CRNS

* Types of numbers : 1) 1
2) Prime
3) Composite

* Prime :

A prime number is a whole number greater than 1 whose only factors are 1 and itself.

ex :- 2, 3, 5, 7, 11, 13, 17, 19, ...

* Relatively prime or Co-prime numbers :-

Two positive integer a and b are relatively prime if gcd (a, b) = 1.

* IMP Notes :-

1) Any two prime numbers are relatively prime.
2) Any two consecutive numbers are relatively prime.
3) A prime number is relatively prime with any other number.
4) Two even numbers are NEVER relatively prime because number 2 is a factor of all even numbers. Hence, they are not relatively prime.
5) Relatively prime numbers don't need to be prime numbers. ex :- 12 and 35.
gcd (12, 35) = 1 ∴ R. Prime

* If $p = 7$ and $q = 1$ to $p-1$

and if p is prime number, then p and q are Relatively prime.

ex: $p = 7$, $q = 1$ to $p-1$
$= 1, 2, 3, 4, 5, 6.$

(q, p)	gcd(q, p)	Relatively prime
(1, 7)	1	✓
(2, 7)	1	✓
(3, 7)	1	✓
(4, 7)	1	✓
(5, 7)	1	✓
(6, 7)	1	✓

* Euler's Totient Function $\phi(n)$:-

→ The totient $\phi(n)$ of a positive integer n greater than 1 is defined to be the number of positive integers less than n that are coprime to n.

It does not hold for 4, 8, 9.

→ $\phi(n) = n - 1$, if n is a prime number.

→ $\phi(m * n) = \phi(m) \cdot \phi(n)$, if m and n are coprime.

→ For composite numbers, (General formula)

$$n = a \times b.$$

$$\phi(n) = n * \left(1 - \frac{1}{P_1}\right) * \left(1 - \frac{1}{P_2}\right) \ldots$$

where, a, b are composite numbers.
P_1, P_2 are distinct prime numbers.

ex:- $n = 1000$

$$n = a \times b$$
$$= \underline{5}^3 \times \underline{2}^3$$

$$\phi(n) = n \cdot \left(1 - \frac{1}{P_1}\right) \cdot \left(1 - \frac{1}{P_2}\right)$$

$$\phi(1000) = 1000 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{2}\right)$$

$$= 1000 \times \frac{4}{5} \times \frac{1}{2}$$

$\therefore \phi(1000) = 400$

(1) $n = 7000 = 7 \times 5^3 \times 2^3$

$$\phi(7000) = 7000 \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{2}\right)$$

$$= 7000 \times \frac{6}{7} \times \frac{4}{5} \times \frac{1}{2}$$

$$= 2400$$

(2) $n = 9 \Rightarrow 3^2$

$$\phi(9) = 9 \cdot \left(1 - \frac{1}{3}\right)$$

$$= 9 \times \frac{2}{3}$$

$$= 6$$

(3) $n = 369 \Rightarrow 3 \times 3 \times 41 = 3^2 \times 41$

$$\phi(369) = 369 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{41}\right)$$

$$= 369 \times \frac{2}{3} \times \frac{40}{41}$$

$$= 240$$

(4) $n = 4 \Rightarrow 2 \times 2 = 2^2$

$$\phi(4) = 4 \cdot \left(1 - \frac{1}{2}\right)$$

$$= 4 \cdot (1/2) = 2$$

(5) $n = 372 \Rightarrow 2 \times 2 \times 30 \times 31$

$= 2^2 \times 3 \times 31$

$\phi(372) = 372 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{31}\right)$

$= 372 \cdot \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{30}{31}\right)$

$= 120$

(6) $n = 15 \Rightarrow 5 \times 3$

$\phi(15) = 15 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{3}\right)$

$= 15 \times \frac{4}{5} \times \frac{2}{3}$

$= 8$

(7) $n = 8 \Rightarrow 2^3$

$\phi(8) = 8 \cdot \left(1 - \frac{1}{2}\right)$

$= 8 \cdot \frac{1}{2}$

$= 4$

Page No.
Date / /

* Modulo Congruent :-

→ Two numbers a & b are said to be congruent modulo n when their difference a - b is integrally divisible by n.
So, a - b is multiple of n.

→ It is denoted as : $a \equiv b \mod n$
which means a - b is divisible by n.

$a \equiv b \mod n \Rightarrow a \mod n = 91$
$b \mod n = 91.$

→ a and b are said to be congruent modulo when they both have same remainder when divisible by n.

ex:- (1) $a = 24, \quad b = 34, \quad n = 10.$

$24 \mod 10 = 4$
$34 \mod 10 = 4$

∴ 24, 34 said to be congruent modulo.

(2) $a = 13, \quad b = 11, \quad n = 1$

$13 \mod 1 = 0$ ∴ Congruent modulo.
$11 \mod 1 = 0$

* Fermat's Theorem :-

→ It states that, if p is a prime number and a is a positive integer which is not divisible by p then,

$$a^{p-1} \equiv 1 \bmod p.$$

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

ex :-

$p = 5$, $a = 2$, $2^4 \bmod 5 = 1$

$16 \bmod 5 = 1$ ✓

$p = 13$, $a = 11$, $11^{12} \equiv 1 \bmod 13$.

$\Downarrow$

$11^{12} \bmod 13 = 1$ ✓

$p = 6$, $a = 2$, $2^5 \bmod 2$

$32 \bmod 6 = 2 \neq 1$ X

* Modulo Arithmetic :-

1. $(A+B) \bmod C = (A \bmod C + B \bmod C) \bmod C$
2. $(A-B) \bmod C = (A \bmod C - B \bmod C) \bmod C$
3. $(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$
4. $(A \hat{} B) \bmod C = ((A \bmod C) \hat{} B) \bmod C$
5. $(A/B) \bmod C = [(A \bmod C) * (B^{-1} \bmod C)] \bmod C$

↳ division is not in syllabus.

