20/01/2020

S-II

Page No.
Date

→ Limitation of knapsack crypto system is, it is hard to store long tuples in smaller devices.

→ It may be possible that with the help of Public key (B) attacker can easyly find out PT.

→ It happens because of poor combination of r and q.

→ KA KnapSack Crypto system says that tuples should atleast start with 2 digits and not all numbers should be of 2 digits

→ It is advicable to select r of 3 digits or sometimes depending on nature of private tuple we can go upto 5 digits.

→ Select q such that there will be less diffience between sum of elements in private tuple.

→ Select q as prime number.

Known as Probablistic system

Page No.
Date

Rabin Crypto System : (Probablistic)

* Also known as probabilistic crypto system

* Possible Attacks are same as RSA

* with this receiver needs to implement algorithm to decide which of 4 decrypted text to consider as PT

① Key Generation
→ select 2 large prime numbers p & q in form of $4k+3$ and $p \neq q$

→ $n = p * q$

→ public key is n
→ private key is q or (q, n)

② Encryption
{
$CT = PT^2 \bmod n$
return CT
}

③ Decryption
{
$a_1 \leftarrow +(CT^{(p+1)/4}) \bmod p$

$a_2 \leftarrow -(CT^{(p+1)/4}) \bmod p$

$b_1 \leftarrow +(CT^{(q+1)/4}) \bmod q$

$b_2 \leftarrow -(CT^{(q+1)/4}) \bmod q$

$PT_1 \leftarrow$ Chinese_Reminder (a_1, b_1, p, q)
$PT_2 \leftarrow$ " (a_1, b_2, p, q)
$PT_3 \leftarrow$ " (a_2, b_1, p, q)
$PT_4 \leftarrow$ " (a_2, b_2, p, q)

Page No. —
Date

Ex:1

p = 23 (4×5+3) q = 7 (4×1+3)

n = 161

PT = 24

$CT = 24^2 \bmod 161$

$CT = 93$

$a_1 = 93^{\frac{23+1}{4}} \bmod 23 = 93^6 \bmod 23$

$= (93^3)^2 \bmod 23$

$a_1 = (1 \times 1) \bmod 23 =$

$a_1 = 1$

$a_2 = -(93^6 \bmod 23) = -1 \bmod 23$

$\boxed{a_2 = 22}$

$b_1 = +\{93^2 \bmod 7\} = 4$

$b_2 = -\{93^2 \bmod 7\} = -4 \bmod 7 = 3$

$PT_1 = \begin{cases} a_1 \bmod p = 1 \bmod 23 \\ b_1 \bmod q = 4 \bmod 7 \end{cases}$

Chinese Reminder.

$m = 23 \times 7 = 161$

$m_1 = 7 \quad m_2 = 23$

$m_1^{-1} = 7^{-1} \bmod 23 = 10$

3	23	7	2	0	1	-3
3	7	2	1	1	-3	10
2	2	1	0	-3	10	-23

10

$m_2^{-1} = 23^{-1} \bmod 7$

$= 23^{7-2} \bmod 7$

$= 23^5 \bmod 7$

$= 1 \times 23^2 \bmod 7$

$= 1 \times 4 \bmod 7$

$= 4$

$X = (1 \times 7 \times 10 + 4 \times 23 \times 4) \bmod 161$

$= 70 + 368 \bmod 161$

$= (438) \bmod 161$

$PT_1 = 116$ (which is wrong)

→ $PT_2 = \begin{cases} 1 \bmod 23 \\ 3 \bmod 7 \end{cases}$

$m = 161$

$m_1 = 7 \qquad m_2 = 23$

$X = (1 \times 7 \times 10 + 3 \times 23 \times 4) \bmod 161$

$= 70 + 276 \bmod 161$

$= 346 \bmod 161$

$\boxed{PT_2 = 24}$ (i.e. In this case PT_2 is correct but which is not always the case)

→ $PT_3 = \begin{cases} 22 \bmod 23 \\ 4 \bmod 7 \end{cases}$

$PT_3 = 22 \times 7 \times 10 + 4 \times 23 \times 4 \bmod 161$

$= 1540 + 368 \bmod 161$

$\boxed{PT_3 = 137}$

$PT_4 = \begin{cases} 22 \bmod 23 \\ 13 \bmod 7 \end{cases}$

$PT_4 = 22 \times 7 \times 10 + 23 \times 23 \times 24 \bmod 161$

$= 1540 + 276 \bmod 161$

$\boxed{PT_4 = 45}$

Ex=2 $p = 31$ $q = 11$

$PT = 1006$

$n = p * q = 341$

} PT > N we won't get PT from CT even if we calculate e in that case mention which decrypted is congruent to PT. here 324 is

$CT = 1006^e \bmod 341 = \boxed{289}$

$a_1 = 289^{\frac{31+1}{4}} \bmod 31$

$= 289^8 \bmod 31$

$= 14$

$a_2 = 289^8 \bmod 31 = -14 \bmod 31 = 17$

$b_1 = 289^{12/4} \bmod 11$

$= 289^3 \bmod 11 = 5$

$b_2 = -5 \bmod 11 = 6$

Here; in Rabin Crypto System.

