Khoa An Toàn Thông Tin
Bộ Môn: Khoa Học An Toàn Thông Tin

CHƯƠNG 3
MẬT MÃ KHOÁ CÔNG KHAI

Nội dung

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

- Hệ thống khoá công khai

GIỚI THIỆU

- Đặc điểm của hệ mật KCK:
  - Mỗi bên có một khoá công khai và một khoá bí mật.
  - Bên gửi dùng khoá công khai của bên nhận để mã hoá.
  - Bên nhận dùng khoá bí mật của mình để giải mã.

GIỚI THIỆU

- Hệ mật RSA:
  - Độ an toàn của hệ RSA dựa trên độ khó của việc phân tích số nguyên thành thừa số nguyên tố
- Hệ mật xếp ba lô Merkle - Hellman:
  - Hệ mật này dựa trên tính khó giải của bài toán tổng các tập con (Bài toán xếp ba lô – Knapsack problem. Bài toán này là bài toán NP-khó).

GIỚI THIỆU

- Hệ mật McEliece:
  - Hệ mật McEliece dựa trên tính NP- khó của bài toán giải mã đối với các hệ mã cyclic tuyến tính.
- Hệ mật ElGamal:
  - Hệ mật ElGamal dựa trên tính khó giải của bài toán logarit rời rạc.

Nội dung

Một số kiến thức toán học

- Cấu trúc đại số
- Số học modulo

Một số kiến thức toán học

- **Cấu trúc đại số:**
  - **Định nghĩa nhóm:** Tập hợp G 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)
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.

  - Số phần tử trong một nhóm được gọi là *cấp* của nhóm

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 với 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 $R \neq \emptyset$ với 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
    - 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 trừ phần tử 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 $n \mid a$
  - 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
- Số b được gọi là đại diện của a, 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:

    $Z_n = \{ 0, 1, 2, 3, \ldots, n-1 \}$.

...						
-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	17	18	19	20
21	22	23	24	25	26	27
...						

Các phần tử cùng cột đồng dư với nhau mod 7

Một số kiến thức toán học

- **Các phép toán số học trên Modulo**

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

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

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

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 ước số chung lớn nhất**:
  - **Input:** Hai số nguyên a và b, với a >= b.
  - **Output:** Ước số chung lớn nhất của a và b

Một số kiến thức toán học

- **Ví dụ: Tìm gcd(4864, 3458)**

4864 = 1. 3458 + 1406
3458 = 2. 1406 + 646
1406 = 2. 646 + 114
646 = 5. 114 + 76
114 = 1. 76 + 38
76 = 2. 38 + 0

a	*b*	*r*
4864	3458	
3458	1406	1406
1406	646	646
646	114	114
114	76	76
76	38	38
38	0	0

gcd(4864, 3458) = 38

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 sau đây (gọi là thuật toán Euclide mở rộng).

Một số kiến thức toán học

- **Phần tử nghịch đảo:**
  - Cho a ∈ Zn. Một số nguyên x∈ Zn được gọi là nghịch đảo của a theo mod n nếu ax ≡ 1 mod n.
  - a là khả nghịch theo mod n khi và chỉ khi gcd(a,n) = 1
- **Thặng dư thu gọn và phần tử nguyên thủy**
  - Tập Zn = {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 $Z_p^* = \{1, 2, \ldots, p-1\}$

Một số kiến thức toán học

- **Thặng dư thu gọn và phần tử nguyên thủy**
  - Tập Z_n^* lập thành một nhóm đối với phép nhân của Z_n, vì trong tập này phép chia theo mod n bao giờ cũng thực hiện được. Tập này được gọi là *nhóm nhân* của Z_n
  - Ký hiệu $\phi(n)$ (hàm Euler) là số phần tử nhỏ hơn n và nguyên tố cùng nhau với n. Như vậy nhóm Z_n^* có cấp là $\phi(n)$.
  - Ta nói phần từ $g \in Z_n^*$ có cấp m, nếu m là số nguyên dương bé nhất sao cho $g^m = 1$ trong Z_n^*.
  - Ta luôn có $m|\phi(n)$. Vì vậy, với mọi $b \in Z_n^*$ ta luôn có $b^{\phi(n)} \equiv 1 \bmod n$

