HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGÂN HÀNG MẬT MÃ HỌC

(ngành Điện-Điện Tử)

Phần 1

1.1.Nêu ưu nhược điểm của các hệ mật khóa bí mật

+ Ưu điểm:

- Đơn giản (Thời gian xử lý nhanh, phần cứng yêu cầu thấp)

- Hiệu quả cao (Hệ số mở rộng bản tin R = 1; ví dụ với DES vào 64 bit ra 64 bit)

→ Dễ sử dụng cho các ứng dụng nhạy cảm với trễ và các ứng dụng di động.

+ Nhược điểm:

- Phải dùng kênh an toàn để truyền khóa (khó thiết lập, tốn kém)

- Việc tạo, giữ bí mật khóa phức tạp (khi làm việc trên mạng phải tạo nhiều khóa).

- Khó xây dựng các dịch vụ an toàn khác (như đảm bảo tính toàn vẹn, xác thực và chữ ký số)

→Để khắc phục các nhược điểm này phải sử dụng Hệ mật khóa công khai.

1.2. Nêu ưu nhược điểm của các hệ mật khóa công khai

+Ưu điểm:

- Không sử dụng kênh an toàn (nhược điểm của hệ mật khóa bí mật)

- Dễ bảo vệ,lưu trữ và sinh khóa

- Dễ tạo các dịch vụ an toàn khác

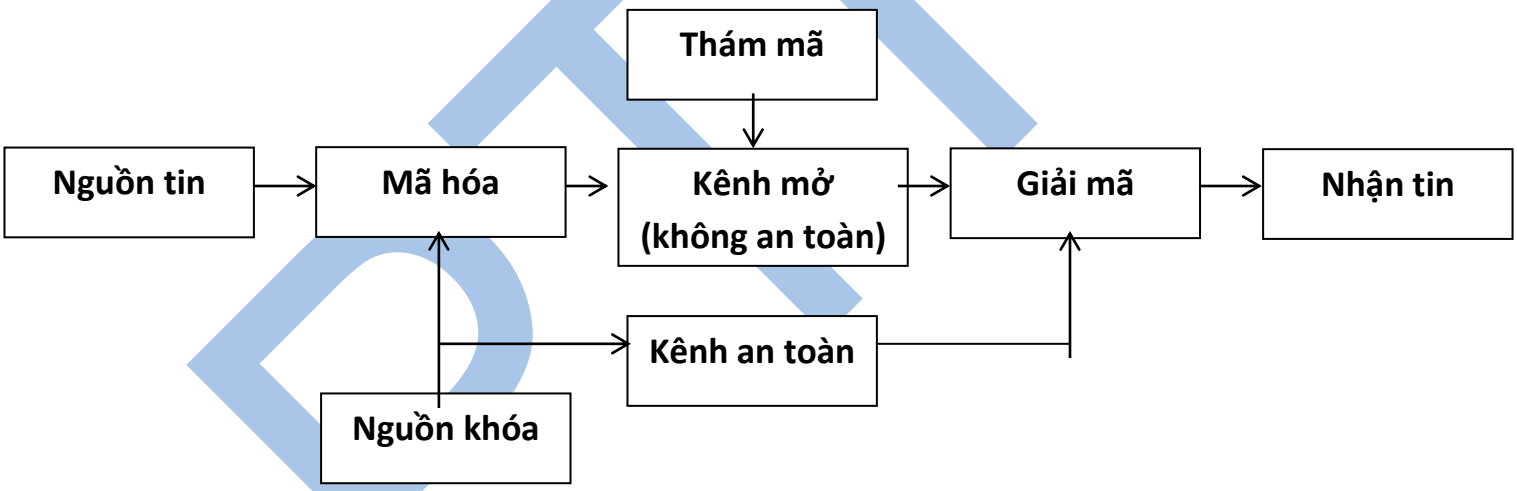
+Nhược điểm:

- Phức tạp (với trường số lớn thì phần cứng phức tạp)

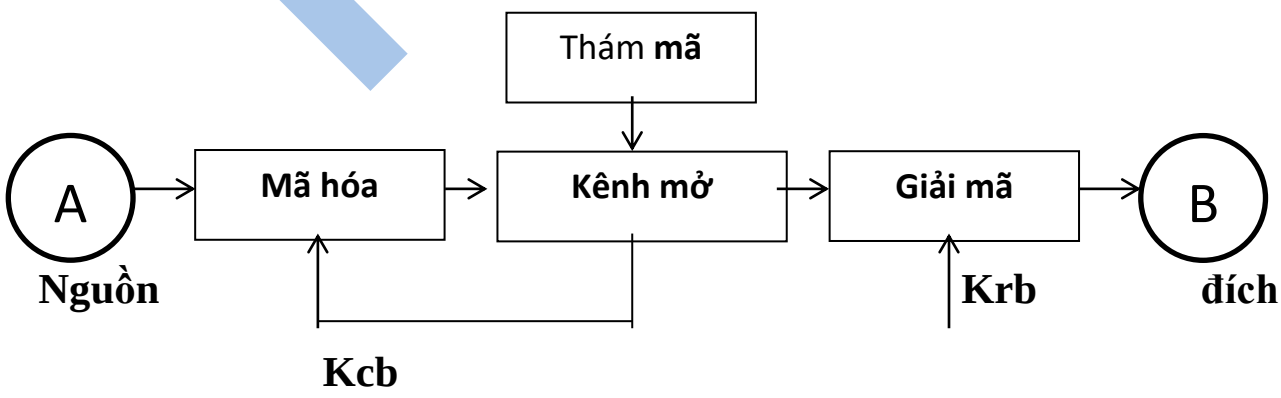
- Hiệu quả không cao

→ khó thực hiện các dịch vụ nhạy cảm đối với độ trễ và dịch vụ di động

1.3.Sơ đồ chức năng hệ thống truyền tin sử dụng mật khóa bí mật



1.4.Sơ đồ chức năng hệ thống truyền tinsử dụng mật khóacông khai



1.5.Mô tả hệ mật mã dịch vòng : xem trong bài giảng

1.6. Mô tả hệ mật Affine

– Mã hóa: $C \equiv aM + b \ mod \ n$ (đây là PT tuyến tính)

– Giải mã: $M \equiv C - b \ a - 1 \ mod \ n$

– Điều kiện để tồn tại: để có $a - 1$ thì $a, n = 1$ hay gcd $a, n = 1$; ƯCLN(a,n) =1

Nhận xét: Do khoảng trống xuất hiện nhiều lần trong văn bản, nên khi mã hóa nên mã hóa cả khoảng trống để giảm số lần xuất hiện

1.7. Mô tả hệ mật mã dòng Quá trình xử lý thông tin thực hiện trên từng bit

- Mã hóa : Ci = Mi + Ki mod 2

- Giải mã : Mi = Ci + Ki mod 2

Nhận xét: - Để hệ thống an toàn, dãy bit khóa ngẫu nhiên phải dài hơn bản tin |Ki|>|Mi|

- Việc tạo dãy ngẫu nhiên tốn kém và việc lưu trữ không hiệu quả, do đó phải tạo dãy giả ngẫu nhiên

1.8.Đa thức nguyên thủy? Giải thích pt đồng dư tạo m dãy

Đa thức bất khả quy bậc m được gọi là đa thức nguyên thủy nếu nó là ước của $x^n + 1 , n = 2^m - 1$; nhưng không là ước của $x^p + 1, p < n$

(có nghĩa là chia hết cho 1 và chính nó OK,tương tự số nguyên tố)

1.9.ứng dụng chữ kí số

Mua hàng trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến, kê khai thuế, nộp thuế trực tiếp qua mạng Internet.

1.10. Khái niệm , tính chất của hàm băm

Hàm băm là 1 ánh xạ h(x) thỏa mãn 2 tính chất : tính chất nén và tính chất dễ tính toán

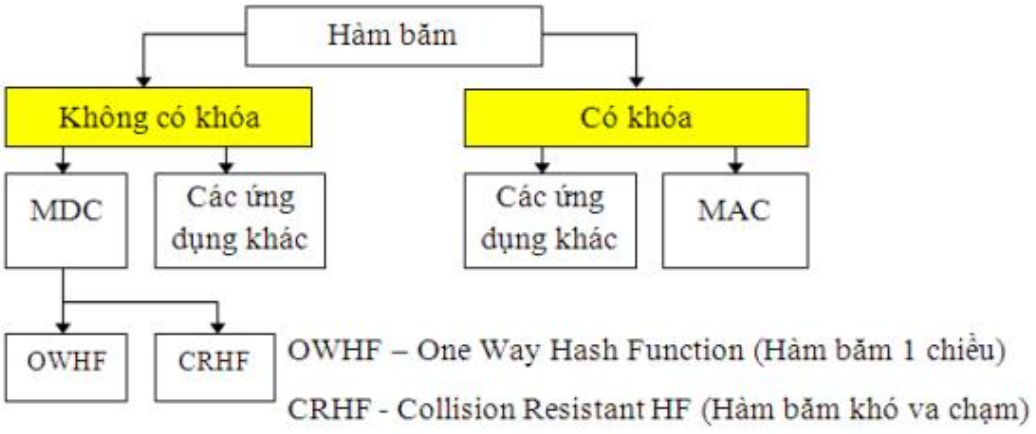
Các tính chất khác của hàm băm:

- Khó tìm nghịch ảnh : biết x thì sẽ biết y=h(x) nhưng nếu biết y sẽ khó tìm được x

-Khó tìm nghịch ảnh thứ 2 : biết x khó xác định $x' \neq x$ sao cho h(x)=h(x')

-Khó va chạm : khó xác định cặp x và x' để h(x)=h(x')

1.11.Phân loại , ứng dụng của hàm băm



MDC: Manipullation Detection Code: Mã phát hiện sửa đổi.

MAC: Message Authentication Code: Mã xác thực thông báo.

