30Oct

RSA

$Y = x^e \bmod n$

$X = y^d$

→ e may be choosen small but d is always large.

→ 1024 – 3072

x^8

$x \cdot x = x^2$
$x^2 \cdot x = x^3$
$x^3 \cdot x = x^4$
⋮
$x^7 \cdot x = x^8$

$x \cdot x = x^2$
$x^2 \cdot x^2 = x^4$
$x^4 \cdot x^4 = x^8$

$x^{2^{1024}}$

$x \cdot x = x^2$
$x^2 \cdot x^2 = x^3$
$x^3 \cdot x = x^4$
⋮
$x^{2^{1024}-1} \cdot x = x^{2^{1024}}$

Steps $\Rightarrow 2^{1024} - 1$

→ Linear complexity

$x \cdot x = x^2$
$x^2 \cdot x^2 = x^4$
$x^4 \cdot x^4 = x^8$
⋮
$x^{2^{1023}} \cdot x^{2^{1023}} = x^{2^{1024}}$

Steps = 1024

→ logarithmic complexity

x^{26}

$x \cdot x = x^2$ — SQ
$x^2 \cdot x = x^3$ – MUL
$x^3 \cdot x^3 = x^6$ – SQ
$x^6 \cdot x^6 = x^{12}$ – SQ
$x^{12} \cdot x = x^{13}$ – MUL
$x^{13} \cdot x^{13} = x^{26}$ → SQ

→ minimum no. of steps.

#SAM (Square & Multiply ~~op~~ algorithm)

→ The algorithm is based on scaling the bit of the exponent from left to right

→ In every iteration (it means for every exponent bit) the current result is squared.

↳ If and only if currently scanned exponent bit has the value 1, a multiplication of current result by x is executed following the squaring.

$x^{26} \rightarrow 11010 = x^{h_4 h_3 h_2 h_1 h_0}$

$XX = X^2$
$XX^2 = X^3$
$X^3 X^3 = X^6$
$X^6 X = X^7$

$10 + 1 = 11$

$11 + 11 = 110$

$110 + 110 = 1100$

$1101 + 1101 = 11010$

initial bit processed by $h_4 = 1$

#0 → x^1

#1a $(x^1)^2 = x^{10_2}$ → SQ bit processed by $h_3 = 1$

#1b $(x^2 x) = x^{10_2} x^1 = x^{11_2}$ → MUL since $h_3 = 1$

#2a $(x^3)^2 = (x^{11_2})^2 = x^{110_2}$ → SQ bit processed h_2.

→ no MUL since $h_2 = 0$.

#3a $(x^6)^2 = (x^{110_2})^2 = x^{1100_2}$ → SQ bit processed h_1

MUL since $h_1 = 1$

3b $(x^{12})x = x^{1100_2} x^{1_2} = x^{1101_2}$

#4a $(x^{13})^2 = (x^{1101_2})^2 = x^{11010_2}$

↳ SQ bit processed h_0

→ no mul since $h_0 = 0$

4b

x^{21} x^{10101} $x^{h_4 h_3 h_2 h_1 h_0}$

0 $\longrightarrow x^1$ → initial bit processed by $h_4 = 1$

1a $(x^1)^2 = x^{10_2}$ → Sq bit processed by $h_3 = 0$.

1b → no MUL since $h_3 = 0$

2a $(x^2)^2 = (x^{10_2})^2 \Rightarrow x^{100_2}$ → Sq bit processed by $h_2 = 1$ → $10 + 10 = 100$

2b $(x^4)x = x^{100_2} \cdot x^{1_2} = x^{101_2}$ → MUL since $h_2 = 1$. → $100 + 1 = 101$

3a $(x^5)^2 = (x^{101_2})^2 \Rightarrow x^{1010_2}$ → Sq bit processed by $h_1 = 0$ → $101 + 101 = 1010$

3b → No MUL since $h_1 = 0$

4a $(x^{10})^2 = (x^{1010_2})^2 = x^{10100_2}$ → Sq bit processed by $h_0 = 1$ → $1010 + 1010 = 10100$

4b $(x^{20})x = (x^{10100_2})(x^{1_2}) = x^{10101_2}$ → MUL since $h_0 = 1$

Squaring → 4 times Multiplication → 2 times.