25

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

Một số kiến thức toán học

- **Thặng dư thu gọn và phần tử nguyên thủy**
  - Cho $\alpha \in Z_n^*$, nếu $ord(\alpha) = \phi(n)$ thì **α là phần tử sinh** nhóm nhân Z_n^*.
  - Người ta đã chứng minh được rằng: Nếu $\alpha \in Z_n^*$ là phần tử sinh, khi đó $\beta = \alpha^i \bmod n$ **là** phần tử sinh khi và chỉ khi $gcd(i, \phi(n)) = 1$.
  - Nếu $\phi(n) = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ (p_i là các số nguyên tố khác nhau) thì $\alpha \neq 0$ là phần tử sinh khi và chỉ khi $\alpha^{\phi(n)/p_i} \neq 1, \forall i = 1..k$

27

Một số kiến thức toán học

- **Thặng dư thu gọn và phần tử nguyên thủy**
  - Nếu p là một số nguyên tố thì $\phi(p) = p - 1$, ta có: với mọi $b \in Z_p^*$

$$b^{p-1} \equiv 1 \bmod p$$

  - Nếu b có cấp p – 1 thì các phần tử b, b^2,..., b^{p-1} đều khác nhau và lập thành Z_p^*. Theo thuật ngữ đại số, khi đó ta nói Z_p^* là một nhóm cyclic và b là một phần tử sinh (hay phần tử nguyên thủy) của nhóm đó.

Một số kiến thức toán học

- **Định lý Ferma (Định lý Ferma nhỏ)**
  - Nếu p là số nguyên tố và gcd(a,p) = 1 thì

$$\mathbf{a^{p-1} \equiv 1 \bmod p}$$

- **Ví dụ:**
  - Vì 5 và 7 là các số nguyên tố. 2 và 3 đều có ước chung lớn nhất với 5 và 7 là 1 , nên theo định lý Ferma ta có:
    - $2^{7-1} \bmod 7 = 1$ (= $2^6 \bmod 7 = 64 \bmod 7 = 1$)
    - $3^{5-1} \bmod 5 = 1$ (= $3^4 \bmod 5 = 81 \bmod 5 = 1$)
- Kết quả trên có thể được dùng để kiểm tra tính nguyên tố của một số nguyên p nào đó.

Một số kiến thức toán học

- **Định lý Ole (Euler):** Định lý Ole là tổng quát hoá của Định lý Ferma
  - Nếu $\mathbf{a \in Z_n^*}$ thì $\mathbf{a^{\Phi(n)} \equiv 1 \bmod n}$
  - *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

- **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}... p_k^{ek} là phân tích ra thừa số nguyên tố của n thì:

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

Một số kiến thức toán học

- Ví dụ:
  - Tính Φ(37); Φ(25); Φ(18); Φ(21)?

Φ(37) = 37 – 1 = 36

Φ(25) = Φ(5^2) = 20

Φ(18) = Φ(2). Φ(9) = 1. Φ(3^2) = 6

Φ(21) = Φ(3). Φ(7) = 2.6 = 12

Một số kiến thức toán học

- Bài tập: Cho n = 27
  - Tìm phần tử nguyên thủy nhỏ nhất của Z_n^*.
  - Từ phần tử nguyên thủy vừa tìm được, tìm tất cả các phần tử nguyên thủy của Z_n^*.

Một số kiến thức toán học

- **Kiểm tra tính nguyên tố**
  - Giả sử cần phải tìm một số nguyên tố rất lớn. Lấy ngẫu nhiên một số đủ lớn, ta cần phải kiểm tra xem số đó có phải là số nguyên tố không?
    - Cách 1: Thử bằng phép chia
    - Cách 2: sử dụng các phép kiểm tra tính nguyên tố thống kê dựa trên các tính chất mà mọi số nguyên tố phải thỏa mãn, nhưng có một số số không nguyên tố, gọi là giả nguyên tố cũng thoả mãn tính chất đó

Một số kiến thức toán học

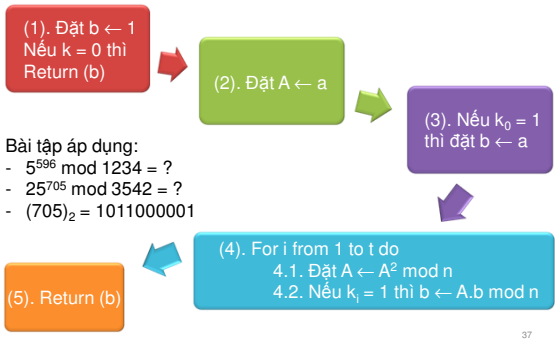
- Cụ thể là phép kiểm tra dựa trên Định lý Ferma như sau:
  - Nếu số n cần kiểm tra tính nguyên tố là số nguyên tố, thì nó sẽ thoã mãn định lý Ferma đối với mọi số a nhỏ hơn nó $a^{n-1} \bmod n = 1$.
  - Như vậy, lấy ngẫu nhiên số a và kiểm tra xem nó có tính chất trên không. Nếu có thì n có thể là số nguyên tố, nếu cần độ tin cậy lớn hơn, thì ta kiểm tra liên tiếp nhiều lần như vậy với các số ngẫu nhiên a được chọn. Sau mỗi lần qua được phép thử, xác suất để n là số nguyên tố lại tăng lên

