



Các hệ mật cổ điển

- **Mã dịch vòng (MDV – Shift cipher):**

Giả sử $P = C = K = Z_{26}$ với $0 \leq k \leq 25$, ta định nghĩa:

$$y = e_k(x) = x + k \bmod 26$$

$$x = d_k(y) = y - k \bmod 26$$

- **Ví dụ:**

- **Bản rõ:** HOC TAP TOT LAO DONG TOT
- **Khoá k = 5**

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

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

S_I

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

 S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	1	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

 S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

 S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

 S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

 S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

 S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

 S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11



Các hệ mật cổ điển

❖ Mã Affine:

Cho $P = C = \mathbb{Z}_{26}$, $K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}$. Giả sử:

$$K = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}; \text{UCLN}(a, 26) = 1\}$$

Với $k = (a, b) \in K$ ta định nghĩa:

$$y = e_k(x) = ax + b \bmod 26$$

$$x = d_k(y) = a^{-1}(y - b) \bmod 26$$

❖ Ví dụ:

- Cho $k = (7, 3)$. Bắn rõ: It is nice today

- Tìm bản mã.
 - Giải mã bản mã thu được



Các hệ mật cổ điển

- Mô tả hệ mã Vigenere:

Cho m là số nguyên dương. Ta định nghĩa $P = C = K = (Z_{26})^m$. Với khoá $k = (k_1, k_2, \dots, k_m)$ ta xác định:

$$e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

$$\text{Và } d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

(Các phép toán đều thực hiện trên Z_{26} .)

- Nhận xét:

- Số khoá: **26^m**.

⇒ Tấn công tìm khoá vét cạn là không khả thi



❖ Tạo $x_0 = L_0 R_0 = IP(x)$

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

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP(x)



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

❖ Với $B_1 = b_1 b_2 b_3 b_4 b_5 b_6 = 110100_2$

- Ta có $b_1 b_6 = 10_2$ là biểu diễn nhị phân của hàng r của S_1 . Vậy $r = 2$
- 4 bit $b_2 b_3 b_4 b_5 = 1010$ là biểu diễn nhị phân của cột c của S_1 . Vậy $c = 10$
- Khi đó $S_1(B_1) = S_1(2,10) = 9$. Biểu diễn dưới dạng nhị phân ta có

$$C_1 = S_1(2,10) = 9 = 1001_2$$

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



Xác thực và chữ ký số

❖ Định nghĩa:

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

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

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

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





Xác thực và chữ kí số

❖ Chữ kí số RSA:

▫ Sơ đồ hệ thống chữ kí số RSA là bộ 5 (P, A, K, S, V), trong đó

- $P = A = \mathbb{Z}_n$ với $n = p \cdot q$ là tích của 2 số nguyên tố lớn p và q
- $K = \{(k_s, k_v), k_s = d, k_v = (n, e): \text{và } e \cdot d \equiv 1 \pmod{\phi(n)}\}$
- Hàm ký $\text{sig}_k: P \rightarrow A$ và hàm kiểm tra chữ kí $\text{ver}_k: P \times A \rightarrow \{\text{đúng}, \text{sai}\}$

được định nghĩa như sau:

$$s = \text{sig}_{k_s}(m) = m^d \pmod{n}$$

$$\text{ver}_{k_v}(m, s) = \text{đúng} \Leftrightarrow m = s^e \pmod{n}$$

❖ Ví dụ

- $p = 31, q = 23$
- $n = 31 * 23 = 713$
- $\Phi(n) = 30 * 22 = 660$
 - $d = 223$ với $\text{gdc}(223, 660) = 1$



Công khai: (713, 367)
Bí mật : (223)

- Thông điệp cần ký: 439

- Ký:

$$s = 439^{223} \bmod 713 \\ = 284$$



- Kiểm tra chữ ký:

$$439 = 284^{367} \bmod 713 \\ \Leftrightarrow \text{đúng}$$



❖ Mô tả sơ đồ E:

- ❑ Cho số nguyên tố p: bài toán logarit rời rạc trên Z_p là khó và giả sử $\alpha \in Z_p$ là phần tử nguyên thủy
- ❑ Chọn số $a \in Z_p$ và tính $\beta = \alpha^a \text{ mod } p$
- ❑ Giá trị p, α , β là công khai, còn a là mật
- ❑ Chọn số ngẫu nhiên (mật) $k \in Z_{p-1}$. Định nghĩa:

$$\text{sig}_k(x) = (\gamma, \delta)$$
- ❑ Trong đó: $\gamma = \alpha^k \text{ mod } p$; $\delta = (x - a \cdot \gamma) \cdot k^{-1} \text{ mod } (p - 1)$, với $x, \gamma \in Z_p$ và $\delta \in Z_{p-1}$, ta định nghĩa: **Ver(x, γ, δ) = true $\Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$**