⑥ SAM for modular Exponentiation

Input

base element x

exponent $H = \sum_{i=0}^{t} h_i 2^i$ with $h_i \in 0, 1$ & $h_t = 1$

and modulus n.

Output

$x^H \bmod n$.

Initialization $r = x$

Algorithm

1 For $i = t-1$ Down To 0

1.1 $r = r^2 \bmod n$

If $h_i = 1$

$r = r \times \bmod x$

2 RETURN (r)

$H = t+1$

$\log_2 H = t+1$

SQ = t

MUL = hamming weight

it means number of 1s in binary representation

(0.5t) = Avg no. of multiplication.

↳ cryptography has good random property, having half no. of 1s is good.

Because the exponent used in cryptography have happen often good random properties assuming that half of theirs bits have value 1 is good/valid approximation

Que) How many operations are req. on avg for an exponentiation with 1024 bit exponent.

↳ SQ = 999
MUL = 500

SQ + # MUL ⇒ 1.5t
⇒ 1.5(1024)
⇒ 1536

linear complexity
$2^{1024} \approx 10^{300}$.

Speed up techniques for RSA :→

→ Fast ~~expo~~ encryption with short public exponent

→ The public key e can be coosen to be a very small in practice 3 values $e=3, e=17, e=2^{16}+1$

	e	binary	
2^1+1	3	11_2	⇒ 3
2^4+1	17	10001_2	⇒ 5
$2^{16}+1$	$2^{16}+1$	$100000\ 0000\ 0000\ 0001_2$	⇒ 17

this exponent has low hamming weights so used in cryptography for encryption.

⊙ This results in particularly low no operation for performing an exponention (low hamming weight)

↳ Interestingly RSA is still secured if such short exponents are being used note that private key 'd' still has in general full bit length t+1 even though e is short.

⊛ RSA is fastest key algorithm.

Fast decryption with CRT (chinese remainder theorem)

↳ Transformation of i/p into CRT domain.

$x \quad n(p,q)$

$x_p \equiv x \bmod p$

$x_q \equiv x \bmod q$

↳ Exponentiation in CRT domain.

$$y_p \equiv x_p^{d_p} \bmod p$$

$$y_q = x_q^{d_q} \bmod q$$

where $d_p \equiv d \bmod p-1$

$d_q \equiv d \bmod p-1$

↳ Note that d_p & d_q are bounded by p & q respectively and the same result hold for transform result y_p & y_q.

↳ Since the 2 primes are inpractice choosen to have roughly the same bit length, the 2 exponents as well as y_p & y_q hav about half the bit length n.

Inverse transformation into problem domain.

$$y = \left[[q C_p] y_p + [p C_q] y_q \right] \bmod n.$$

where C_p & C_q are computed as

$C_p = q^{-1} \bmod p$

$C_q = p^{-1} \bmod q$

Que) Let the RSA parameter be given by $p=11, q=13, e=7$, 10/10

$d = e^{-1} \bmod (120)$ $(n=143)$

$= 7^{-1} \bmod (120)$

$= 103$

Que Compute RSA decryption for cypher text $y=15$ using CRT

$\Rightarrow$ 1 $[y^d \bmod n]$ $\quad 15^{103} \bmod 143$

$y_p = 15 = 4 \bmod 11$

$y_q = 15 = 2 \bmod 13$

$y_p = 4 \bmod 11$

$y_q = 2 \bmod 13$

$d_p \equiv 103 \equiv 3 \bmod 10$

$d_q \equiv 103 \equiv 7 \bmod 12$

$x_p \equiv y_p^{d_p} = 4^3 \bmod 11 \Rightarrow 64 \bmod 11 = 9 \bmod 11$

$x_q = y_q^{d_q} = 2^7 \bmod 13 \Rightarrow 128 \bmod 13 \Rightarrow 11 \bmod 13$

