HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NHẬP MÔN MẬT MÃ HỌC

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NỘI DUNG

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

CHƯƠNG 03
CÁC HỆ MẬT KHÓA CÔNG KHAI

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

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.

Bài 01. Bổ túc cơ sở toán học

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

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.

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 ord(G) hoặc |G|; cấp của phần tử a là ord(a) hoặc |a|.

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)

Một số kiến thức toán học

- **Vành: Cho một tập R ≠ ∅ 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**

Một số kiến thức toán học

- Trường là một tập hợp F với hai phép toán cộng và nhân, thoả mãn tính chất sau:
  - F là một vành
  - Với phép nhân F \{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:
  - $a - b = a + (-b)$
  - $a / b = a.b^{-1}$

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:

$$a = n.q + r, 0 < r < n$$

    - *q* được gọi là thương, ký hiệu là *a* div *n*
    - *r* được gọi là số dư, ký hiệu là *a* mod *n*
  - **Định nghĩa quan hệ đồng dư trên tập số nguyên:** a ≡ b mod n khi và chỉ khi a và b có phần dư như nhau khi chia cho n.

Một số kiến thức toán học

- **Ví dụ:**
  - 100 mod 11 = 1;
  - 34 mod 11 = 1,
  - ⇒ 100 ≡ 34 mod 11
- **Đại diện của a mod n:** Số b được gọi là đại diện của a theo mod n, nếu
  - a ≡ b mod n (hay a = qn + b) và 0 ≤ b < n.
  - **Ví dụ:** -12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7 ≡ 9 mod 7.
    ⇒ 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, …, n-1 }.

…						
-21	-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	11	18	19	20
21	22	23	24	25	26	27
…						

Các phần tử cùng cột đều đồng dư với 3 mod 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) mod n = [a mod n + b mod n] mod n (*)

(a.b) mod n = [a mod n . b mod n] mod n (**)

- 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, …, n-1 }.

Một số kiến thức toán học

- Z_n với các phép toán theo Modulo tạo thành vành 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) ≡ (a+c) mod n, thì b ≡ c mod n
  - Nhưng (ab) ≡ (ac) mod n, thì b ≡ c mod n chỉ khi nếu a là nguyên tố cùng nhau với n
- **Ví dụ: Tính (11*19 + 10^{17}) mod 7 = ?**

Một số kiến thức toán học

- **Giải:**
  - Áp dụng các tính chất của modulo, ta có:
    - $(11 * 19 + 10^{17}) \bmod 7$
    - $= ((11 * 19) \bmod 7 + 10^{17} \bmod 7) \bmod 7$
    - $= ((11 \bmod 7 * 19 \bmod 7) \bmod 7 + (10 \bmod 7)^{17}) \bmod 7$
    - $= ((4 * 5) \bmod 7 + (((3^2)^2)^2)^2 * 3 \bmod 7) \bmod 7$
    - $= (6 + ((2^2)^2)^2 * 3 \bmod 7) \bmod 7$
    - $= (6 + 4 * 3) \bmod 7 =$ **4**
- **Bài tập: Tính 11^{207} mod 13 = ?**

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 gcd(a,b) là ước số chung lớn nhất của a và b
    - Ví dụ: gcd(12, 18) = 6, gcd(-18, 27) = 9, gcd(7,15) = 1
    - Với mọi a ta có gcd(a, 0) = a
    - Ta cũng quy ước gcd(0, 0) = 0

Một số kiến thức toán học

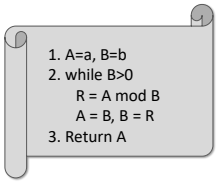
- **Số nguyên tố:**
  - Số nguyên a > 1 được gọi là số nguyên tố, nếu a không có ước số nào khác ngoài 1 và chính a.
- **Nguyên tố cùng nhau:**
  - Hai số a và b được gọi là nguyên tố cùng nhau nếu chúng không có ước chung nào khác 1, tức là gcd(a,b)=1.
  - **Ví dụ:** gcd(8,15) = 1, tức là 8 và 15 là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

Một số kiến thức toán học

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

Một số kiến thức toán học

- **Thuật toán Euclide tìm GCD(a, b):**



- **Tính GCD(1970, 1066)?**

Một số kiến thức toán học

- **Giải:**

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	
gcd(1970, 1066) = 2	

Một số kiến thức toán học

- **Thuật toán Euclide mở rộng:**
  - Nếu 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 Euclide mở rộng.
  - Điều cần và đủ để có nghịch đảo là d = 1 và khi đó x là nghịch đảo của a mod b và y là nghịch đảo của b mod a
  - Ta mở rộng thuật toán Euclide:
    - Tìm ước chung lớn nhất của a và b,
    - Tính nghịch đảo trong trường hợp GCD(a, b) = 1.

Một số kiến thức toán học

Thuật toán Euclide mở rộng

Input: Hai số nguyên dương a, b (a ≥ b)
Output: d = gcd(a, b) và số nguyên x, y thỏa mãn ax + by = d

1. If b = 0 then d ← a, x ← 1, y ← 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. $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a - qb, \quad x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$
   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 ← a, x ← x_2, y ← y_2
5. Return(d, x, y)

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

Một số kiến thức toán học

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

- a = 1759, b = 550

d = 1, x ← -111, y ← 355

1759x + 550y = 1
Hay $550^{-1} \bmod 1759 = 355$
$1759^{-1} \bmod 550 = -111$

Một số kiến thức toán học

- **Bài tập áp dụng:**
  - Tìm các nghịch đảo sau (nếu có)
    - $127^{-1} \bmod 319 = ?$
    - $254^{-1} \bmod 1028 = ?$
    - $1031^{-1} \bmod 3713 = ?$
    - $508^{-1} \bmod 819 = ?$
    - $9773^{-1} \bmod 7079 = ?$