Phần 2

***2.1.(Diffie-Hellman) Tính khóa chung với p=11,α=7**

Gs A chọn x=4 , B chọn y=7

A chọn x=4 và gửi cho B:$7^4 mod\ 11 = 3$

B chọn y=7 và gửi cho A: $7^7 mod\ 11 = 6$

A nhận 6, B nhận 3 → k= $6^4 mod\ 11 = 3^7 mod\ 11 = 9$

2.2.(Diffie-Hellman) Tính khóa chung với p=13,α=11

Gs A chọn x=7 , B chọn y=5

A chọn x=7 và gửi cho B:$11^7 mod\ 13 = 2$

B chọn y=5 và gửi cho A: $11^5 mod\ 13 = 7$

A nhận 7, B nhận 2 → k= $7^7 mod\ 13 = 2^5 mod\ 13 = 6$

2.3.(Diffie-Hellman) Tính khóa chung với p=17,α=10

Gs A chọn x=3 , B chọn y=5

A chọn x=3 và gửi cho B:$10^3 mod\ 17 = 14$

B chọn y=5 và gửi cho A: $10^5 mod\ 17 = 6$

A nhận 6, B nhận 14 → k= $6^3 mod\ 17 = 14^5 mod\ 17 = 12$

2.4.(Diffie-Hellman) Tính khóa chung với p=19,α=3

Gs A chọn x=13 , B chọn y=11

A chọn x=13 và gửi cho B:$3^{13} mod\ 19 = 14$

B chọn y=11 và gửi cho A: $3^{11} mod\ 19 = 10$

A nhận 10, B nhận 14 → k= $10^{13} mod\ 19 = 14^{11} mod\ 19 = 13$

***2.5.(Omura-Massey) Truyền khóa bảo mật k từ A đến B với**

P=17,k=7, giả sử A(3,11) và B(5,13) THAY "M=" --> K TRONG DE BÀI SAU DO TÍNH BÌNH THUONG TRONG DANG BÀI OMURA-MASSEY

P=17 → p-1=16

A chọn (3,11) làm khóa bí mật thỏa mãn 3x11=33≡1 mod 16

B chọn (5,13) làm khóa bí mật thỏa mãn 5x13=65≡1 mod 16

Giả sử A cần gửi bản tin M=2 cho B . Qúa trình truyền tin như sau:

+ A tính $2^3 mod 17 = 8$ và gửi cho B → B tính $8^5 mod 17 = 9$ và gửi lại cho A

+ A tính $9^{11} mod 17 = 15$ và gửi cho B → B nhận 15 và giải mã ra bản tin M $=15^{13} mod 17 = 2$

2.6.(Omura-Massey) Truyền khóa bảo mật k từ A đến B với

P=19,k=6, giả sử A(5,11) và B(7,13)

P=19 → p-1=18

A chọn (5,11) làm khóa bí mật thỏa mãn 5x11=55≡1 mod 18

B chọn (7,13) làm khóa bí mật thỏa mãn 7x13=91≡1 mod 18

Giả sử A cần gửi bản tin M=2 cho B . Qúa trình truyền tin như sau:

+ A tính $2^5 mod 19 = 13$ và gửi cho B → B tính $13^7 mod 19 = 10$ và gửi lại cho A

+ A tính $10^{11} mod 19 = 14$ và gửi cho B → B nhận 14 và giải mã ra bản tin M $=14^{13} mod 19 = 2$

2.7.(Omura-Massey) Truyền khóa bảo mật k từ A đến B với

P=23,k=6, giả sử A(7,19) và B(5,9)

P=23 → p-1=22

A chọn (7,19) làm khóa bí mật thỏa mãn 7x19=133≡1 mod 22

B chọn (5,9) làm khóa bí mật thỏa mãn 5x9=45≡1 mod 22

Giả sử A cần gửi bản tin M=2 cho B . Qúa trình truyền tin như sau:

+ A tính $2^7 mod 23 = 13$ và gửi cho B → B tính $13^5 mod 23 = 4$ và gửi lại cho A

+ A tính $4^{19} mod 23 = 9$ và gửi cho B → B nhận 9 và giải mã ra bản tin M $=9^9 mod 23 = 2$

2.8.(Omura-Massey) Truyền khóa bảo mật k từ A đến B với

P=23,k=5, giả sử A(13,17) và B(3,15)

P=23 → p-1=22

A chọn (13,17) làm khóa bí mật thỏa mãn 13x17=221≡1 mod 22

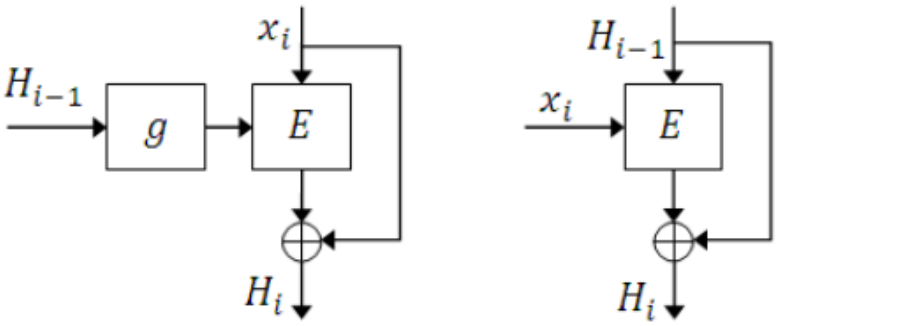
B chọn (3,15) làm khóa bí mật thỏa mãn 3x15=45≡1 mod 22

Giả sử A cần gửi bản tin M=1 cho B . Qúa trình truyền tin như sau:

+ A tính $1^{13} mod 23 = 1$ và gửi cho B → B tính $1^3 mod 23 = 1$ và gửi lại cho A

+ A tính $1^{17} mod 23 = 1$ và gửi cho B → B nhận 15 và giải mã ra bản tin M $=1^{15} mod 23 = 1$ (số to quá máy tính đếch tính được :v)

2.9.Mô tả sơ đồ Matyas-Oseas và Davies-Mayer → so sánh điểm khác



a) Sơ đồ Matyas-Mayer–Oseas *b) Sơ đồ Davies-Mayer*

a) Đầu vào x được phân chia thành các khối n bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh.
Ta được t khối n bit: x=(x1,x2,...,xt).
Phải xác định trước một giá trị ban đầu n bit (ký hiệu IV).Đầu ra là Ht được xác định như sau:

$$\begin{cases} H_0 = IV \\ H_i = E_{g(H_i-1)}x(i) \oplus x_i, 1 \le i \le t \end{cases}$$

b) Đầu vào x được phân chia thành các khối k bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh.
Biểu thị thông báo đã độn thành t khối k bit : x=(x1,x2,...,xt).
Xác định trước một giá trị ban đầu n bit (ký hiệu IV).Đầu ra là Ht được xác định như sau:

$$\begin{cases} H_0 = IV \\ H_i = E_{x_i}(H_i) \oplus H_{i-1}, 1 \le i \le t \end{cases}$$

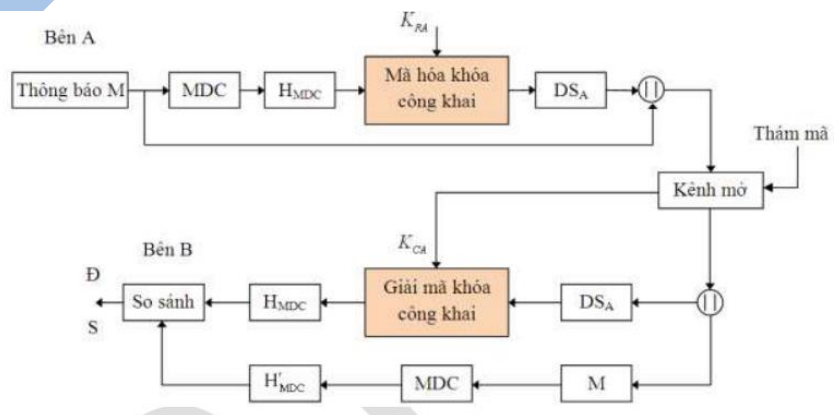
2.10.Các phương pháp đảm bảo tính toàn vẹn của dữ liệu

– Dùng MAC.

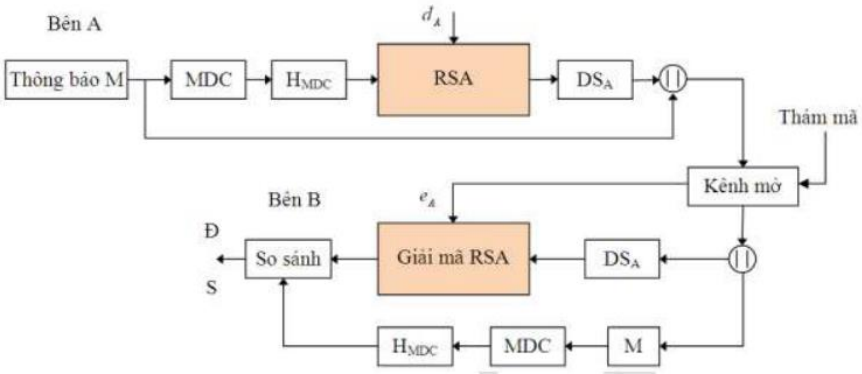
– Dùng các sơ đồ chữ ký số.

– Gắn (trước khi mã hoá) một giá trị thẻ xác thực bí mật vào văn bản được mã.

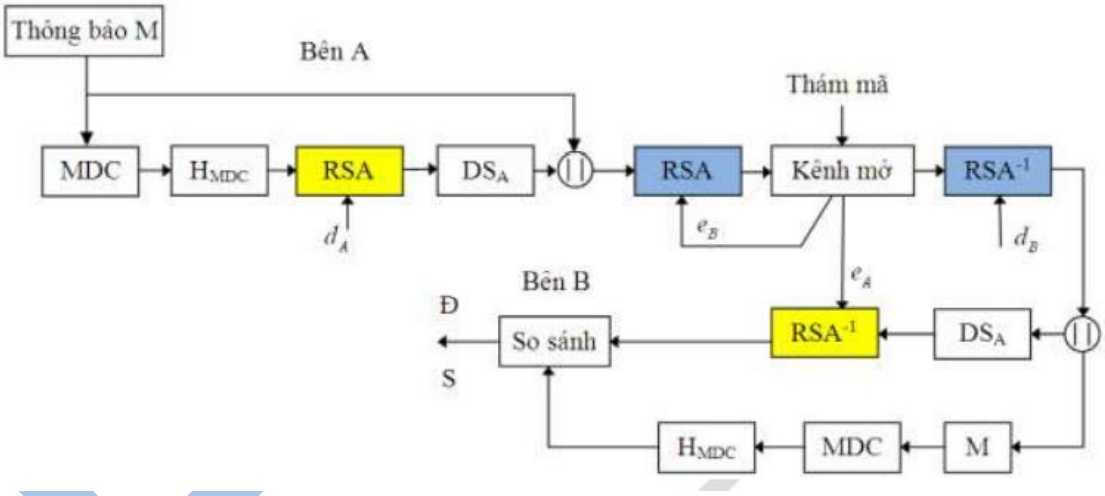
2.11.a.Mô tả sơ đồ chữ kí số sử dụng hàm băm không khóa