$X = q\,C_p\,x_p + [p\,C_q]\,x_q$

$C_p = 13^{-1} \bmod 11$

$C_q = 11^{-1} \bmod 13$

(i) $13^9 \bmod 11 \Rightarrow$ $13 \bmod 11 \Rightarrow 2$; $13^2 \Rightarrow 4$; $13^4 \bmod 11 \Rightarrow 5$; $13^8 \cdot 25 \bmod 11 \Rightarrow 3$; $3 \times 2 \Rightarrow 6 \bmod 11$

(ii) $11^{11} \bmod 13$

1	$11 \bmod 13 \Rightarrow 11$
2	$121 \bmod 13 \Rightarrow 4$
4	$16 \bmod 13 \Rightarrow 3$
8	$\Rightarrow 9$

$8 \times 2 \times 1 \neq 9 \times 4 \times 11 \bmod 13$

$\Rightarrow 6$

$6 \cdot 36 \bmod 13$

$\times 11$

396

$X \Rightarrow [13 \times 6 \times (9) + (11)(6)(11)] \bmod 143$

$\Rightarrow 13 \times 54 + 121 \times 6$

$702 + 726$

$1428 \bmod 143$

$\Rightarrow (141)$

$54 \times 13 = 702$

$143 \times 9 = 1287$

$1428 - 1287 = 141$

⑥ Security of RSA

1) Brute force attack →

This involves trying all possible private keys Several approaches all equivalent in effort to factoring the product of two prime.

2) Timing attack →

This depends on running time of decryption attack.

3) Choosen cipher text attack

This type of attack exploits properties of RSA algorithm.

→ 3 approaches in factoring

(i) Factoring n into two prime p, q enables us to

$\phi(n) = (p-1)(q-1)$

(ii) $\boxed{d = e^{-1} \bmod \phi(n)}$

(ii) Determine $\phi(n)$ directly without determination of p & q

(iii) Determine d directly without finding $\phi(n)$.

Diffe-Hellman Key exchange (DHKE)

10 Oct

→ This is first published public key algorithm appeared in seminal papere by W Diffe & M Hellman in paper → (New Direction in Cryptography)

→ {SHS, TLS,

Z_n^* → The set Z_n^* consists of elements integers {0, ----(n-1)} for which gcd (i, n) = 1 forms an abelian group under multiplication under multiplication n.
The identity element e = 1

$Z_9^* = \{1, 2, 4, 5, 7, 8\}$

	1	2	4	5	7	8
1						
2						
3						

X	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

* Cyclic Group

① A group (G, o) is finite |G|
|G| ⇒ (no. of element present in group = cardinality / order)

Order of an element → The order of element a of group (G, ·) is the smallest positive integer s.t.

$a^k = a.a.a \underbrace{\dots\dots a}_{k \text{ times}} = 1$ (1 is identity element)

$Z_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$

Que) find order of 3.

$a = 3 \bmod 11$

$a^2 = 3^2 \bmod 11 = 9$

$a^4 = 3^4 \bmod 11 \Rightarrow 81 \bmod 11 \Rightarrow 4$

$a^8 = 3^8 \bmod 11 \Rightarrow 16 \bmod 11 \Rightarrow 5$

$a^{16} \Rightarrow 3^{16} \bmod 11 \Rightarrow 25 \bmod 11 \Rightarrow$

So order of $3 \Rightarrow 5$ in Z_{11}^*

$a^5 \Rightarrow 4 \times 8 \bmod 11 \Rightarrow 1$

$a^6 \Rightarrow 3 \bmod 11$

$a^7 \Rightarrow 9 \bmod 11$

$a^8 \Rightarrow 5 \bmod 11$

$a^9 \Rightarrow 4 \bmod 11$

$a^{10} \Rightarrow 1 \bmod 11$

11/oct

* $|Z_n^*| \Rightarrow \phi(n)$

$|Z_{11}^*| \Rightarrow 10. \quad |Z_p^*| = p-1 \Rightarrow \phi(p)$

$(3,9,5,4,1)$ this cycle will repeat again & again.