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

Một số kiến thức toán học

- Một trong những bài toán cơ bản của số học là **phân tích ra thừa số** nguyên tố số a, 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 **duy nhất** thành tích các lũy thừa của các số nguyên tố.
  - **Ví dụ:** 51 = 3 x 17; 3600 = $2^4 \times 3^2 \times 5^2$

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 GCD(18, 300) = $2^1 \times 3^1 \times 5^0 = 6$

Một số kiến thức toán học

- **Định lý Fermat (Định lý Ferma nhỏ)**

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

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 Ferma ta có:
    - $2^{7-1} \bmod 7 = 1$ (= $2^6 \bmod 7 = 64 \bmod 7 = 1$)
    - $3^{5-1} \bmod 5 = 1$ (= $3^4 \bmod 5 = 81 \bmod 5 = 1$)

Một số kiến thức toán học

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

Một số kiến thức toán học

- **Các tính chất của hàm ϕ(n):**
  - Dễ dàng thấy, nếu p là số nguyên tố Φ(p) = p-1
  - Nếu gcd(m, n) = 1, thì: Φ(m.n) = Φ(m).Φ(n)
  - Nếu n = $p_1^{e1} \ldots p_k^{ek}$ là phân tích ra thừa số nguyên tố của n thì:

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

Một số kiến thức toán học

- **Ví dụ:**
  - Tính $\phi(37)$; $\phi(25)$; $\phi(18)$; $\phi(21)$?

$\phi(37) = 37 - 1 = 36$

$\phi(25) = \phi(5^2) = 20$

$\phi(18) = \phi(2).\phi(9) = 1.\phi(3^2) = 6$

$\phi(21) = \phi(3).\phi(7) = 2.6 = 12$

Một số kiến thức toán học

- **Định lý Ole:** Định lý Ole là tổng quát hoá của Định lý Fermа

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

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

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

Một số kiến thức toán học

- **Định nghĩa:**
  - Nhóm nhân của Z_n là $Z_n^* = \{a \in Z_n | (a, n) = 1\}$
  - Cấp của Z_n^* là số các phần tử trong Z_n^*. KH: $|Z_n^*|$
  - 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 $r \equiv s \bmod \phi(n)$ thì $a^r \equiv a^s \bmod n$; $\forall a$
- **Định nghĩa cấp của phần tử:**
  - Cho $a \in Z_n^*$. Cấp a kí hiệu ord(a) là số nguyên dương nhỏ nhất t sao cho: $a^t \equiv 1 \bmod n$ (t>0)
  - **Lưu ý:** Cho $a \in Z_n^*$, ord(a) = t và $a^s \equiv 1 \bmod n$ khi đó t là ước của s. Đặc biệt $t | \phi(n)$

Một số kiến thức toán học

- **Ví dụ:**
  - Tính cấp của các phần tử trong Z_{20}^*?
    - Ta có $n = 20 = 2^2.5$; $\phi(20) = 8 = |Z_{20}^*|$
    - $Z_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

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

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:

$$Z_n^* = \{\alpha^i \bmod n | \ 0 \le i \le \phi(n) - 1\}$$

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

Một số kiến thức toán học

Tính chất phần tử sinh

1. Z_n^* có phần tử sinh nếu và chỉ nếu $n = 2, 4, p^k$ hoặc $2.p^k$. Trong đó p là số nguyên tố lẻ và $k \ge 1$.
2. Nếu α là một phần tử sinh của Z_n^* thì: $Z_n^* = \{\alpha^i \bmod n | \ 1 \le i \le \phi(n) - 1\}$
3. Giả sử α là một phần tử sinh của Z_n^*. Khi đó: **$b = \alpha^i \bmod n$** cũng là phần tử sinh của Z_n^* nếu và chỉ nếu $\gcd(i, \phi(n)) = 1$.
   Nếu Z_n^* là xyclic thì số phần tử sinh là $\phi(\phi(n))$
4. $\alpha \in Z_n^*$ là phần tử sinh Z_n^* nếu và chỉ nếu $\alpha^{\phi(n)/p_i} \neq 1 \bmod n$ đối với mỗi nguyên tố của $\phi(n)$

Một số kiến thức toán học

- **Ví dụ:**

  (1) Z_{25}^* là nhóm xyclic 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}^*.

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 $\phi(37) = 36$; $p - 1 = 36 = 2^2 . 3^2$
    - Tìm phần tử sinh nhỏ nhất thoả mãn:

      $$\begin{cases} x^{36/2} \bmod 37 \neq 1 \\ x^{36/3} \bmod 37 \neq 1 \end{cases} \quad \text{với } x \in Z_{37}^* \quad (*)$$

    - 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 $(i, \phi(37)) = 1$ 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}

Một số kiến thức toán học

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

Một số kiến thức toán học

- **Định lí phần dư Trung Hoa**

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

$$\begin{aligned} x &\equiv a_1 (\bmod n_1) \\ x &\equiv a_2 (\bmod n_2) \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a_k (\bmod n_k) \end{aligned}$$

Một số kiến thức toán học

- **Giải hệ phương trình modulo:**
  - Cho :

    $x \equiv a_1 \bmod n_1$
    $x \equiv a_2 \bmod n_2$
    $\ldots$
    $x \equiv a_k \bmod n_k$

  - Với GCD(n_i, n_j) = 1, $\forall$ i ≠ 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:

    $$x = \left(\sum_{i=1}^{k} a_i N_i M_i \right) \bmod N$$

  - Trong đó: $N = n_1 \ldots n_k$; $N_i = N/n_i$; $M_i = N_i^{-1} \bmod n_i$.