$PT < N$ & $PT^2 > N$

↳ $PT > N$ we can't get PT back from CT

Page No.
Date

$$PT_1 = \begin{cases} 14 \mod 31 \\ 5 \mod 11 \end{cases}$$

$m = 31 \times 11 = 341$

$m_1 = 11 \quad m_2 = 31$

$M_1^{-1} = 11^{-1} \mod 31$

$= 17$

2	31	11	9 0 1 -2
1	11	9	2 1 -2 3
4	9	2	1 -2 3 -14
2	2	1	0 3 -14 -
	1	0	-14

$-14 + 31 = 17$

$M_2^{-1} = 31^{-1} \mod 11$

$= 6^{31} \mod 11$

$M_2^{-1} = 5$

$PT_1 = 14 \times 11 \times 17 + 31 * 5 \times 5 \mod 341$

$= 3393 \mod 341$

$= 324$

324
+341
+341
1006

324 is congruante to 1006

$$PT_2 = \begin{cases} 14 \mod 31 \\ 6 \mod 31 \end{cases}$$

$PT_2 = 14 \times 11 \times 17 + 6 \times 31 \times 5 \mod 341$

$= 2618 + 930 \mod 341$

$= 138$

$$PT_3 = \begin{cases} 17 \mod 31 \\ 5 \mod 11 \end{cases}$$

(Remaining)

Q. $P = 11$, $Q = 7$, $PT = 38$

22/01/2020

Page No.
Date

* Diffie - Hellman (key Exchange Algorithm) :-

→ Man In the Middle problem :-

consider machine A, B, C with IPs :

A = x, x, 27, 101

C = x, x, 27, 103

B = x, x, 27, 102

→ Now somehow C gets IPs of A & B and C is acting as A when communicating with B & act as B when communicating with A.

→ A, B, C gets a common prime number n.

→ B will ~~calculate~~ generate private no. x and calculate $g^x \bmod n$

→ B will send this number to assumed A (C)

→ C will generate a private no. z and calculate $g^{xz} \bmod n$.

→ C will send $g^{xz} \bmod n$ to B and B will also calculate $g^{xz} \bmod n$ which is key B/w C & B.

→ A decides a private key 'y' and sends $g^y \bmod n$ to assumed B which actually is C.

→ C will calculate $g^{yz} \bmod n$ and it will send $g^z \bmod n$ to A and then A will calculate $g^{yz} \bmod n$. which is key b/w A & C.

→ So,

$k_1 = g^{yz} \bmod n$ b/w A & C

$k_2 = g^{xz} \bmod n$ b/w B & C

→ Now whenever A sends Data to Assumed B, C can manipulate data using k_1 & k_2 and send manipulated data to B, and same during B wants to same data.

* How to find Primitive Root:

Consider prime no. $P=7$

$$\phi(7) = 6$$

$$\boxed{X = a_m^i \bmod n ;}$$

where $i = 1$ to $\phi(p)$ and

a_m is also $m = 1$ to $\phi(p)$

Page No.
Date

Ex:1

P=7

m \ i	1	2	3	4	5	6	
am 1	1	1	1	1	1	1	× i=1 not
2	2	4	1	2	4	1	× i=3 not
3	3	2	6	4	5	1	✓ i=6 possible
4	4	2	1	4	2	1	× i=3 not
5	5	4	6	2	3	1	✓ i=5 possible
6	6	1	6	1	6	1	

steps:-

→ in table starting with 1st row mark where 1st 1 is ~~encoust~~ encontered for each row.

→ Primitive root is value of a when am where i when 1st 1 is encountes i = ϕ(n)

Ex:2 P=11 ϕ(11)=10

m \ i	1	2	3	4	5	6	7	8	9	10	11	
1	1	1	1	1	1	1	1	1	1	1	1	
✓ 2	2	4	8	5	10	9	7	3	6	1		
not possible because 1 comes to early i=10 × 3	3	9	5	4	1			×				
4	4	5	9	3	1					×		
5	5	3	4	9	1			×				
✓ 6	6	3	7	9	10	5	8	4	2	1		
7	7	5	2	3	10	4	6	9	8	1		✓
✓ 8	8	9	6	4	10	3	2	5	7	1		
× 9	9	4	3	5	1							
× 10	10	1	2	1	2	1	2	1	2	1		
11												

Primitive roots: 2, 6, 7, 8

Page No.
Date

Given

Q. $x = 3$ $y = \underset{\downarrow}{g}^{x} \bmod p$ $g = 5$ $p = 7$

$5^3 \bmod 7 = 4$

$4^3 \bmod 7$

Key = 1

Q $x = 9$ $y = 5$ $p = 11$, $g = 8$

$8^5 \bmod 11 = 10$

$10^9 \bmod 11$

Key = 10

PRD

(S-II continues)