** ex :-

(1) $(11 \hat{} 7) \bmod 4$

$= [(11 \bmod 4) \hat{} 7] \bmod 4$

$= (3 \hat{} 7) \bmod 4$

$= 3$

(2) $23^{3} \bmod 30$

→ $A = 23$
$B = 3$
$C = 30.$

$(A \uparrow B) \bmod C = ((A \bmod C) \uparrow B) \bmod C$

$\therefore 23^3 \bmod 30 = ((23 \bmod 30) \uparrow 3) \bmod 30.$

$= 23^3 \bmod 30.$

$= 12167 \bmod 30$

$= 17.$

(3) $11^7 \bmod 13 = (11-13)^7 \bmod 13$

$= (-2)^7 \bmod 13$

$= -128 \bmod 13.$

$= -11$

$= 2$

$+13$
$+13$
$+13$

(∵ negative modulo)

(4) $7^{256} \bmod 13 = (7-13)^{256} \bmod 13$

$= -6^{256} \bmod 13$

$= (-4)^{16\times4} \bmod 13$

$= (256)^{16} \bmod 13$

$= (9)^{16} \bmod 13$

(∵ $256 \% 13 = 9$)

$= (-4)^{16} \bmod 13$

(∵ $9 \% 13 = -4$)

$= (256)^4 \bmod 13$

$= (9)^4 \bmod 13$

$= \boxed{9}$

$= (36)^{128} \bmod 13$

$= (10)^{128} \bmod 13$ (∵ $36 \% 13 = 10$)

$= (100)^{64} \bmod 13$

$= (9)^{64} \bmod 13$ (∵ $100 \% 13 = 9$)

$= (-4)^{64} \bmod 13$ (∵ $9 \% 13 = -4$)

~~$= (16)^{28} \bmod 13$~~

~~$= (3)^{28} \bmod 13$~~ (∵ $16 \% 13 = 3$)

~~$= (9)^{14} \bmod 13$~~

~~$= (27)^7 \bmod 13$~~

(5) $88^7 \bmod 187 = (88 \times 88^6) \bmod 187$

$= \left[(88 \,\%.\, 187)(88^6 \,\%.\, 187)\right] \bmod 187$

(∵ Multiplicative rule)

$= \left[(88 \bmod 187)\{88^3 \cdot 88^3 \bmod 187\}\right] \bmod 187$

$= \left[(88 \bmod 187)\{((88^3 \bmod 187)(88^3 \bmod 187)) \bmod 187\}\right] \bmod 187.$

$= \left[(88)\{((44)(44)) \bmod 187\}\right] \bmod 187$

$(\because 88^3 \,\%.\, 187 = 44)$

$= \left[88 \cdot (66)\right] \bmod 187.$

$(\because (44 \times 44) \bmod 187 = 66)$

$= 5808 \bmod 187$

$= 11$

* Multiplicative inverse :-

→ The modular multiplicative inverse of an integer p is another integer x such that the product px is congruent to 1 with respect to the modulus m.

$$p \cdot x \equiv 1 \mod m.$$

p = integer number
x = inverse of p

$$p \cdot \frac{1}{p} \equiv 1 \mod m \quad \text{OR}$$

$$p \cdot p^{-1} \equiv 1 \mod m$$

e = public , d = private

Page No.
Date / /

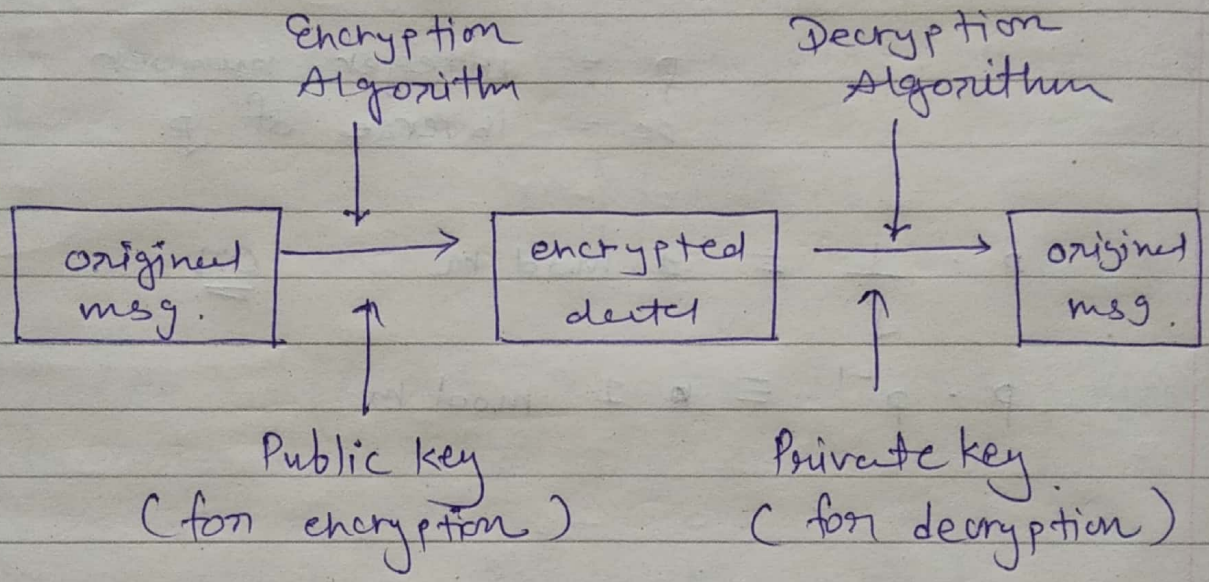
* RSA :- (Rivest, Shamir, Adleman)

Public key encryption (Asymmetric)

Algorithm

Public key encryption

Private key decryption.



1) Choose two different large prime numbers p, q.
2) Calculate $n = p \times q$.
3) Calculate $\phi(n) = (p-1)(q-1)$.
4) Choose 'e' such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$ / $\gcd(e, \phi(n)) = 1$.
5) Calculate 'd' such that $de \equiv 1 \mod \phi(n)$.

$\Rightarrow d = e^{-1} \mod \phi(n)$.

* cipher text $c = p^e \% n$

* plain text $p = c^d \% n$.

6) public key (e, n).
private key (d, n).

** ex :-

(1) $p = 3$, $q = 11$, $e = ?$, $d = ?$, $c = ?$,
Plain text $= 31 = p'$.

~~$p = ?$~~
~~↓~~
~~Plain text~~

→ $n = p \cdot q = 11 \times 3 = 33$

→ $\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$.

→ $\gcd(e, \phi(n)) = 1$

$\gcd(\text{●}, e, 20) = 1$

$\therefore \boxed{e = 7}$

→ $de \equiv 1 \mod \phi(n)$

$\therefore d(7) \equiv 1 \mod 20$
$\therefore 7 \cdot d \mod 20 = 1$
$\therefore 7 \cdot 3 \mod 20 = 1$ (Assuming d and satisfying condition)
$\therefore \boxed{d = 3}$

→ cipher text $c = p^e \% n$

$= (31)^7 \% 33$

$= (-2)^7 \% 33$

$= (-128) \% 33 + 33$

~~→ Plain text $p' = c^d \% n$~~

$= -29 + 33$

$= 4$

/* → We can also find plain text from cipher text using the formula written below

plain text $p' = c^d \% n$

* Factorization Attack / Problem :-
* Attacks on RSA / Security of RSA :-

Read from print.