Một số kiến thức toán học

- **Ví dụ giải hệ phương trình:**
  - x ≡ 10 mod 11
    x ≡ 19 mod 21
    x ≡ 20 mod 26

    X ≡ 670 mod 6006

  - x ≡ 7 mod 9
    x ≡ 4 mod 10
    x ≡ 15 mod 23

    X ≡ 1924 mod 2070

Một số kiến thức toán học

- **Định lý:**
  - Nếu (n_1, n_2) = 1 thì cặp phương trình đồng dư:

    $x \equiv a \bmod n_1$

    $x \equiv a \bmod n_2$

    Có nghiệm duy nhất $x \equiv a \bmod n_1.n_2$

Một số kiến thức toán học

- **Định nghĩa thặng dư bậc hai và bất thặng dư bậc hai:**
  - Cho $a \in Z_n^*$, a được gọi là thặng dư bậc hai theo modulo n (hay bình phương modulo n) nếu $\exists x \in Z_n^*$: $x^2 \equiv a \bmod n$. 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 Z_p^*. Khi đó $a \in Z_p^*$ là một thặng dư bậc hai modulo p nếu và chỉ nếu $a = \alpha^i \bmod p$ với i là số nguyên chẵn
- **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 Z^*_{17}.
  - Tìm Q_{17}, $\bar{Q}_{17}$

Một số kiến thức toán học

i	0	2	4	6	8	10	12	14
$\alpha^i \bmod 17$	1	9	13	15	16	8	4	2

- Vậy Q_{17} = {1, 2, 4, 8, 9, 13, 15, 16}

  $\overline{Q_{17}}$ = {3, 5, 6, 7, 10, 11, 12, 14}

Một số kiến thức toán học

- **Định lý:**
  - Cho n = p.q, với p, q là hai số nguyên tố, $p \neq q$. Khi đó $a \in Z^*_n$ 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 $x \in Z^*_n$. thỏa mãn $x^2 = a \bmod n$ 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 $n = p_1^{e_1}.p_2^{e_2} \dots p_k^{e_k}$, 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 mod 15? 1 mod 15?**
  - Căn bậc hai của 4 mod 15 là: 2, 13, 7, 8
  - Căn bậc hai của 1 mod 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 (T37)

Một số kiến thức toán học

- **Định nghĩa:**
  - Cho n ≥ 3 là các số nguyên lẻ có phân tích:

$$n=p_1^{e_1}.p_2^{e_2}\dots p_k^{e_k}$$

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

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

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

1	Nếu n là số nguyên lẻ và $m_1 \equiv m_2 \bmod n$ thì: $\left(\frac{m_1}{n}\right)=\left(\frac{m_2}{n}\right)$
2	Nếu n là số nguyên lẻ thì: $\left(\frac{2}{n}\right)=\begin{cases}1 & nếu\ n\equiv\pm1\ mod\ 8\\ -1 & nếu\ n\equiv\pm3\ mod\ 8\end{cases}$
3	Nếu n là số nguyên lẻ thì: $\left(\frac{m_1.m_2}{n}\right)=\left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$ Đặc biệt nếu $m=2^k.t$ (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 số nguyên lẻ thì: $\left(\frac{m}{n}\right)=\begin{cases}-\left(\frac{n}{m}\right) & nếu\ m,n\equiv3 mod\ 4\\ \left(\frac{n}{m}\right) & TH\ còn\ lại\end{cases}$

Một số kiến thức toán học

- **Bài tập áp dụng:**
  - Tính ký hiệu Jacobi:
    - A) $\left(\frac{7411}{9283}\right)$
    - B) $\left(\frac{6278}{9975}\right)$

Một số kiến thức toán học

- **Giải:**
  - **A)**

$$\left(\frac{7411}{9283}\right)\overset{(4)}{=}-\left(\frac{9283}{7411}\right)\overset{(1)}{=}-\left(\frac{1872}{7411}\right)\overset{(3)}{=}-\left(\frac{2}{7411}\right)^4.\left(\frac{117}{7411}\right)$$

$$\overset{(2)}{=}-(1)^4.\left(\frac{117}{7411}\right)\overset{(4)}{=}-\left(\frac{7411}{117}\right)\overset{(1)}{=}-\left(\frac{40}{117}\right)\overset{(3)}{=}-\left(\frac{2}{117}\right)^3.\left(\frac{5}{117}\right)$$

$$=-(-1)^3.\left(\frac{5}{117}\right)=\left(\frac{117}{5}\right)=\left(\frac{2}{5}\right)=-1$$

Một số kiến thức toán học

- **B) Ta có:** $\left(\frac{a}{m.n}\right)=\left(\frac{a}{m}\right).\left(\frac{a}{n}\right)$

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

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

$$=-(1)$$

Bài 02. Một số kiến thức toán học

- **Số nguyên Blum:**
  - Là một hợp số có dạng n = p.q trong đó p, q là các số nguyên tố khác nhau thỏa mãn: $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$.
- **Định lý:**
  - Cho n = p.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 mod n

Một số kiến thức toán học

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

Một số kiến thức toán học

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

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

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

Một số kiến thức toán học

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

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

Một số kiến thức toán học

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

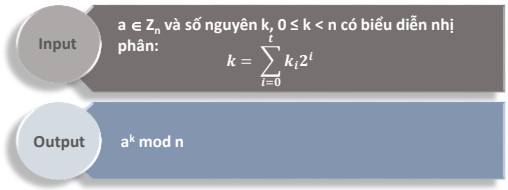
1. Dùng thuật toán Euclide mở rộng tìm a, b: ap + bq = 1
2. Tính:
   - $r = c^{(p+1)/4} \bmod p$
   - $s = c^{(q+1)/4} \bmod q$
   - x = (aps + bqr) mod n
   - y = (aps - bqr) mod n
3. Return $(\pm x, \pm y)$

Thuật toán 4: Tìm căn bậc hai của a mod p, p là số nguyên tố
Input: Số nguyên tố lẻ p, số nguyên a, $1 \le a \le p - 1$
Output: 2 căn bậc hai của a mod p nếu $a \in Q_p$

