Bài tập mã hoá và giải mã tổng hợp trong An toàn và bảo mật thông tin Caesar Affine Vigenere HILL RSA El Gamal

báo cáo (Trường Đại học Kinh tế, Đại học Đà Nẵng)

EBOOKBKMT.COM

HỖ TRỢ TÀI LIỆU HỌC TẬP

AN TOÀN VÀ BẢO MẬT THÔNG TIN

BÀI TẬP

MÃ HOÁ VÀ GIẢI MÃ CƠ BẢN

PHẦN 1: CÁC PHƯƠNG PHÁP MÃ HOÁ CỔ ĐIỂN

Mã hóa dịch vòng Caesar

$$P = C = K = Z_n$$

$$e_k(x) = (x+k) \bmod n$$

$$d_k(y) = (y-k) \bmod n$$

Câu 1: Cho k=17, X = ATTACK. Hãy thực hiện mã hóa bằng Caesar theo Z_{26}.

X = ATTACK = (0, 19, 19, 0, 2, 10)   K =17

$y_1 = e_k(x_1) = (x_1 + k) \bmod n = (0+17) \bmod 26 = 17$ $y_4 = y_1 = 17$

$y_2 = (19+17) \bmod 26 = 10$ $y_5 = (2+17) \bmod 26 = 19$

$y_3 = y_2 = 10$ $y_6 = (10+17) \bmod 26 = 1$

Bản mã: $Y = (y_1, y_2, y_3, y_4, y_5, y_6) = (17, 10, 10, 17, 19, 1)$ = RKKRTB

Câu 2: Cho K = 12, cho bản mã Y = ZAFTUZSUYBAEEUNXQ. Giải mã dữ liệu và cho ra bản rõ theo mã dịch vòng Caesar

K = 12, n = 26, Y = ZAFTUZSUYBAEEUNXQ = (25, 0, 5, 19, 20, 25, 18, 20, 24, 1, 0, 4, 4, 20, 13, 23, 16)

Giải mã: Ta có $x = d_k(y) = (y-k) \bmod n$

$x_1 = d_k(y_1) = (y_1-k) \bmod n = (25 -12) \bmod 26 = 13$ => N	$x_9 = (24 -12) \bmod 26 = 12$ => M $x_{10} = (1 – 12) \bmod 26 = 15$ => P
$x_2 = (0 – 12) \bmod 26 = 14$ => O	$x_{11} = (0 -12) \bmod 26 = 14$ => O
$x_3 = (5 – 12) \bmod 26 = 19$ => T	$x_{12} = (4 – 12) \bmod 26 = 18$ => S
$x_4 = (19 – 12) \bmod 26 = 7$ => H	$x_{13} = (4 – 12) \bmod 26 = 18$ => S
$x_5 = (20 – 12) \bmod 26 = 8$ => I	$x_{14} = (20 – 12) \bmod 26 = 8$ => I
$x_6 = (25 – 12) \bmod 26 = 13$ => N	$x_{15} = (13 – 12) \bmod 26 = 1$ => B
$x_7 = (18 – 12) \bmod 26 = 6$ => G	$x_{16} = (23 – 12) \bmod 26 = 11$ => L
$x_8 = (20 – 12) \bmod 26 = 8$ => I	$x_{17} = (16 – 12) \bmod 26 = 4$ => E

Bản rõ: X = NOTHING IMPOSSIBLE

Câu 3: Phá mã bản mã sau (Caesar): Y = CSYEVIXIVQMREXIH Z_{26}

Theo mã hóa Caesar có phương pháp mã hóa và giải mã là phép cộng trừ modulo 26. Ta có thể thử tất cả 25 trường hợp của k như sau:

K	PlainText	K	PlainText
1	BRXDUHWHUPLQDWHG	14	OEKQHUJUHCYDQJUT
2	AQWCTGVGTOKPCVGF	15	NDJPGTITGBXCPITS
3	ZPVBSFUFSNJOBUFE	16	MCIOFSHSFAWBOHSR
4	*YOUARETERMINATED*	17	LBHNERGREZVANGRQ
5	XNTZQDSDQLHMZSDC	18	KAGMDQFQDYUZMFQP
6	WMSYPCRCPKGLYRCB	19	JZFLCPEPCXTYLEPO
7	VLRXOBQBOJFKXQBA	20	IYEKBODOBWSXKDON
8	UKQWNAPANIEJWPAZ	21	HXDJANCNAVRWJCNM
9	TJPVMZOZMHDIVOZY	22	GWCIZMBMZUQVIBML
10	SIOULYNYLGCHUNYX	23	FVBHYLALYTPUHALK
11	RHNTKXMXKFBGTMXW	24	EUAGXKZKXSOTGZKJ
12	QGMSJWLWJEAFSLWV	25	DTZFWJYJWRNSFYJI
13	PFLRIVKVIDZERKVU		