* CRT (Chinese Remainder Theorem) :-

→ CRT is used to solve a set of different quadratic congruence equations with one variable but different moduli which are relatively prime as shown below :-

$$X \equiv a_1 \bmod m_1$$
$$X \equiv a_2 \bmod m_2$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$X \equiv a_k \bmod m_k$$

$m_1, m_2, \ldots, m_k$ relatively prime (They are known as moduli)

→ CRT states that above equation has a unique solution,

$$M_1 = \frac{m}{m_1}, \qquad m = m_1 \cdot m_2 \cdot m_3 \cdots m_k$$

$$M_1 M_1^{-1} \equiv 1 \bmod m_1$$

Find M_k^{-1}

$$M_2 M_2^{-1} \equiv 1 \bmod m_2$$
$$\vdots \qquad \vdots$$
$$M_k M_k^{-1} \equiv 1 \bmod m_k$$

$$X = \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1} \right) \bmod m$$

→ ex:-

(1) $X \equiv 2 \bmod 3$ $\quad X \equiv a_1 \bmod m_1$

$X \equiv 3 \bmod 5$

$X \equiv 2 \bmod 7$

→ $m = m_1 \cdot m_2 \cdot m_3$

$= 3 \cdot 5 \cdot 7$

$= 105$

→ $M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

→ $M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$\therefore 35\, M_1^{-1} \equiv 1 \bmod 3$

$\therefore M_1^{-1} = 2$ $\quad \left(\because 35\, \underline{M_1^{-1}} \,\%\, 3 = 1 \right)$

put values here.

→ $M_2 \; M_2^{-1} \equiv 1 \mod m_2$

$\therefore 21 \; M_2^{-1} \equiv 1 \mod 5$

$\therefore M_2^{-1} = 1 \quad (\because M_2^{-1} \cdot 21 \;\%\; 5 = 1)$

→ $M_3^{-1} \cdot 15 \equiv 1 \mod 7$

$\therefore M_3^{-1} = 1. \quad (\because m_3^{-1} \cdot 15 \;\%\; 7 = 1)$

→ $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod m.$

$= (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \mod 105$

$= (140 + 63 + 30) \mod 105$

$= 233 \mod 105$

$\therefore \boxed{X = 23}$

* Quadratic Congruence Modulo Composite:-

→ $x^2 \equiv 36 \mod 77$ → 7, → 11

$x^2 \equiv 36 \mod 11$	$x^2 \equiv 36 \mod 7$
$\Rightarrow x^2 \equiv 3 \mod 11$	$\Rightarrow x^2 \equiv 1 \mod 7$

$\Rightarrow x \equiv \pm 3 \mod 11$

& $x \equiv \pm 1 \mod 7$

$\Rightarrow x \equiv 3 \mod 11$

$x \equiv -3 \mod 11$

$x \equiv -1 \mod 70$

$x \equiv 1 \mod 70$

$\therefore (a_1, a_2, a_3, a_4) = (3, -3, 1, -1)$

$\therefore (m_1, m_2) = (7, 11)$

* Rabin Crypto System :-

→ Rabin crypto system is based on quadratic congruence.

→ The Rabin cryptosystem can be thought of as an RSA cryptosystem in which the value of e and d are fixed.

→ Disadvantage :. It is not deterministic that is decryption creates 4 plaintext. So, extra complexity is required.

* Key generation :-

→ Choose two large prime numbers p and q in the form of $4k+3$ and $p \neq q$.

$$4k+3 = 3 \bmod 4$$

→ $n = p \times q$.

→ n ← public key

(p, q) ← private key.

→ Encryption : $c_t = p_t^2 \bmod n$

→ Decryption : $m_p = \sqrt{c} \bmod p = \pm c_t^{\frac{p+1}{4}} \% p$

$m_q = \sqrt{c} \bmod q = \pm c_t^{\frac{q+1}{4}} \% q.$

ex:- → $p = 23$, $q = 7$ Alice sender Bob receiver.

(1) → Bob the receiver selects $p = 23$ and $q = 7$. Note that both are congruent to 3 mod 4. Bob calculates n and announces 'n' as public key and keeps p and q secret.

$$n = p \times q. = 23 \times 7 = 161$$

(2) → Alice wants to send (P_t) plain text $P_t = 24$. Here value of n and P_t is relatively prime and $P_t < n$.

Alice calculates cipher text C_t,

$$C_t = P_t^2 \bmod n$$

$$= (24)^2 \bmod 161$$

$$\therefore C_t = 93$$

∴ Alice sends 93 to Bob.

(3) → Bob receives 93 and calculates 4 values,

$$m_p = \pm C_t^{\frac{(p+1)}{4}} \bmod p \; ; \; m_q = \pm C_t^{\frac{(q+1)}{4}} \bmod q.$$

$$m_p = \pm 93^{\left(\frac{23+1}{4}\right)} \bmod 23.$$

$$= \pm (93)^6 \bmod 23$$

$$= \pm (1)^6 \bmod 23 \quad (\because 93 \bmod 23 = 1)$$

$$= \pm 1 \bmod 23$$

$$m_q = \pm 93^{\left(\frac{7+1}{4}\right)} \bmod 7$$

$$= \pm (93)^2 \bmod 7$$

$$= \pm (2)^2 \bmod 7 \quad (\because 93 \bmod 7 = 2)$$

$$= \pm 4 \bmod 7$$

(4) $\rightarrow$ $a_1 = 1 \bmod 23 = 1$

$b_{21} = -1 \bmod 23 = -1 + 23 = 22$ ($\because -$)

$a_2 = 4 \bmod 7 = 4$

$b_2 = -4 \bmod 7 = -4 + 7 = 3$

$\therefore (a_1, a_2, b_1, b_2) = (1, 4, 22, 3)$

and moduli : $(m_1, m_2) = (23, 7)$.

* Elgamal Crypto system :-

* key Generation :-

(1) Select large prime number P.

(2) Select decryption key D. (Private key)

(3) Select ~~second part of~~ encryption key E_1.