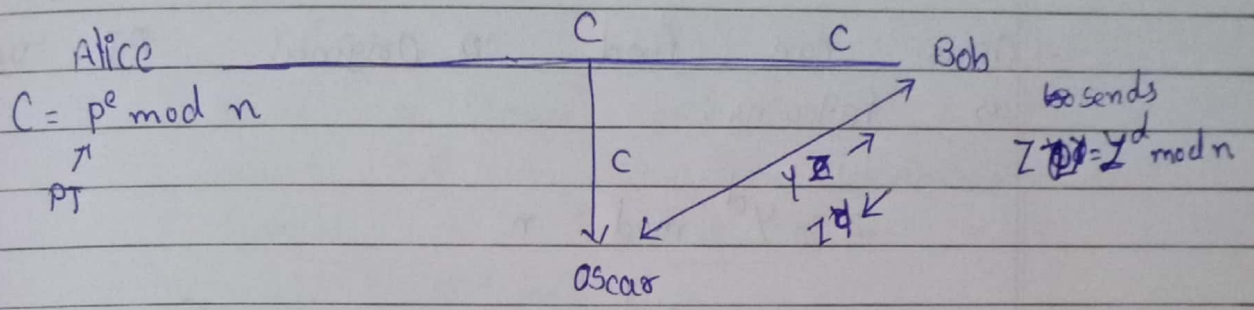
Scanned by CamScanner

27/01/2020 PRD

S-II (countinue)

Page No.
Date

★ Attack of RSA



doesn't have private key

Select $x \in Z_n^*$

cal. $y = C * x^e \bmod n$

→ Alice and Bob are communicating with public-private key. Alice generates cipher text $C = p^e \bmod n$ and sends to Bob.

→ Oscar is configured in N/w such that, he will ask for decryption to Bob.

→ Oscan can easyly intercept 'C' and can manipulate CT with following steps.

① Select $x \in Z_n^*$

② $y = C * x^e \bmod n$

③ Send y to Bob.

→ Bob decrypts $z = y^d \bmod n$ and sends decrypted text back to oscar.

→ Oscar can find original PT using y as following:

$$z = y^d \bmod n$$

$$= (c * x^e)^d \bmod n \qquad (y = c * x^e \bmod n)$$

$$= c^d * x^{ed} \bmod n \qquad (x^{ed} = x^{k\phi(n)+1})$$

$$= c^d * x \bmod n$$

$$= (p^e)^d * x \bmod n \qquad (c = p^e \bmod n)$$

$$z = p * x \bmod n \qquad (p^{ed} = p^{k*\phi(n)+1})$$

$$\therefore \boxed{p = z * x^{-1} \bmod n}$$

Page No.
Date

* Elgamal Crypto System :-

① Key Generation :

{

→ Select a large prime p, select 'd' to be a member of Group $G = \langle Z_p^*, * \rangle$ such that $1 \le d \le p-2$;

→ Select 'e_1' to be a primitive root in Group $G = \langle Z_p^*, * \rangle$

→ $e_2 \leftarrow e_1^d \bmod p$

→ Public key $\leftarrow e_1, e_2, p$

→ Private key $\leftarrow d$

}

② Encryption

{

→ select a random integer 'r' in Group $G = \langle Z_p^*, * \rangle$

→ $C_1 \leftarrow e_1^r \bmod p$

→ $C_2 \leftarrow PT * e_2^r \bmod p$

→ Send C_1, C_2

}

Page No.
Date

③ Decryption

{

PT ← [$C_2 (C_1^d)^{-1}$ mod p]

return P;

}

Ex:-1 P = 19 d = 7 r = 6 PT = 9.

$e_1 = 2$

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

$e_2 = 2^7 \bmod 19 = 14$

encrypt

$C_1 = e_1^r \bmod n = 2^6 \bmod 19 = 7$

$C_2 = PT * e_2^r \bmod n = 9 * 14^6 \bmod 19 = 6$

~~CT (x, y)~~ $C_2 = 6$

~~CT = C6 * 7 = 42~~

Send 7 & 6

$(a^n)^{-1} \bmod p = a^{p-1-n} \bmod p$

Page No. Date

decrypt :-

$PT = 6 * (7^7)^{-1} \bmod 19$

$= 6 * (7)^{-1} \bmod 19$

$= 6 * 7^{19-2} \bmod 19$

$= 6 * 7^{17} \bmod 19$

$= 6 * 11 \bmod 19$

$= 66 \bmod 19$

$\boxed{PT = 9}$

$\begin{cases} (a^n)^{-1} \bmod p = a^{(p-1)-1} \bmod n \\ \therefore (a^n)^{-1} \bmod p = a^{p-1-n} \bmod n \\ \therefore (7^7)^{-1} \bmod 19 = 7^{19-1-7} \bmod n \end{cases}$