Cyclic group

① A group G which contains an element α with maximum order

order $|\alpha| = |G|$

is said to be cyclic.

→ Element with maximum order are called generators or primitive elements.

Que) find order of 2

$a = 2$

$a^2 \Rightarrow 4$

$a^3 \Rightarrow 8$

$a^4 \Rightarrow 5$

$a^5 \Rightarrow 10$

$a^6 \Rightarrow 9$

$a^7 \Rightarrow 7$

$a^8 \Rightarrow 3$

$a^9 \Rightarrow 6$

$a^{10} \Rightarrow 1$

$\{1,2,3,4,5,6,7,8,9,10\}$

$\{2^{10}, 2^1, 2^8, \ldots\}$

∴ [2 is called generator/primitive elements]

(1) $\text{ord}(2) = |Z_{11}^*| = 10$

(2) Z_{11}^* is a cyclic group

(3) 2 is a primitive element

$\text{ord } Z_{11}^* \Rightarrow$

$1 \to 1$
$2 \to 10$
$3 \to 5$
$4 \to 5$
$5 \to 5$
$6 \to 10$
$7 \to 10$
$8 \to 10.$
$9 \to 5$
$10 \to 2.$

$\therefore$ primitive elements of $Z_{11}^* = 2, 6, 7, 8.$

$*5$	$*6$	$*7$
$5^1 = 5$	$6^1 \Rightarrow 6$	
$5^2 = 3$	$6^2 \Rightarrow 3$	
$5^3 = 4$	$6^3 \Rightarrow 7$	
$5^4 \Rightarrow 9$	$6^4 \Rightarrow 9$	
$5^5 \Rightarrow 1$	$6^5 \Rightarrow 10$	
$5^6 \Rightarrow 5$	$6^6 \Rightarrow 5$	
$5^7 \Rightarrow 3$	$6^7 \Rightarrow 8$	
	$6^8 \Rightarrow 4$	
	$6^9 \Rightarrow 2$	
	$6^{10} \Rightarrow 1$	

Que) $3^{7812245763} \mod 11$

a) 10
b) 5
c) 6
d) 7

3 | 9 | 5 | 4 | 1
× × × ×

Que) $2^{78546987\,8310} \mod 11$

$\longrightarrow$ (1)

$2^{10} \Rightarrow 1$

Que) Z_7^*

order of 2 $\to$ (3) | order of 1 $\to$ (1)

$2 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$
$2^4 \bmod 7 \Rightarrow 2$
$2^5 \bmod 7 \Rightarrow 4$

* For every prime p

Z_p^* is an abelian cyclic group

$a^p = a \bmod p$

$a^{p-1} = 1 \bmod p$

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

$|Z_p^*| = \phi(p)$

$\{ a^{|Z_p^*|} = 1 \bmod p \}$

Result

Let G be a finite cyclic group

Then every $a \in G$ it holds that $|G|$

① $a = 1$

② order a divides $|G|$

◎ No. of primitive elements $\Rightarrow \phi(|G|)$

Let G be finite cyclic group then it holds that no. of primitive elements of G is $\phi(|G|)$

② if $|G|$ is prime then all the elements except $a=1$, are primitive element.

Note → Z_p^* used in Diff Hellman.

$|Z_3^*| = 2$

16/Oct

Diffie-Hellman Setup.

① choose a large prime

② Choose $a \in [2, 3, \ldots p-2]$

③ Publish p, a. [domain parameters].