Trong 25 trường hợp trên, chỉ có trường hợp k=4 thì bản giải mã tương ứng là có ý nghĩa. Do đó bản rõ ban đầu là: *YOUARETERMINATED*

Câu 4: Bản rõ "HELPME" được mã hóa thành bản mã "DAHLIA". Hãy tìm K biết bản mã được hình thành theo Caesar thuộc Z_{26}

X = HELPME = (7, 4, 11, 15, 12, 4) Y = DAHLIA = (3, 0, 7, 11, 8, 0)

Theo hàm mã hóa có:

$y_1 = e(x_1) = (x_1 + k) \bmod 26$

=> 3 = (7 + k) mod 26 ⇔ (7+k) = i*26 + 3 (i€N, k = 1..25)

=> k = 22

Mã hóa Affine

*Cho P = C = Z_n, K = {(a, b), thuộc Z_n*Z_n với **GCD(a,n) = 1**}*

$e_k(x) = (ax + b) \bmod n$

$d_k(y) = (a^{-1}*(y-b)) \bmod n$

Điều kiện: e_k phải là song ánh: $\forall y \in Z_n, \exists! x \in Z_n, ax + b \equiv y (\bmod n)$

a và n là 2 số nguyên tố cùng nhau: GCD (a, n) = 1

Chú ý: Khi a=1 ta có mã dịch vòng Caesar

Với n=26, a = {3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}

Câu 1: Cho bản rõ X = ATTACK, mã hóa Affine trên Z_{26} với K = (5, 3)

X = ATTACK = (0, 19, 19, 0, 2, 10), K = (a, b) = (5, 3), n=26

Mã hóa:

$y_1 = e_k(x_1) = (ax_1+b) \bmod n = (5*0+3) \bmod 26 = 3$

$y_2 = e_k(x_2) = (ax_2+b) \bmod n = (5*19+3) \bmod 26 = 20$

$y_3 = e_k(x_3) = (ax_3+b) \bmod n = (5*19+3) \bmod 26 = 20$

$y_4 = e_k(x_4) = (ax_4+b) \bmod n = (5*0+3) \bmod 26 = 3$

$y_5 = e_k(x_5) = (ax_5+b) \bmod n = (5*2+3) \bmod 26 = 13$

$y_6 = e_k(x_6) = (ax_6+b) \bmod n = (5*10+3) \bmod 26 = 1$

Bản mã: Y = (y_1, y_2, y_3, y_4, y_5, y_6) = (3, 20, 20, 3, 13, 1) = DUUDNB

Câu 2: Hãy giải mã thông điệp "AXG" bằng hệ mã Affine với K = (a, b) = (7, 3) trên Z_{26}

Y = AXG = (0, 23, 6)   K = (a, b) = (7, 3),   n = 26

Giải mã:

$x_1 = d_k(y_1) = a^{-1}(y_1 – b) \bmod n = 7^{-1}(0 – 3) \bmod 26$

$= (7^{-1} \bmod 26 * (-3) \bmod 26) \bmod 26 = (15*23) \bmod 26 = 7$

$x_2 = d_k(y_2) = a^{-1}(y_2 – b) \bmod n = 7^{-1}(23 – 3) \bmod 26$

$= (7^{-1} \bmod 26 * 20 \bmod 26) \bmod 26 = (15*20) \bmod 26 = 14$

$x_3 = d_k(y_3) = a^{-1}(y_3 – b) \bmod n = 7^{-1}(6 – 3) \bmod 26$

$= (7^{-1} \bmod 26 * 3 \bmod 26) \bmod 26 = (15*3) \bmod 26 = 19$

Bản rõ: $X = (x_1, x_2, x_3) = (7, 14, 19)$ = HOT

Tính $7^{-1} \bmod 26$

Cho $r_0 = 26$, $r_1 = 7$, $r_i = r_{i+1}*q_{i+1} + r_{i+2}$

$s_0 = 1$, $s_1 = 0$, $s_i = s_{i-2} – q_{i-1}*s_{i-1}$, $t_0 = 0$, $t_1 = 1$, $t_i = t_{i-2} – q_{i-1}*t_{i-1}$

Thuật toán Euclide mở rộng được biểu diễn qua bảng sau:

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	s_i	t_i
0	26	3	7	5	1	0
1	7	1	5	2	0	1
2	5	2	2	1	1	-3
3	2	2	1	0	-1	4
4					3	-11

Kiểm tra: $r_0*s + r_1*t = GCD(r_0, r_1) = 1$

$\Rightarrow 7^{-1} \bmod 26 = (-11) \bmod 26 = -11+26 = 15$

Hệ mã hóa Vigenere

Cho m là một số nguyên dương cố định nào đó. Định nghĩa $P = C = K = (Z_n)^m$.