Một số kiến thức toán học

- Thuật toán nhân bình phương có lặp

Input	a ∈ Z_n và số nguyên k, 0 ≤ k < n có biểu diễn nhị phân: $k = \sum_{i=0}^{l} k_i 2^i$
Output	$a^k \bmod n$

- Thuật toán nhân bình phương có lặp:



Bài tập áp dụng:
- 5^{596} mod 1234 = ?
- 25^{705} mod 3542 = ?
- $(705)_2$ = 1011000001

Một số kiến thức toán học

- Định lí phần dư Trung Hoa

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

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\ldots\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots$$
$$x \equiv a_k \pmod{n_k}$$

Một số kiến thức toán học

Giải hệ phương trình modulo:

- Cho :

  $x \equiv a_1 \bmod n_1$
  $x \equiv a_2 \bmod n_2$
  …
  $x \equiv a_k \bmod n_k$
- 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…n_k. N_i = N/n_i. M_i = N_i^{-1} mod n_i.

Một số kiến thức toán học

– Ví dụ giải hệ phương trình:

- a) x ≡ 10 mod 11
  x ≡ 19 mod 21
  x ≡ 20 mod 26

  X ≡ 670 mod 6006

- b) 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 gcd (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

- Bài toán giải phương trình đồng dư:
  – Phương trình đồng dư có dạng: ax ≡ b mod n;
    - d = GCD(a, n)
    - Nếu d không là ước của b ⇒ phương trình vô nghiệm
    - d|b ⇒ phương trình có d nghiệm:
      – $x_j = (b/d) \cdot x^* + j \cdot (n/d) \bmod n, j = 1 \rightarrow d$
      – Với $x^* = (a/d)^{-1} \bmod (n/d)$
  – Ví dụ:
    - Giải phương trình đồng dư: 4x ≡ 6 mod 26

Một số kiến thức toán học

- Giải:
  - Thấy gcd(4, 26) = 2 và 2|6 $\Rightarrow$ phương trình có 2 nghiệm
  - Ta có: $x^* = (4/2)^{-1} \bmod (26/2) = 2^{-1} \bmod 13 = 7$
  - Nghiệm: $x_1 = (6/2) \cdot 7 + (26/2) \bmod 26 = 8$

    $x_2 = (6/2) \cdot 7 + 2.(26/2) \bmod 26 = 21$

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: $\bar{Q}_n$
  - Tập các số nguyên nguyên tố với n được phân hoạch thành 2 tập con là Q_n và $\bar{Q}_n$
  - **Ví dụ:** Q_{17} và $\bar{Q}_{17}$

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

- Định lý:
  - Cho n = p.q, với p, q là hai số nguyên tố, p ≠ q. Khi đó a ∈ Z^*_n là thặng dư bậc hai theo modulo n nếu và chỉ nếu a ∈ Q_p và a ∈ Q_q.
- Hệ quả:

$$|Q_n| = \frac{(p-1).(q-1)}{4}$$

$$|\bar{Q}_n| = \frac{3.(p-1).(q-1)}{4}$$

Một số kiến thức toán học

- Định nghĩa căn bậc hai của một số modulo n:
  - Cho a ∈ Q_n. Nếu x ∈ 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 ∈ 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?

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:

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

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

Một số kiến thức toán học

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

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

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

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

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

- Một số tính chất KH Jacobi:

(1) Nếu $m_1 \equiv m_2 \bmod n$ thì: $\left(\frac{m_1}{n}\right) \equiv \left(\frac{m_2}{n}\right)$

(2) $\left(\frac{2}{n}\right) = \begin{cases} 1 & neu\ n \equiv \pm 1 \bmod 8 \\ -1 & neu\ n \equiv \pm 3 \bmod 8 \end{cases}$

(3) $\left(\frac{m_1 . m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$

Đặc biệt nếu $m = 2^k.t$ (với t là số lẻ) thì: $\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \cdot \left(\frac{t}{n}\right)$