Thuật toán Euclide mở rộng

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

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

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

❖ Hàm $\phi(n)$

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

❖ Các tính chất của hàm $\phi(n)$:

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

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

❖ Định nghĩa:

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

❖ Định lý Euler:

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

❖ Định nghĩa cấp của phần tử:

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

CRYPTOGRAPHY
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 $k \geq 1$.

2

Nếu α là một phần tử sinh của Z_n^* thì:

$$Z_n^* = \{\alpha^i \bmod n \mid 1 \leq i \leq \phi(n) - 1\}$$

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 $\alpha^{\phi(n)/p_i} \not\equiv 1 \pmod{n}$ đối với mỗi nguyên tố của $\phi(n)$



Mã khối

❖ Mô tả thuật toán:

- Với bản rõ cho trước x
- Tạo xâu x_0 theo hoán vị cố định ban đầu IP.
- Ta có: $x_0 = \text{IP}(x) = L_0 R_0$
- Trong đó L_0 gồm 32 bit đầu và R_0 là 32 bit cuối.

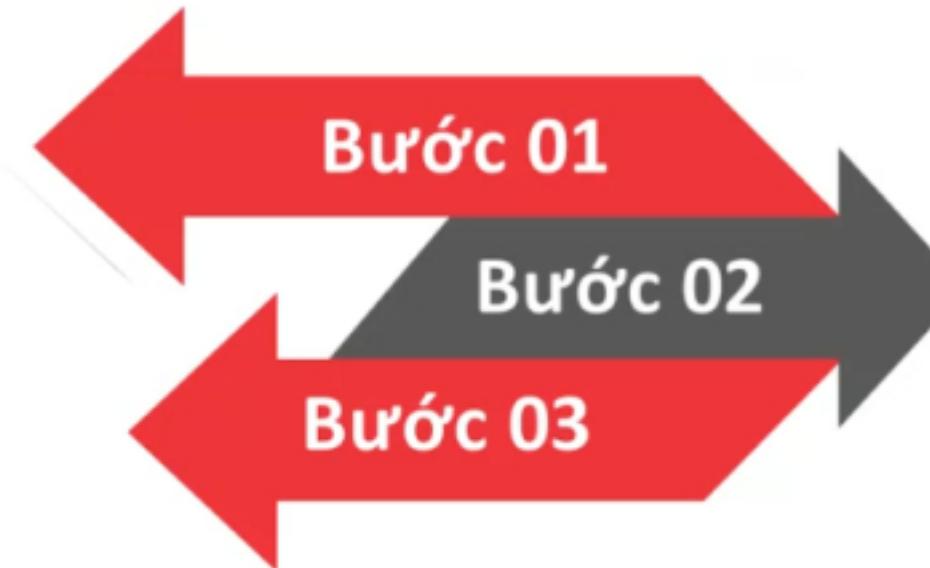
Bước 01

IP								
58	50	42	34	26	18	10	2	
60	52	44	36	28	20	12	4	
62	54	46	38	30	22	14	6	
64	56	48	40	32	24	16	8	
57	49	41	33	25	17	9	1	
59	51	43	35	27	19	11	3	
61	53	45	37	29	21	13	5	
63	55	47	39	31	23	15	7	



❖ Mô tả thuật toán:

- Với bản rõ cho trước x
- Tạo xâu x_0 theo hoán vị cố định ban đầu IP.
- Ta có: $x_0 = IP(x) = L_0R_0$
- Trong đó L_0 gồm 32 bit đầu và R_0 là 32 bit cuối.



Áp dụng phép hoán vị ngược IP^{-1} cho xâu bit $R_{16}L_{16}$, ta thu được bản mã y.
Tức là $y = IP^{-1}(R_{16}L_{16})$.
(Hãy chú ý thứ tự đã đảo của L_{16} và R_{16})

IP ⁻¹								
40	8	48	16	56	24	64	32	5
39	7	47	15	55	23	63	31	4
38	6	46	14	54	22	62	30	3
37	5	45	13	53	21	61	29	2
36	4	44	12	52	20	60	28	1
35	3	43	11	51	19	59	27	0
34	2	42	10	50	18	58	26	9
33	1	41	9	49	17	57	25	8

Bước 1

- Biến thứ nhất A được mở rộng thành một xâu bit độ dài 48 theo một hàm mở rộng cố định E.
- E(A) gồm 32 bit của A (được hoán vị theo cách cố định) với 16 bit xuất hiện hai lần.