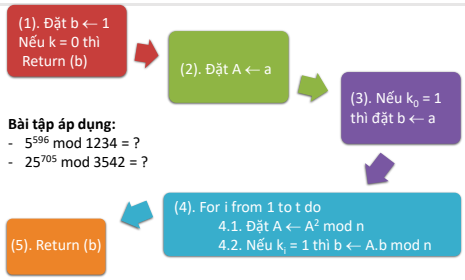
1. Tính kí hiệu $\left(\frac{a}{p}\right)$ nếu $\left(\frac{a}{p}\right)$ = -1 thì Return "a không có căn bậc hai theo mod p
2. Chọn số nguyên b: $1 \le b \le p - 1$ sao cho: $\left(\frac{b}{p}\right)$ = -1 (tức $b \notin Q_p$)
3. Phân tích: $p - 1 = 2^s . t$ (t là số lẻ)
4. Tính $a^{-1} \bmod p$
5. Đặt $c \leftarrow b^t \bmod p$; $r \leftarrow a^{(t+1)/2} \bmod p$
6. 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 $d \equiv -1 \bmod p$ thì đặt $r \leftarrow r.c \bmod p$
   - 6.3. $c \leftarrow c^2 \bmod p$
7. Return (r, -r)

Một số kiến thức toán học

- **Thuật toán nhân bình phương có lặp**



Một số kiến thức toán học



Bài tập áp dụng:
- 5^{596} mod 1234 = ?
- 25^{705} mod 3542 = ?

Một số kiến thức toán học

- **Tính 5^{596} mod 1234 = ?**
  - Ta có 596 = 2^9 + 2^6 + 2^4 + 2^2. Áp dụng tt nhân bình phương có lặp ta có bảng sau:

i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
b	1	1	625	625	67	67	1059	1059	1059	1013

  - Vậy 5^{596} mod 1234 = 1013

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 ≠ 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.

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 ∈ Z_{19}^*.**
  - Ta có bảng tính:

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

$\log_2 7$ = ?
$\log_2 15$ =?

  - $\log_2 7 = \log_2 2^6 = 6.\log_2 2 = 6$; $\log_2 15 = \log_2 2^{11} = 11.\log_2 2 = 11$;

Giới thiệu một số hệ mật KCK

- **$\log_2 x$ với mọi x ∈ 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

Thuật toán:
Bước lớn bước nhỏ

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 $m = \lceil\sqrt{ord(\alpha)}\rceil$
2. Lập bảng (j, α^j mod n) với $j = \overline{0 \to m-1}$
3. Tính $\beta.(\alpha^{-m})^i$ mod n với $i = \overline{0 \to m-1}$
4. Tra bảng (j, α^j) cho tới khi thỏa mãn $\beta.(\alpha^{-m})^i = \alpha^j$
5. Khi đó: $\log_\alpha\beta = m.i + j$

Giới thiệu một số hệ mật KCK

- **Bài tập áp dụng:**
  - Cho α = 31 là phần tử sinh của Z_{61}^*. Hãy tìm $\log_{31}45$ trên Z_{61}^*.
  - Cho α = 17 là phần tử sinh của Z_{97}^*. Hãy tìm $\log_{17}15$ trên Z_{97}^*.

Giới thiệu một số hệ mật KCK

- **Giải: Tìm $\log_{31}$ 45 trên Z_{61}^***
  - Ta có: $m = \lceil\sqrt{ord(31)}\rceil = \lceil\sqrt{60}\rceil = 8$
  - Ta lập bảng (j, 31^j) với $j = \overline{0 \to 7}$

Log_{31} 45 = mi + j
= 8.3 + 2 = **26**

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

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

i	0	1	2	3	4	5	6	7
45. 12^i mod 61	45	52	14	46	3	36	5	60

CHƯƠNG 3. CÁC HỆ MẬT KCK

Nội dung các bài học trong chương 03

Bài 03. Bài tập áp dụng

- **1) Dùng thuật toán Euclide tìm phần tử nghịch đảo:**
  - 357^{-1} mod 1137
  - 213^{-1} mod 1577
- **2) Giải hệ phương trình:**

$$\begin{cases} 5x \equiv 13 \ mod\ 17 \\ 4x \equiv 39 \ mod\ 53 \\ 7x \equiv 9 \ mod\ 19 \end{cases}$$

- **3) Tính ϕ(490); ϕ(768)**

Bài 03. Bài tập áp dụng

- **4)** Dùng thuật toán Euclide mở rộng tìm UCLN của 1573, 308. Tìm cặp x, y thỏa mãn: 1573x+308y = 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

Bài 03. Bài tập áp dụng

- **Chữa bài tập**

CHƯƠNG 3. CÁC HỆ MẬT KCK

Nội dung các bài học trong chương 03

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?

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 bất kì. Trên thực tế điều này rất khó đảm bảo.
  - Ý tưởng về một hệ mật khoá 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…

Giới thiệu một số hệ mật KCK

- **Hệ mật RSA, Rabin:**
  - Độ an toàn của hệ RSA và Rabin 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).

Giới thiệu một số hệ mật KCK

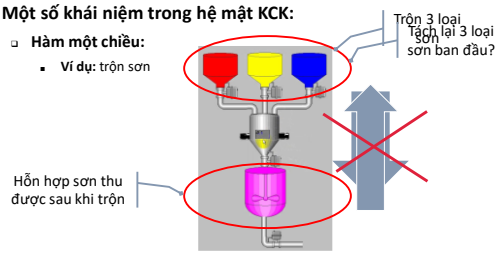
- **Hệ mật ElGamal:**
  - Hệ mật ElGamal dựa trên tính khó giải của bài toán logarithm rời rạc trên các trường hữu hạn
- **Hệ mật trên các đường cong Elliptic:**
  - Các hệ mật này là biến thể của các hệ mật khác (chẳng hạn như hệ mật ElGamal), chúng làm việc trên các đường cong Elliptic chứ không phải 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.