(4) $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{Nếu } n \equiv m \equiv 3 \bmod 4 \\ \left(\frac{n}{m}\right) & m \equiv 1 \bmod 4\ or\ n \equiv 1 \bmod 4 \end{cases}$

Một số kiến thức toán học

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

- Giải:

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

b) $$9975=3\cdot5^2\cdot7\cdot19$$
$$\left(\frac{6278}{9975}\right)=\left(\frac{6278}{3}\right)\left(\frac{6278}{5}\right)^2\left(\frac{6278}{7}\right)\left(\frac{6278}{19}\right)$$
$$=\left(\frac{2}{3}\right)\left(\frac{3}{5}\right)^2\left(\frac{6}{7}\right)\left(\frac{8}{19}\right)=(-1)\left(\frac{5}{3}\right)^2\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{2}{19}\right)^3$$
$$=(-1).\left(\frac{2}{3}\right)^2.(1).(-1)(-1)^3=-1$$

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

Thuật toán 1: Tìm căn bậc hai của a mod p **(p ≡3 mod 4)**
Input: Số nguyên tố lẻ p; p ≡ 3 mod 4 và a ∈ Q_p
Output: 2 căn bậc hai của a mod p

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

Thuật toán 2: Tìm căn bậc hai của a mod p **(p ≡ 5 mod 8)**
Input: Số nguyên tố lẻ p, với p ≡ 5 mod 8 và a ∈ Q_p.
Output: 2 căn bậc hai của a mod p

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

Thuật toán 3: Tìm căn bậc hai của c mod n, trong đó n = p.q và p ≡ 3 mod 4; q ≡ 3 mod 4

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

Ouput: 2 căn bậc hai của a mod p nếu $a \in Q_p$.

1. Tính ký hiệu $\left(\frac{a}{p}\right)$ nếu $\left(\frac{a}{p}\right) = -1$ thì Return "a không có căn bậc hai theo modulo 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 $d = \left(r^2.a^{-1}\right)^{2^{s-i-1}} \bmod p$
   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)

55

Một số kiến thức toán học

- 1. Tính KH Jacôbi:

$$\left(\frac{29}{199}\right);\left(\frac{21}{211}\right);\left(\frac{47}{97}\right);\left(\frac{5}{97}\right);$$

- 2. Áp dụng các 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

56

Một số kiến thức toán học

3) Giải hệ phương trình:
$$\begin{aligned} 5x &\equiv 20 \bmod 6 \\ 6x &\equiv 6 \bmod 5 \\ 4x &\equiv 5 \bmod 77 \end{aligned}$$

4) Dùng thuật toán Euclide tìm phần tử nghịch đảo:
  - $357^{-1} \bmod 1137$
  - $213^{-1} \bmod 1577$

5) Tính $\phi(490)$; $\phi(768)$

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

57

Một số kiến thức toán học

- 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.

58

Một số kiến thức toán học

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

a	1	2	3	4	5	6	7	8	9
$\log_2 a$	18	1	13	2	16	14	6	3	8

a	10	11	12	13	14	15	16	17	18
$\log_2 a$	17	12	15	5	7	11	4	10	9

59

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

1. Tính $m = \left\lfloor \sqrt{ord(\alpha)} \right\rfloor$
2. Lập bảng $(j, \alpha^j \bmod n)$ với $j = \overline{0 \to m-1}$
3. Tính $\beta.(\alpha^{-m})^i \bmod n$ 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: $\log_\alpha \beta = m.i + j$

60

Một số kiến thức toán học

- 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}^*.

Nội dung

Các hệ mật khoá công khai

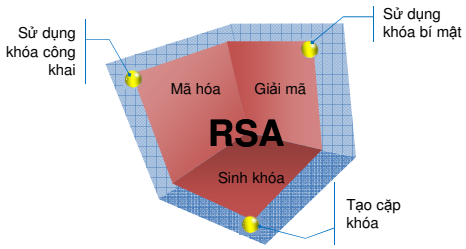
Hệ mật RSA

- 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.