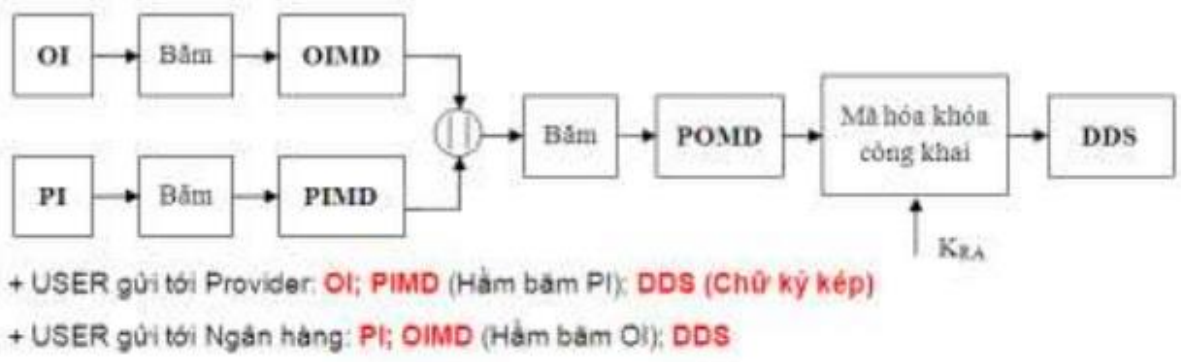
2.12.a. Xây dựng sơ đồ chữ kí số không bảo mật dùng RSA



2.12.b.Mô tả sơ đồ chữ kí số có bảo mật dùng RSA



2.13.Mô tả sơ đồ xây dựng chữ kí kép. Ý nghĩa của chữ kí kép trong giao dịch điện tử an toàn



• Khi mua hàng nếu không xem hàng có thể bị lừa đảo, nhưng có thể kiện được vì các thông tin về đơn hàng và chi trả các bên đều có ràng buộc.

• Giao dịch trên mạng vẫn có rủi ro, nhưng so với tiện ích sử dụng thì vẫn thấp hơn

2.14.Các chế độ hoạt động của DES

+ Các chế độ mã khối:

- Chế độ Quyển mã điện tử ECB (Electronic Code Book mode)

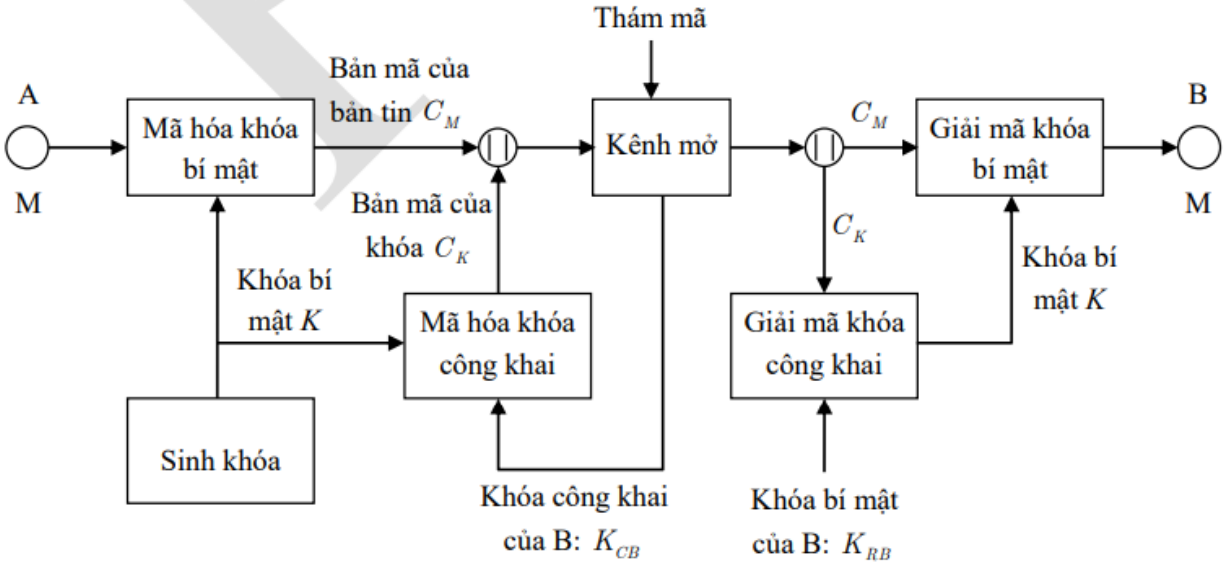
- Chế độ Liên kết mã khối CBC (Cipher Block Chaining mode)

+ Các chế độ mã dòng :

- Chế độ Phản hồi đầu ra OFB (Output Feedback Mode).

- Chế độ Phản hồi mật mã CFB (Code Feedback Mode)

2.15.Mô tả mô hình truyền tin bảo mật theo kiến trúc PGP



Phần 3

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	-			

***3.1.(từ 1 →12 mã dịch vòng)**

PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC

Khóa k=4,ta có bản rõ:

LOVE_MEANS_NEVER_HAVING_TO_SAY_YOU_ARE_SORRY

3.2. TPIEWI_WSQI_GVC_SJ_QC_LIEVX_AMPP_FVIEO

Khóa k=4

PLEASE_SOME_CRY_OF_MY_HEART_WILL_BREAK

3.3.RFS_NX_YMJ_RTXY_NSYJQQNLJSY_TK_YMJ_FSNRFQX_FSI_YMJ_RTXY_XNQQD

Khóa k=5

MAN_IS_THE_MOST_INTELLIGENT_OF_THE_ANIMALS_AND_

THE_MOST_SILLY

3.4.

YMJ_KTTQNXM_RFS_XJJPX_MFUUNSJXX_NS_YMJ_INXYFSHJ_YMJ_BNXJ_ LWTBX_NY_ZSIJW_MNX_KJJY

Khóa k=5

THE_FOOLISH_MAN_SEEKS_HAPPINESS_IN_THE_DISTANCE_

THE_WISE_GROWS_IT_UNDER_HIS_FEET

3.5.

APTL_PZ_TVYL_CHSBHISL_AOHU_TVULF_FVB_JHU_NLA_TVYL_TVULF_IBA_ FVB_JHUUVA_NLA_TVYL_APTL

Khóa k=7

TIME_IS_MORE_VALUABLE_THAN_MONEY_YOU_CAN_GET_

MORE_MONEY_BUT_YOU_CAN_MORE_TIME

3.6. PACGHJUHHCRICGRFWRUCRICPHGLFLQH

Khóa k=3

MY_DEGREE_OF_DOCTOR_OF_MEDICINE

3.7. RCEIJLWJJETKEITHYTWETKERJINHNSJ

Khóa k=5

MY_DEGREE_OF_DOCTOR_OF_MEDICINE

3.8.

LID_LSDMWDRSXDIZIVBHEBDGSRUYIVMRKDWSQIDJIEVDLEWDRSXDP IEVRIHDXLIDWIGVIXDSJDPMJI

K=4 (theo xác suất p(D)trong bản mã lớn nhất sẽ bằng p(_)trong bản rõ)

HE_WHO_IS_NOT_EVERYDAY_CONQUERING_SOME_FEAR_HAS_NOT_LEARNED_THE_SECRET_OF_LIFE.

3.9.

XMQIDMWDQSVIDZEPYEFPIDXLERDQSRIBDBSYDGERDKIXDQSVIDQSRIBDFYXDBSYDGERRSXDKIXDQSVIDXMQI

K=4 như trên

TIME_IS_MORE_VALUABLE_THAN_MONEY_YOU_CAN_GET_

MORE_MONEY_BUT_YOU_CAN_MORE_TIME

3.10

YMJEKTTQNXMERFSEXJJPXEMFUUNSJXXENSEYMJEINXYFSHJEYMJ EANXJELWTAXENYEZSIJWEMNXEKJJY

K=5

THE_FOOLISH_MAN_SEEKS_HAPPINESS_IN_THE_DISTANCE_

THE_WISE_GROWS_IT_UNDER_HIS_FEET

3.11

ZNKFZX_KFYOMTFULFOTZKRROMKTIKFOYFTUZFQTUBRKJMKFH_ZFOSGMOTGZOUT

K=6

THE_TRUE_SIGN_OF_INTELLIGENCE_IS_NOT_KNOWLEDGE_BUT_IMAGINATION.

3.12

_IDRIZIVDORS_DXLIDPSZIDSJDSYVDTEVIRXWD JSVDYWDXMPPD_IDLEZIDFIGSQIDTEVIRXW

K=4

WE_NEVER_KNOW_THE_LOVE_OF_OUR_PARENTS_FOR_US_TILL_WE_HAVE_BECOME_PARENTS.

***3.13(hoán vị)**

-EHOHWSI-ON-E-TREVADYC-YQNOREUGNIOS--EMAEFH-R-SATONEL-NRA-DEEHTES-ERCO-TL-FEFI

Đầu tiên ta chia dãy chữ này thành 13 phần bằng nhau như sau:

-EHOHW| SI-ON-| E-TREV| ADYC-Y| QNOREU| GNIOS-| -EMAEF| H-R-SA| TONEL-| NRA-DE| EHTES-| ERCO-T| L-FEFI

Ta có bảng của phép hoán vị ngược : (ý nghĩa: đổi vị trí 1 từ bản mã sang ví trí 3 của bản rõ)

1	2	3	4	5	6
3	2	1	6	5	4

HE_WHO|_IS_NO|T_EVER|YDAY_C|ONQUER|ING_SO|ME_FEA|R_HAS_|NOT_LE|ARNED_|THE_SE|CRET_O|F_LIFE

3.14(hoán vị)

-AMNTSI-MEH--SOTENITGLLI-NETTFO-AEH-AINMASL-TDN-MEH--SOTLISL--Y-

-AMNTSI-| MEH--SOT| ENITGLLI| -NETTFO-| AEH-AINM| ASL-TDN-| MEH- -SOT| LISL--Y-

Ta có bảng của phép hoán vị ngược : (ý nghĩa: đổi vị trí 1 từ bản mã sang ví trí 4 của bản rõ)

1	2	3	4	5	6	7	8
4	2	1	3	8	6	5	7

MAN_IS_T|HE_MOST_|INTELLIG|ENT_OF_T|HE_ANIMA|LS_

AND_|THE_MOST| _SILLY

***3.15.Xây dựng M dãy với đa thức nguyên thủy $g(x) = 1 + x + x^4$**

Và đa thức mầm $b(x) = 1 + x$. Biết rằng phương trình tạo ra M dãy có dạng $a(x) \equiv b(x).x^i mod\ g(x)$, i=0,1,2,...