Ex-2

$p = 11 \quad p = 7 \quad d = 9 \quad e = 5$

$e_1 = 2$

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

$e_2 = 2^9 \bmod 11 = 6$

$C_1 = 2^5 \bmod 11 = 10$

$C_2 = 7 * 6^5 \bmod 11 = 4$

$PT = 4 \times (10)^{9-1} \bmod 11$

$= 4 * 10^{11-1-9} \bmod 11$

$= 4 \times 10 \bmod 11$

$= 40 \bmod 11$

$\boxed{PT = 7}$

03/02/2020

Proof of Elagamal Algo :=

$PT = [c_2 (c_1^d)^{-1}] \bmod p$

$(\because c_2 = PT * e_2^r \bmod p) = [(PT * e_2^r)(c_1^d)^{-1}] \bmod p$

$(e_2 = e_1^d \bmod p) = [(PT * e_1^{rd})(c_1^d)^{-1}] \bmod p$

$(c_1 = e_1^r \bmod p) = [(PT * e_1^{rd}) * (e_1^{rd})^{-1}] \bmod p$

$= PT * e^{rd} * (e^{rd})^{-1} \bmod p$

$= PT \bmod p$

→ Security depends on selection of 'r' and 'd'

→ In this crypto system both host are having some private information as d and r where d is generated by Receiver and r is generated by sender.

Page No.
Date

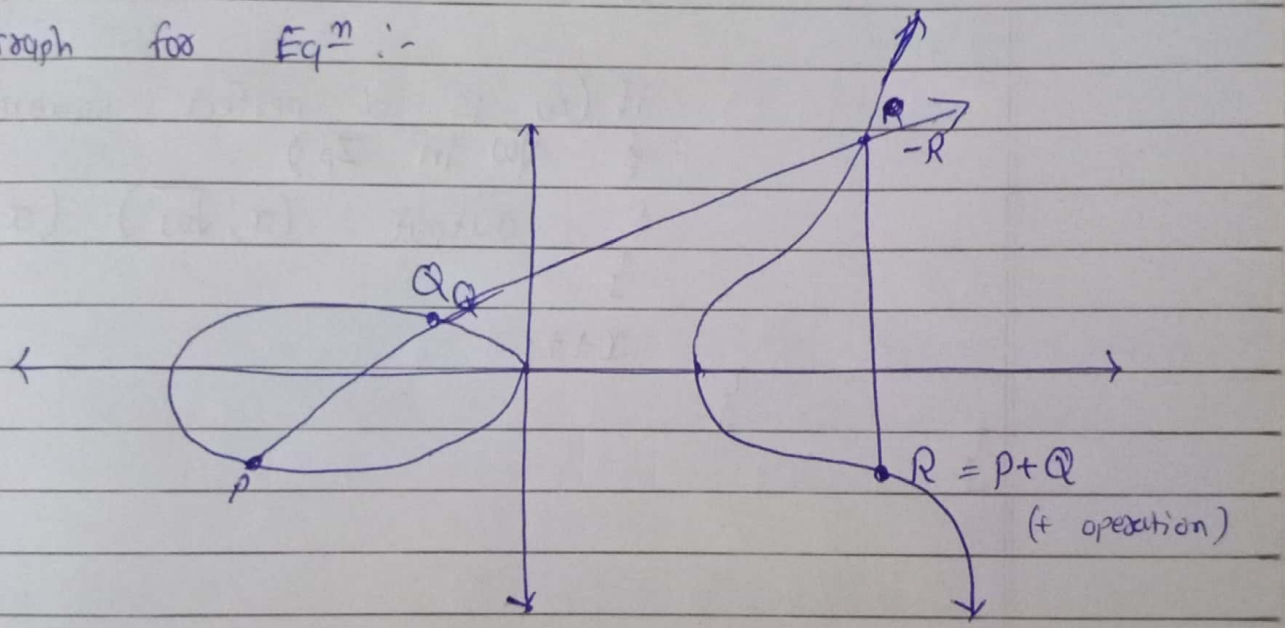
* Eliptic - Curve Crypto System :-

Curve eqn we use : $y^2 = x^3 + ax + b \mod p$

↓ we get Group on apply

\+ (addition of points)

Graph for Eqn :-



Page No.
Date

* Find all points for a curve eqn :-
Let { p, a, b ; p is prime. }

```
x = 0;

while(x < p)
{
    w = x^3 + ax + b  mod  p

    if (w is a perfect square
    ∉ √w in Zp)
    ∈ output (x, √w) (x, -√w)
    }                    ↓
                    (Additive
                     inverse)
    x++;
  }
}
```

Ex:-

$y^2 = x^3 + x + 1 \mod 13$

$x = 0$

$y^2 = 0 + 0 + 1 \mod 13$

$y^2 = 1 \mod 13$

$y = 1$

$\therefore (0, 1) \quad (0, -1)$

$\downarrow +13$ as it is -ve

$(0, 12)$

Page No.
Date

$x = 1$

$y^2 = 1 + 1 + 1 \mod 13$

$= 3 \mod 13$ (not perfect square, add 13 we get 16)

$y^2 = 16 \mod 13$ (Add upto value is $\leq p^2 = 13^2$)

$y = 4 \mod 13$

$\therefore y = 4$

(0, 4) (0, -4)

(10, 9)

$x = 2$

$y^2 = 2^3 + 2 + 1$

$= 11 \mod 13$

$11+13 = 24+13 = 37+13 = 50+13 = 63+13 = 76+13 = 89+13 = 102+13 = 115 \ldots$

not perfect square even if sum + add 13.