64

Hệ mật RSA



65

Hệ mật RSA

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

  (P, C, K, E, D) *(1)*

  –Mỗi khóa k ∈ 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:

    $e.d \equiv 1 \bmod \phi(n)$

  - 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

66

Hệ mật RSA

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

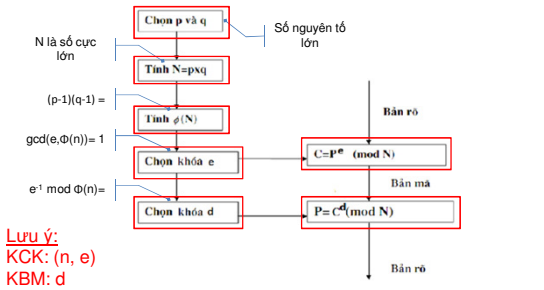
  P = C = Z_n, trong đó n là tích của 2 số nguyên tố

  K = {k=(k_e, k_d): k_e=(n,e), k_d=d, gcd(e, ϕ(n))= 1, e.d ≡1 mod ϕ(n)

  Hàm mã hóa e và giải mã d được xác định bởi

$$y = e_{k_e}(x) = x^e mod\ n\ \forall x \in P$$
$$d_{k_d}(y) = y^d mod\ n$$

Hệ mật RSA



Lưu ý:
KCK: (n, e)
KBM: d

Hệ mật RSA

- Sinh khóa
  - p = 31, q = 23
  - n = 31 * 23 = 713
  - Φ(n) = 30 * 22 = 660
    - → e = 223 với gdc(223,660) = 1
    - → d = 223^{-1} mod 660 = 367

⇒ Công khai : (713, 223)
Bí mật : (367)

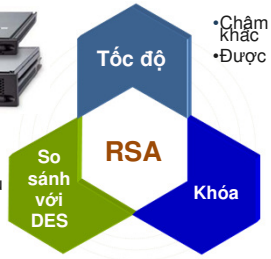
- Thông điệp cần mã hóa : 439
- Mã hóa :
  C = 439^{223} mod 713
  = 284

⇒

- Giải mã :
  P = 284^{367} mod 713
  = 439

Hệ mật RSA

- Một số vấn đề khác của RSA:



- Chậm so với các hệ khác
- Được cứng hóa

- Bổ sung cho nhau
- DES nhanh hơn RSA
- Khóa DES có độ dài bé

- Thiết bị sinh khóa
- Bảo vệ khóa công khai
- Cơ chế phân phối khóa

Hệ mật RSA

- 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 dấu được** là:

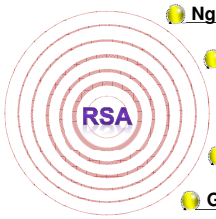
$$N = (1 + \gcd(e-1, p-1))(1 + \gcd(d-1, q-1))$$

Ví dụ về điểm bất động: với cặp khóa **(*n,e*)=(35,17)**, bản tin ***m* = 8**, ta có bản mã

$$c = 8^{17} mod\ 35 = 8$$

Hệ mật RSA

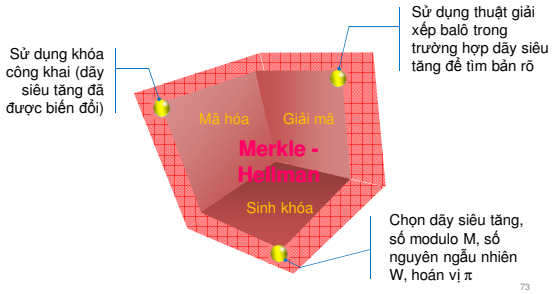
- Ứng dụng của RSA:



- **Ngân hàng**
- **E-comercial**
- **Các giao thức công nghệ thông tin**
- **Chính phủ điện tử**
- **Gửi và nhận văn bản**

Các hệ mật khoá công khai

2. Hệ mật Merkle – Hellman:



73

Hệ mật Merkle – Hellman

- Hệ mật Merkle – Hellman xuất phát từ bài toán xếp ba lô tổng quát
- Bài toán ba lô tổng quát:
  - Cho tập giá trị **A={a_1, a_2, …, a_n }** và một số dương C. Hỏi có tồn tại một tập con nằm trong A sao cho tổng tập con đó bằng C (Hỏi có tồn tại véc tơ nhị phân ***v* =(v_1, v_2, …, v_n)** để cho:

    $C = v_1a_1 + v_2a_2 + … + v_na_n$ với $v_i \in \{0,1\}$, i = 1…n
  - **Đây là bài toán "Khó", có độ phức tạp là hàm mũ *O*(2^n)**
  - **Ví dụ:** Dãy số nguyên (17, 38, 73, 4, 11, 1), C = 53

74

Ví dụ:

- C = 53
- dãy số nguyên: (17, 38, 73, 4, 11, 1)

Loại 73, vì 73 > 53

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

Thử 38, C = 53 – 38 = 15, thấy tổng số hạng còn lại 4 + 11 = 15. Vậy lời giải: v=(0,1,0,1,1,0),T = 53 = 38 + 4 + 11