Với khoá $K = (k_1, k_2, \ldots, k_m)$ *ta xác định :*

$e_K(x_1, x_2, \ldots, x_m) = \{(x_1+k_1) \bmod n, \ldots, (x_m+k_m) \bmod n\}$

$d_K(y_1, y_2, \ldots, y_m) = \{(y_1-k_1) \bmod n, \ldots, (y_m-k_m) \bmod n\}$

Với x, y thuộc $(Z_n)^m$

Câu 1: Giả sử m = 6 và từ khoá là CIPHER. Từ khoá này tương ứng với dãy số K = (2,8,15,4,17). Giả sử bản rõ là xâu: "thiscryptosystemisnotsecure"

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15
18	19	4	12	8	18	13	14	19	18	4	2
2	8	15	7	4	17	2	8	15	7	4	17
20	1	19	19	12	9	15	22	8	15	8	19

20	17	4
2	8	15
22	25	19

Bởi vậy, dãy ký tự tương ứng của xâu bản mã sẽ là:

V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T

Câu 2: Giải mã bản mã sau, giả sử mã hóa Vigenere được sử dụng với từ khóa là LEG: Y = "PBVWEOYEZTST"

Y = “PBVWEOYEZTST” = (15, 1, 21, 22, 4, 14, 24, 4, 25, 19, 18, 19)

K = “LEG” = (11, 4, 6)

15	1	21	22	4	14
11	4	6	11	4	6
4	23	15	11	0	8
E	X	P	L	A	I
24	4	25	19	18	19
11	4	6	11	4	6
13	0	19	8	14	13
N	A	T	I	0	N

Bản rõ X = EXPLAINATION

Câu 3: Xét phương pháp Vigenere. Biết bản mã “PVRLHFMJCRNFKKW” có bản rõ tương ứng là “networksecurity”. Hãy tìm khóa K.

X = networksecurity = (13, 4, 19, 22, 14, 17, 10, 18, 4, 2, 20, 17, 8, 19, 24)

Y = PVRLHFMJCRNFKKW = (15, 21, 17, 11, 7, 5, 12, 9, 2, 17, 13, 5, 10, 10, 22)

Theo thuật toán Vigenere trên Z_{26} ta có hàm mã hóa:

$y_i = e_K(x_i) = (x_i + k_i) \bmod 26 \Rightarrow k_i = (y_i - x_i) \bmod 26$ Ta có bảng:

X	13	4	19	22	14	17	10	18	4	2	20	17	8	19	24
Y	15	21	17	11	7	5	12	9	2	17	13	5	10	10	22
K	2	17	24	15	19	14	2	17	24	15	19	14	2	17	24
K(Z26)	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y

Vậy từ khóa là CRYPTO

Phương pháp mã hóa HILL

Cho m là một số nguyên dương cố định. Cho P = C = $(Z_n)^m$ và K là tập hợp các ma trận khả nghịch $m_x m$, với một khóa k € K ta xác định:

$$e_k(x) = x*K$$

$$d_k(y) = yK^{-1}$$

*Cách tìm ma trận nghịch đảo K^{-1} (với m=2)	Với m bất kỳ:
- Tính det(K) = $|a\ b\ c\ d| = ad - bc$ - Tìm phần bù ma trận K: $P_K = (d\ \ -b\ \ -c\ a)$ - Tính ma trận nghịch đảo: $K^{-1} = (\det(K))^{-1} * P_K$	- Tính det(K): Tổng các tích chéo chính trừ tổng tích chéo phụ. - Tìm bù: Sử dụng phụ đại số C^T

Câu 1: Hệ mã hóa Hill, m=2, Z_{26}. Mã hóa xâu P = "HELP" với K = (3 3 2 5)

- Mã hóa:

$$P = HELP = \{P_1 = HE = (7,4)\ P_2 = LP = (11,15)$$

$$C_1 = e_k(P_1) = P_1 \times K = (7\ 4\ )(3\ 3\ 2\ 5\ ) = (3\ 15\ ) = DP$$

$$C_2 = e_k(P_2) = P_2 \times K = (11\ 15\ )(3\ 3\ 2\ 5\ ) = (11\ 4\ ) = LE$$

=> Bản mã: C = DPLE

Câu 2: Cho hệ mã hóa Hill có m=2 vành Z_{26}, ma trận khóa K = (12 5 3 7)**.**
Hãy giải mã xâu C = "GJFC"

- Giải mã:

$$C = GJFC = \{C_1 = GJ = (6,9)\ C_2 = FC = (5,2)$$

* Tìm ma trận nghịch đảo K^{-1} với K = (12 5 3 7)

- Ta có det(K) = (12*7 – 5*3) mod 26 = 17

- Do GCD(17, 26) = 1 nên theo thuật toán Euclide mở rộng ta tính $det(K)^{-1} = 23$ theo bảng sau:

Tính 17^{-1} mod 26

Cho $r_0 = 26$, $r_1 = 17$, $r_i = r_{i+1}*q_{i+1} + r_{i+2}$

$s_0 = 1$, $s_1 = 0$, $s_i = s_{i-2} – q_{i-1}*s_{i-1}$, $t_0 = 0$, $t_1 = 1$, $t_i = t_{i-2} – q_{i-1}*t_{i-1}$