$x = 3$ $y^2 = 3^3 + 3 + 1 = 31 \mod 13 = 5 \mod 13$

$5+13 = 18 \ldots$

no perfect square $\leq p^2$

$x = 4$ $y^2 = 4^3 + 4 + 1 = 69 \mod 13 = 4 \mod 13$

$4+13 = 17+13 = 30$

$y = 2$

(4, 2) (4, -2)

(4, 11)

Page No.
Date

$x=5$

$y^2 = 5^3 + 5 + 1 \mod 13$

$= 131 \mod 13$

$y = 1$

$(5,1)$ $(5,12)$

$x=6$

not

$x=7$

$(7,0)$ $(7,0)$

$x=8$

$y^2 = 8^3 + 8 + 1 \mod 13$

$= 1 \mod 13$

$y = 1$

$(8,1)$ $(8,12)$

$x=9$

$y^2 = 9^3 + 9 + 1 \mod 13$

$= 11 \mod 13$

not possible

$x=10$ $y^2 = 10^3 + 10 + 1 \mod 13$

$= 1011 \mod 13$

$= 10 \mod 13$

$= 10 + 13 + 13 \mod 13$

$= 6^2 \mod 13$ $\therefore y = 6$

$(10,6)$

$(10,7)$

Page No.
Date

x=11

$y^2 = 11^3 + 11 + 1 \mod 13$

$= 4 \mod 13$

$y = 2$

(11,2) (11,11)

x=12

$y^2 = 12^3 + 12 + 1 \mod 13$

$= 12 \mod 13$

$= 12 + 13 \mod 13$

$= 25 \mod 13$

$y = 5$

(12,5) (12,8)

→ Eliptic curve is

$\sum_{11} (2,3)$

p=11 a=2 b=3

$y^2 = x^3 + 2x + 3$

$x=0 = 3 \mod 11$

$= 3 + 11 + 11 \mod 11 = 25 \mod 13$

$y = 5$

(0,5) (0,6)

Page No.
Date

$x=1$

$y^2 = 1^3 + 2\times1 + 3 = 5 \mod 11$

not

$x=2$ $y^2 = 2^3 + 2*2 + 3 \mod 11$

$= 15 \mod 11$

$= 81 \mod 11$

$y = 9$

$(2,9)$ $(2,2)$

$x=3$ $y^2 = 3^3 + 3*2 + 3 \mod 11$

$= 35 \mod 11$

$= 2 \mod 11$

not

$x=4$ $y^2 = 4^3 + 4*2 + 3 \mod 11$

$= 9 \mod 11$

$y = 3$

$(4,3)$ $(4,8)$

$x=5$ $y^2 = 5^3 + 5*2 + 3 \mod 11$

$= 138 \mod 11$

$= 6 \mod 11$

not

Page No.
Date

$x = 6$ $y^2 = 6^3 + 2 \times 6 + 3 \mod 11$

$= 231 \mod 11$

$= 0 \mod 11$

not : (6,0) (6,0)

$x = 7$ $y^2 = 7^3 + 2 \times 7 + 3 \mod 11$

$= 8 \mod 11$

not

$x = 8$ $y^2 = 8^3 + 8 \times 2 + 3 \mod 11$

$= 3 \mod 11$

$= 25 \mod 11$

$y = 5$

(8, 5) (8, 6)

$x = 9$

$y^2 = 9^3 + 9 \times 2 + 3 \mod 11$

$= 2 \mod 11$

not

$x = 10$ $y^2 = 10^3 + 10 \times 2 + 3 \mod 11$

$= 0 \mod 11$

(10,0) (10,0)

Page No.
Date

* line eq^n for 2 points

p1 (x_1, y_1) p2(x_2, y_2)