75

Cách giải bài toán:

Hệ mật Merkle – Hellman

- Bài toán xếp ba lô là bài toán khó, có độ phức tạp là hàm mũ, nhưng nếu A là dãy siêu tăng thì bài toán này giải được với độ phức tạp tuyến tính $O(n)$
- Dãy siêu tăng:
  - Cho dãy số nguyên dương (a_1, …, a_n), dãy này được gọi là dãy siêu tăng nếu:

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

  - Ví dụ: {1, 4, 11, 17, 38, 73} là một dãy siêu tăng
  - Khi đó bài toán được giải như sau:

Hệ mật Merkle – Hellman

```
for (i = n; i >= 1; i --){
    if(C >= a_i){
        v_i = 1; C = C - a_i
    }else v_i = 0;
}
if (C == 0) "Bài toán có lời giải là véc tơ v";
else "Bài toán không có lời giải";
```

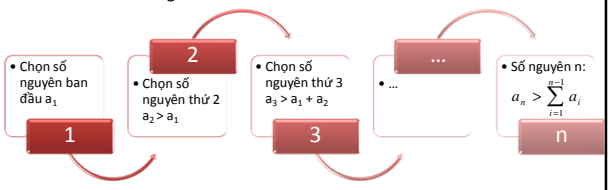
Ví dụ:

- (1) Cho dãy siêu tăng (12, 17, 33, 74, 157, 316, 620, 1230, 2460); tổng C = 4401
- (2) Cho dãy siêu tăng (5, 7, 13, 30, 57, 116, 230, 460, 920); tổng C = 1508

Hệ mật Merkle – Hellman

- 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**.

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

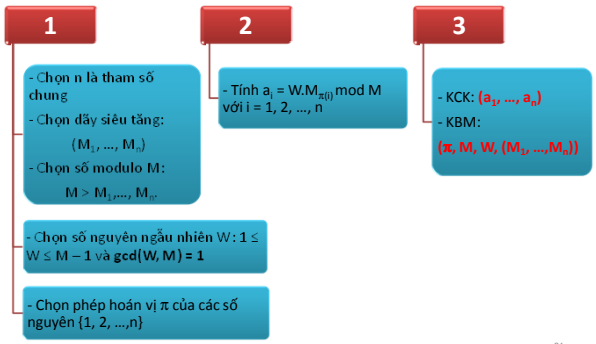


Ví dụ:

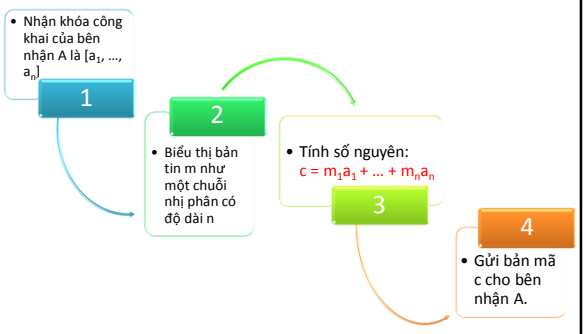
Dãy	Tổng	Số hạng tiếp theo
[]		
[1	1	2
[1, 2	1 + 2 = 3	4
[1, 2, 4	1 + 2 + 4 = 7	9
[1, 2, 4, 9	1 + 2 + 4 + 9 = 16	19
...	...	...

- Dãy siêu tăng vừa được chọn được gọi là **"ba lô dễ"**.

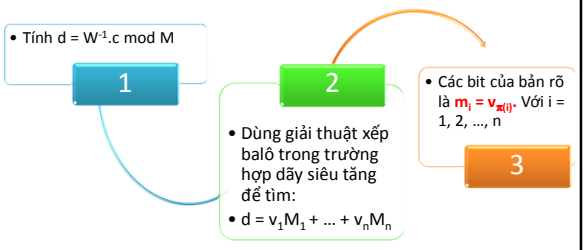
- Thuật toán tạo khóa



- Mã hóa:



- Giải mã:



Hệ mật Merkle – Hellman

- Ví dụ:
  - 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 thực hiện giải mã ngược lại từ bản mã vừa thu được.**