(4) Select second part of encryption key

$$E_2 = E_1^D \bmod P.$$

(5) Public key = (E_1, E_2, P)

Private key = D

Ex:- $P = 11$, $D = 3$, $E_1 = 2$.

$$\therefore E_2 = E_1^D \bmod P$$

$$= (2)^3 \bmod 11 = 8 \bmod 11 = 8.$$

$\therefore$ Public key = $(E_1, E_2, P) = (2, 8, 11)$

$\therefore$ Private key = 3.

* Encryption Process :-

(1) Select Random integer R

(2) $C_1 = E_1^R \bmod P$

(3) $C_2 = (PT \times E_2^R) \bmod P$

(4) $CT = (C_1, C_2)$.

P	= 11
D	= 3
E_1	= 2
E_2	= 8

Ex:- R = 4 , P.T = 7

$\therefore C_1 = (2)^4 \bmod 11$

$= 16 \bmod 11 = 5$

$\therefore C_2 = (7 \times 8^4) \bmod 11$

$= 6$

$\therefore CT = (C_1, C_2) = (5, 6)$

* Decryption Process :-

$$PT = [C_2 \times (C_1^D)^{-1}] \bmod P.$$

$$\therefore PT = [6 \times (5^3)^{-1}] \bmod 11$$

$\therefore$ RT $= \left[6 \bmod 11 \cdot (5^3)^{-1} \bmod 11 \right] \bmod 11$

($\because$ multiplication rule).

$= \left[(6) \cdot \{ (125)^{-1} \bmod 11 \} \right] \bmod 11$

$= \left[6 \cdot 3 \right] \bmod 11$

$\because \quad (125)^{-1} \bmod 11$

$\Rightarrow \quad 125 \cdot x \bmod 11 = 1$

$\Rightarrow \quad 125 \cdot 3 \bmod 11 = 1$

$\therefore \boxed{3}$

$= 18 \bmod 11$

$= 7$

* Elliptic Curve Cryptography :-

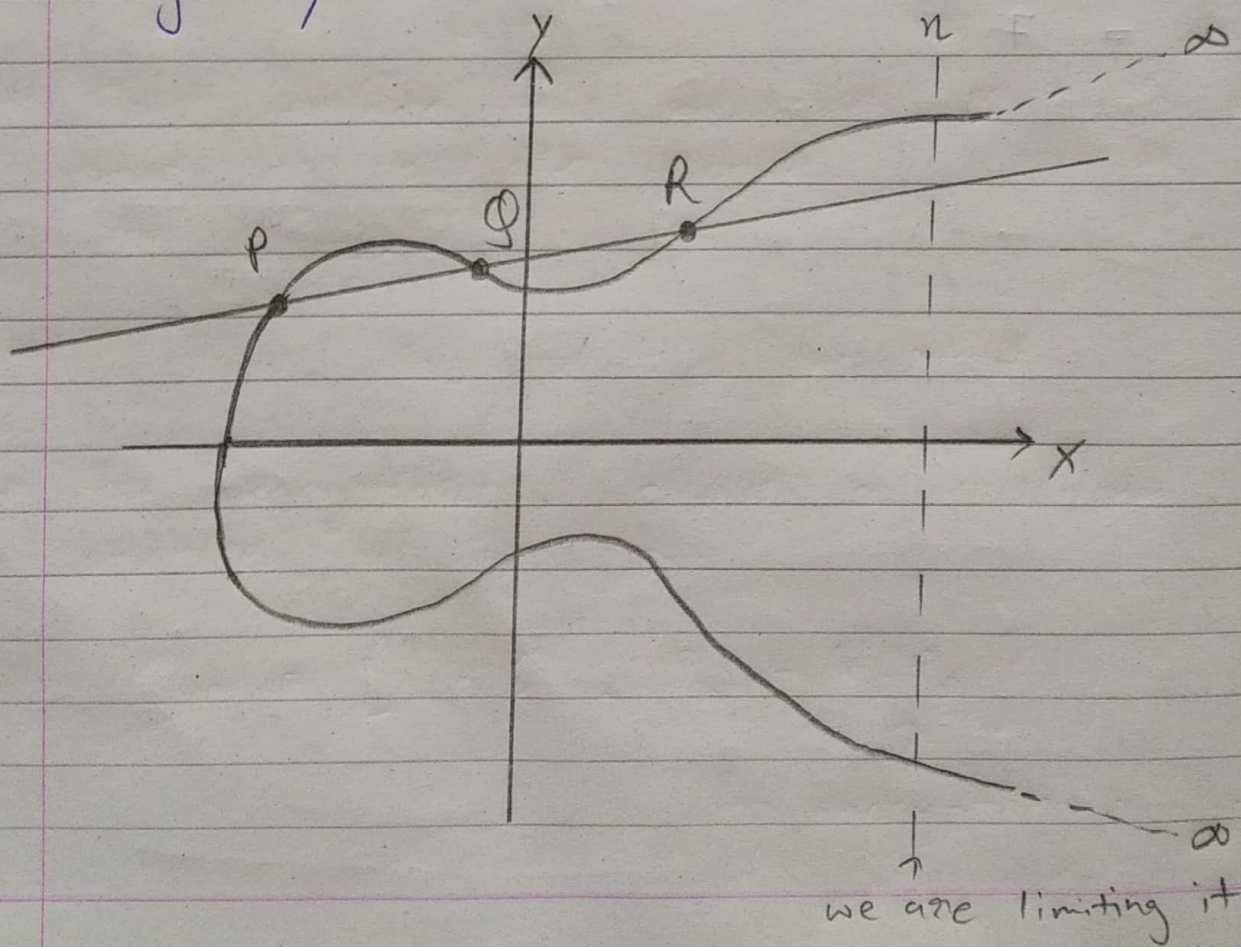
→ It is asymmetric / public key cryptosystem.

→ It provides equal security with smaller key size (as compared to RSA) as compared to non ECC algorithms.

→ Small key size and high security.

→ Elliptic curves are defined by some mathematical functions – cubic function.

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



→ Symmetric to x-axis.

→ If we draw a line, it will touch a maximum of 3 points.

→ ECC uses the concept of trapdoor function.

** Algorithm :-

1. Let $E_p(a, b)$ be the Elliptic curve.

2. Consider the eqn $Q = kP$.

where, Q, P → points on the curve
$k < n$.

k and P are given ⇒ Q is easy to find

Q and P are given ⇒ k is difficult to find.

3. ** User A key generation :-

Select private key n_A, $n_A < n$

Calculate public key P_A, $P_A = n_A \times G$
↑
global point.

4. ** User B key generation :-

Select private key n_B , $n_B < n$

Calculate public key P_B , $P_B = n_B \times G$.

