợp 1:** sử dụng mật mã khóa công khai để mã hóa



→ Khoá công khai e_b của Alice cần được chứng thực,
Vì có thể **Bob** đã nhận **khóa giả mạo e_i** .



Xác thực và chữ kí số

Vấn đề chứng thực khóa công khai:

- Trước hết, ta hãy xem xét một số vấn đề trong sử dụng Khóa công khai:
 - **Trường hợp 2:** sử dụng chữ ký số
 - Alice nhận m và chữ ký $s = Sig_B(m)$ từ Bob.
 - Alice sử dụng khóa công khai của Bob e_b để kiểm tra chữ ký.
 - Nếu $Ver_{e_b}(s, m) = TRUE$, thì Alice có thể tin Bob đã ký m .
 - Nhưng Bob **không công nhận e_b** là khóa công khai của mình thì sao ?

➔ **Khoá công khai e_b của Bob cần được chứng thực !**



Xác thực và chữ kí số

Vấn đề chứng thực khóa công khai:

- Qua 2 trường hợp ta thấy: Trong mỗi trường sử dụng Khóa công khai đã nẩy sinh vấn đề **CHỨNG THỰC KHÓA CÔNG KHAI**
- Đấy là vấn đề cơ bản cần phải giải quyết trong ứng dụng mật mã khóa công khai.



Xác thực và chữ kí số

Vấn đề chứng thực khóa công khai: Giải pháp?

- Cần có một Trung tâm chứng thực tin cậy:
 - **Trusted Certification Authority – CA**
- CA phát hành các **Chứng thư số** gắn **Khóa công khai** với **Thực thể xác định** (**Con người, Cơ quan,...**).
- **Thực thể** đăng ký **khóa công khai** với **CA**
- **CA** tạo **chứng thư số** gắn **thực thể** với **khóa công khai**
- **CA** ký vào **chứng thư số**



Xác thực và chữ kí số

Quá trình tạo chứng thư số

- **Thực thể** đăng ký **khóa công khai** với **CA**
- **CA** tạo **chứng thư số** gắn **thực thể** với **khóa công khai**
- **CA** ký vào **chứng thư số**



Xác thực và chữ ký số

Sử dụng chứng thư số

- Sử dụng **khoá công khai** của CA để kiểm tra chứng thư số (cần xác thực)
- Nếu đúng thì có thể tin chứng thư đó do CA phát hành và có thể sử dụng **khoá công khai** lấy ra từ **chứng thư số** (của đối tác).

Một số nội dung của chứng thư số



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

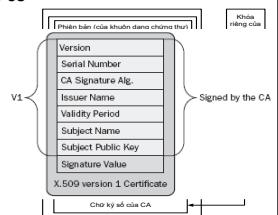
16 September 2021 | Page 181



Xác thực và chữ ký số

Một số nội dung của chứng thư số

- Tên của CA phát hành chứng thư
- Tên của chủ thẻ chứng thư
- Thời gian hợp lệ
- Khoá công khai của chủ thẻ
-
- Chữ ký số của CA cho chứng thư
- ...



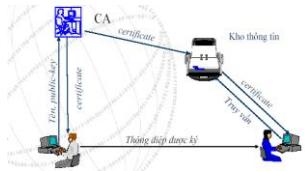
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

16 September 2021 | Page 181



Xác thực và chữ ký số

Quy trình cấp phát và sử dụng chứng thư



- Người sử dụng gửi yêu cầu tới nhà cung cấp chứng thư
- Nhà cung cấp chứng thư tạo chứng thư và gửi lại cho người dùng
- Chứng thư đã được ký bằng khoá riêng của nhà cung cấp chứng thư

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

16 September 2021 | Page 182

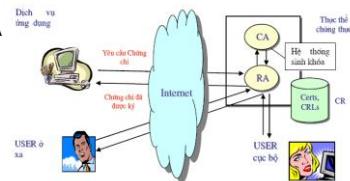


Xác thực và chữ ký số

Mô hình hệ thống chứng thực đơn giản

Một số giải pháp

- EJBCA, Window CA
- OpenCA,....



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

16 September 2021 | Page 181



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

16 September 2021 | Page 183