Giới thiệu một số hệ mật KCK

- Một chú ý quan trọng là một hệ mật khoá 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

Giới thiệu một số hệ mật KCK

- **Một số khái niệm trong hệ mật KCK:**
  - **Hàm một chiều:**
    - **Ví dụ:** trộn sơn



Giới thiệu một số hệ mật KCK

- **Một số khái niệm trong hệ mật KCK:**
  - **Đặc tính một chiều:** Hàm mã khoá 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.q, trong đó p, q là các số nguyên tố lớn, giả sử b là một số nguyên dương.
      - Khi đó hàm $f(x) = x^b \bmod n$ là một hàm một chiều.
  - **Hàm cửa sập một chiều:** thông tin bí mật cho phép Bob dễ dàng tìm hàm của e_k.

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

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 ⇒ 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 ⇒ mất 500 phút ⇔ **hơn 8 giờ** để tìm ra p, q
  - Nếu biết trước giá trị p = 18.313 và q = 22.307 ⇒ mất chưa tới **10s** để tính ra N

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	$1,4.\ 10^{10}$	3,9 giờ
75	$9.\ 10^{12}$	104 ngày
100	$2,3.\ 10^{15}$	74 năm
200	$1,2.\ 10^{23}$	$3,8.10^{9}$ năm
300	$1,5.\ 10^{29}$	$4,9.10^{15}$ năm
500	$1,3.\ 10^{39}$	$4,2.10^{25}$năm

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.

Giới thiệu một số hệ mật KCK

- **Sơ đồ chung của hệ mật khóa công khai được cho bởi**

$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ (1)

  - Mỗi khóa $k \in \mathcal{K}$ 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.q
  - Chọn một số e sao cho gcd(e, ϕ(n))= 1 và tính số d sao cho: e.d $\equiv$1 mod ϕ(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):**

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

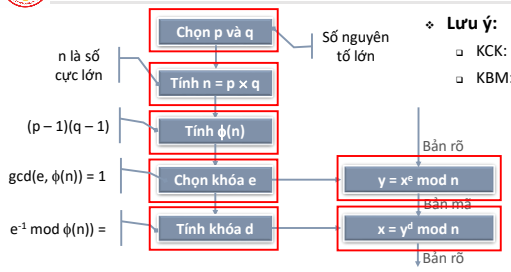
$\mathcal{K}$ = {k=(k_e, k_d) với k_e = (n, e); k_d = d sao cho gcd(e, ϕ(n)) = 1, e.d $\equiv$ 1 mod ϕ(n)}

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

$$y = E_{k_e}(x) = x^e \bmod n \qquad \forall x \in \mathcal{P}$$

$$x = D_{k_d}(y) = y^d \bmod n \qquad \forall y \in \mathcal{C}$$

Giới thiệu một số hệ mật KCK



- **Lưu ý:**
  - KCK: k_E = (n, e)
  - KBM: k_D = d

Giới thiệu một số hệ mật KCK

- **Ví dụ: Cho hệ mật RSA với p = 37, q = 41 và số mũ mã hoá e = 211.**
  - Hãy tính số mũ giải mã d.
  - Hãy mã hoá bản tin x = 47 và giải mã bản mã vừa thu được.

Giới thiệu một số hệ mật KCK

- **Giải:**
  - Ta có: n = p.q = 37. 41 = 1517
  - Φ(n) = 36. 40 = 1440.
  - Ta có: ed $\equiv$ 1 mod Φ(n)
  - $\Rightarrow$ Tính $d = e^{-1} \bmod \Phi(n)$
  - $\Leftrightarrow$ tính $211^{-1} \bmod 1440$ =?

Giới thiệu một số hệ mật KCK

Tính $211^{-1} \bmod 1440$?

Số mũ giải mã:
d = - 389 mod 1440
⇔ **d = 1051**

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	1440	211	1	0	0	1
6	174	1	-6	211	174	0	1	1	-6
1	37	-1	7	174	37	1	-1	-6	7
4	26	5	-34	37	26	-1	5	7	-34
1	11	-6	41	26	11	5	-6	-34	41
2	4	17	-116	11	4	-6	17	41	-116
2	3	-40	273	4	3	17	-40	-116	273
1	1	57	-389	3	1	-40	57	273	-389
1	0	-97	662	1	0	57	-97	-389	662

Giới thiệu một số hệ mật KCK

- **Để mã hóa bản tin x = 47 ta tính $y = x^e \bmod n = 47^{211} \bmod 1517$**
  - Phân tích $211 = 2^7 + 2^6 + 2^4 + 2^1 + 2^0$. Áp dụng phương pháp nhân bình phương có lặp ta có bảng tính sau:

i	0	1	2	3	4	5	6	7
k_i	1	1	0	0	1	0	1	1
A	47	692	1009	174	1453	1062	713	174
b	47	667	667	667	1305	1305	544	**602**

  - Vậy bản mã thu được là $y = 47^{211} \bmod 1517 = 602$

Giới thiệu một số hệ mật KCK

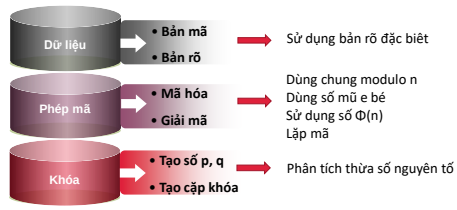
- **Để giải mã bản mã y = 602, ta tính $x = y^d \bmod n = 602^{1051} \bmod 1517$**
  - Ta phân tích: $1051 = 2^{10} + 2^4 + 2^3 + 2^1 + 2^0$. Áp dụng phương pháp nhân bình phương có lặp ta có bảng tính sau:

i	0	1	2	3	4	5	6	7	8	9	10
k_i	1	1	0	1	1	0	0	0	0	0	1
A	602	1358	1009	174	1453	1062	713	174	1453	1062	713
b	602	1370	1370	211	149	149	149	149	149	149	**47**

  - Vậy bản rõ $x = 602^{1051} \bmod 1517 = 47$

Giới thiệu một số hệ mật KCK

- **Độ an toàn của hệ mật RSA**



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.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))
    - VD: KCK (n, e) = (35, 17); m = 8. Khi đó bản mã $c = 8^{17} \bmod 35 = 8$
      ⇒ mã hóa thông báo = thông báo ban đầu
    - Với n = 33, e = 3 ⇒ có bao nhiêu điểm bất động?