5. ** $K_A = n_A \times P_B$

$K_B = n_B \times P_A$

* ECC Encryption :-

→ Let the msg be M.

→ First encode this message M into a point on elliptic curve. Let this point be P_m.

Now, this point is encrypted.

→ For encryption, chose a random positive integer K.

$$C_m = \{ KG , P_m + k \cdot P_B \}$$

for encryption public key of B is used.

ECC Decryption :-

→ For decryption, multiply 1st point in the pair with receiver's secret key.

i.e. $K G \times n_B$ | for decryption private key of B is used.

Then subtract it from the 2nd point in the pair.

$$= P_m + k \cdot P_B - (K G \cdot n_B)$$

| but w.k.t. $P_B = n_B \cdot G$

$$= P_m + k(n_B \cdot G) - K G \cdot n_B$$

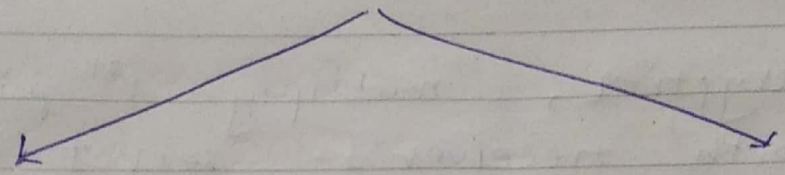
$$= P_m + K G \cdot n_B - K G \cdot n_B$$

$$= P_m$$

↑

original point / plain text.

* Substitution Cipher.



Monoalphabetic cipher	Poly alphabetic cipher
Ceuser cipher / shift / Adyptive	Vigenere cipher
Multiplicative cipher	Autokey cipher
Playfair cipher	One time pad cipher
Affine cipher	Vernam cipher
Hill cipher	

(1) Ceuser cipher / Shift cipher / Adyptive cipher :-

→ $P = C = K = Z_{26}$

$e_k(x) = (x+k) \bmod 26 \quad ; x, k \in Z_{26}$

$e_k(x) = (x-k) \bmod 26$

→ ex :- Plain text : student , $k = 11$

s	t	u	d	e	n	t
18	19	20	3	4	13	19

+k

mod 26 : 3 4 5 14 15 24 4

∴ cipher text : DEFOPZE

$Z_n = \{0, 1, 2, \ldots, (n-1)\}$.

$T = t_1 - q \cdot t_2$

Page No.
Date / /

(2) Multiplicative cipher :-

→ $e_k(P) = C = (P \times K) \bmod 26$.
(Plain text → cipher)

→ $d_k(C) = P = (C * K^{-1}) \bmod 26$.
(Cipher text → Plain)

** Find multiplicative inverse of 11 in Z_{26}.

→ First check, $\gcd(11, 26) = 1$ is true or not.

Here, $\gcd(11, 26) = 1$ ∴ true,

∴ multiplicative inverse exists.

quotient q	r_1	r_2	remainder r	t_1 (BY DEFAULT)	t_2	T $t_1 - q t_2$.
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26.
	gcd 1	0		-7	26	

→ $26 - 7 = \boxed{19}$ ← Answer.

Multiplicative inverse.

(3) Affine cipher :-

→ $K = (a, b)$

$\gcd(a, 26) = 1$

$e_k(x) = (ax + b) \% 26$ encryptim

$d_k(x) = a^{-1}(y - b) \% 26$ decryption

→ ex :- $k = (7, 3) = (a, b)$

Plain text = student

$e_k(x) = (ax + b) \% 26$

$\therefore e_k(x) = (7x + 3) \% 26.$

	s	t	u	d	e	n	t
x	18	19	20	3	4	13	19
find this → $e_k(x)$	25	6	13	24	5	16	6
cipher text	z	g	n	y	f	q	g

→ $e_k(18) = [(7)(18) + 3] \% 26$

$= 129 \% 26 = 25$

→ $e_k(19) = [(7)(19) + 3] \% 26$

$= 136 \% 26$

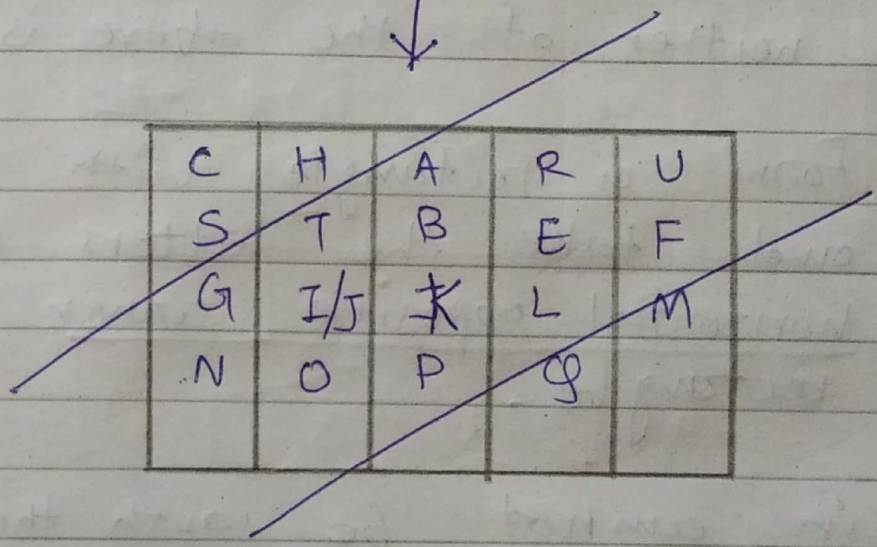
$= 6.$

→ Likewise, do this for every ac.

(4) Playfair cipher :-

→ key : CHARUSAT

→ Plain Text : University or UNIVERSITY



C	H	A	R	U
S	T	B	E	F
G	I/J	K	L	M
N	O	P	Q	

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

UN → HQ

IV → FX

ER → DU

SI → BF

TY → DW

→ If both the letters are in same column.

⇒ Take the letter below each one (going back to the top if at the bottom).

→ If both the letters are in same row

⇒ Take the letter to the right of each one (going back to left most if at the rightmost position).

→ If neither of the above is true

⇒ Form a rectangle with two letters and take the letters on the horizontal opposite corner at the rectangle.

→ Pair cannot be with the same letters

hellow he lx lo
↓
bogus letter

→ ex:- Key : CHARUSAT
P.T : HELLO.