slop

$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)} \mod p$$

$$\boxed{\lambda = (y_2 - y_1) * (x_2 - x_1)^{-1} \mod p}$$

Case-I) ~~Case-I~~) If $x_1 \neq x_2$ & $y_1 \neq y_2$

slop $\lambda = \frac{(y_2 - y_1)}{x_2 - x_1} \mod p$

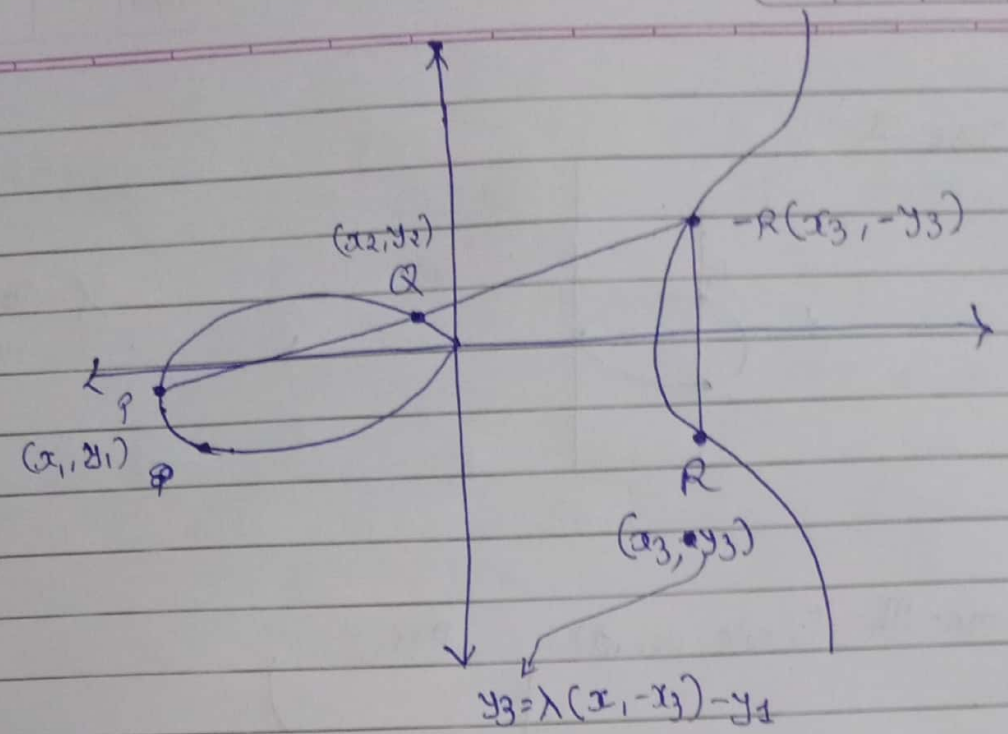
$y - y_1 = \lambda(x - x_1)$ line eq^n

$-y_3 - y_1 = \lambda(x_3 - x_1)$ (y has some point on line)

$-y_3 = \lambda(x_3 - x_1) + y_1$

$\boxed{y_3 = \lambda(x_1 - x_3) - y_1} \mod p$

still unknown



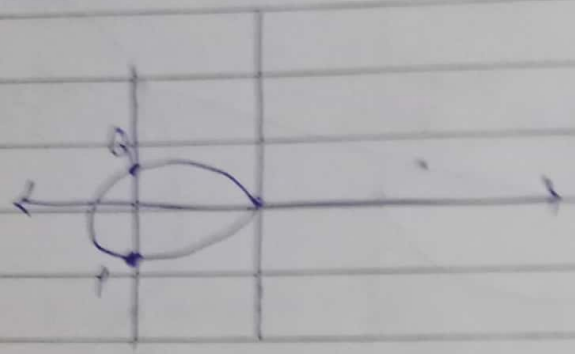
Case I) ~~$x_1 \neq x_2$ & $y_1 \neq y_2$~~

$(x_1 + \lambda(x - x_1))^2 = x^3 + ax + b$ Solving we get x_1, x_2, x_3 (not required to solve)

$\Rightarrow x_1 + x_2 + x_3 = \lambda^2$

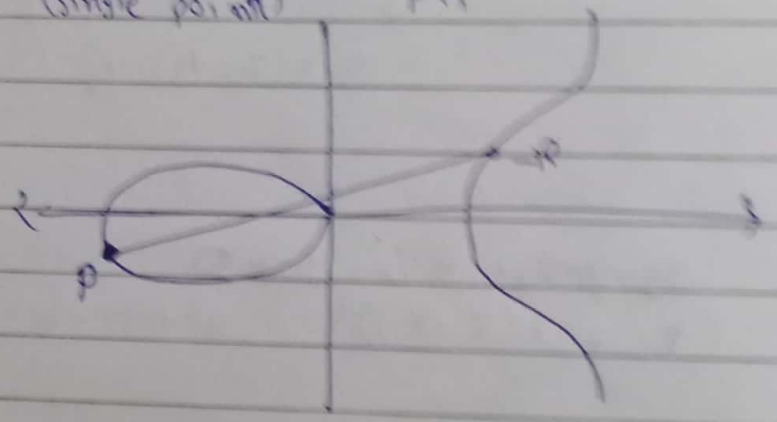
$$\boxed{x_3 = \lambda^2 - x_1 - x_2} \mod p$$

case-II



$\lambda = \infty$
not exist

case-III (single point) $P+P$



$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$
$$= \lambda^2 - 2x_1 \quad (\text{as } x_1 = x_2)$$

$$y_3 = \lambda(x_3 - x_1) - y_1 \bmod p$$

Page No.
Date

Summary:-

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & ; \text{if } P = Q \\ \dfrac{y_2 - y_1}{x_2 - x_1} & ; \text{if } P \neq Q,\ x_1 \neq x_2 \\ \infty & ; \text{if } P = -Q \end{cases}$$

Page No.
Date

* Elipticle Algamal Crypti system

Steps:-

→ We have host A and host B. A selects $E_p(a,b)$ as the Eliptical curve over GF(p)

→ A selects e_1 the co-ordinates are (x_1, x_2) and e_1 is on the curve $E_p(a,b)$. A selects d as any random integer.

→ Host A calculates $e_2(x_2, y_2)$ where

$$e_2 = d * e_1$$

↓

~~represent~~ is repetative addition.