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**
    - $\mathcal{P} = Z_n$; $\mathcal{C} = Z_n$
    - $\mathcal{K}$ = {k=(k_e, k_d): k_e = n, k_d = (p, q), n = p.q}
    - Hàm mã hóa e và giải mã d được xác định như sau:
      - Với mỗi x ∈ P, để lập mã cho x ta tính $y = e_{k_e}(x, k) = x^2 mod\ n$
      - Hàm giải mã: $x = d_{k_d}(y)$ trong đó $d_{k_d}(y)$ là hàm tính căn bậc hai của y mod 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.q = 437
    - ⇒ 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

- **Giải:**
  - Ta có x = $101001001_2 = 329_{10}$
  - Bản mã y = x^2 mod n = 329^2 mod 437 = 302
  - Để giải mã y ta tìm căn bậc hai của 302 mod 437
    - Trước hết ta tìm (a, b): 19a + 23b = 1

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	23	19	1	0	0	1
1	4	1	-1	19	4	0	1	1	-1
4	3	-4	5	4	3	1	-4	-1	5
1	1	5	-6	3	1	-4	5	5	-6
3	0	-19	23	1	0	5	-19	-6	23

⇒ a = - 6; b = 5

Giới thiệu một số hệ mật KCK

- **Tính r = 302^5 mod 19 = 6; s = 302^6 mod 23 = 16**
- **Tính:**
  - x = (aps + bqr) mod n = (-6).19.16 + 5.23.6 mod 437 = -260 = 177 mod 437
  - y = (aps - bqr) mod n = (-6).19.16 - 5.23.6 mod 437 = -329 = 108 mod 437
- **4 nghiệm căn bậc hai 302 mod 437 là (177; 260, 108, 329)**
- **Dãy nhị phân tương ứng:**
  - x_1 = 177 = 10110001; x_2 = 260 = 100000100;
  - x_3 = 108 = 1101100; x_4 = 329 = 101**001** **001**;

Giới thiệu một số hệ mật KCK

- **Đánh giá hiệu quả**
  - Thuật toán mã hoá 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 hoá, tuy nhiên về mặt tốc độ nó cung tương đương với thuật toán giải mã RSA.

Giới thiệu một số hệ mật KCK

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

Giới thiệu một số hệ mật KCK

- **Ví dụ:** Sử dụng hệ mật Elgamal với số nguyên tố p = 211, phần tử sinh α = 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.

Giới thiệu một số hệ mật KCK

- **Giải:**
  - Ta tính α^a mod 211 = 39^{113} mod 211. Ta phân tích 113 = $2^6 + 2^5 + 2^4 + 2^0$. Áp dụng phương pháp nhân và bình phương có lặp ta có bảng giá trị sau:

i	0	1	2	3	4	5	6
k_i	1	0	0	0	1	1	1
A	39	44	37	103	59	105	53
b	39	39	39	39	191	10	**108**

  - Vậy KCK của A là **(p, α, α^a) = (211, 39, 108)**

Giới thiệu một số hệ mật KCK

- Tính $y_1 = \alpha^k$ mod p = 39^{23} mod 211. Phân tích 23 = $2^4 + 2^2 + 2^1 + 2^0$. Áp dụng phương pháp nhân bình phương có lặp ta có bảng tính sau:

i	0	1	2	3	4
k_i	1	1	1	0	1
A	39	44	37	103	59
b	39	28	192	192	**145**

- Vậy: y_1 = 145

Giới thiệu một số hệ mật KCK

- Tính $y_2 = x.(\alpha^a)^k$ mod 211 = 34.$(108)^{23}$ mod 211. Trước hết ta tính $(108)^{23}$ mod 211 =?. Áp dụng phương pháp nhân bình phương có lặp ta có bảng sau:

i	0	1	2	3	4
k_i	1	1	1	0	1
A	108	59	105	53	66
b	108	42	190	190	**91**

- Khi đó $\delta = m(\alpha^a)^k$ mod 211 = 34. 91 mod 211 = 140
- Vậy bản mã **y = (y_1, y_2) = (145, 140)**

Giới thiệu một số hệ mật KCK

- **Giải mã y = (y_1, y_2) = (145, 140).**
  - Ta tính $(y_1^a)^{-1}\ mod\ p = y_1^{p-1-a}$ mod 211 = $145^{211-1-113}$ mod 211 = 145^{97} mod 211. Ta phân tích 97 = $2^6 + 2^5 + 2^0$

i	0	1	2	3	4	5	6
k_i	1	0	0	0	0	1	1
A	145	136	139	120	52	172	44
b	145	145	145	145	145	42	**160**

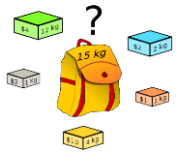
  - Khôi phục bản rõ x bằng cách tính **x = y_2. y_1^{p-1-a} = 140. 160 mod 211 = 34**

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 $a_1, a_2, ..., a_n$ và một tổng S. Tính giá trị v_i để cho:

$S = v_1a_1 + v_2a_2 + ... + v_na_n$ với $v_i \in \{0,1\}$



  - **Ví dụ:**
    - Cho S = 53, dãy số nguyên (17, 38, 73, 4, 11, 1)

Giới thiệu một số hệ mật KCK

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

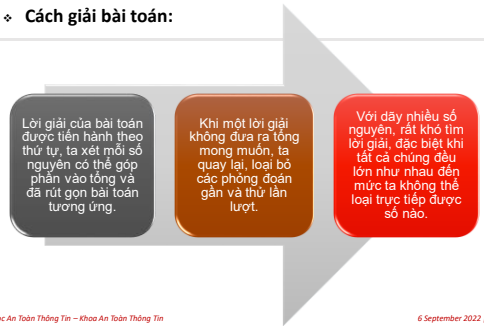
Loại 73, vì 73 > 53

Thử 17, S = 53 – 17 = 36, Loại 38, nhưng 4 + 11 + 1 < 36. Vậy 17 không có trong lời giải