Begins letter

HE → UT
L(X) → ZI
LO → QJ

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

(5) Hill cipher :-

→ Terminologies used :-

→ Matrix arithmetic modulo 26.
→ Square matrix
→ Determinant
→ Multiplicative inverse (Adjoint matrix).

→ $C = E(P * K) \bmod 26$ (encryption)

→ $P = D(C * K^{-1}) \bmod 26$. (decryption)

→ ex:-

Key = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$, Plain text is HE - $\begin{bmatrix} 7 \\ 4 \end{bmatrix}$

→ Encryption = $(P \cdot K) \bmod 26$.

$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26.$

$2 \times 2 \quad 2 \times 1$

$$K^{-1} = \frac{1}{|K|} K^{T}$$

$$= \begin{bmatrix} 33 \\ 34 \end{bmatrix}_{2\times 1} \quad \text{mod } 26$$

$$\therefore \quad C = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

∴ Cipher text : 7, 8
H I

→ Decryption = $(k^{-1} \cdot c) \bmod 26$

$= [(k^{-1} \cdot \bmod 26)(c \cdot \bmod 26)] \bmod 26$

$k^{-1} = \frac{1}{|K|} \; K^T$

$= \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$

$= 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 15 & 17 \\ -20 & 9 \end{bmatrix}$

$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \bmod 26$

$C \cdot \bmod 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 \\ 8 \end{bmatrix}$

∴ Decryption $= [(k^{-1} \bmod 26)(C \bmod 26)] \bmod 26$

$= \begin{bmatrix} 15 & 17 \\ -20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 105 + 136 \\ -140 + 72 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 241 \\ 212 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$

∴ Plaintext : HE

Polyalphabetic cipher:-

(1) Vigenere cipher :-

→ : Easy to decrypt.

→ In this method, length of key should be same as length of plain text. If it is not same, then characters of key will be repeated.

→ ex:- Plaintext : student , K = (2, 8, 15, 7)

P.T.	s	t	u	d	e	n	t
x	18	19	20	3	4	13	19
+K	2	8	15	7	2	8	15
C.T.	20	1	9	10	6	21	8

mod 26

(2) Autokey cipher :-

→ e.g. key = N = 13
Plain text = HELLO

∴ H E L L O
+ N H E L L

Cipher text ⇒

(3) One time pad cipher :-

→ To overcome limitations of vigenere and auto key.

Plain text = SPOURAL
Key = WINTERS.

(Key should be different and any characters).

(4) Vernam cipher :-

→ eg. Plain text = O A K
Key = S O N.

O ⇒ 14 ⇒ 0 1 1 1 0
S ⇒ 18 ⇒ 1 0 0 1 0.
XOR Result ⇒ 1 1 1 0 0 ⇒ 28

∴ 28 − 26 = 2.
⇓
C
∴ Cipher text is 'C'.

* Transposition Cipher :-

1. Rail fence cipher
2. Single Columnar
3. Double Columnar.

(1) Rail fence cipher :-

→ eg. using 3 rails.
Plain text :
we are discovered flee at once.

w				e				c				r				l								
	e		r		d		s		o		e		e		f		e			e	d			
		a				i				v				d										

												t						e						
											o				c									
										n														

Then reads off :

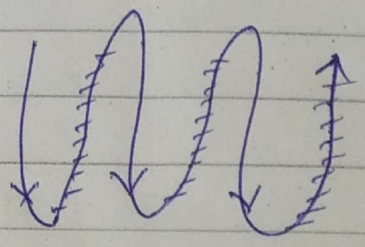
wecrlte erdsoeefeaoc aivden

~~→ Decryption is easy to try.~~

(2) Route cipher :-

→ Plain text : we are discovered flee at once.
Key : 3

→ encryption : write it in a matrix in spiral route.



w	r	i	o	r	f	e	o	e					
e	e	s	v	e	l	q	n						
a	d	c	e	d	e	t	c						

(3) Columnar transposition :-
key : ZEBRAS

Z	E	B	R	A	S
6	3	2	4	1	5

P.T. : We are discovered flee at once.

Regular

6	3	2	4	1	5
w	e	a	r	e	d
i	s	c	o	v	e
r	e	d	f	l	e
e	a	t	o	n	c
e	q	k	j	e	q

nulls

Irregular

6	3	2	4	1	5
w	e	a	r	e	d
i	s	c	o	v	e
r	e	d	f	l	e
e	a	t	o	n	c
e					

empty.

→ encrypted column by column.

eovlne acdtlk esecaq ⟹ same without last chars.
rnofoj deecq wiree

* ECC : Elliptic Curve Cryptography :-

* Examples :-

*) Formulas :-

$P = (x_1, y_1)$

$Q = (x_2, y_2)$

$y^2 = ax^3 + bx + c$

→ $P + Q = (x_3, y_3)$

where, $x_3 = \lambda^2 - x_1 - x_2$

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

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

→ if $P = Q \Rightarrow \underline{2P = (x_3, y_3)}$

(1) Find points on Elliptic curve : $y^2 = (x^3 + ax + b) \bmod 11$

$E_{11}(1, 6)$.

→ Here, $a = 1$, $b = 6$.

x	y^2	y	$y^2 \bmod 11$
0	6	0	0
1	8	1	1
2	5	2	4
3	3	3	9
4	8	4	5
5	4	5	3
6	8	6	3
7	4	7	5
8	9	8	9
9	7	9	4
10	4	10	1

→ points : (2, 4) , (2, 7)
(3, 5) , (3, 6)
(5, 2) , (5, 9)
(7, 2) , (7, 9)
(8, 3) , (8, 8)
(10, 2) , (10, 9).

(2) $P = (3, 10) = (x_1, y_1)$

$Q = (9, 7) = (x_2, y_2)$

$E_{23}(1, 1)$. Find $P+Q$, $2P$, $-P$.

→ Here, $P \neq Q$.