BẢNG CHỌN E BIT						
32	1	2	3	4	5	
4	5	6	7	8	9	
8	9	10	11	12	13	
12	13	14	15	16	17	
16	17	18	19	20	21	
20	21	22	23	24	25	
24	25	26	27	28	29	
28	29 ^o	30	31	32	1	

❖ Số nguyên Blum:

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

❖ Định lý:

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

❖ Căn bậc hai chính:

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

Các hộp thê:

o

S ₁															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S ₂															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

 S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	2	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

 S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

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

Tìm căn bậc hai của $a \text{ mod } p$ ($p \equiv 3 \pmod{4}$)

Thuật toán 1: Input: Số nguyên tố lẻ p ; $p \equiv 3 \pmod{4}$ và $a \in Q_p$

Output: 2 căn bậc hai của $a \text{ mod } p$

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

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	15	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

 S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

 S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Thuật toán 2:

Tìm căn bậc hai của $a \text{ mod } p$ ($p \equiv 5 \pmod{8}$)

Input: Số nguyên tố lẻ p ; $p \equiv 5 \pmod{8}$ và $a \in Q_p$

Output: 2 căn bậc hai của $a \text{ mod } p$

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

Thuật toán 3:

Tìm căn bậc hai của $c \bmod n$ ($n = p \cdot q$ và $p \equiv 3 \pmod{4}$;
 $p \equiv 3 \pmod{4}$)

Input: Số nguyên n ; p, q và $c \in Q_n$

Output: 4 căn bậc hai của $c \bmod n$

1. Dùng thuật toán Euclide mở rộng tìm $a, b: ap + bq = 1$
2. Tính:

$$r = c^{(p+1)/4} \bmod p$$

$$s = c^{(q+1)/4} \bmod q$$

$$x = (aps + bqr) \bmod n$$

$$y = (aps - bqr) \bmod n$$

3. Return $(\pm x, \pm y)$

Thuật toán 3:

Tìm căn bậc hai của $c \bmod n$ ($n = p \cdot q$ và $p \equiv 3 \pmod{4}$;
 $p \equiv 3 \pmod{4}$)

Input: Số nguyên n ; p, q và $c \in Q_n$

Output: 4 căn bậc hai của $c \bmod n$

1. Dùng thuật toán Euclide mở rộng tìm $a, b: ap + bq = 1$
2. Tính:

$$r = c^{(p+1)/4} \bmod p$$

$$s = c^{(q+1)/4} \bmod q$$

$$x = (aps + bqr) \bmod n$$

$$y = (aps - bqr) \bmod n$$

3. Return $(\pm x, \pm y)$

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

Bước 4

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tìm căn bậc hai của $a \text{ mod } p$, p là số nguyên tố.

Thuật toán 4: Input: Số nguyên tố lẻ, số nguyên a , $1 \leq a \leq p - 1$

Output: 2 căn bậc hai của $a \text{ mod } p$ 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 : $1 \leq b \leq p - 1$ sao cho: $\left(\frac{b}{p}\right) = -1$ (tức $b \notin Q_p$)
3. Phân tích: $p - 1 = 2^s \cdot t$ (t là số lẻ)
4. Tính $a^{-1} \text{ mod } p$
5. Đặt $c \leftarrow b^t \text{ mod } p$; $r \leftarrow a^{(t+1)/2} \text{ mod } p$
6. For i from 1 to $s - 1$ do
 - 6.1. Tính $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \text{ mod } p$
 - 6.2. Nếu $d \equiv -1 \text{ mod } p$ thì đặt $r \leftarrow r \cdot c \text{ mod } p$
 - 6.3. $c \leftarrow c^2 \text{ mod } p$
7. Return $(r, -r)$

(1). Đặt $b \leftarrow 1$
Nếu $k = 0$ thì
Return (b)



(2). Đặt $A \leftarrow a$



(3). Nếu $k_0 = 1$
thì đặt $b \leftarrow a$



Bài tập áp dụng:

- $5^{596} \bmod 1234 = ?$
- $25^{705} \bmod 3542 = ?$

(4). For i from 1 to t do

4.1. Đặt $A \leftarrow A^2 \bmod n$

4.2. Nếu $k_i = 1$ thì $b \leftarrow A.b \bmod n$



(5). Return (b)

❖ Các hoán vị PC – 1 và PC – 2:

PC – 1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC – 2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32



Giới thiệu một số hệ mật KCK

- ❖ Ví dụ: \mathbb{Z}_{19}^* có phần tử sinh là 2. Hãy tính $\log_2 x$ với mọi $x \in \mathbb{Z}_{19}^*$.
 - Ta có bảng tính:

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

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

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 $(j, \alpha^j \text{ mod } n)$ với $j = \overline{0 \rightarrow m - 1}$
3. Tính $\beta \cdot (\alpha^{-m})^i \text{ mod } n$ với $i = \overline{0 \rightarrow m - 1}$
4. Tra bảng (j, α^j) cho tới khi thỏa mãn $\beta \cdot (\alpha^{-m})^i = \alpha^j$
5. Khi đó: $\log_{\alpha}\beta = m \cdot i + j$



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 $j = \overline{0 \rightarrow 7}$

$$\begin{aligned}\log_{31} 45 &= mi + j \\ &= 8.3 + 2 = 26\end{aligned}$$

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

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

i	0	1	2	3	4	5	6	7
$45 \cdot 12^i \text{ mod } 61$	45	52	14	46	3	36	5	60



Giới thiệu một số hệ mật KCK

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

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

$$\begin{aligned}\log_{17} 15 &= mi + j \\ &= 10 \cdot 3 + 1 = 31\end{aligned}$$

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

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

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



Giới thiệu một số hệ mật KCK

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

$$(P, C, K, E, D) \quad (1)$$

- ❑ Mỗi khóa $k \in K$ gồm có 2 thành phần $k = (k_e, k_d)$, k_e là khóa công khai dành cho việc mã hóa, còn k_d là khóa bí mật dành cho việc giải mã.

- ❖ **Để xây dựng hệ mật RSA**

- ❑ Chọn trước 2 số nguyên tố lớn p và q , tính $n = p \cdot q$
- ❑ Chọn một số e sao cho $\text{gcd}(e, \phi(n)) = 1$ và tính số d sao cho: $e \cdot d \equiv 1 \pmod{\phi(n)}$
- ❑ Mỗi cặp khóa $k = (k_e, k_d)$, với $k_e = (n, e)$, $k_d = d$ là một cặp khóa cho mỗi người dùng cụ thể