Thử 38, S = 53 – 38 = 15, thấy tổng số hạng còn lại 4 + 11 = 15.
Vậy lời giải: **S = 53 = 38 + 4 + 11**

Giới thiệu một số hệ mật KCK

- **Cách giải bài toán:**



Giới thiệu một số hệ mật KCK

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

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

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

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

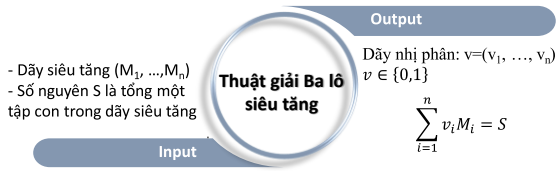
Giới thiệu một số hệ mật KCK

S = 96	73?	Yes	1
96 -73 = 23	38?	No	0
23	17?	Yes	1
23 – 17 = 6	11?	No	0
6	4?	Yes	1
6 – 4 = 2	1?	Yes	1
2 – 1 = 1	Không có lời giải		

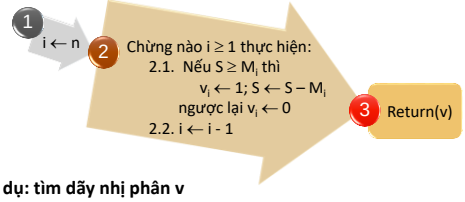
S = 95	73?	Yes	1
95 -73 = 22	38?	No	0
22	17?	Yes	1
22 – 17 = 5	11?	No	0
5	4?	Yes	1
5 – 4 = 1	1?	Yes	1
1 – 1 = 0	Có lời giải		

Giới thiệu một số hệ mật KCK

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



Giới thiệu một số hệ mật KCK



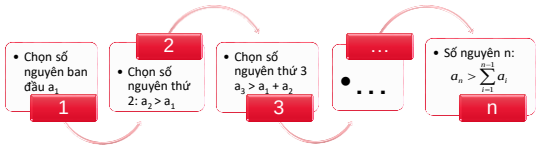
- **Ví dụ: tìm dãy nhị phân v**
  - (1) Cho dãy siêu tăng (12, 17, 33, 74, 157, 316, 620, 1230, 2460); tổng S = 4401
  - (2) Cho dãy siêu tăng (5, 7, 13, 30, 57, 116, 230, 460, 920); tổng S = 1508

Giới thiệu một số hệ mật KCK

- **Hệ mật Merkle – Hellman:**
  - **Kĩ 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.

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:



Giới thiệu một số hệ mật KCK

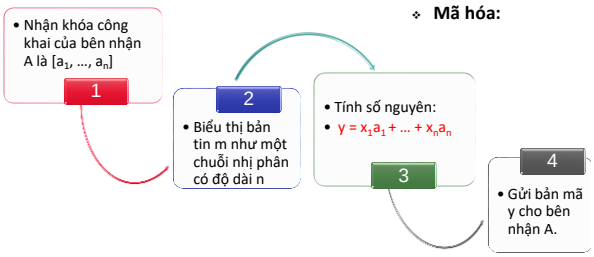
- **Để xây dựng hệ mật Merkle – Hellman**
  - Chọn n là tham số chung
  - Chọn dãy siêu tăng: $M_1, \ldots, M_n$
  - Chọn số modulo M: $M > M_1, \ldots, M_n$
  - Chọn số nguyên ngẫu nhiên W: $1 \le W \le M - 1$ và (W, M) = 1
  - Chọn phép hoán vị π của các số nguyên {1, 2, …,n}
  - Tính $\mathbf{a_i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

Giới thiệu một số hệ mật KCK

- **Sơ đồ chung của hệ mật Merkle – Hellman:**
  - $\mathcal{P} = (Z_2)^n$, $\mathcal{C} = Z_M$
  - $\mathcal{K}$ = {k=(k_e, k_d) với k_e = ($a_1, \ldots, a_n$); k_d = (π, M, W($M_1, \ldots, M_n$)}
  - Hàm mã hóa e và giải mã d được xác định như sau:
    - Với mỗi x = ($x_1, x_2, \ldots, x_n$) ∈ $\mathcal{P}$, để lập mã cho x ta tính
      $$y = e_{k_e}(x) = x_1a_1 + x_2a_2 + \cdots + x_na_n$$
    - Hàm giải $x = d_{k_d}(y) = (v_{\pi_{(1)}}, \ldots, v_{\pi_{(n)}}) = (x_1, x_2, \ldots, x_n)$ .Trong đó $v_{\pi_{(i)}}$ thu được khi giải bài toán xếp ba lô cho dãy siêu tăng: $d = v_1M_1 + v_2M_2 + \cdots + v_nM_n$ với $d = W^{-1} . y \bmod M$

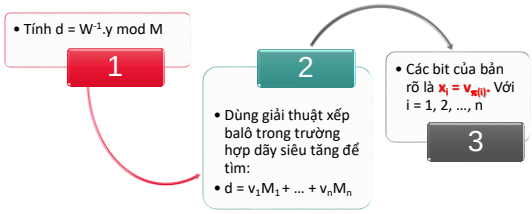
Giới thiệu một số hệ mật KCK

- **Mã hóa:**



Giới thiệu một số hệ mật KCK

- **Giải mã:**



Giới thiệu một số hệ mật KCK

- **Bài tập:**
  - Cho n = 6, dãy 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: π(1) = 3, π(2) = 6, π(3) = 1, π(4) = 2, π(5) = 5, π(6) = 4
  - **Thực hiện mã hóa bản tin m = 101101, và giải mã ngược lại từ bản mã vừa thu được.**