Với m=4, $g(x) = 1 + x + x^4$

$a(x) \equiv b(x).x^i mod(1 + x + x^4)$

*Cách 1:

Coi $1 + x + x^4 = 0 \rightarrow 1 + x = x^4$. Mà $b(x) = 1 + x \rightarrow 1100$

Ta có bảng trạng thái của M-dãy:

STT	a(x)	$\underset{a}{\rightarrow}$
0	$1 + x$	1100
1	$x + x^2$	0110
2	$x^2 + x^3$	0011
3	$1 + x + x^3$	1101
4	$1 + x^2$	1010
5	$x + x^3$	0101
6	$1 + x + x^2$	1110
7	$x + x^2 + x^3$	0111
8	$1 + x + x^2 + x^3$	1111
9	$1 + x^2 + x^3$	1011
10	$1 + x^3$	1001
11	1	1000
12	x	0100
13	x^2	0010
14	x^3	0001
15	$1 + x$	1100

Khi lấy bất kì 1 cột nào trong 4 cột của $\underset{a}{\rightarrow}$ ta sẽ được 1 M-dãy

Chu kì của dãy $t = 2^m - 1 = 2^4 - 1 = 15$

Số con 1 trong dãy $N_1 = 2^{m-1} = 2^3 = 8$

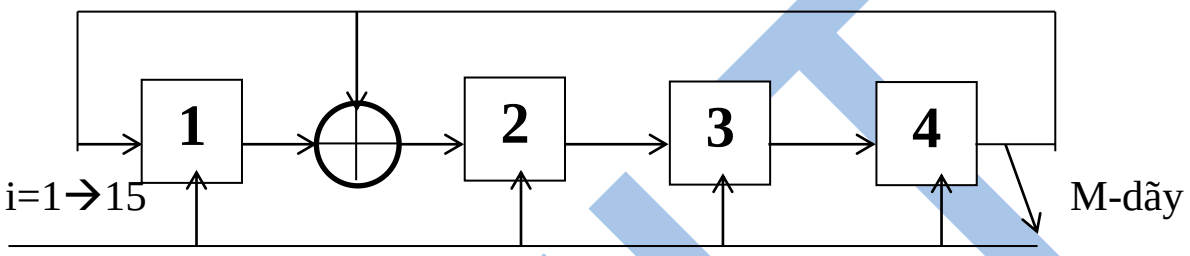
Số con 0 trong dãy $N_0 = 2^{m-1} - 1 = 2^3 - 1 = 7$

Khi $m \rightarrow \infty$ *ta có* $\lim_{m\to\infty} p(0) = \lim_{m\to\infty} p(1) = {}^1/_2$

*Cách 2:

Cấu trúc tổng quát mạch điện phần cứng M-dãy được thực hiện bằng các thanh ghi dịch hồi tiếp tuyến tính như sau:

$$g_0 = g_1 = g_4 = 1, g_2 = g_3 = 0$$



Nhịp	Trạng thái			
	M1	M2	M3	M4
0	1	1	0	0
1	0	1	1	0
2	0	0	1	1
3	1	1	0	1
4	1	0	1	0
5	0	1	0	1
6	1	1	1	0
7	0	1	1	1
8	1	1	1	1
9	1	0	1	1
10	1	0	0	1
11	1	0	0	0
12	0	1	0	0
13	0	0	1	0
14	0	0	0	1
15	1	1	0	0

3.16.Xây dựng M dãy với đa thức nguyên thủy $g(x) = 1 + x^3 + x^4$

Và đa thức mầm $b(x) = 1 + x$. Biết rằng phương trình tạo ra M dãy có dạng $a(x) \equiv b(x).x^i mod\ g(x)$, i=0,1,2,...

Với m=4, $g(x) = 1 + x^3 + x^4$

$a(x) \equiv b(x).x^i mod(1 + x^3 + x^4)$

*Cách 1:

Coi $1 + x^3 + x^4 = 0 \rightarrow 1 + x^3 = x^4$. Mà $b(x) = 1 + x \rightarrow 1100$

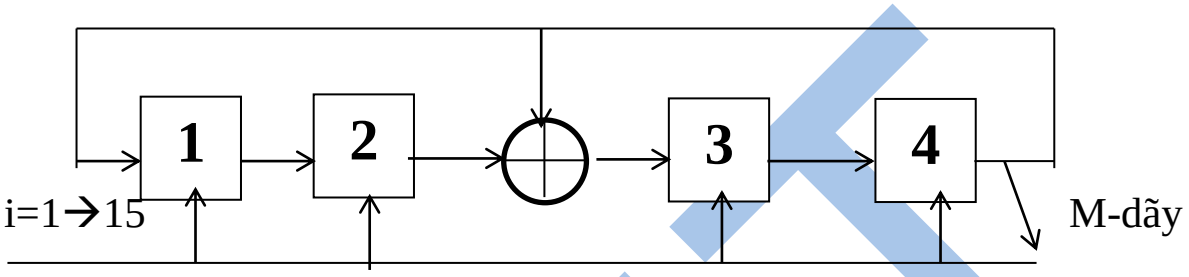
Ta có bảng trạng thái của M-dãy:

STT	a(x)	$\rightarrow$ a
0	$1 + x$	1100
1	$x + x^2$	0110
2	$x^2 + x^3$	0011
3	1	1000
4	x	0100
5	x^2	0010
6	x^3	0001
7	$1 + x^3$	1001
8	$1 + x + x^3$	1101
9	$1 + x + x^2 + x^3$	1111
10	$1 + x + x^2$	1110
11	$x + x^2 + x^3$	0111
12	$1 + x^2$	1010
13	$x + x^3$	0101
14	$1 + x^2 + x^3$	1011
15	$1 + x$	1100

*Cách 2:

Cấu trúc tổng quát mạch điện phần cứng M-dãy được thực hiện bằng các thanh ghi dịch hồi tiếp tuyến tính như sau:

$$g_0 = g_3 = g_4 = 1, g_1 = g_2 = 0$$



Nhịp	Trạng thái			
	M1	M2	M3	M4
0	1	1	0	0
1	0	1	1	0
2	0	0	1	1
3	1	0	0	0
4	0	1	0	0
5	0	0	1	0
6	0	0	0	1
7	1	0	0	1
8	1	1	0	1
9	1	1	1	1
10	1	1	1	0
11	1	0	0	0
12	1	0	1	0
13	0	1	0	1
14	1	0	1	1
15	1	1	0	0

***3.17.**

a)Hãy tạo M dãy theo phương trình đồng dư sau:

$\boldsymbol{a(x) \equiv b(x)c^i(x) mod(1 + x + x^2 + x^3 + x^4), i = 1, 2, \ldots}$

Với đa thức mầm $\boldsymbol{b(x) = 1}$ và $\boldsymbol{c(x) = 1 + x^2 + x^4 \leftrightarrow (024)}$

b)Tìm tất cả các đa thức nguyên thủy có $\boldsymbol{ord(c(x)) = 15}$ trong dãy này

có $h(x) = 1 + x + x^2 + x^3 + x^4$

a) Ta có $c(x) = 1 + x^2 + x^4 \leftrightarrow (024)$;Bậc $m = \deg(c(x)) = 4$

→ $M = 2^m - 1 = 15$ → i=1:15

Ta có $C = \{c^i(x) mod\ z^5 + 1; i = 1{:}\ 15\}$

={(024),(034),(1),(013),(014),(2),(124),(012),(3),(023),(123),(4),(134),(234),(0)}

$B = b(x).C\ mod\ z^5 + 1 = 1.C\ mod\ z^5 + 1 = C$

$A = B\ mod\ h(x) = C\ mod\ h(x)$

={(13),(12),(1),(013),(23),(2),(03),(012),(3),(023),(123),(0123),(02),(01),(0)}

b) Xét $C = \{c^i(x) mod\ z^5 + 1; i = 1{:}\ 15\}$; cấp của C(x) : ord(c(x))=15

ta có c(x)=(024) là phần tử nguyên thủy

→ $c^i(x)$ là đa thức nguyên thủy → $i \in \{1,2,4,7,8,11,13,14\}$

→ các đa thức nguyên thủy có ord(c(x))=15 là :

$C^1(x) = (024) = 1 + x^2 + x^4$; $C^{14}(x) = (234) = x^2 + x^3 + x^4$

$C^2(x) = (034) = 1 + x^3 + x^4$; $C^{13}(x) = (134) = x + x^3 + x^4$

$C^4(x) = (013) = 1 + x + x^3$; $C^{11}(x) = (123) = x + x^2 + x^3$

$C^7(x) = (124) = x + x^2 + x^4$; $C^8(x) = (012) = 1 + x + x^2$

3.18.a)Hãy tạo M dãy theo phương trình đồng dư sau:

$\boldsymbol{a(x) \equiv b(x)c^i(x) mod(1 + x + x^2 + x^3 + x^4), i = 1, 2, \ldots}$

Với đa thức mầm $\boldsymbol{b(x) = 1 + x}$ và $\boldsymbol{c(x) = 1 + x + x^2} \leftrightarrow$ (012)

b)Tìm tất cả các đa thức nguyên thủy có $\boldsymbol{ord(c(x)) = 15}$ trong dãy này

có $h(x) = 1 + x + x^2 + x^3 + x^4$

a) Ta có $c(x) = 1 + x + x^2 \leftrightarrow (012)$;Bậc $m = \deg(c(x)) = 4$

→ $M = 2^m - 1 = 15$ → i=1:15

Ta có $C = \{c^i(x) mod\ z^5 + 1; i = 1{:}\ 15\}$

={(012),(024),(3),(034),(023),(1),(123),(013),(4),(014),(134),(2),(234),(124),(0)}

$B = b(x).C\ mod\ z^5 + 1 = (1 + x).C\ mod\ z^5 + 1$

={(03),(1234),(34),(13),(0124),(12),(14),(0234),(04),(24),(0123),(23),(02),(0134),(01)}