Thuật toán Euclide mở rộng được biểu diễn qua bảng sau:

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	s_i	t_i
0	26	1	17	9	1	0
1	17	1	9	8	0	1
2	9	1	8	1	1	-1
3	8	8	1	0	-1	2
4					2	-3

Kiểm tra: $r_0*s + r_1*t = GCD(r_0, r_1) = 1$

=>17^{-1} mod 26 = (-3) mod 26 = -3+26 = 23

- Phần bù ma trận K: $P_K = \ (7\ -5\ -3\ 12\ )$

- Khóa nghịch đảo: $K^{-1} = Det(K)^{-1} \times P_K = 23 \times (7\ -5\ -3\ 12\ ) = (5\ 15\ 9\ 16\ ) mod\ 26$

$$P_1 = \ e_k(C_1) \ = \ C_1 \times K = (6\ 9\ )(5\ 15\ 9\ 16\ ) = (7\ 0\ ) \ = \ HA$$

$$P_2 = \ e_k(C_2) \ = \ C_2 \times K = (5\ 2\ )(5\ 15\ 9\ 16\ ) = (17\ 3\ ) \ = \ RD$$

=> Bản rõ: P = HARD

Hệ mã hóa dòng (Stream Cipher)

Mật mã dòng là một bộ (P,C,K,L,F,E,D) thoả mãn dược các điều kiện sau:

1. *P là một tập hữu hạn các bản rõ có thể.*
2. *C là tập hữu hạn các bản mã có thể.*
3. *K là tập hữu hạn các khoá có thể (không gian khoá)*
4. *L là tập hữu hạn các bộ chữ của dòng khoá.*
5. *F = (f1 f2...) là bộ tạo dòng khoá. Với* $i \geq 1$, $fi : K \times P\ i\text{ -1} \rightarrow L$
6. *Với mỗi* $z \in L$ *có một quy tắc mã* $ez \in E$ *và một quy tắc giải mã tương ứng* $dz \in D$. $ez : P \rightarrow C$ *và* $dz : C \rightarrow P$ *là các hàm thoả mãn* $dz(ez(x))= x$ *với mọi bản rõ* $x \in P$.

Các mã dòng thường được mô tả trong các bộ chữ nhị phân tức là $P= C=L= Z_2$. *Trong trường hợp này, các phép toán mã và giải mã là phép cộng theo modulo 2.*

$y_i = e_{zi}(x_i) = x_i + z_i \bmod 2$

$x_i = d_{zi}(x_i) = y_i + z_i \bmod 2$

Câu 1: Mã hóa ký tự 'A' bởi Alice

Ký tự 'A' trong bảng mã ASCII được tướng ứng với mã $65_{10}=1000001_2$ được mã hóa bởi hệ khóa $z_1,\ldots,z_7$=0101101

Hàm mã hóa:

Plaintext x_i	1000001	= 'A' (ASCII symbol)
Key stream z_i	0101101	
Ciphertext y_i	1101100	= 'I' (ASCII symbol)

Hàm giải mã:

Ciphertext y_i	1101100	= 'I' (ASCII symbol)
Key stream z_i	0101101	
Plaintext x_i	1000001	= 'A' (ASCII symbol)

Mã hóa One-Time Pad (OTP)

Trong hệ mã hóa OTP ta có: $|\boldsymbol{P}|=|\boldsymbol{C}|=|\boldsymbol{K}|$ ***với*** $x_i, y_i, k_i \in \{0, 1\}$

$$Encrypt: e_{ki}(x_i) = x_i + k_i \bmod 2$$

$$Decrypt: d_{ki}(y_i) = y_i + k_i \bmod 2$$

Để có thể đạt được mức độ bảo mật của OTP, tất cả những điều kiện sau phải được thỏa mãn:

- ✔ *Độ dài của chìa khóa phải đúng bằng độ dài văn bản cần mã hóa.*
- ✔ *Chìa khóa chỉ được dùng một lần.*
- ✔ *Chìa khóa phải là một số ngẫu nhiên thực.*

PHẦN 2: HỆ MÃ HOÁ KHOÁ CÔNG KHAI

Hệ mã hóa công khai RSA

Bước 1: Tạo khóa

1. *Chọn 2 số nguyên tố lớn ngẫu nhiên p và q và tính n = pq. Cần chọn p và q sao cho M < 2^{i-1}<n<2^i. Với i = 1024 thì n là một số nguyên khoảng 309 chữ số.*
2. *Tính số làm modulo hệ thống: n = pq và* $\phi(n) = (p-1)(q-1) = \phi(pq)$
3. *Chọn ngẫu nhiên khóa mã hóa b:* $\{1 < b < \phi(n)\ GCD(b,\ \phi(n) = 1$
4. *Giải phương trình để tìm khóa giải mã a:* $a = b^{-1}\ mod\ \phi(n) - Euclide\ mở\ rộng.$ *Tức* $b * a = 1\ mod\ \phi(n)$ *với* $0 \leq a \leq \phi(n)$
5. *Khóa công khai (mã hóa):* $K_{publish} = \{b, n\}$
6. *Khóa bí mật (giải mã):* $K_{private} = \{a, p, q\}$