Hệ mật Merkle – Hellman

- 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

Hệ mật Merkle – Hellman

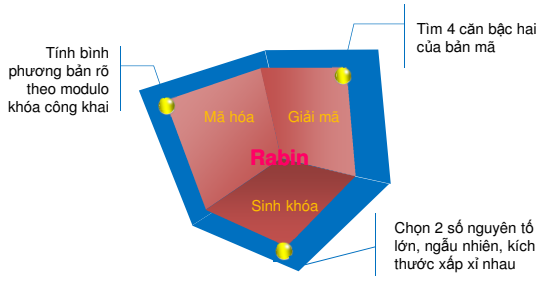
- Giải mã:
  - Tính $W^{-1} \bmod M = 635^{-1} \bmod 737 = 513$
  - Tính $W^{-1} c \bmod M = 513*1605 \bmod 737 = 136$.
  - Giải bài toán xếp ba lô trong trường hợp dãy siêu tăng:

$$136 = 12v_1 + 17v_2 + 33v_3 + 74v_4 + 157v_5 + 316v_6$$

  - 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:

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

3. Hệ mật Rabin



Hệ mật Rabin

- Thuật toán tạo khoá
  - Tạo 2 số nguyên tố lớn, ngẫu nhiên và phân biệt p và q có kích thước xấp xỉ nhau, p ≡ q ≡ 3 mod 4.
  - Tính ***n = p.q***
  - Khoá công khai là ***n***
  - Khoá bí mật là các cặp số **(*p*, *q*).**

Hệ mật Rabin

Mã hóa	**Giải mã**
B thực hiện:	A thực hiện:
Nhận khoá công khai của A: n	Tìm **4 căn bậc hai** của **c mod n** là **m_1, m_2, m_3 hoặc m_4**.
Biểu thị bản tin dưới dạng một số nguyên m nằm trong dải **[0, n -1]**	Thông báo của người gửi là một trong 4 giá trị **m_1, m_2, m_3 hoặc m_4**. Bằng một cách nào đó A sẽ quyết định m là giá trị nào
Tính **$c = m^2$ mod n**. Gửi c cho A	

Hệ mật Rabin

- Ví dụ: Hệ mã Rabin với các số nguyên tố p = 19, q= 23.
  + Tìm bản mã của m = 329

  + Xác định 4 bản giải mã có thể có từ bản mã thu được nói trên
  - Tạo khóa:
    - Tính n = p.q = 437
    - ⇒ Khóa công khai là 437, khóa bí mật là (19 , 23)
  - Mã hóa: Bản mã c được tính như sau:
    - $c = m^2 \bmod n = 329^2 \bmod 437 = ???$
  - Giải mã: ???

Hệ mật Rabin

- 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.

Hệ mật Rabin

- Độ an toàn của hệ mật Rabin:
  - Tấn công bản rõ có lựa chọn: an toàn
  - Không hoàn toàn an toàn với tấn công bản mã có lựa chọn.

4. Hệ mật Elgamal

- **Sơ đồ chung của hệ mật Elgamal**

  P = Z_p^* C = Z_p^* x Z_p^* , với p là một số nguyên tố

  K = {k=(k_e, k_d): k_e=(p,α, β), k_d=a ∈[1, p-2], β= $\alpha^a \bmod p$} , ở đây α là một phần tử nguyên thủy của Z_p^*

  Hàm mã hóa e và giải mã d được xác định bởi:

  – Với mỗi x∈P, để lập mã cho x ta chọn thêm một số ngẫu nhiên k ∈Z_{p-1} rồi tính

  $$e_{k_e}(x,k) = (y_1,y_2) \text{ với } y_1 = \alpha^k \bmod p,\ y_2 = x.\beta^k \bmod p$$

  – Hàm giải mã:

  $$x = d_{k_d}(y) = d_{k_d}(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$$

Hệ mật Elgamal

- **Tạo khoá:** Mỗi đầu liên lạc tạo một khoá công khai và một khoá bí mật tương ứng:
  - Tạo 1 số nguyên tố p lớn và một phần tử sinh α của nhóm nhân Z_p^* của các số nguyên mod p.
  - Chọn một số nguyên ngẫu nhiên a, $1 \le a \le p-2$ và tính $\beta = \alpha^a \bmod p$
  - Khoá công khai là bộ 3 số (p, α, β), khoá bí mật là a.

Hệ mật Elgamal

- **Mã hoá:** B mã hoá một thông báo m để gửi cho A bản mã cần gửi. B phải thực hiện các bước sau:
  - Nhận khoá công khai (p, α, β) của A.
  - Biểu thị bản tin dưới dạng một số nguyên m thuộc $\{1, \ldots, p-1\}$
  - Chọn số nguyên ngẫu nhiên k, $1 \le k \le p-2$
  - Tính $y_1 = \alpha^k \bmod p$ và $y_2 = m.\beta^k \bmod p$.
  - Gửi bản mã **$c = (y_1, y_2)$** cho A.