$A = B\ mod\ h(x) = C\ mod\ h(x)$

={(03),(0),(012),(13),(3),(12),(023),(1),(123),(013),(0123),(23),(02),(2),(01)}

b) Xét $C = \{c^i(x) mod\ z^5 + 1; i = 1{:}\ 15\}$; cấp của C(x) : ord(c(x))=15

ta có c(x)=(012) là phần tử nguyên thủy

→ $c^i(x)$ là đa thức nguyên thủy → $i \in \{1,2,4,7,8,11,13,14\}$

→ các đa thức nguyên thủy có ord(c(x))=15 là :

$C^1(x) = (012) = 1 + x + x^2$; $C^{14}(x) = (124) = x + x^2 + x^3$

$C^2(x) = (024) = 1 + x^2 + x^4$; $C^{13}(x) = (234) = x^2 + x^3 + x^4$

$C^4(x) = (034) = 1 + x^3 + x^4$; $C^{11}(x) = (134) = x + x^3 + x^4$

$C^7(x) = (123) = x + x^2 + x^3$; $C^8(x) = (013) = 1 + x + x^3$

Thuật toán nhân và bình phương:

Tính $x = a^b \, mod \, c$

Dùng máy tính chuyển b từ hệ Decima sang hệ Binary sau đó đếm thứ tự bit từ 0

Ví dụ: $302_{10} = 100101110_2$

→ $302 = 2^1 + 2^2 + 2^3 + 2^5 + 2^8 = 2 + 4 + 8 + 32 + 256$

(đếm thứ tự từ phải qua trái)

Vậy $a^{302} mod \, c = (a^2 * a^4 * a^8 * a^{32} * a^{256}) mod \, c$

Lấy $a^2 mod \, c \, , a^4 mod \, c \, , a^8 mod \, c \, , a^{32} mod \, c, a^{256} mod \, c$

Nhân kết quả với nhau là ra đáp án.

***3.19.Cho hệ mật RSA với p=13,q=17**

a) Tính $n \, , \varphi(n)$ b) Tính d biết e=19

c) Mã hóa cho bản tin M=7 bằng thuật toán nhân và bình phương

a) n=pq=221 , $\varphi(n) = (p-1)(q-1) = 192$

b) e=19 thỏa mãn $(e, \varphi(n)) = 1$

$ed \equiv 1 mod \varphi(n)$ → 19d ≡ 1mod192

→ 19d=1+192k → $d = \frac{1+192k}{19}$

Với k=9 tìm được d=91 (với p,q nhỏ ta có thể giải pt đồng dư)

Vậy khóa công khai là (221,19) và khóa bí mật là 91

Hoặc khóa công khai là (221,91) và khóa bí mật là 19

c)ta có k=e=19=16+2+1 → 10011: $k_4k_3k_2k_1k_0$

(1) : b<= 1

(2) : A<= M=7

(3) : $k_0 = 1$ → b <= M=7

(4) : for i= 1:4

i=1 => $A = A^2 = 7^2 = 49$; $k_1 = 1$ → b <= A*b mod n= 49.7mod221=122

i=2 => $A = A^2 = 49^2 mod\ n = 191$; $k_2 = 0$ → b <= 122

i=3 => $A = A^2 = 191^2 mod\ n = 16$; $k_3 = 0$ → b <= 122

i=4=> $A = A^2 = 16^2 mod\ n = 35$; $k_4 = 1$ → b<= 35.122mod221=71

(5) : vậy b=71

3.20. Cho hệ mật RSA với p=19,q=17

a) Tính n , $\varphi(n)$ b) Tính d biết e=91

c) Mã hóa cho bản tin M=6 bằng thuật toán nhân và bình phương

a) n=pq=323 , $\varphi(n) = (p-1)(q-1) = 288$

b) e=91 thỏa mãn $(e, \varphi(n)) = 1$

$ed \equiv 1 mod \varphi(n)$ → 91d ≡ 1mod288

→ 91d=1+288k → $d = \frac{1+288k}{91}$

Với k=6 tìm được d=19 (với p,q nhỏ ta có thể giải pt đồng dư)

Vậy khóa công khai là (323,91) và khóa bí mật là 19

Hoặc khóa công khai là (323,19) và khóa bí mật là 91

c) ta có k=e=91=64+16+8+2+1 → 1011011: $k_6k_5k_4k_3k_2k_1k_0$

(1) : b<= 1

(2) : A<= M=6

(3) : $k_0 = 1$ → b <= M=6

(4) : for i= 1:6

i=1 => $A = A^2 = 6^2 = 36$; $k_1 = 1$ → b <= A*b mod n= 36.6mod n=216

i=2 => $A = A^2 = 36^2 mod\ n = 4$; $k_2 = 0$ → b <= 216

i=3 => $A = A^2 = 4^2 mod\ n = 16$; $k_3 = 1$ → b <= 16.216mod n= 226

i=4 => $A = A^2 = 16^2 mod\ n = 256$; $k_4 = 1$ → b<= 256.226mod n=39

i=5 => $A = A^2 = 256^2 mod\ n = 290$; $k_5 = 0$ → b <= 39

i=6 => $A = A^2 = 290^2 mod\ n = 120$; $k_2 = 1$ → b <= 120.39mod n=158

(5) : vậy b=158

3.21. Cho hệ mật RSA với p=19,q=23

a) Tính n , $\varphi(n)$ b) Tính d biết e=41

c) Mã hóa cho bản tin M=9 bằng thuật toán nhân và bình phương

a) n=pq=437 , $\varphi(n) = (p-1)(q-1) = 396$

b) e=41 thỏa mãn $(e, \varphi(n)) = 1$

$ed \equiv 1 mod \varphi(n)$ → 41d ≡ 1mod 396

→ 41d=1+396k → $d = \frac{1+396k}{41}$

Với k=3 tìm được d=29

Vậy khóa công khai là (437,41) và khóa bí mật là 29

Hoặc khóa công khai là (437,29) và khóa bí mật là 41

c) ta có k=e=41=32+8+1 → 101001: $k_5k_4k_3k_2k_1k_0$

(1) : b<= 1

(2) : A<= M=9

(3) : $k_0 = 1$ → b <= M=9

(4) : for i= 1:5

i=1 => $A = A^2 = 9^2 = 81$; $k_1 = 0$ → b <= 9

i=2 => $A = A^2 = 81^2 mod\ n = 6$; $k_2 = 0$ → b <= 9

i=3 => $A = A^2 = 6^2 mod\ n = 36$; $k_3 = 1$ → b <= 36.9mod n= 324

i=4 => $A = A^2 = 36^2 mod\ n = 422$; $k_4 = 0$ → b<= 324

i=5 => $A = A^2 = 422^2 mod\ n = 225$; $k_5 = 1$ → b <= 255.324mod n=358

(5) : vậy b=358

3.22. Cho hệ mật RSA với p=23,q=29

a) Tính n , $\varphi(n)$ b) Tính d biết e=29

c) Mã hóa cho bản tin M=8 bằng thuật toán nhân và bình phương

a) n=pq=667 , $\varphi(n) = (p-1)(q-1) = 616$

b) e=29 thỏa mãn $(e, \varphi(n)) = 1$

$ed \equiv 1 mod \varphi(n)$ → 29d ≡ 1mod 616

→ 29d=1+616k → $d = \frac{1+616k}{29}$

Với k=4 tìm được d=85

Vậy khóa công khai là (667,85) và khóa bí mật là 29

Hoặc khóa công khai là (667,29) và khóa bí mật là 85

c) ta có k=e=29=16+8+4+1 → 11101: $k_4k_3k_2k_1k_0$

(1) : b<= 1

(2) : A<= M=8

(3) : $k_0 = 1$ → b <= M=8

(4) : for i= 1:4

i=1 => $A = A^2 = 8^2 = 64$; $k_1 = 0$ → b <= 8

i=2 => $A = A^2 = 64^2 mod\ n = 94$; $k_2 = 1$ → b <= 8.94 mod n=85

i=3 => $A = A^2 = 94^2 mod\ n = 165$; $k_3 = 1$ → b <= 165.85mod n= 18

i=4 => $A = A^2 = 165^2 mod\ n = 545$; $k_4 = 1$ → b<= 545.18 mod n=472

(5) : vậy b=472

***3.23. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.**

a) Hãy xây dựng khóa công khai cho A, với p =17 và α = 3 là phần tử nguyên thủy của $\mathbb{Z}_{17}$, giả sử khóa bí mật của A là a = 6 .

b) Giả sử B chọn số ngẫu nhiên k = 4 , hãy mã hoá bản tin M = 7 gửi từ B đến A bằng khóa công khai tại phần a

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b

+ Tạo khóa: A chọn $\boldsymbol{p}$ = **17**;$\boldsymbol{\alpha}$ = **3**; a = 6;

A tính $3^6 mod 17 = 15$ → Khóa công khai của A: (17,3,15)

và khóa bí mật của A: a = 6

+ Mã hóa: B cần gửi bản rõ m = 7 cho A

Bước 1: B nhận khóa công khai của A: (17,3,15)

Bước 2: B chọn k = 4 ,$\gamma = 3^4 mod 17 = 13$; $\delta = 7 * 15^4 mod 17 = 10$

Bước 3: B gửi bản mã C = (13,10) cho A

+ Giải mã: A nhận bản mã C và giải mã

Bước 1: A tính $\gamma^{16-6} = 13^{10} mod 17 = 16$

Bước 2: A tính $\delta * \gamma^{p-1-a} = 10 * 16 mod 17 = 7$

3.24. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với p =17 và α =11 là phần tử nguyên thủy của $\mathbb{Z}_{17}$, giả sử khóa bí mật của A là a = 5 .

b) Giả sử B chọn số ngẫu nhiên k = 7 , hãy mã hoá bản tin M = 8 gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b

+ Tạo khóa: A chọn $\boldsymbol{p} = \mathbf{17}$;$\boldsymbol{\alpha} = 11$; a = 5;

A tính $11^5 mod 17 = 10$ → Khóa công khai của A: (17,11,10)

và khóa bí mật của A: a = 5

+ Mã hóa: B cần gửi bản rõ m = 8 cho A

Bước 1: B nhận khóa công khai của A: (17,11,10)