Bước 2: Mã hóa với $K_{publish} = \{b, n\}$

$$y = e_{Kpub}(x) = x^b\ mod\ n$$

$$x \in Z_n = \{0, 1, \ldots, n-1\}$$

Bước 3: Giải mã với $K_{private} = \{a, p, q\}$

$$x = d_{K_{pri}}(y) = y^a\ mod\ n$$

Alice gửi dữ liệu cho	*Bob*
x=4 | Kpu={b,n} = {3,33}<=Bob $y = x^b mod\ n = 4^3 mod33=31$	*1. Choose p=3, q=11* *2. n=pq=33, N=20* *3. Choose b=3, GCD(20,3)=1* 4. $a = b^{-1} mod\ N = 3^{-1} mod20 = 7 => K_{pri}$ *A=> y = 31 |* $K_{pri}=\{a,p,q\}=\{7,3,11\}$ $x=y^a\ mod\ n = 31^7\ mod\ 33 = 4$

Câu 1: Cho hệ mã hóa RSA với p=5, q=7, b=5

a. Hãy tìm khóa công khai K_{pub} và khóa bí mật K_{pri}
b. Hãy thực hiện mã háo chuỗi "secure" và giải mã ngược lại bản mã có được.

a. Tạo khoá

1. p = 5, q = 7, b = 5
2. Modulo hệ thống n = pq = 5*7 = 35. $\phi(n) = \phi(pq) = (p-1)(q-1) = 24$
3. Tìm $a = b^{-1} \, mod \, \phi(n) = 5^{-1} \, mod \, 24 = 5$
4. K_{pub} = {b, n} = {5, 35}
5. K_{pri} = {a, p, q} = {5, 5, 7}

b. Mã hóa X = "Secure" với K_{pub} = {b, n} = {5,35}

x_1 = S = 18 => $y_1 = e_{Kpub}(x_1) = x_1^b$ mod n = 18^5 mod 35 = 23 (Bình phương & nhân)

x_2 = E = 4 => $y_2 = x_2^b$ mod n = 4^5 mod 35 = 9

x_3 = C = 2 => $y_3 = 2^5$ mod 35 = 32

x_4 = U = 20 => $y_4 = 20^5$ mod 35 = 20

x_5 = R = 17 => $y_5 = 17^5$ mod 35 = 12

x_6 = E = 4 => $y_6 = 4^5$ mod 35 = 9

Y = "XJGUMJ"

c. Giải mã Y = "XJGUMJ" = {23, 9, 32, 20, 12, 9} với K_{pri} = {a, p, q} = {5, 5, 7}

n = pq = 35

$x_1 = d_{Kpri}(y_1) = y_1^a$ mod n = 23^5 mod 35 = 18
$x_2 = 9^5$ mod 35 = 4
$x_3 = 32^5$ mod 35 = 2
$x_4 = 20^5$ mod 35 = 20
$x_5 = 12^5$ mod 35 = 17
$x_6 = 9^5$ mod 35 = 4

=> Bản rõ X = "SECURE"

Câu 2: Cho hệ mã hóa RSA có p = 103, q = 113, b = 71. Hãy tìm khóa công khai K_{pub} và khóa bí mật K_{pri} của hệ mã trên. Sau đó mã hóa thông điệp X= 1102 và giải mã ngược lại kết quả nhận được.

- Tạo khóa:

1. Hai số nguyên tố: p = 103, q = 113 (TM)
2. Modulo hệ thống: n = pq = 103*113 = 11639,

   $\phi(n) = \phi(pq) = (p-1)(q-1) = (103-1)(113-1) = 11424$

3. Khóa mã hóa b = 71 thỏa mãn: $\{1 < b < \phi(n)\ (TM)\ GCD(b,\ \phi(n) = 1\ (TM)$
4. Tìm khóa giải mã: $a = b^{-1}\ mod\ \phi(n) = 71^{-1}\ mod\ 11424 = 9815$

Theo thuật toán Euclide mở rộng tính 71^{-1} mod 11424 với $r_0 = 11424$, $r_1 = 71$, $r_i = r_{i+1}*q_{i+1} + r_{i+2}$, $s_0 = 1$, $s_1 = 0$, $s_i = s_{i-2} - q_{i-1}*s_{i-1}$, $t_0 = 0$, $t_1 = 1$, $t_i = t_{i-2} - q_{i-1}*t_{i-1}$. Thuật toán được biểu diễn qua bảng sau:

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	s_i	t_i
0	11424	160	71	64	1	0
1	71	1	64	7	0	1
2	64	9	7	1	1	-160
3	7	7	1	0	-1	161
4	1				10	-1609