Diffie-Hellman key Exchange

Alice	Bob
① choose a k $a = K_{pr}, A \in \{2,3,\dots p-2\}$	① choose b $b = K_{pr}, B \in \{2,3,\dots p-2\}$
② compute A = public key of Alice. $= K_{pub} = \alpha^a \bmod p$	② Compute B = public key of Bob $\alpha^b \bmod B$

$A = K_{pub}A$ →

← $B = K_{pub}B$

$K_{AB} = B^a \bmod p$ $\quad$ $K_{AB} = A^b \bmod p$.

Proof of correctness.

What Alice computes

$B^a \bmod p = (\alpha^b)^a \bmod p = \alpha^{ab} \bmod p$

What Bob computes →

$A^b \bmod p = (\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$

} session key = join secret key

Que) The DH parameters are $p = 29$ & $\alpha = 2$

→ let $b = 12$ $\quad$ $a = 5$

$A \Rightarrow 2^5 \bmod 29 = 3$ $\quad$ $B = 2^{12} \bmod 29 = 7$

$K_{AB} \Rightarrow (2)^{60} \bmod 29 \Rightarrow 16$.

$3^{12} \bmod 29 \Rightarrow 16$

Que) Why we don't think of 1 & p-1 in 'α' member.

→ Basic idea of DHKE is that exponentiation of Z_p^* p=prime, is a → one way function & that exponentiation is commutative

→ Commutational aspect of DHKE are quite similar to those of RSA

→ should have similar length as RSA model it means 1024 or beyond in order to provide strong security.

→ the integer α need to have a special property it should be a primitive element.

→ If we want to use it as symmetric key for algorithm such as AES, we can simply take the 128 most significant bit.

*Discrete logarithmic Problem (DLP)

DLP in prime fields → DLP over Z_p^*

→ given finite cyclic group Z_p^* with order p-1 primitive element $\alpha \in Z_p^*$ & another element $\beta \in Z_p^*$.

DLP is problem of determining the integer $\alpha^x \equiv \beta \bmod p$.

$1 \le x \le p-1$

$x = \log_\alpha \beta \bmod p$ → provided p should be sufficiently large

Que) $Z_{11}^* \Rightarrow [2^x \equiv 9 \bmod 11]$

$x \equiv \log_2 9 \bmod 11$

$x = 6$

Que) $6^x \equiv 9 \bmod 13$

$\Rightarrow x = 4$

Que) $5^x \equiv 41 \bmod 47$

$Z_{47}^* = \alpha = 5 \quad \beta = 41$

$5^6 \bmod 13$

10×10.

$100 \bmod 13 \Rightarrow 9$

Solve DLP $a^x \equiv b \bmod n$.

(i) check $\gcd(a,n) \equiv 1$

(ii) There should exist a primitive element mod n

(iii) construct the table.

Que $5^x \equiv -1 \bmod 13$

$5^x \equiv 12 \bmod 13$

(i) $\gcd[5,13] = 1$

(ii) $(2)^x \equiv 2^6 \bmod 13$

$a^j \equiv a^k \bmod n$ iff $j \equiv k \bmod \phi(n)$

$gx \equiv 6 \bmod 12$

$x = 2$

$2^1 = 2$ $\quad 2^{11} \Rightarrow 7$

$2^2 = 4$ $\quad 2^{12} \Rightarrow 1$

$2^3 = 8$

$2^4 \Rightarrow 3$

$2^5 \Rightarrow 6$

$2^6 \Rightarrow 12$

$2^7 \Rightarrow 11$

$2^8 \Rightarrow 9$

$2^9 \Rightarrow 5$

$2^{10} \Rightarrow 10$

16/oct

(1) $g^x = 8 \bmod 13$

$x = 2$

$(2^8)^x = (2^4) \bmod 13$

$8x = 4 \bmod 12$

$(x = 2, 5, 8, 11, \ldots)$

(78)

Z_{13}^* → primitive element is (2).

GR 1

Que $11^x \equiv 7 \bmod 13$

$(2^7)^x = (2^{11}) \bmod 12$

↳ $7x = 11 \bmod 12$

$x = 5$

385 385 228 63 70 11

- Oscar knows α, A, B, p

he is interested in finding (a, b) $K_{AB} = \alpha^{ab} \bmod p$

compute $a = \log_\alpha A \bmod p$ → (DLP)

Generalized DLP

(applied to any cyclic grp).