Bước 2: B chọn k = 7 ,$\gamma = 11^7 mod 17 = 3$; $\delta = 8 * 10^7 mod 17 = 6$

Bước 3: B gửi bản mã C = (3,6) cho A

+ Giải mã: A nhận bản mã C và giải mã

Bước 1: A tính $\gamma^{17-1-5} = 3^{11} mod 17 = 7$

Bước 2: A tính $\delta * \gamma^{p-1-a} = 6 * 7\, mod 17 = 8$

3.25. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với p =19 và α =13 là phần tử nguyên thủy của $\mathbb{Z}_{19}$, giả sử khóa bí mật của A là a = 4.

b) Giả sử B chọn số ngẫu nhiên k = 5 , hãy mã hoá bản tin M = 7 gửi từ B đến A bằng khóa công khai tại phần a)

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b)

+ Tạo khóa: A chọn $\boldsymbol{p}$ = 19;$\boldsymbol{\alpha}$ = 13; a = 4;

A tính $13^4 mod 19 = 4$ → Khóa công khai của A: (19,13,4)

và khóa bí mật của A: a = 4

+ Mã hóa: B cần gửi bản rõ m = 7 cho A

Bước 1: B nhận khóa công khai của A: (19,13,4)

Bước 2: B chọn k = 5 ,$\gamma = 13^5 mod 19 = 14$; $\delta = 7 * 4^5 mod 19 = 5$

Bước 3: B gửi bản mã C = (14,5) cho A

+ Giải mã: A nhận bản mã C và giải mã

Bước 1: A tính $\gamma^{19-1-4} = 14^{14} mod 19 = 9$

Bước 2: A tính $\delta * \gamma^{p-1-a} = 5 * 9 \, mod 17 = 7$

3.26. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với p =19 và α =14 là phần tử nguyên thủy của $\mathbb{Z}_{19}$, giả sử khóa bí mật của A là a = 6 .

b) Giả sử B chọn số ngẫu nhiên k = 5 , hãy mã hoá bản tin M = 4 gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b

+ Tạo khóa: A chọn $\boldsymbol{p}$ = 19;$\boldsymbol{\alpha}$ = 14; a = 6;

A tính $14^6 mod 19 = 7$ → Khóa công khai của A: (19,14,7)

và khóa bí mật của A: a = 6

+ Mã hóa: B cần gửi bản rõ m = 4 cho A

Bước 1: B nhận khóa công khai của A: (19,14,7)

Bước 2: B chọn k = 5 ,$\gamma = 14^5 mod 19 = 10$; $\delta = 4 * 7^5 mod 17 = 6$

Bước 3: B gửi bản mã C = (10,6) cho A

+ Giải mã: A nhận bản mã C và giải mã

Bước 1: A tính $\gamma^{19-1-6} = 10^{12} mod 19 = 7$

Bước 2: A tính $\delta * \gamma^{p-1-a} = 6 * 7\ mod 19 = 4$

***3.27. Cho $\mathbb{Z}_{13}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{13}$**

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{13}$

b) Giải bài toán logarit rời rạc: Tìm $log_a y$ với α là phần tử nguyên thuỷ và y $\in \mathbb{Z}_{13}$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{13}$

a) có p=13, α=2 ; ta có bảng giá trị

I	1	2	3	4	5	6	7	8	9	10	11	12
2^i Mod13	2	4	8	3	6	12	11	9	5	10	7	1
$\log_2 i$	12	1	4	2	9	5	11	3	8	10	7	6
$\log_7 i$	12	11	8	10	3	7	1	9	4	2	5	6
6^i Mod13	6	10	8	9	2	12	7	3	5	4	11	1
$\log_6 i$	12	5	8	10	9	1	7	3	4	2	11	6
$\log_{11} i$	12	7	4	2	3	11	5	9	8	10	1	6

Do 12=2^2 * 3 → N(i)=12(1-1/2)(1-1/3)=4

các giá trị i thỏa mãn (i,12)=1 là i=(1,5,7,11)

→ có 4 phần tử nguyên thủy : $2^1 = 2; 2^5 = 6; 2^7 = 11; 2^{11} = 7$

b) như bảng tìm các log của các cặp số nghịch đảo

c)

I	1	2	3	4	5	6	7	8	9	10	11	12
i^2	1	4	9	3	12	10	10	12	3	9	4	1

→Các thặng dư bậc 2 Q={1;3;4;9;10;12}

$\sqrt{1} = (1; 12), \sqrt{3} = (4; 9), \sqrt{4} = (2; 11), \sqrt{9} = (3; 10), \sqrt{10} = (6; 7), \sqrt{12} = (5; 8)$

3.28. Cho $\mathbb{Z}_{17}$, biết $\alpha = 3$ là phần tử nguyên thuỷ của $\mathbb{Z}_{17}$

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{17}$

b) Giải bài toán logarit rời rạc: Tìm $log_a y$ với α là phần tử nguyên thuỷ và $y \in \mathbb{Z}_{17}$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{17}$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^i Mod17	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$\log_3 i$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
$\log_5 i$	16	2	15	4	11	1	5	6	14	13	9	3	12	7	10	8
7^i Mod17	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
$\log_7 i$	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8
$\log_6 i$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

16=2^4 → N(i)=16(1-1/2)(1-1/2)=4

Các giá trị i thỏa mãn (i,16)=1 là i=(1,5,11,15)

→Có 4 phần tử nguyên thủy $3^1 = 3; 3^5 = 5; 3^{11} = 7; 3^{15} = 6$

b) như bảng

c)

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i^2	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

→Các thặng dư bậc 2 Q={1;2;4;8;9;13;15;16}

$$\sqrt{1} = (1;16), \sqrt{2} = (6;11), \sqrt{4} = (2;15), \sqrt{8} = (5;12), \sqrt{9} = (3;14),$$
$$\sqrt{13} = (9;8), \sqrt{15} = (10;7), \sqrt{16} = (4;13)$$

3.29. Cho $\mathbb{Z}_{11}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{11}$

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{11}$

b) Giải bài toán logarit rời rạc: Tìm $log_a y$ với α là phần tử nguyên thuỷ và y $\in \mathbb{Z}_{11}$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{11}$

a) có p=11, α =2

i	1	2	3	4	5	6	7	8	9	10
2^i Mod11	2	4	8	5	10	9	7	3	6	1
$\log_2 i$	10	1	8	2	4	9	7	3	6	5
$\log_6 i$	10	9	2	8	6	1	3	7	4	5
7^i Mod11	7	5	2	3	10	4	6	9	8	1
$\log_7 i$	10	3	4	6	2	7	1	9	8	5
$\log_8 i$	10	7	6	4	8	3	9	1	2	5

Do 10=2 * 5 → N(i)=10(1-1/2)(1-1/5)=4

các giá trị i thỏa mãn (i,10)=1 là i=(1,3,7,9)

→ có 4 phần tử nguyên thủy: 2,8,7,6

b)*như bảng*

c)

i	1	2	3	4	5	6	7	8	9	10
i^2	1	4	9	5	3	3	5	9	4	1

→Các thặng dư bậc 2 Q={1;3;4;5;9}

$$\sqrt{1} = (1;10), \sqrt{3} = (6;5), \sqrt{4} = (2;9), \sqrt{5} = (4;7), \sqrt{9} = (3;8)$$

3.30. Cho $\mathbb{Z}_{19}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{19}$

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{19}$

b) Giải bài toán logarit rời rạc: Tìm $log_a y$ với α là phần tử nguyên thuỷ và y $\in \mathbb{Z}_{19}$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{19}$

a) b) có p=19, α =2

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^i Mod19	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3^i Mod19	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
14^i Mod19	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
$\log_2 i$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
$\log_{10} i$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9
$\log_3 i$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9
$\log_{13} i$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
$\log_{14} i$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9
$\log_{15} i$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Do 18=3^2 * 2 → N(i)=18(1-1/2)(1-1/3)=6

các giá trị i thỏa mãn (i,18)=1 là i=(1,5,7,11,13,17)

→ có 6 phần tử nguyên thủy :2,13,14,15,3,10

c)

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i^2	1	4	9	16	6	17	13	7	5	5	7	13	17	6	16	9	4	1

Phần 4

***4.1. Cho đường cong Elliptic $y^2 = (x^3 + x + 1) mod 13$**

Xây dựng nhóm E_{13} với P=(1,4) là phần tử nguyên thủy (tìm các điểm của E_{13}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 13 \neq 0$

i	1	2	3	4	5	6	7	8	9	10	11	12
2^i	2	4	8	3	6	12	11	9	5	10	7	1

Theo nguyên tắc tính các điểm :

+Điểm P(1,4)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 13 = \frac{1}{2} mod 13 = 7$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 7^2 - 1 - 1 = 47 mod 13 = 8$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 7(1 - 8) - 4 = -53 mod 13 = 12$

→2P(8,12)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 13 = \frac{12-4}{8-1} mod 13 = \frac{8}{7} mod 13 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 3^2 - 1 - 8 = 0 mod 13 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 3(1 - 0) - 4 = -1 mod 13 = 12$

→3P(0,12)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 13 = \frac{12-4}{0-1} mod 13 = -8 mod 13 = 5$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 5^2 - 1 - 0 = 24 mod 13 = 11$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 5(1 - 11) - 4 = -54 mod 13 = 11$

→4P(11,11)

+Điểm 5P=P+4P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{11-4}{11-1} mod 13 = \frac{7}{10} mod 13 = 2$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 2^2 - 1 - 11 = -8 mod 13 = 5$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 2(1-5) - 4 = -12 mod 13 = 1$

→5P(5,1)

+Điểm 6P=P+5P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{1-4}{5-1} mod 13 = -\frac{3}{4} mod 13 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 9^2 - 1 - 5 = 75 mod 13 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 9(1-10) - 4 = -85 mod 13 = 6$

→6P(10,6)

+Điểm 7P=P+6P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{6-4}{10-1} mod 13 = \frac{2}{9} mod 13 = 6$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 6^2 - 1 - 10 = 25 mod 13 = 12$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 6(1-12) - 4 = -70 mod 13 = 8$

→7P(12,8)

+Điểm 8P=P+7P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{8-4}{12-1} mod 13 = \frac{4}{11} mod 13 = 11$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 11^2 - 1 - 12 = 108 mod 13 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 11(1-4) - 4 = -37 mod 13 = 2$

→8P(4,2)

+Điểm 9P=P+8P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{2-4}{4-1} mod 13 = \frac{-2}{3} mod 13 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 8^2 - 1 - 4 = 59 mod 13 = 7$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 8(1-7) - 4 = -52 mod 13 = 0$

→9P(7,0)