Vậy 71^{-1} mod 11424 ≡ (-1609) mod 11424 = -1609+11424 = 9815

5. Khóa công khai K_{pub} = {b, n} = {71, 11639}
6. Khóa bí mật K_{pri} = {a, p, q} = {9815, 103, 113}

- Mã hóa X = 1102 với K_{pub} = {b, n} = {71, 11639}

x = 1102 => y= $e_{Kpub}(x) = x^b$ mod n = 1102^{71} mod 11639 = 2345

=> Bản mã Y = 2345

Theo thuật toán Bình phương và nhân tính 1102^{71} mod 11639 = 2345 với x = 1102, k = 71 = 1000111, n = 11639. Khởi tạo p = 1 thuật toán được biểu diễn qua bảng:

b[i]	p=p*p	p(mod n)	p=p*x	p(mod n)
1	1	1	1102	1102
0	1214404	3948	-	3948
0	15586704	2083	-	2083
0	4338889	9181	-	9181
1	84290761	1123	1237546	3812
1	14531344	5872	6470944	11299
1	127667401	10849	11955598	2345

- Giải mã Y = 2345 với K_{pri} = {a, p, q} = {9815, 103, 113}. Tính n = pq = 11639

$x = d_{Kpri}(y) = y^a \bmod n = 2345^{9815} \bmod 11639 = 1102$

=> Bản rõ X = 1102

Theo thuật toán Bình phương và nhân tính 2345^{9815} mod 11639 = 1102 với x = 2345, k = 11639 = 10011001010111, n = 11639. Khởi tạo p = 1 thuật toán được biểu diễn qua bảng sau:

b[i]	p=p*p	p(mod n)	p=p*x	p(mod n)
1	1	1	2345	2345
0	5499025	5417	-	5417
0	29343889	1970	-	1970
1	3880900	5113	11989985	1815
1	3294225	388	909860	2018
0	4072324	10313	-	10313
0	106357969	787	-	787
1	619369	2502	5867190	1134
0	1285956	5666	-	5666
1	32103556	3194	7489930	6053
0	36638809	10876	-	10876
1	118287376	219	513555	1439
1	2070721	10618	24899210	3389
1	11485321	9267	21731115	1102

Hệ mật mã ElGamal

Bước 1: Tạo khóa

- *Cho p là một số nguyên tố sao cho bài toán logarit rời rạc trong Zp là khó giải.*
- *Chọn phần tử nguyên thủy $\alpha \in Zp^*$*
- *Chọn $a \in \{2, 3, \ldots, p\text{-}2\}$ là khóa bí mật thứ nhất (Khóa người nhận, giải mã)*
- *Tính $\beta = \alpha^a$ mod p.*
- *Khi đó: $K_{pub} = (p, \alpha, \beta)$ gọi là khóa công khai, và $K_{pri} = (a)$ là khóa bí mật.*

Bước 2: Xây dựng hàm mã hóa dữ liệu

- *Chọn 1 số ngẫu nhiên bí mật $k \in Z_{p-1}$, Ta xác định: $k \in Z_{p-1} = \{0, 1, \ldots, p\text{-}2\}$*
- *Định nghĩa: $e_{K_{pub}}(x, k) = (y_1, y_2)$ với $y_1 = \alpha^k \bmod p$ và $y_2 = x\beta^k \bmod p$*

Bước 3: Giải mã

Với $y_1, y_2 \in Zp^*$ ta xác định: $d_{K_{pri}}(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$

A (gửi)	B (nhận)
Choose private key $K_{priA}=\alpha_A$ Compute $K_{pubA}=\alpha^{aA}$ mod p = bA bB<==B $k_{AB} = bB^{aA} = \alpha^{aA*aB}$ mod p $y = x*k_{AB}$ mod p	Choose private key $K_{priB}=\alpha_B$ $K_{pubB}= \alpha^{aB}$ mod p = bB A==> bA $k_{AB} = bA^{aB} = \alpha^{aB*aA}$ mod p A==>y $x = y*k_{AB}^{-1}$ mod p

Bài tập 1: Trong hệ mật mã Elgamal, lấy p = 5987, α = 2, a = 913, k = 1647. Hãy mã hóa bản rõ x = 122 và giải mã ngược lại kết quả đó.