Hệ mật Elgamal

- **Giải mã:** để khôi phục bản rõ m từ c, A sử dụng khóa riêng a để tính $y_2.(y_1^a)^{-1} \bmod p$
- **Ví dụ:** cho $p = 17$, phần tử sinh $\alpha = 3$ và giả sử người dùng A chọn khóa bí mật $a = 3$
  - Hãy tìm khóa công khai của A.
  - Giả sử chọn số ngẫu nhiên $k = 4$. Hãy thực hiện mã hóa bản tin $m = 7$ với khóa công khai của A
  - Giải mã bản mã vừa thu được.

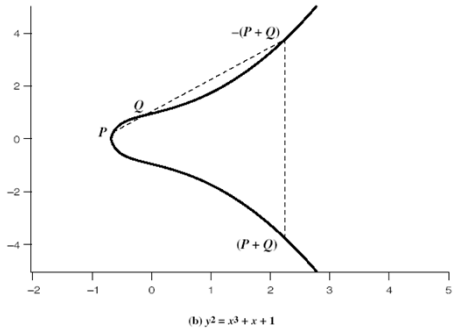
Hệ mật Elgamal

- **Bài tập về nhà:** cho p = 2579, α=32, giả sử dung khóa bí mật a = 765
  - Xác định khóa công khai (p, α, β)
  - Giả sử chọn ngẫu nhiên k = 853. Mã hóa bản tin m = 1299.
  - Giải mã bản mã vừa thu được?

Hệ mật ECC

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

Hệ mật ECC



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

Hệ mật ECC

- **Đường cong Elliptic hữu hạn**
  - Mã đường cong Elliptic sử dụng đường cong Elliptic 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

Hệ mật ECC

- **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.

Hệ mật ECC

- Ta định nghĩa phép toán trên E là phép cộng, đường cong Elliptic E tạo thành một nhóm Abel (các phép toán thực hiện trên Z_p)
- 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:
  1. Nếu $x_2 = x_1$, $y_2 = -y_1$ thì $P + Q = O$,
  2. Ngược lại $P + Q = (x_3, y_3)$ trong đó:
     - $x_3 = \lambda^2 - x_1 - x_2$
     - $y_3 = \lambda(x_1 - x_3) - y_1$ và $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, \text{if } P = Q \end{cases}$

Hệ mật ECC

3. $P + O = O + P = P, \forall P \in E$

4. Phép lấy nghịch đảo được tính toán khá dễ dàng, nghịch đảo của (x, y) là – (x, y) và = (x, – y)

Hệ mật ECC

- **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

Hệ mật ECC

- 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

Bảng kết quả

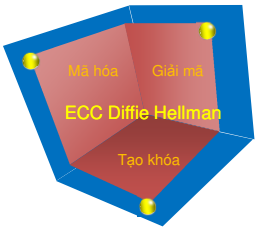
Hệ mật ECC

- Bài tập:
  - 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.

Hệ mật ECC

- Hệ mật trên đường cong elliptic:



Tạo khóa

Bước 1

- Chọn $E_p(a,b)$
- Chọn G là phần tử nguyên thủy với bậc lớn, tức là n lớn sao cho nG = O

Bước 2

- Hai người sử dụng A và B chọn khoá riêng của mình: $n_A < n$, $n_B < n$
- Tính các khoá công khai của A và B: $P_A = n_A \times G$, $P_B = n_B \times G$.
- Công bố công khai P_A và P_B.

Bước 3

- KCK: $E_p(a,b)$, G, P_A, P_B.
- KBM: n_A, n_B

Quá trình mã hóa và giải mã

Mã hóa	Giải mã
B thực hiện:	A thực hiện:
Mã hóa M thành điểm: $P_M \in E_p(a, b)$	A nhận P_C
Nhận KCK: P_A	A tính: $P_M = P2 – n_A P1$
Chọn số k ngẫu nhiên và tính bản mã P_C là một cặp điểm $\in E_p(a, b)$ theo nguyên tắc: $P_c = [P1=(kG), P2=(P_M + kP_A)]$ Gửi P_C cho A	

109

Hệ mật ECC

- 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.

110

Hệ mật ECC

- 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.

Minimum Size (bits) of Public Keys	
RSA	ECC
1024	160
2048	224
3072	256
7680	384
15360	512

Figure 1. RSA and ECC Performance (Source: RSA)[6]