→ Số lượng phần tử của nhóm $E_{13}(1,1) = 2 * 9 = 18$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (18-k)P(x, 13-y)

+Điểm 10P= -8P →10P(4,-2)=10P(4,11)

+Điểm 11P= -7P →11P(12,-8)=11P(12,5)

+Điểm 12P= -6P →12P(10,-6)=12P(10,7)

+Điểm 13P= -5P →13P(5,-1)=13P(5,12)

+Điểm 14P= -4P →14P(11,-11)=14P(11,2)

+Điểm 15P= -3P →15P(0,-12)=15P(0,1)

+Điểm 16P= -2P →16P(8,-12)=16P(8,1)

+Điểm 17P= -P →17P(1,-4)=17P(1,9)

+Điểm 18P=0

Các điểm nguyên thủy kP có (k,18)=1

Hay k={1,5,7,11,13,17}

→các điểm nguyên thủy: P,5P,7P,11P,13P,17P

4.2. Cho đường cong Elliptic $y^2 = (x^3 + x + 1) mod 13$

Xây dựng nhóm E_{13} với P=(5,1) là phần tử nguyên thủy (tìm các điểm của E_{13}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 13 \neq 0$

i	1	2	3	4	5	6	7	8	9	10	11	12
2^i	2	4	8	3	6	12	11	9	5	10	7	1

Theo nguyên tắc tính các điểm :

+Điểm P(5,1)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2+a}{2y_1} mod 13 = 38 mod 13 = 12$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 12^2 - 5 - 5 = 134 mod 13 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 12(5-4) - 1 = 11 mod 13 = 11$

→2P(4,11)

+Điểm 3P=P+2P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{11-1}{4-5} mod 13 = -10 mod 13 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 3^2 - 5 - 4 = 0 mod 13 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 3(5-0) - 1 = 14 mod 13 = 1$

→3P(0,1)

+Điểm 4P=P+3P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{1-1}{0-5} mod 13 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 0^2 - 5 - 0 = -5 mod 13 = 8$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 0(5-8) - 1 = -1 mod 13 = 12$

→4P(8,12)

+Điểm 5P=P+4P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{12-1}{8-5} mod 13 = \frac{11}{3} mod 13 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 8^2 - 5 - 8 = 51 mod 13 = 12$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 8(5-12) - 1 = -57 mod 13 = 8$

→5P(12,8)

+Điểm 6P=P+5P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{8-1}{12-5} mod 13 = 1 mod 13 = 1$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 1^2 - 5 - 12 = -16 mod 13 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 1(5-10) - 1 = -6 mod 13 = 7$

→6P(10,7)

+Điểm 7P=P+6P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{7-1}{10-5} mod 13 = \frac{6}{5} mod 13 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 9^2 - 5 - 10 = 66 mod 13 = 1$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 9(5-1) - 1 = 35 mod 13 = 9$

→7P(1,9)

+Điểm 8P=P+7P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{9-1}{1-5} mod 13 = -2 mod 13 = 11$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 11^2 - 5 - 1 = 115 mod 13 = 11$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 11(5-11) - 1 = -67 mod 13 = 11$

→8P(11,11)

+Điểm 9P=P+8P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 13 = \frac{11-1}{11-5} mod 13 = \frac{10}{6} mod 13 = 6$

$x_3 = \lambda^2 - x_1 - x_2 mod 13 = 6^2 - 5 - 11 = 20 mod 13 = 7$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 13 = 6(5-7) - 1 = -13 mod 13 = 0$

→9P(7,0)

→ Số lượng phần tử của nhóm $E_{13}(1,1) = 2 * 9 = 18$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (18-k)P(13-y)

+Điểm 10P= -8P →10P(11,-11)=10P(11,2)

+Điểm 11P= -7P →11P(1,-9)=11P(1,4)

+Điểm 12P= -6P →12P(10,-7)=12P(10,6)

+Điểm 13P= -5P →13P(12,-8)=13P(12,5)

+Điểm 14P= -4P →14P(8,-12)=14P(8,1)

+Điểm 15P= -3P →15P(0,-1)=15P(0,12)

+Điểm 16P= -2P →16P(4,-11)=16P(4,2)

+Điểm 17P= -P →16P(5,-1)=17P(5,12)

+Điểm 18P=0

Các điểm nguyên thủy kP có (k,18)=1

Hay k={1,5,7,11,13,17}

→các điểm nguyên thủy: P,5P,7P,11P,13P,17P

***4.3. Cho đường cong Elliptic $y^2 = x^3 + x + 6 mod 17$**

Xây dựng nhóm E_{17} với P=(2,4) là phần tử nguyên thủy (tìm các điểm của E_{17}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

+Điểm P(2,4)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 17 = \frac{13}{8} mod 17 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 60 mod 17 = 9$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -60 mod 17 = 8$

→2P(9,8)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{8-4}{9-2} mod 17 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = -2 mod 17 = 15$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -43 mod 17 = 8$

→3P(15,8)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{8-4}{15-2} mod 17 = 16$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 1$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = 12 mod 17 = 12$

→4P(1,12)

+Điểm 5P=P+4P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{12-4}{1-2} mod 17 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 78 mod 17 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -76 mod 17 = 9$

→5P(10,9)

+Điểm 6P=P+5P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{9-4}{10-2} mod 17 = 7$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 37 mod 17 = 3$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -11 mod 17 = 6$

→6P(3,6)

+Điểm 7P=P+6P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{6-4}{3-2} mod 17 = 2$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = -1 mod 17 = 16$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -32 mod 17 = 2$

→7P(16,2)

+Điểm 8P=P+7P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{2-4}{16-2} mod 17 = 12$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 126 mod 17 = 7$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -64 mod 17 = 4$

→8P(7,4)

+Điểm 9P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{4-4}{7-2} mod 17 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = -9 mod 17 = 8$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -4 mod 17 = 13$

→9P(8,13)

+Điểm 10P=P+9P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{13-4}{8-2} mod 17 = 10$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 90 mod 17 = 5$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -34 mod 17 = 0$

→10P(5,0)

→ Số lượng phần tử của nhóm $E_{17}(1,6) = 2 * 10 = 20$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (20-k)P(17-y)

+Điểm 11P= -9P →11P(8,-13)=11P(8,4)

+Điểm 12P= -8P →12P(7,-4)=12P(7,13)

+Điểm 13P= -7P →13P(16,-2)=13P(16,15)

+Điểm 14P= -6P →14P(3,-6)=14P(3,11)

+Điểm 15P= -5P →15P(10,-9)=15P(10,8)

+Điểm 16P= -4P →16P(1,-12)=16P(1,5)

+Điểm 17P= -3P →17P(15,-8)=17P(15,9)

+Điểm 18P= -2P →18P(9,-8)=18P(9,9)

+Điểm 19P= -P →19P(2,-4)=19P(2,13)

+Điểm 20P=0

Các điểm nguyên thủy kP có (k,20)=1

Hay k={1,3,7,9,11,13,17,19}

→các điểm nguyên thủy: P,3P,7P,9P,11P,13P,17P,19P

4.4. Cho đường cong Elliptic $y^2 = x^3 + x + 1 mod 17$

Xây dựng nhóm E_{17} với P=(0,1) là phần tử nguyên thủy (tìm các điểm của E_{17}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

+Điểm P(0,1)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 17 = 2^{-1} mod 17 = 9 mod 17 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 81 mod 17 = 13$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -118 mod 17 = 1$

→2P(13,1)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{1-1}{13-0} mod 17 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = mod 17 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = mod 17 = 16$

→3P(4,16)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{16-1}{4-0} mod 17 = 195 mod 17 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 60 mod 17 = 9$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -73 mod 17 = 12$

→Điểm 4P(9,12)

+Điểm 5P=P+4P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{12-1}{9-0} mod 17 = 5$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 16 mod 17 = 16$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -81 mod 17 = 4$

→Điểm 5P(16,4)

+Điểm 6P=P+5P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{4-1}{16-0} mod 17 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = -7 mod 17 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -31 mod 17 = 12$

→Điểm 6P(10,12)

+Điểm 7P=P+6P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{12-1}{10-0} mod 17 = 132 mod 17 = 13$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 159 mod 17 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -79 mod 17 = 6$

→Điểm 7P(6,6)

+Điểm 8P=P+7P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{6-1}{6-0} mod 17 = 15$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = 219 mod 17 = 15$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -226 mod 17 = 12$

→Điểm 8P(15,12)

+Điểm 9P=P+8P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{12-1}{15-0} mod 17 = 88 mod 17 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 17 = -6 mod 17 = 11$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 17 = -34 mod 17 = 0$

→Điểm 9P(11,0)

+Điểm 10P= -8P →10P(15,-12)=10P(15,5)

+Điểm 11P= -7P →11P(6,-6)=11P(6,11)

+Điểm 12P= -6P →12P(10,-12)=12P(10,5)

+Điểm 13P= -5P →13P(16,-4)=13P(16,13)

+Điểm 14P= -4P →14P(9,-12)=14P(9,5)

+Điểm 15P= -3P →15P(4,-16)=15P(4,1)

+Điểm 16P= -2P →16P(13,-1)=16P(13,16)

+Điểm 17P= -P →17P(0,-1)=17P(0,16)

+Điểm 18P=0

Các điểm nguyên thủy kP có (k,18)=1

Hay k={1,5,7,11,13,17}

→các điểm nguyên thủy: P,5P,7P,11P,13P,17P

***4.5. Cho đường cong Elliptic $y^2 = x^3 + x + 1 mod 11$**

Xây dựng nhóm E_{11} với P=(1,5) là phần tử nguyên thủy (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

+Điểm P(1,5)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 11 = \frac{2}{5} mod 11 = 18 mod 11 = 7$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 47 mod 11 = 3$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -19 mod 11 = 3$

→2P(3,3)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{3-5}{3-1} mod 11 = 10$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 96 mod 11 = 8$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -75 mod 11 = 2$

→3P(8,2)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{2-5}{8-1} mod 11 = -24 mod 11 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 72 mod 11 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -50 mod 11 = 5$

→4P(6,5)

+Điểm 5P=P+4P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{5-5}{6-1} mod 11 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -7 mod 11 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -5 mod 11 = 6$

→5P(4,6)

+Điểm 6P=P+5P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{6-5}{4-1} mod 11 = \frac{1}{3} mod 11 = 4$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 11 mod 11 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -1 mod 11 = 10$

→6P(0,10)