↳ let α be a primitive element.

cyclic group $\beta = \alpha(\alpha \alpha \alpha \ldots \alpha_0) = \begin{cases} \alpha^x & \text{when multiply} \\ x\alpha & \text{when add.} \end{cases}$

(x times. any operation either +/×)

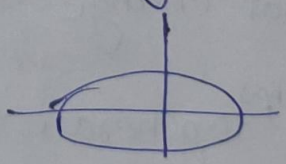
$|G| = n$ → order is n.

*which other cyclic group makes good DLP?

↳ ① Z_p^* → multiplicative group of prime field.

② $GF(2^m)^*$ → all polynomials except zero polynomial. ($m > 1$) (extension field)

③ Elliptical curve → the point in grp lies on ellipse



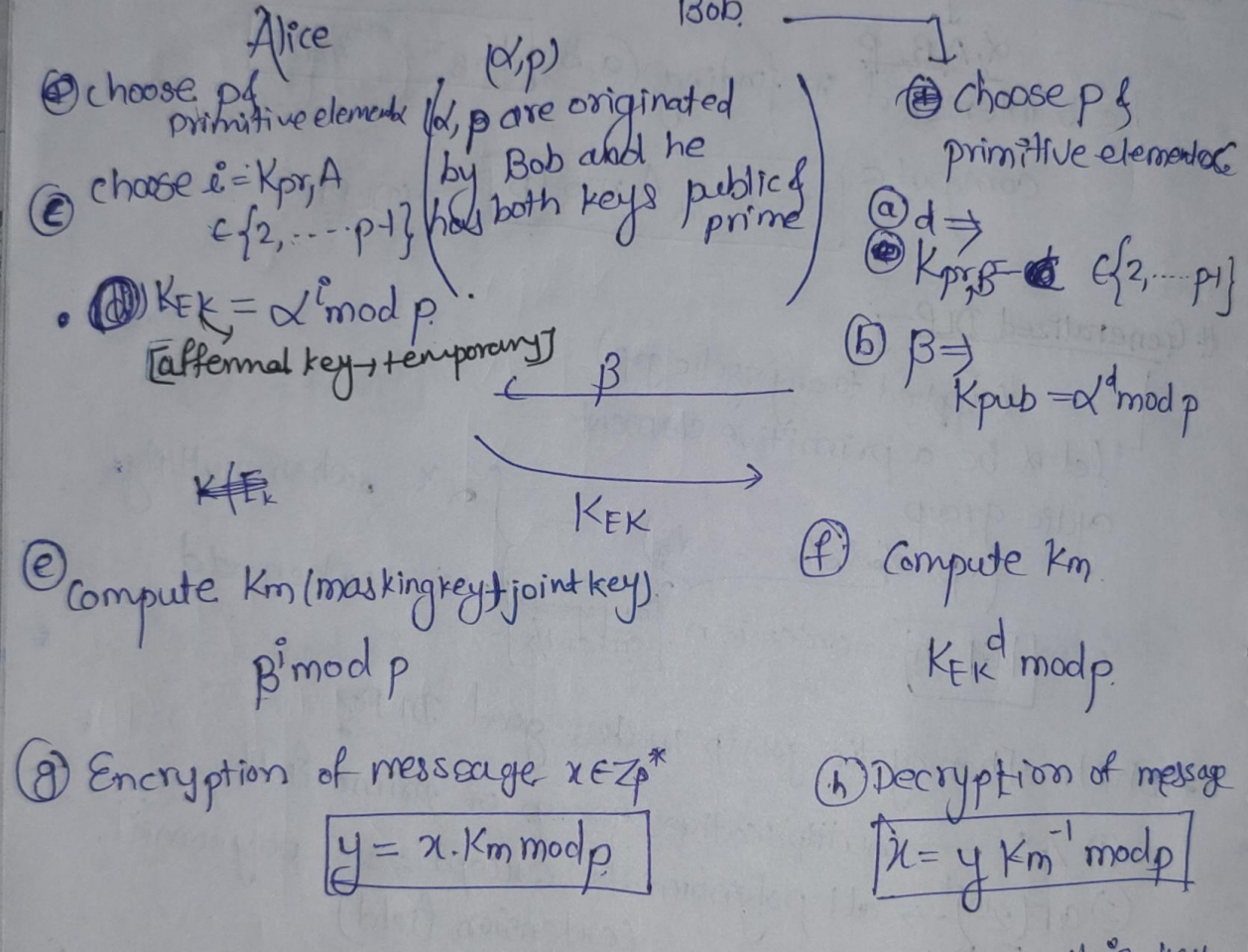
$\left[\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1\right]$