- Bước 1: Tạo khóa

p = 5987, Z_p = {0, …, 5988}; α = 2 ∈ Zp* (TM), a = 913 ∈ {2, 3, …, p-2} (TM)

Tính $\beta = \alpha^a \bmod p = 2^{913} \bmod 5987 = 4087$. Theo thuật toán bình phương và nhân có x = 2, k = 913 = 1110010001, n = 5987 ta có bảng sau.

b[i]	p=p*p	p=p (mod n)	p=p * x	p=p (modn)
1	1	1	2	2
1	4	4	8	8
1	64	64	128	128
0	16384	4410	-	4410
0	19448100	2324	-	2324
1	5400976	702	1404	1404
0	1971216	1493	-	1493
0	2229049	1885	-	1885
0	3553225	2934	-	2934
1	8608356	5037	10074	4087

=> $K_{pub} = (p, \alpha, \beta) = (5987, 2, 4087)$ $K_{pri} = (a) = (913)$

- Bước 2: Mã hóa bản rõ x = 122 với $K_{pub} = (p, \alpha, \beta) = (5987, 2, 4087)$

$k = 1647 \in Z_{p-1}$ (TM)

Ta có: $e_{K_{pub}}(x, k) = (y_1, y_2)$ với y_1 y_2 thỏa mãn:

$y_1 = \alpha^k \, mod \, p = 2^{1647} mod \, 5987 = 955$ Theo thuật toán Bình phương và nhân với x=2, k=1647=11001101111, n=5987 ta có bảng sau:

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	2	2
1	4	4	8	8
0	64	64	-	64
0	4096	4096	-	4096
1	16777216	1642	3284	3284
1	10784656	2069	4138	4138
0	17123044	224	-	224
1	50176	2280	4560	4560
1	20793600	749	1498	1498
1	2244004	4866	9732	3745
1	14025025	3471	6942	955

$y_2 = x\beta^k \, mod \, p = 122 * 4087^{1647} mod \, 5987 = ((122 \, mod \, 5987) * (4087^{1647} mod \, 5987)) \, mod \, 5987 = (122 * 129) \, mod \, 5987 = 3764$

Theo thuật toán Bình phương và nhân tính 4087^{1647} mod 5987 với x=4087, k=1647=11001101111, n=5987 ta có bảng sau:

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	4087	4087
1	16703569	5826	23810862	563
0	316969	5645	-	5645
0	31866025	3211	-	3211
1	10310521	907	3706909	956
1	913936	3912	15988344	3054
0	9326916	5157	-	5157
1	26594649	395	1614365	3862
1	14915044	1427	5832149	811
1	657721	5138	20999006	2597
1	6744409	3047	12453089	129

Vậy bản mã Y = (y_1, y_2) = (955, 3764)

- Bước 3: Giải mã Y = (y_1, y_2) = (955, 3764) với K_{pri} = (a) = (913)

$$d_{K_{pri}}(y_1, y_2) \;=\; y_2(y_1^a)^{-1}\, mod\ p \;=\; 3764 * (955^{913})^{-1}\, mod\ 5987$$

= (3764 mod 5987 * $(955^{913})^{-1}$ mod 5987) mod 5987

= (3764 mod 5987 * $(955^{913}$ mod $5987)^{-1}$ mod 5987) mod 5987

= (3764 * 129^{-1} mod 5987) mod 5987 = (3764*3388) mod 5987 = 122

=> Bản rõ X = 122

Theo thuật toán Bình phương và nhân tính 955^{913} mod 5987 = 129 với x=955, k=913, n=5987

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	955	955
1	912025	2001	1910955	1102
1	1214404	5030	4803650	2076
0	4309776	5123	-	5123
0	26245129	4108	-	4108
1	16875664	4298	4104590	3495
0	12215025	1545	-	1545
0	2387025	4199	-	4199
0	17631601	5873	-	5873

1	34492129	1022	976010	129

Theo thuật toán Euclide mở rộng tính 129^{-1} mod 5987 với $r_0 = 5987$, $r_1 = 129$, $r_i = r_{i+1}*q_{i+1} + r_{i+2}$, $s_0 = 1$, $s_1 = 0$, $s_i = s_{i-2} - q_{i-1}*s_{i-1}$, $t_0 = 0$, $t_1 = 1$, $t_i = t_{i-2} - q_{i-1}*t_{i-1}$. Thuật toán được biểu diễn qua bảng sau:

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	s_i	t_i
0	5987	46	129	53	1	0
1	129	2	53	23	0	1
2	53	2	23	7	1	-46
3	23	3	7	2	-2	93
4	7	3	2	1	5	-232
5	2	2	1	0	-17	789
6	1				56	-2599

=> 129^{-1} mod 5987 = (-2599) mod 5987 = -2599 + 5987 = 3388

Bài tập 2: Cho hệ mật mã ElGramal có p = 83, α = 5 là một phần tử nguyên thủy của Zp*, a = 71 (phần tử bí mật mà người nhận chọn). Hãy tìm khóa công khai K_{pub} và khóa bí mật K_{pri} của hệ mã trên.

Cho k = 47. Hãy mã hóa bản rõ x = 23 và giải mã ngược lại kết quả đó.