+Điểm 7P=P+6P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{10-5}{0-1} mod 11 = -5 mod 11 = 6$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 35 mod 11 = 2$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -11 mod 11 = 0$

→7P(2,0)

→ Số lượng phần tử của nhóm $E_{11}(1,1) = 2 * 7 = 14$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (14-k)P(11-y)

+Điểm 8P= -6P →8P(0,-10)=8P(0,1)

+Điểm 9P = -5P →9P(4,-6)=9P(4,5)

+Điểm 10P= -4P →10P(6,-5)=10P(6,6)

+Điểm 11P= -3P →11P(8,-2)=11P(8,9)

+Điểm 12P= -2P →12P(3,-3)=12P(3,8)

+Điểm 13P= -P →13P(1,-5)=13P(1,6)

+Điểm 14P=0

Các điểm nguyên thủy kP có (k,14)=1

Hay k={1,3,5,9,11,13}

→các điểm nguyên thủy: P,3P,5P,9P,11P,13P

4.6. Cho đường cong Elliptic $y^2 = x^3 + x + 3 mod 11$

Xây dựng nhóm E_{11} với P=(5,1) là phần tử nguyên thủy (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

+Điểm P(5,1)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 11 = 38 mod 11 = 5$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 15 mod 11 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 4 mod 11 = 4$

→2P(4,4)

+Điểm 3P=P+2P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 17 = \frac{4-1}{4-5} mod 11 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 55 mod 11 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 39 mod 11 = 6$

→3P(0,6)

+Điểm 4P=P+3P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{6-1}{0-5} mod 11 = -1 mod 11 = 10$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 95 mod 11 = 7$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -21 mod 11 = 1$

→4P(7,1)

+Điểm 5P=P+4P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{1-1}{7-5} mod 11 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -12 mod 11 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -1 mod 11 = 10$

→5P(10,10)

+Điểm 6P=P+5P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{10-1}{10-5} mod 11 = 81 mod 11 = 4$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 1 mod 11 = 1$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 15 mod 11 = 4$

→6P(1,4)

+Điểm 7P=P+6P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{4-1}{1-5} mod 11 = -9 mod 11 = 2$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -2 mod 11 = 9$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -9 mod 11 = 2$

→7P(9,2)

+Điểm 8P=P+7P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{2-1}{9-5} mod 11 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -5 mod 11 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -4 mod 11 = 7$

→8P(6,7)

+Điểm 9P=P+8P : $\lambda = \frac{y_2-y_1}{x_2-x_1} mod 11 = \frac{7-1}{6-5} mod 11 = 6 mod 11 = 6$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 25 mod 11 = 3$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 11 mod 11 = 0$

→9P(3,0)

→ Số lượng phần tử của nhóm $E_{11}(1,3) = 2 * 9 = 18$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (18-k)P(11-y)

+Điểm 10P= -8P →10P(6,-7)=10P(6,4)

+Điểm11P = -7P →11P(9,-2)=11P(9,9)

+Điểm 12P= -6P →12P(1,-4)=12P(1,7)

+Điểm 13P= -5P →13P(10,-10)=13P(10,1)

+Điểm 14P= -4P →14P(7,-1)=14P(7,10)

+Điểm 15P= -3P →15P(0,-6)=15P(0,5)

+Điểm 16P= -2P →16P(4,-4)=16P(4,7)

+Điểm 17P= -P →13P(5,-1)=13P(5,10)

+Điểm 18P=0

Các điểm nguyên thủy kP có (k,18)=1

Hay k={1,5,7,11,13,17}

→các điểm nguyên thủy: P,5P,7P,11P,13P,17P

4.7. Cho đường cong Elliptic $y^2 = x^3 + x + 1 mod 11$

Xây dựng nhóm E_{11} với P=(4,6) là phần tử nguyên thủy (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

+Điểm P(4,6)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 11 = \frac{49}{12} mod 11 = 588 mod 11 = 5$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 17 mod 11 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -16 mod 11 = 6$

→2P(6,6)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{6-6}{6-4} mod 11 = 0$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -10 mod 11 = 1$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -6 mod 11 = 5$

→3P(1,5)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{5-6}{1-4} mod 11 = 4$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 11 mod 11 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 10 mod 11 = 10$

→4P(0,10)

+Điểm 5P=P+4P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{10-6}{0-4} mod 11 = 10$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 96 mod 11 = 8$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -46 mod 11 = 9$

→5P(8,9)

+Điểm 6P=P+5P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{9-6}{8-4} mod 11 = \frac{3}{4} mod 11 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 69 mod 11 = 3$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 3 mod 11 = 3$

→6P(3,3)

+Điểm 7P=P+6P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{3-6}{3-4} mod 11 = 3 mod 11 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 2 mod 11 = 2$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -11 mod 11 = 0$

→7P(2,0)

→ Số lượng phần tử của nhóm $E_{11}(1,1) = 2 * 7 = 14$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (14-k)P(11-y)

+Điểm 8P= -6P →8P(3,-3)=8P(3,8)

+Điểm 9P = -5P →9P(8,-9)=9P(8,2)

+Điểm 10P= -4P →10P(0,-10)=10P(0,1)

+Điểm 11P= -3P →11P(1,-5)=11P(1,6)

+Điểm 12P= -2P →12P(6,-6)=12P(6,5)

+Điểm 13P= -P →13P(4,-6)=13P(4,5)

+Điểm 14P=0

Các điểm nguyên thủy kP có (k,14)=1

Hay k={1,3,5,9,11,13} →các điểm nguyên thủy: P,3P,5P,9P,11P,13P

4.8. Cho đường cong Elliptic $y^2 = x^3 + x + 3 mod 11$

Xây dựng nhóm E_{11} với P=(9,2) là phần tử nguyên thủy (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thủy .

Điều kiện tồn tại : $\Delta = (4 * a^3 + 27 * b^2) mod 17 \neq 0$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

+Điểm P(9,2)

+Điểm 2P=P+P : $\lambda = \frac{3{x_1}^2 + a}{2y_1} mod 11 = 61 mod 11 = 6$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 18 mod 11 = 7$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 10 mod 11 = 10$

→2P(7,10)

+Điểm 3P=P+2P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 17 = \frac{10-2}{7-9} mod 11 = 7$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 33 mod 11 = 0$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 61 mod 11 = 6$

→3P(0,6)

+Điểm 4P=P+3P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{6-2}{0-9} mod 11 = -20 mod 11 = 2$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -5 mod 11 = 6$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 4 mod 11 = 4$

→4P(6,4)

+Điểm 5P=P+4P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{4-2}{6-9} mod 11 = 3$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = -6 mod 11 = 5$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 10 mod 11 = 10$

→5P(5,10)

+Điểm 6P=P+5P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{10-2}{5-9} mod 11 = 9$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 67 mod 11 = 1$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 70 mod 11 = 4$

→6P(1,4)

+Điểm 7P=P+6P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{4-2}{1-9} mod 11 = -3 mod 11 = 8$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 54 mod 11 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = -10 mod 11 = 1$

→7P(10,1)

+Điểm 8P=P+7P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{1-2}{10-9} mod 11 = 10$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 81 mod 11 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 48 mod 11 = 4$

→8P(4,4)

+Điểm 9P=P+8P : $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod 11 = \frac{4-2}{4-9} mod 11 = -18 mod 11 = 4$

$x_3 = \lambda^2 - x_1 - x_2 mod 11 = 3 mod 11 = 3$

$y_3 = \lambda(x_1 - x_3) - y_1 mod 11 = 22 mod 11 = 0$

→9P(3,0)

→ Số lượng phần tử của nhóm $E_{11}(1,3) = 2 * 9 = 18$

Dựa vào tính chất kP(x,y)= - kP(x, - y) và – kP(x, -y) = (18-k)P(11-y)

+Điểm 10P= -8P →10P(4,-4)=10P(6,7)

+Điểm11P = -7P →11P(10,-1)=11P(10,10)

+Điểm 12P= -6P →12P(1,-4)=12P(1,7)

+Điểm 13P= -5P →13P(5,-10)=13P(5,1)

+Điểm 14P= -4P →14P(6,-4)=14P(6,7)

+Điểm 15P= -3P →15P(0,-6)=15P(0,5)

+Điểm 16P= -2P →16P(7,-10)=16P(7,1)

+Điểm 17P= -P →13P(9,-2)=13P(9,9)

+Điểm 18P=0

Các điểm nguyên thủy kP có (k,18)=1

Hay k={1,5,7,11,13,17}

→các điểm nguyên thủy: P,5P,7P,11P,13P,17P

// Tính (k,18)=1

Tìm fact(1+18*i);i=1,2,...

Các điểm nguyên thủy k sẽ là các số hạng < 18

\\ Thực hiện tìm tổng số điểm ở đầu bài làm

Tìm các phần tử nguyên thủy khi thay đổi giá trị a và b

+ Ví dụ câu 4.1 và 4.2,p=13,a=b=1

Các giá trị thặng dư bậc 2: $\{i^2 mod p, i = 1,2,..,12\}$

$\rightarrow Q_{13} = \{1,4,9,3,12,10\}$

Các căn bậc 2 : $\sqrt{1} = (1,12), \sqrt{4} = (2,11), \sqrt{9} = (3,10)$

$\sqrt{3} = (4,9), \sqrt{12} = (5,8), \sqrt{10} = (6,7)$

X	0	1	2	3	4	5	6	7	8	9	10	11	12
y^2	1	3	11	5	4	1	2	0	1	11	10	4	12
$y^2 \in Q_{13}$	Có	có			Có	Có		Ko	Có		Có	có	có
y1	1	4			2	1		0	1		6	2	5
y2	12	9			11	12		0	12		7	11	8

Mặc dù 0 không thuộc Q nhưng 0 có căn bậc 2 là 0

Theo bảng ta có được 18 điểm trên trục 0xy như sau:

{(0,1);(0,12);(1,4);(1,9);(4,2);(4,11);(5,1);(5,12);(7,0);(8,1);(8,12);(10,6);(10,7);

(11,2);(11,11);(12,5);(12,8);0}

+ Câu 4.3,p=17, a=1,b=6 thì ta tìm được 20 điểm trên trục 0xy
+ Câu 4.4,p=17, a=b=1 thì có 18 điểm
+ Câu 4.5 và 4.7,p=11, a=1,b=3 thì ta có 14 điểm
+ Câu 4.6 và 4.8,p=11, a=b=1 thì ta có 18 điểm