- Attack against DLP → self study.

Elgamal Encryption

↳ 1985 by Taher Elgamal

- very similar to DH but reordering the steps.
- Its security is bound on DLP & DH
- Z_p^* → p prime



→ Bob computes its private key d & public key β this key pair does not change it can be used for encrypting many msg.

→ Alice however has to generate a new public, private key pair for encryption of every msg. (denoted by → K_{EK} & i respectively)

and this key is affermal key.

eg → Bob generates the elgamal keys (~~KPG~~) & alice encrypts the message $x=26$.

$p=29$, $\alpha=2$, ~~β~~ $=d=12$, $i=5$.

Alice	Bob.
ⓒ $i^0=5$	ⓐ $d=12$
	ⓑ $\beta \Rightarrow K_{pub}\ B = (2)^{12} \bmod 29$. $\Rightarrow$ ⑦
ⓓ $K_{EK}=(2)^5 \bmod 29$ $\Rightarrow$ ③	
ⓔ $K_m \Rightarrow (7)^5 \bmod 29$ $\rightarrow$ ⑯	ⓕ $K_m \Rightarrow (3)^{12} \bmod 29$ $\Rightarrow 16$
ⓖ $y = 26 \cdot 16 \bmod 29$ $\Rightarrow 416 \bmod 29$ $\Rightarrow$ ⑩	ⓗ $x=(10)[16]^{-1} \bmod 29$ $\Rightarrow 10 \times 16^{-1} \bmod 29$

$7 \bmod 29 = 7$
$7^2 \bmod 29 \Rightarrow 20$
7^4 400 mod 29 ⇒

→ Elgamal is probabilistic encryption scheme it means two identical msg x_1 & $x_2 \in Z_p^*$ using same public key results into 2 cipher text y_1 & y_2 where $y_1 \neq y_2$ this is because i is choosen at random from $(2,3,\ldots p^2)$ for each encryption. & thus also the session key [Km] $= \underline{\beta^i \bmod p}$ used for encryption is choosen at random for each each encryption.

K_{EK} must be different for every plain text.

$x_1 = x_2$

$y_1 \neq y_2$

$K_{EK} = \alpha^i \bmod p$

18/Oct

Proof of correctness

We have to show that

proof $d_{KPR}(Y, E_{EK}) = Y K_m^{-1} \bmod p$

(we are performing 2 different operation for alice & Bob)

$\Rightarrow x K_m^{[K_m]^{-1}} \bmod p$

$\Rightarrow x K_m [K_{EK}^{d}]^{-1} \bmod p$

$x \beta^{i} [K_{EK}^{d}]^{-1} \bmod p$

$\Rightarrow x \beta^{i} [\alpha^{id}]^{-d} \bmod p$

$\Rightarrow [x \alpha^{di}][\alpha^{-id}] \bmod p$

$\Rightarrow \boxed{x \bmod p}$

Self study

(#) Computational Aspect of Engamal Encryption

Elliptical Curve Cryptosystem (ECC)

- ECC provides same level of security or discrete logarithm with considerably shorter operand.