→ Host announces (Σ, e_1, e_2) → public key

d → private key.

Page No.
Date

Encryption :-

→ B will select one point on the curve ab
PT. B calculates ~~$e_1 = k * e_1$~~

$$C_1 = k * e_1$$

$$C_2 = PT + k * e_2$$

and k is random integer selected by B.

multiplication is repetative addition.

→ B will send C_1 & C_2 to host A.

Decryption :-

→ A will Calculate

$$PT = C_2 - (d * C_1)$$

$(d * C_1)$ → repetative Addition.

$C_2 -$ → addition with inverse point

Page No.
Date

Ex:- $E_{67}(2,3)$

$y^2 = x^3 + 2x + 3 \mod 67$

$x=0$

$y^2 = 3 \mod 67$

$67^2 = 4489$

$x=2$

$y^2 = 8 + 4 + 3 \mod 67$

$= 484 \mod 67$

$y = 22$

$e_1 = (2, 22)$
$\quad\; x_1, y_1$

selected $d=4$

$e_2 = 4 * e_1$

$= e_1 + e_1 + e_1 + e_1$

$= (e_1 + e_1) + (e_1 + e_2)$

as x points are same

$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(2)^2 + 2}{2(22)} = \frac{14}{44} = 8$

$= 8 \times 44^{-1} \mod 67$

q	r1	EE x_2	r2	t1	t2	t
1	67	44	23	0	1	-1
1	44	23	21	1	-1	2
1	23	21	2	-1	2	-3
10	21	2	1	2	-3	32
2	2	1	0	-3	32	
	1	0		32		

44^{-1}

$\therefore 140 \times 32 \mod 67$

$\lambda = 46$

$x_3 = \lambda^2 - 2x_1 \mod 67$

$= 46^3 - 2 * 2 \mod 67$

$x_3 = 35$

$y_3 = \lambda (x_1 - x_3) - y_1 \mod 67$

$= 46(2-35) - 22 \mod 67$

$= 46(353) - 22$

$= 1058 - 1540 \mod 67$

$y_3 = 1$

$C_1 = (35, 1)$

Date

$\therefore e_2 = 4 * e_1$

$= (e_1 + e_1) + (e_1 + e_1)$

$= (35,1) + (35,1)$

↓ both are same calculate again.

$\lambda = 63 \qquad x_3 = ? \qquad y_3 = ?$

$\boxed{e_2 = (13,45)}$

$PT = (24,26) \qquad k = 2$

$C_2 = (24,26) PT + k * e_2$

$= (24,26) + 2 * (13,45)$

$= (24,26) + (13,45) + (13,45)$

$\lambda = \frac{3x_1^2 + 9}{2y_1} = \frac{3 * 13^2 + 2}{2 * 45} = \frac{509}{90} \mod 67$

$= 509 * 90^{-1} \mod 67$

$= 509 * 35 \mod 67$

$\lambda = 60$

Page No.
Date

q	r_1	r_2	r	t_1	t_2	t
0	67	90	67	0	1	0
1	90	67	23	1	0	1
2	67	23	21	0	1	-2
1	23	21	2	1	-2	3
10	21	2	1	-2	3	-32
2	2	1	0	3	-32	
	1	0		-32		

$$+ 67$$

$$= 035$$

$$x_3 = \lambda^2 - 2x_1 \mod 67$$

$$= 60^2 - 2(13) \mod 67$$

$$x_3 = 23$$

$$y_3 = 60(13 - 23) - 45 \mod 67$$

$$= 60(-10) - 45 \mod 67$$

$$= -645 \mod 67$$

$$y_3 = 25$$

$$e_2 = (24, 26) + (23, 25)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{25 - 26}{23 - 24} = \frac{-1}{-1} = -1 \times -1^{-1} \mod 67$$

$$\boxed{\lambda = 1}$$

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

$= 1 - 24 - 23 \mod 67$

$= -46 \mod 67$

$x_3 = 21$

$y_3 = \lambda(x_1 - x_3) - y_1 \mod 67$

$= 1(24-21) - 26 \mod 67$

$= 3 - 26 \mod 67$

$= -23 \mod 67$

$y_3 = 44$

Encryption $C_2 = (21, 44)$

decryption:

$PT = C_2 - d * C_1$

$= (21,44) - 2(2(13,35,1))$

$= (21,44) - 2(13,45)$

$= (21,44) - (23,25)$

$= (21,44) + (23,42)$ { additive inverse for (23,25) i.e. (23, 67-25)

$= (21,44) + (23,42)$

$\lambda = \frac{44-44}{23-21} = \frac{-2^{-1}}{2} = -1 \mod 67$

$= -1 \mod 67$

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

$= 66^2 - 21 - 23 = 24$

$y_3 = 66(21 - 24) - 14 \mod 67.$

$= -66 \times 3 - 14$

$= 26$

PT = (24, 26)

Ex-2 $E_{13}(1,1)$ d=4 r=2

PT(12, 5)

$y^2 = x^3 + x + 1$

For e1

x=0 = 1 mod 13

= (0,1) (0,12)