Giới thiệu một số hệ mật KCK

- **Giải:**
  - Tính $a_i = WM_{\pi(i)} \bmod M$, khi đó ta thu được dãy khóa công khai (319, 196, 250, 477, 200, 559)
  - Mã hóa:
    - Để mã bản tin ta tính:

    c = 319*1 + 196*0 + 250*1 + 477*1 + 200*0 + 559*1 = 1605
    - Gửi c cho bên nhận

Giới thiệu một số hệ mật KCK

- **Giải mã:**
  - Tính $W^{-1} \bmod M = 635^{-1} \bmod 737 = 513$
  - Tính W^{-1} c mod M = 513*1605 mod 737 = 136.
  - Giải bài toán xếp ba lô trong trường hợp dãy siêu tăng:

    $136 = 12v_1 + 17v_2 + 33v_3 + 74v_4 + 157v_5 + 316v_6$
  - Ta nhận được: 136 = 12 + 17 + 33 + 74
  - Bởi vậy $v_1 = v_2 = v_3 = v_4 = 1$; $v_5 = v_6 = 0$
  - Sử dụng phép hoán vị π, ta sẽ tìm được các bit của bản rõ:

  $m_1 = v_3 = 1$, $m_2 = v_6 = 0$, $m_3 = v_1 = 1$, $m_4 = v_2 = 1$, $m_5 = v_5 = 0$, $m_6 = v_4 = 1$.

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 dài khoảng từ 200 – 400 chữ số. Chính xác hơn các M_i được chọn như sau:
    - $1 \le M_1 < 2^{200}$
    - $2^{200} \le M_2 < 2^{201}$
    - $2^{201} \le M_3 < 2^{202}$
    - …
  - Như vậy có xấp xỉ 2^{200} lựa chọn cho mỗi M_i.
  - Có thể dùng dãy các số ngẫu nhiên để tạo một ba lô dễ, tạo dãy n số ngẫu nhiêu $r_1, …, r_n$. 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, …, m

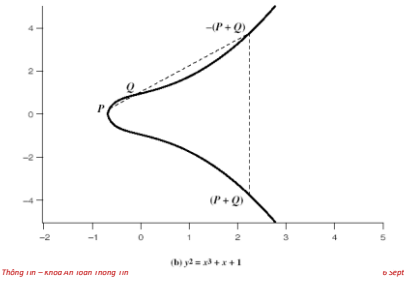
Giới thiệu một số hệ mật KCK

- 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 ($a_1, …, a_n$) 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 dường 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.

Giới thiệu một số hệ mật KCK

- **Hệ mật đường cong Eliptic**
  - **Các đường cong Eliptic:**
    - **Đường cong Elip thực:**
      - Đường cong Elip được định nghĩa bởi phương trình với 2 biến x, y và hệ số thực
      - Xét đường cong Elip 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 Elip
        - 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.

Giới thiệu một số hệ mật KCK



(b) $y^2 = x^3 + x + 1$

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 $\mathbf{E_p(a,b)}$ được xác định trên Z_p
      - Sử dụng các số nguyên modulo số nguyên tố
      - Tốt nhất trong phần mềm
    - Đường cong nhị phân $\mathbf{E_{2^n}(a,b)}$ xác định trên $GF(2^n)$
      - Sử dụng đa thức với hệ số nhị phân
      - Tốt nhất trong phần cứng

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: $y^2 = x^3 + ax + b \pmod p$, trong đó $a, b \in Z_p$ là các hằng số thỏa mãn $4a^3 + 27b^2 \neq 0 \pmod p$ cùng với một điểm đặc biệt O được gọi là điểm vô cực.

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 $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & nếu\ P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & nếu\ P = Q \end{cases}$

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)

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 $z = y^2 = x^3 + x + 6 \bmod 11$
  - **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

Giới thiệu một số hệ mật KCK

- Như vậy ta có 13 điểm trên đường cong: (2,4); (2,7); (3,5); (3,6); (5,2); (5,9); (7,2); (7,9); (8,3); (8,8); (10,2); (10,9); O

x	$z = y^2 = x^3 + x + 6 \bmod 11$	$z \in Q_{11}$?	y
0	6	Không	
1	8	Không	
2	5	Có	(4, 7)
3	3	Có	(5, 6)
4	8	Không	
5	4	Có	(2, 9)
6	8	Không	
7	4	Có	(2, 9)
8	9	Có	(3, 8)
9	7	Không	
10	4	Có	(2, 9)

Giới thiệu một số hệ mật KCK

- **BTVN:**
  - Cho đường cong elliptic trên Z_{19}:

    $y^2 = x^3 + x + 1 \bmod 19.$
  - Tìm tất cả các điểm nằm trên đường cong elliptic này.

Giới thiệu một số hệ mật KCK

- **Hệ mật đường cong Eliptic:**
  - 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 $k_e = (E_p(a,b), G, P_A)$

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: $P_M = e_{k_d}(P_c) = P_2 - n_A P_1$

Giới thiệu một số hệ mật KCK

- **Bài tập:**
  - 1) Cho $E_{17}(1,1)$; G = (0,1)
    - Khóa riêng của A, B lần lượt là: $n_A = 3$; $n_B = 4$. Tính KCK của A, B.
    - Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin P_M = (10,12) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 2.
  - 2) Cho $E_{11}(1, 6)$; G = (2,7)
    - Khóa riêng của B $n_B = 7$. Tính KCK của B.
    - Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin P_M = (10, 9) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 3.

Giới thiệu một số hệ mật KCK

- **Chữa bài tập:**
  - Câu 1)
    - $P_A = (4, 16)$; $P_B = (9, 12)$;
    - $P_C = [kG, P_M + 2P_B] = [(13, 1); (9, 5)]$;
    - $P_M = P_2 – n_B P_1 = (9, 5) – 4(13, 1) = (10, 12)$
  - Câu 2)
    - $P_B = (7,2)$
    - $P_C = [(8,3), (10,2)]$
    - Giải mã: $P_M = (10,2) – 3(7, 2) = (10,2) – (3, 5) = (10, 2) + (3, 6) = (10,9)$

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.

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 mẩu 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.

Tổng kết

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

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.