160-256 bit (ECC) vs 1024-3072 bits (RSA)

- ECC has performance advantages (fewer computation) & bandwidth advantages, short signature & keys over RSA & DL schemes.
- However RSA algorithms which involves short public keys are still much faster than ECC operations.
- ECC is based on DLP.

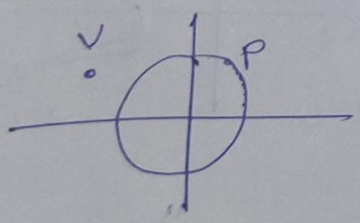
→ How to compute Elliptical Curves.

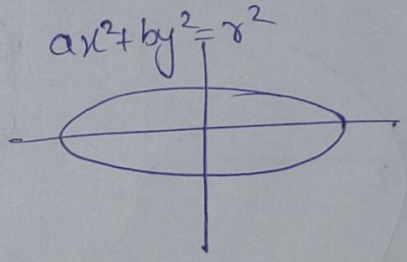
$$a \times k = \underbrace{a + a + a - - - - a}_{k \text{ times}}$$

$$p = ak$$

$x^2 + y^2 = r^2$ over $\mathbb{R}$

$(x, y) \in R$





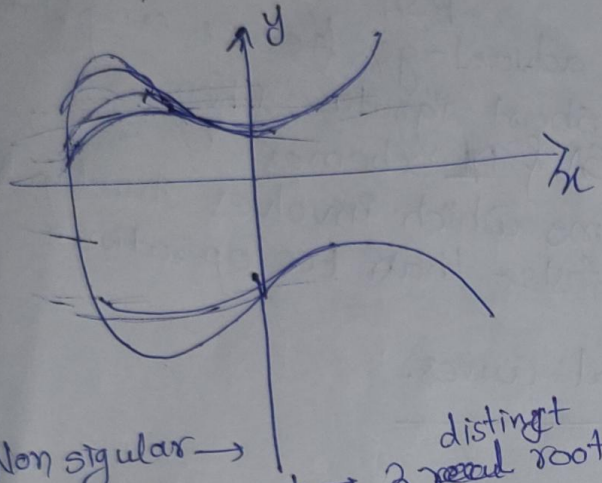
Elliptic curve: → The elliptic curve over Z_p, $p > 3$ is the set of all pairs $(x, y) \in Z_p$ which fulfills.

$$y^2 = x^3 + a \cdot x + b \bmod p.$$

together with an imaginary point of infinity.
(where $a, b \in Z_p$)

and the condition $4a^3+27b^2 \neq 0 \bmod p$.

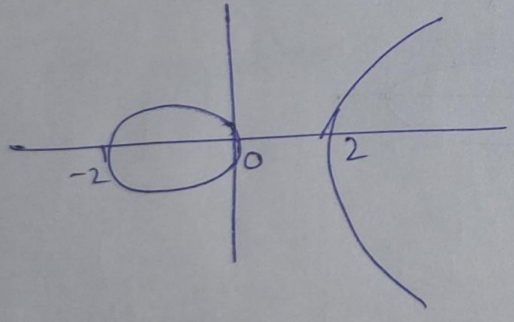
$y^2 = x^3+ax+b$



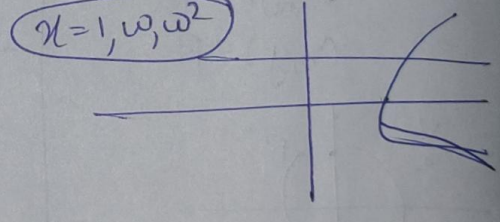
Non singular
→ Geometrically the graph has no intersection, plot has no self intersection or vertices.

Non singular → x^3+ax+b → 3 distinct roots / (real or complex)

* $y^2 = x^3+x$
$x = 0, 2, -2$



* $y^2 = x^3-1$
$x^3 = 1$
$(x-1)(x^2+1+x) = 0$
$x = 1, \omega, \omega^2$



→ It is symmetric wrt x axis