- Tạo khóa:

p = 83 là một số nguyên tố (TM), phần tử nguyên thủy α = 5 ∈ Zp* (TM)

a=71∈ {2, 3, …, p-2} (TM) là phần tử bí mật thứ nhất mà người nhận chọn

Tính $\beta = \alpha^a$ mod p = 5^{71} mod 83 = 80. Theo thuật toán bình phương và nhân có x = 5, k = 71 = 1000111, n = 83, khởi tạo p=1 ta có bảng sau:

b[i]	p=p*p	p=p (mod n)	p=p * x	p=p (mod n)
1	1	1	5	5
0	25	25	-	25
0	625	44	-	44
0	1936	27	-	27
1	729	65	325	76
1	5776	49	245	79
1	6241	16	80	80

=> Khóa công khai K_{pub} = (p, α, β) = (83, 5, 80). Khóa bí mật K_{pri} = (a) = (71)

- Mã hóa dữ liệu X = 23 với K_{pub} = (p, α, β) = (83, 5, 80)

Chọn k = 47 ∈ Zp-1 = {0, 1, …, p-1} (TM)

Ta có: $e_{K_{pub}}(x, k) = (y_1, y_2)$ với y_1 y_2 thỏa mãn:

$y_1 = \alpha^k \; mod \; p = 5^{47} mod \; 83 = 62$ Theo thuật toán Bình phương và nhân với x=5, k=47=101111, n=83 ta có bảng sau:

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	5	5
0	25	25	-	25
1	625	44	220	54
1	2916	11	55	55
1	3025	37	185	19
1	361	29	145	62

$y_2 = x\beta^k \; mod \; p = 23 * 80^{47} mod \; 83 = ((23 \; mod \; 83) * (80^{47} mod \; 83)) \; mod \; 83 = (23 * 18) \; mod \; 83 = 82$

Theo thuật toán Bình phương và nhân tính 80^{47}mod 83 = 18 với x=80, k=47=101111, n=83, khởi tạo p = 1 ta có bảng sau:

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	80	80
0	6400	9	-	9
1	81	81	6480	6
1	36	36	2880	58
1	3364	44	3520	34
1	1156	77	6160	18

Vậy bản mã Y = (y_1, y_2) = (62, 82)

- Giải mã Giải mã Y = (y_1, y_2) = (62, 82) với K_{pri} = (a) = (71)

$$d_{K_{pri}}(y_1, y_2) = y_2(y_1^a)^{-1} \; mod \; p = 82 * (62^{71})^{-1} \; mod \; 83$$

= (82 mod 83 * $(62^{71})^{-1}$ mod 83) mod 83

= (82 mod 83 * $(62^{71}$ mod 83$)^{-1}$ mod 83) mod 83

= (82 * 18^{-1} mod 83) mod 83 = (82*60) mod 83 = 23

=> Bản rõ X = 23

Theo thuật toán Bình phương và nhân tính 62^{71} mod 83 = 18 với x=62, k=71=1000111, n=83, khởi tạo p=1 ta có bảng sau:

b[i]	p=p*p	p=p(mod n)	p = p * x	p = p(mod n)
1	1	1	62	62
0	3844	26	-	26
0	676	12	-	12
0	144	61	-	61
1	3721	69	4278	45
1	2025	33	2046	54
1	2916	11	682	18

Theo thuật toán Euclide mở rộng tính 18^{-1} mod 83 ≡ (-23) mod 83 = -23+83 = 60 với r_0 = 83, r_1 = 18, $r_i = r_{i+1}*q_{i+1} + r_{i+2}$, t_0 = 0, t_1 = 1, $t_i = t_{i-2} – q_{i-1}*t_{i-1}$. Thuật toán được biểu diễn qua bảng sau:

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	t_i
0	83	4	18	11	0
1	18	1	11	7	1
2	11	1	7	4	-4
3	7	1	4	3	5
4	4	1	3	1	-9
5	3	3	1	0	14
6	1				-23

Vậy bản mã là X = 23

Bài kiểm tra

Đề 1:

Cho hệ RSA lấy p = 31, q = 41, b = 71.

a. Hãy tìm khóa công khai Kpub và khóa bí mật Kpri của hệ mã trên.
b. Thông điệp được viết bằng tiếng anh, người ta dùng một hàm chuyển đổi các ký tự thành các số thập phân có hai chữ số như sau:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ví dụ xâu ABC được chuyển thành 00 01 02 và sau đó cắt thành các số có 3 chữ số 000 (=0) và 102 để mã hóa. Bản mã thu được là 1 tập các số ∈ Zn. Hãy thực hiện mã hóa xâu P = "ACTION".

Đề 3:

Cho hệ mật mã ElGramal có p = 1187, α = 79 là một phần tử nguyên thủy của Zp*, a = 113 (phần tử bí mật mà người nhận chọn).

a. Hãy tìm khóa công khai Kpub và khóa bí mật Kpri của hệ mã trên.
b. Thông điệp được viết bằng tiếng anh, người ta dùng một hàm chuyển đổi các ký tự thành các số thập phân có hai chữ số như sau:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ví dụ xâu ABC được chuyển thành 00 01 02 và sau đó cắt thành các số có 3 chữ số 000 (=0) và 102 để mã hóa. Bản mã thu được là 1 tập các số ∈ Zn. Cho k = 15, Hãy mã hóa bản rõ M = "SERIUS".