$e_1 = (0,1)$

$e_2 = d * e_1$

$= 4 * (0,1)$

$= (0,1) + (0,1) + (0,1) + (0,1)$

$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{1}{2} = 1 \times 2^{-1} \mod 13$

$\lambda = 7$

Page No.
Date

EE

6 | 13 | 2 | 1 | 0 | 1 | -6
2 | 1 | 0 | 1 | -6
1 | 0 | -6
+13
7

$x_3 = \lambda^2 - 2x_1$

$x_3 = 49 \mod 13 = 10$

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

$= 7(-6) - 1$

$= -71 \mod 13$

$y_3 = 7$

$(0,1) + (0,1) = (10,7)$

$e_2 = (10,7) + (10,7)$

$\lambda = \frac{3 * 100 + a}{2(7)} = \frac{301}{14}$

$= 301 * 14^{-1} \mod 13$

$= 301 \mod 13$

$\lambda = 2$

~~13 12 10~~

	x_1	x_2		t_1	t_2	
0	13	14	13	0	1	0
1	14	13	1	1	0	1
13	13	1	0	0	1	
	1	0		1		

$x_3 = 4 - 20 \mod 13 = -16 \mod 13$

$\boxed{x_3 = 10}$

$y_3 = 2(10 - 10) - 7 \mod 13$

$= -7 \mod 13$

$\boxed{y_3 = 6}$

$\boxed{e_2 = (10, 6)}$

$C_1 = 2 * e_1$

$= 2 * (0, 1)$

$= (0, 1) + (0, 1)$

$\boxed{C_1 = (10, 7)}$

$C_2 = (12, 5) + 2 * (10, 6)$

$= (12, 5) + (10, 6) + (10, 6)$

$\lambda = 3007 \quad 3007 \quad 3007$

$= \frac{300 + 1}{2 * 6} \cdot 301 * 12^{-1} \mod 13$

$\boxed{\lambda = 11}$

$x_3 = 11^2 - x_1 - x_1 \quad \boxed{x_3 = 10}$

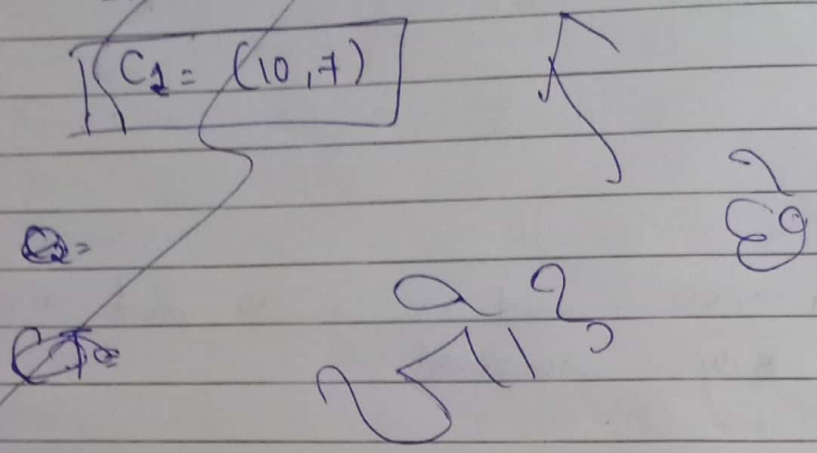
$= 121 - 20 \mod 13$

$= 101 \mod 13$ 340

$y_3 = 11(10-10) - 6 \mod 13$

$y_3 = 7$

$C_2 = (10, 7)$



decrypt

Ex=2

$E_{13}(1,1)$ $\quad d = 4 \quad r = 2$

$e_1 = (4,2)$ $\quad PT = (12,5)$

$e_2 = 4 * (4,2)$

$= 2(2(4,2))$

$= 2((4,2) + (4,2))$

$= 2(8,1)$

$e_2 = (11,2)$

$(4,2) + (4,2)$

$\lambda = \frac{3x_1^2 + a}{2y_1}$

$= \frac{3*16+1}{4} \Rightarrow$

$= 49 * 4^{-1} \mod 13$

$x_3 = 8$

$y_3 = 1$

Page No.
Date

$r = 2$, $C_1 = (8, 1)$

$C_2 = (12, 5) + (4, 11)$

$= (0, 12)$

$PT = e_2 - d * C_1$

$= (0, 12) - (4, 11)$

$= (0, 12) + (4, 2)$

$= (12, 5)$

Proof

$PT = \frac{C_2}{T} - d * C_1$

$= PT + r * e_2 - d * r * e_1$

$= PT + r * d * e_1 - d * r * e_1$ (Additive inverse)

$= PT$

Page No.
Date

Syllabus :-

- → limitation of knapsack
- → Rabin Crypto System
- → Man in the ~~mradit~~ middle
- → Primitive roots
- → choosen cipher text attack on RSA
- → Algamal
- → proof of Algamal
- → How to find points on curve.
- → ~~find~~ ~~Ell~~ Eliptical Elgamal.

Ex

Q: $E_{11}(3,5)$ $d=3$ $r=5$

find e_1, one of point on curve as PT.