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_{public} *= {b, n}*
6. *Khóa bí mật (giải mã):* $K_{private}$ *= {a, p, q}*

Bước 2: Mã hóa với K_{public} *= {b, n}*

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

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

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^bmod n = 4^3mod33=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 mã

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

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

x_3 = C = 2 => $y_3 = 2^5 \bmod 35 = 32$

x_4 = U = 20 => $y_4 = 20^5 \bmod 35 = 20$

x_5 = R = 17 => $y_5 = 17^5 \bmod 35 = 12$

x_6 = E = 4 => $y_6 = 4^5 \bmod 35 = 9$

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

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

=> 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 $1102^{71} \bmod 11639 = 2345$ 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 $2345^{9815} \bmod 11639 = 1102$ 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 $a \in \{2, 3, ..., p-2\}$ là khóa bí mật thứ nhất (Khóa người nhận, giải mã)*
- *Tính $\beta = \alpha^a \bmod p$.*
- *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: $k \in Z_{p-1} = \{0, 1, ..., p-2\}$*
- *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 $K_{pubA}=\alpha^{aA} \bmod p = bA$ bB<==B $k_{AB} = bB^{aA} = \alpha^{aA*aB} \bmod p$ $y = x*k_{AB} \bmod p$	Choose private key $K_{priB}=\alpha_B$ $K_{pubB}= \alpha^{aB} \bmod p = bB$ A==> bA $k_{AB} = bA^{aB} = \alpha^{aB*aA} \bmod p$ A==>y $x = y*k_{AB}^{-1} \bmod p$

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, $Z_p = \{0, \ldots, 5988\}$; $\alpha = 2 \in Zp^*$ (TM), $a = 913 \in \{2, 3, \ldots, p-2\}$ (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 ElGamal 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 $\alpha = 5 \in Zp^*$ (TM)

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

Tính $\beta = \alpha^a \text{ mod } p = 5^{71} \text{ mod } 83 = 80$. 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: (Nguyên bản) 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 chứ 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 2: (Sưu tầm) Cho hệ RSA lấy p = 31, q = 41, b = 271.

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 chứ 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 = "SERIUS".

c. Giả sử bản mã thu được là C = <201, 793, 442, 18> hãy thực hiện giải mã để tìm ra thông điệp bản rõ ban đầu.

Đề 3: (Sưu tầm) Cho hệ RSA lấy p = 29, q = 43, b = 11.

a. Hãy tìm khóa công khai Kpub và khóa bí mật Kpri của hệ mã trên.

b. Để mã hóa các 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 = "TAURUS".

c. Giả sử bản mã thu được là C = <1, 169, 1206, 433> hãy thực hiện giải mã để tìm ra thông điệp bản rõ ban đầu.

Đề 4: (Nguyên bản) Cho hệ mật mã ElGamal 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. Để mã hóa các 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 cặp số (C1, C2) ∈ Zp. Cho k = 15, Hãy mã hóa bản rõ M = "SERIUS".

Đề 5: (Sưu tầm) Cho hệ mật mã ElGamal có p = 1187, α = 79 là một phần tử nguyên thủy của Zp*, a = 113 (phần tử bí mật mà người nhận chọn).

c. Hãy tìm khóa công khai Kpub và khóa bí mật Kpri của hệ mã trên.

d. Để mã hóa các 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 cặp số (C1, C2) ∈ Zp. Cho k = 14, Hãy mã hóa bản rõ M = "TAURUS".

e. Giả sử thu được bản mã là một tập các cặp (C1, C2) là < (358, 305), (1079, 283), (608, 925), (786, 391)>. Hãy giải mã và đưa ra thông điệp ban đầu.

Đáp án:

Đề 2:

a. Kpub = (271, 1271) Kpri = (31,31,41)

b. C = (180, 634, 82, 18)

c. P = (201, 700, 132, 18) = 201700132018.

Tách thành (20, 17, 00, 13, 20, 18) = URANUS

Đề 5:

a. Kpub = (1187, 79, 76) Kpri = (113)

b. (C1, C2) = {(981, 82), (981, 312), (981, 624), (981, 645)}

c. "150 802 001 724" = PICARY