→ $P + Q = (x_3, y_3)$

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

$= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$= \left(\frac{7-10}{9-3}\right)^2 - 3 - 9$

$= \left(\frac{-3}{6}\right)^2 - 12$

$= \frac{1}{4} - 12$

$= 6 - 12$

$= -6 \cdot \mod 23.$

$= 17$

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

$= \left(\frac{-1}{24}\right)\left(3 - 17\right) - 10$

$= \frac{-1}{24}(-14) - 10$

$= +7 - 10$

$= -3 \mod 23$

$= 20.$

$\therefore P + Q = (x_3, y_3) = (17, 20)$ | $a = 1, b = 1$ given

$\rightarrow 2P = (x_3, y_3)$ | For $2P$, $x_1 = x_2$ & $y_1 = y_2$

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

$= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - x_1 - x_2$

$= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

$= \left(\frac{3(3)^2 + 1}{2(10)}\right)^2 - 2(3)$

$= \left(\frac{28}{20}\right)^2 - 6$

$= \frac{-92}{20} \mod 23.$

$= \left(\left(\frac{28}{20}\right)^2 - 6\right) \mod 23$

$= \left[\left(\frac{28}{20}\right)^2 - 6 \mod 23\right] \mod 23$

$= \left[\left(\frac{5}{20}\right)^2 - (-17)\right] \mod 23$

$= \left[(1/4)^2 + 17\right] \mod 23.$

$= ((6)^2 + 17) \mod 23$

$= (36 + 17) \% 23$

$= 7$ ← — — — —

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

$= \left(\frac{28}{20}\right)(3 - 17) - 10$

$= \frac{28}{20}(-14) - 10$

$= \left(-\frac{78}{5}\right) \mod 23.$

$= \left(\frac{-78 \mod 23}{5}\right) \mod 23$

$= \left(\frac{-55}{5}\right) \% 23$

$= -11 \% 23$

$= 12$

$\therefore 2P = (x_3, y_3) = (7, 12)$

$\rightarrow -P = (x_1, -y_1)$

$= (3, -10) \mod 23$

$= (3, 13)$

d = private key component
e = public key component.

Page No.
Date / /

* Digital Signature :-

DS Signing algorithm	DS verification algorithm
I/p : Msg and private key of sender	I/p : Msg and public key of sender
o/p : digital sign.	o/p : verifies the msg digest

* Digital Signature Scheme using RSA algorithm

1) two large prime numbers : p, q.
2) $n = p \times q$.
3) $\phi(n) = (p-1)(q-1)$
4) Choose 'e' such that $1 < e < \phi(n)$ and e is co-prime to $\phi(n)$ or $\gcd(\phi(n), e) = 1$.
5) Calculate d,

$$de \equiv 1 \bmod \phi(n)$$
$$\Rightarrow d \equiv e^{-1} \bmod \phi(n)$$
$$\Rightarrow de \bmod \phi(n) = 1 \quad (*)$$

6) For signing algorithm, Alice creates signature for the message using private key component {d, n}.

$$\text{signature} \rightarrow (S) = \underset{msg}{M}^{d} \bmod n$$

7) Bob receives msg and signature {m, s}. Bob applies the public key of sender (Alice) {e, n} to create msg m'.

$$m' = s^e \bmod n$$

Que :- Alice has public RSA modulo $n = 91$. public key $e = 5$. She wants to sign document $m = 7$.

i) Find sign document.
ii) Show Bob's calculations to verify whether document's valid or not.

i) $n = 91$, $e = 5$, $m = 7$

$\therefore s = m^d \bmod n$

$= (7)^{29} \bmod 91$

$= 63$

ii) Bob's calculations

$m' = s^e \bmod n$

$= (63)^5 \bmod 91$

$= \boxed{7}$

$\therefore m = m'$ $\therefore$ Verified.

$de \equiv 1 \bmod \phi(n)$

$n = 91 = 13 \times 7$

$= p \times q$

$\therefore \phi(n) = 12 \times 6$

$= 72$

$de \equiv 1 \bmod 72$

~~$\therefore de \bmod 72 = 1$~~

~~$\therefore 5d \bmod 72 = 1$~~

$\therefore 5d \equiv 1 \bmod 72$

$\therefore 5d = 1 \bmod 72$

$\therefore 5d \bmod 72 = 1$

$\therefore \boxed{d = 29}$

Private key of Alice → X_A
Public key of Alice → $\{q, \alpha, Y_A\}$.

Page No.
Date / /

* The Elgamal Digital Signature :-

Step 1 : **Key Generation.**

1) Select prime number q.
2) Select a primitive root α of q.
3) Generate a random integer X_A such that $1 < X_A < q-1$.
4) Compute Y_A, $Y_A = (\alpha)^{X_A} \bmod q$.
5) Generate keys for user A,

Private key → X_A
Public key → $\{q, \alpha, Y_A\}$

Step 2 : **Generating Digital Signature**

1) Generate hash code / hash value for sender to sign. for plain text M.

$m = H(M)$, $0 \leq m \leq q-1$.

2) Generate a random integer k such that $1 \leq k \leq q-1$ and $\gcd(k, q-1) = 1$.

3) Compute s_1 and s_2,

$$s_1 = \alpha^k \bmod q.$$

$$s_2 = k^{-1}(m - x_A s_1) \bmod (q-1)$$

Step 3: **Verification of Signature.**

1) Calculate v_1 and v_2 (at receiver's side),

$$v_1 = \alpha^m \bmod q$$

$$v_2 = (y_A)^{s_1} \cdot (s_1)^{s_2} \bmod q.$$

If $v_1 = v_2 \Rightarrow$ Signature valid

$v_1 \neq v_2 \Rightarrow$ Signature invalid.

Example :- $q = 19$, $\alpha = 10$

→ Private key $= x_A$ $\quad 1 < x_A < q-1$

let $x_A = 16$

→ $y_A = \alpha^{x_A} \bmod q = (10)^{16} \bmod 19$
$= 4.$

∴ Public key = $\{q, \alpha, Y_A\}$

$= \{19, 10, 4\}$.

→ Generating digital signature.

let $m = 14$, $0 \le m \le q-1$

let $k = 5$, $1 \le k \le q-1$ and $\gcd(k, q-1) = 1$

→ Computing S_1 and S_2,

→ $S_1 = \alpha^k \bmod q = (10)^5 \bmod 19$

$= 3$

→ $S_2 = k^{-1}(m - X_A S_1) \bmod (q-1)$

∴ $S_2 = (5)^{-1}(14 - (16)(3)) \bmod 18$

⇒ $(5)^{-1} \bmod 18$

let x be the inverse of 5.

$(5)^{-1} \bmod 18 = x$

∴ $18 \bmod 18 = 5x$

∴ $5x \bmod 18 = 1$

∴ $\boxed{x = 11}$ which is inverse of 5

∴ $S_2 = (11)(14 - 48) \bmod 18$

$= (-374) \bmod 18$

$= -14 \bmod 18$ (∵ we got neg again ∴ do mod.