Giới thiệu một số hệ mật KCK

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

$P = C = \mathbb{Z}_n$, trong đó n là tích của 2 số nguyên tố

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

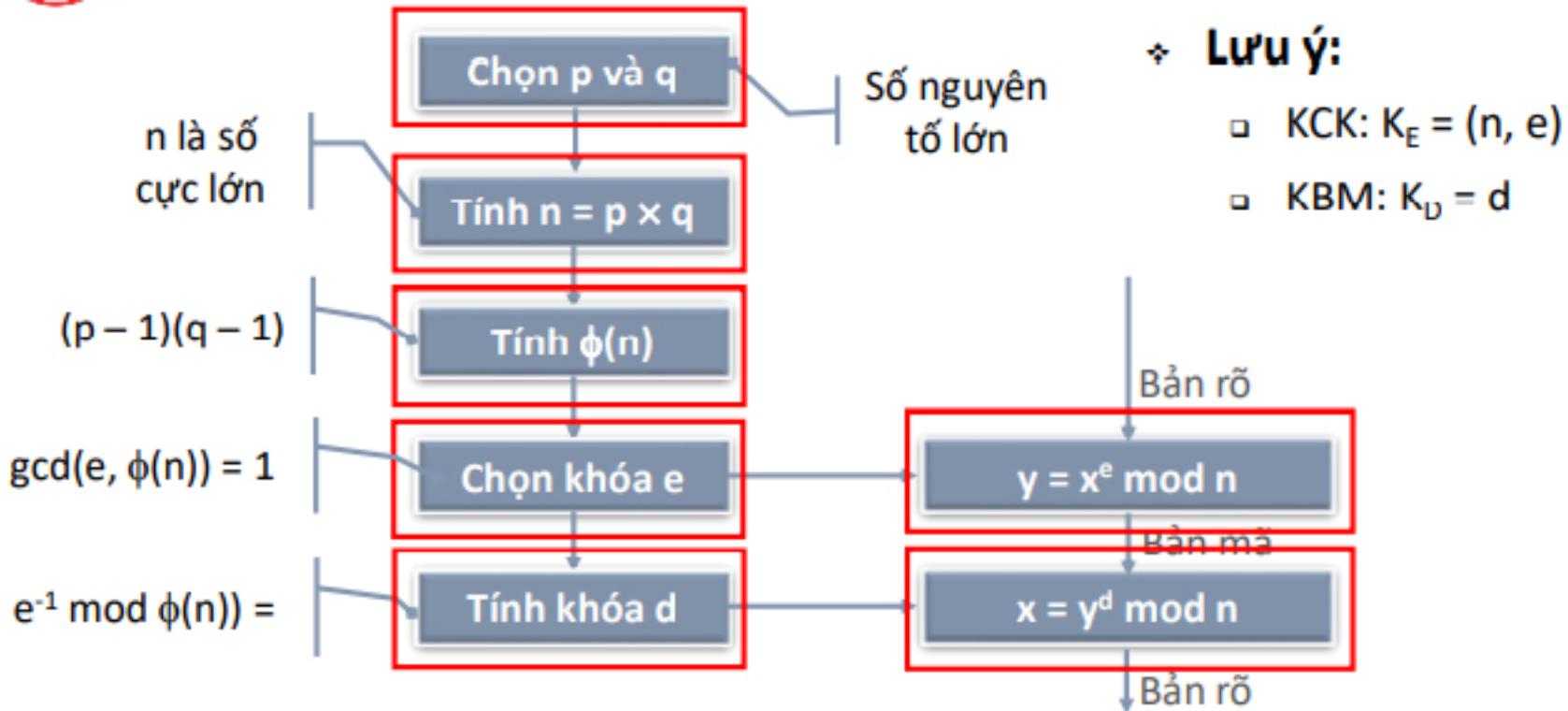
Hàm mã hóa E và giải mã D được xác định bởi:

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

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



Giới thiệu một số hệ mật KCK





Giới thiệu một số hệ mật KCK

❖ Hệ mật Rabin:

▫ Sơ đồ chung của hệ mật Rabin

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



Giới thiệu một số hệ mật KCK

❖ Hệ mật ElGamal:

▫ Sơ đồ chung của hệ mật Elgamal:

- $P = Z_p^*$; $C = Z_p^* \times Z_p^*$ với p là số nguyên tố
- $K = \{k = (k_e, k_d) : k_e = (p, \alpha, \beta), k_d = a \in [1, p - 2], \beta = \alpha^a \text{ mod } p\}$ 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 $x \in P$, để lập mã cho x ta chọn thêm một số ngẫu nhiên $k \in Z_{p-1}$ rồi tính $e_{k_e}(x, k) = (y_1, y_2)$ với $y_1 = \alpha^k \text{ mod } p$, $y_2 = x \cdot \beta^k \text{ mod } p$
 - Hàm giải mã: $x = d_{k_d}(y) = d_{k_d}(y_1, y_2) = y_2 (y_1^a)^{-1} \text{ mod } p$



Giới thiệu một số hệ môt KCK

1

$i \leftarrow n$

2

Chứng nào $i \geq 1$ thực hiện:

2.1. Nếu $S \geq M_i$ thì

$v_i \leftarrow 1; S \leftarrow S - M_i$

ngược lại $v_i \leftarrow 0$

2.2. $i \leftarrow i - 1$

3

Return(v)

❖ 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 m^{át} KCK

- ❖ Ta đ^{ịnh} 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 đ^{ịnh} 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 đ^ó:
 - $x_3 = \lambda^2 - x_1 - x_2$
 - $y_3 = \lambda(x_1 - x_3) - y_1$

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



Giới thiệu một số hệ mật KCK

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



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 $k_e = (F_p(a, b), G, P_A)$; $k_d = n_A$
- 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: $\bar{P}_M = e_{k_d}(P_c) = P_2 - n_A P_1$

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75	
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8	
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79	
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08	
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e	
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df	
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	

Hộp thể S-box

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb	
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e	
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25	
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92	
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84	
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06	
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b	
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73	
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e	
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b	
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4	
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f	
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef	
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61	
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d	

Hộp thể ngược InvS-box

❖ VD:

□ Vòng 1: SubBytes

	y																
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AddRoundKey Vòng 0

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix} \xrightarrow{\text{SubBytes}} \begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