$= 4$

→ Verification of signature,

1) $v_1 = \alpha^m \bmod q$

$= (10)^{14} \bmod 19$

$= 16$

and $v_2 = (Y_A)^{s_1} (s_1)^{s_2} \bmod q.$

$= (4)^3 (3)^4 \bmod 19$

$= (64)(81) \bmod 19$

$= 16$

$\therefore v_1 = v_2 \Rightarrow$ signature accepted.

* Digital Signature Standard :-

DSS or DSA

1) $q \rightarrow$ prime divisor

$p \rightarrow$ prime number such that $(p-1) \bmod q = 0.$

$g \rightarrow$ any integer $1 < g < p$ such that,

$g^q \bmod p = 1$ and $g = h^{\frac{(p-1)}{q}} \bmod p.$

2) Generating keys :-

Private key x → random integer such that $0 < x < q$.

public key y ⇒ $y = g^x \bmod p$.

→ Private key : $\{p, q, g, x\}$

→ Public key : $\{p, q, g, y\}$

3) Signature generation :-

→ Choose any random integer k such that $0 < k < q$.

→ $r = (g^k \bmod p) \bmod q$

→ $s = [k^{-1}(H(m) + x \cdot r)] \bmod q$.

→ Signature : $\{r, s\}$.

→ This signature bundle along with the plain text is passed to the receiver.

4). Verifying signature :-

$t = H(m)\, s^{-1} \bmod q.$

$u_1 = r\, s^{-1} \bmod q.$

$v = (g^{t} \cdot y^{u_1} \bmod p) \bmod q.$

if $v = r \Rightarrow$ accepted.

Example :- $H(m) = 3$ $\quad p = 7$ $\quad x = 5$

$h = 2$ $\quad q = 3$ $\quad k = 2$

$g = h^{\frac{(p-1)}{q}} \bmod p.$ $\quad | \quad 1 < g < p$, $g^{q} \bmod p = 1$

$= (2)^{6/3} \bmod 7$

$= 4 \bmod 7$

$\therefore \boxed{g = 4}$

→ Generating keys,

private key = $\{p, q, g, x\}$

public key = $\{p, q, g, y\}$

$$y = g^x \bmod p = (4)^5 \bmod 7$$

$$\therefore \boxed{y = 2}$$

→ Signature generation ;. $\{r, s\}$

$$r = (g^k \bmod p) \bmod q.$$

$$= ((4)^2 \bmod 7) \bmod 3$$

$$= 2 \bmod 3$$

$$\therefore \boxed{r = 2}$$

$$s = [k^{-1}(H(m) + X r)] \bmod q$$

$$= [(2)^{-1}(3 + (5)(2))] \bmod 3$$

$$= [2(13)] \bmod 3$$

$$= 26 \bmod 3.$$

$$= 2$$

$(2)^{-1} \bmod 3$

let x' be the inve. of 2.

$\therefore 2^{-1} \bmod 3 = x'$

$\therefore 1 \bmod 3 = 2x'$

$\therefore 2x' \bmod 3 = 1$

$\therefore \boxed{x' = 2}$

→ Verifying Signature,

$$t = H(m)\, s^{-1} \bmod q$$
$$= (3)(2)^{-1} \bmod 3$$
$$= (3 \cdot 2) \bmod 3$$
$$= 6 \bmod 3$$
$$\therefore \boxed{t = 0}$$

$2^{-1} \bmod 3$

$2x' \bmod 3 = 1$

$\boxed{x' = 2}$

$$y = g \cdot s^{-1} \bmod q$$
$$= 2\,(2)^{-1} \bmod 3$$
$$= 4 \bmod 3$$
$$\therefore \boxed{y = 1}$$

$$v = (g^t \cdot y^y \bmod p) \bmod q.$$
$$= [(4)^0 \cdot (2)^1 \bmod 7] \bmod 3$$
$$= [2 \bmod 7] \bmod 3$$
$$= 2 \bmod 3$$
$$\therefore \boxed{v = 2}$$

→ Here, $v = 2$ and $r = 2$

$\therefore v = r$ ⇒ Signature verified

* Linear Congruential :-

$$X_i = (a X_{i-1} + b) \bmod m$$

ex :- $a = 4$ $\quad b = 5$

$m = 17$ $\quad i = 1, 2, 3, \ldots$

$X_0 = 7$

Find bit sequence w.r.t. mod 2.

$\rightarrow X_1 = (a X_0 + b) \bmod m$

$= (4(7) + 5) \bmod 17$

$= 33 \bmod 17$

$= 16$

$\rightarrow X_2 = (a X_1 + b) \bmod m$

$= (4(16) + 5) \bmod 17$

$= 69 \bmod 17$

$= 1$

$\rightarrow X_3 = (a X_2 + b) \bmod m$

$= (4(1) + 5) \bmod 17$

$= 9 \bmod 17$

$= 9$

$\rightarrow X_4 = (a X_3 + b) \bmod m$

$= (4(9) + 5) \bmod 17$

$= 41 \bmod 17$

$= 7$

$\therefore$ Random Numbers : 7, 16, 1, 9, 7, ...

* Find bit sequence wrt. mod 2 for calculated random numbers.

$X_0 = 78 \mod 2 = 1$
$X_1 = 16 \mod 2 = 0$
$X_2 = 1 \mod 2 = 1$
$X_3 = 9 \mod 2 = 1$
$X_4 = 7 \mod 2 = 1$

* Quadratic Residue Generator :-

$$X_{i+1} \equiv X_i^2 \mod n$$

* Blum Blum Shub :-

$$X_i \equiv X_{i-1}^2 \mod n$$

→ large prime p and q.

$n = p * q.$

X_0 such that $gcd(x_0, n) = 1.$

→ Bit sequence :-

$$b_i \equiv x_i \mod 2.$$

Ex: $p = 11$

$q = 19$

$x_0 = 100$

→ $n = p \cdot q = 11 \times 19 = 209$.

→ $x_1 = x_0^2 \bmod n$

$= (100)^2 \bmod 209 = 177$.

→ $x_2 = x_1^2 \bmod n$

$= (177)^2 \bmod 209 = 188$

→ $x_3 = x_2^2 \bmod n$

$= (188)^2 \bmod 209 = 23$

→ $x_4 = x_3^2 \bmod n$

$= (23)^2 \bmod 209. = 111$

∴ Bit sequence,

$x_1 \bmod 2. = 177 \bmod 2 = 1$

$x_2 \bmod 2 = 188 \bmod 2 = 0$

$x_3 \bmod 2 = 23 \bmod 2 = 1$

$x_4 \bmod 2 = 111 \bmod 2 = 1$

∴ Bit sequence = 1011

- By Rushik Rathod.