UNIT-8

Number Theory:

The Euclidean Algorithm, modular arithmetic, Fermat's & Euler's theorems, the chinese remainder theorem, Discrete logarithms.

finite fields:

finite fields of the form GF(p), Finite fields of the form $GF(2^n)$.

Public key cryptography:

Principles, Public key cryptography algorithms: RSA algorithm, Diffie Hellman key exchange, Elliptic curve cryptography.

---

① The Euclidean Algorithm :-

The Euclidean algorithm is a way to find the greatest common divisor (GCD) of two positive integers. (i.e, two integers are "relatively prime" if and only if their only common positive integer factor is 1.) $\Rightarrow$ gcd(a,b) = 1.

Greatest common Divisor (GCD)

* The GCD of 'a' and 'b' is the largest integer that divides both a and b. such that their remainder is zero.

$\therefore$ GCD(0,0) = 0

* GCD(a,-b) = gcd(-a,b) = gcd(a,-b)

* GCD(a,b) = gcd(|a|, |b|).

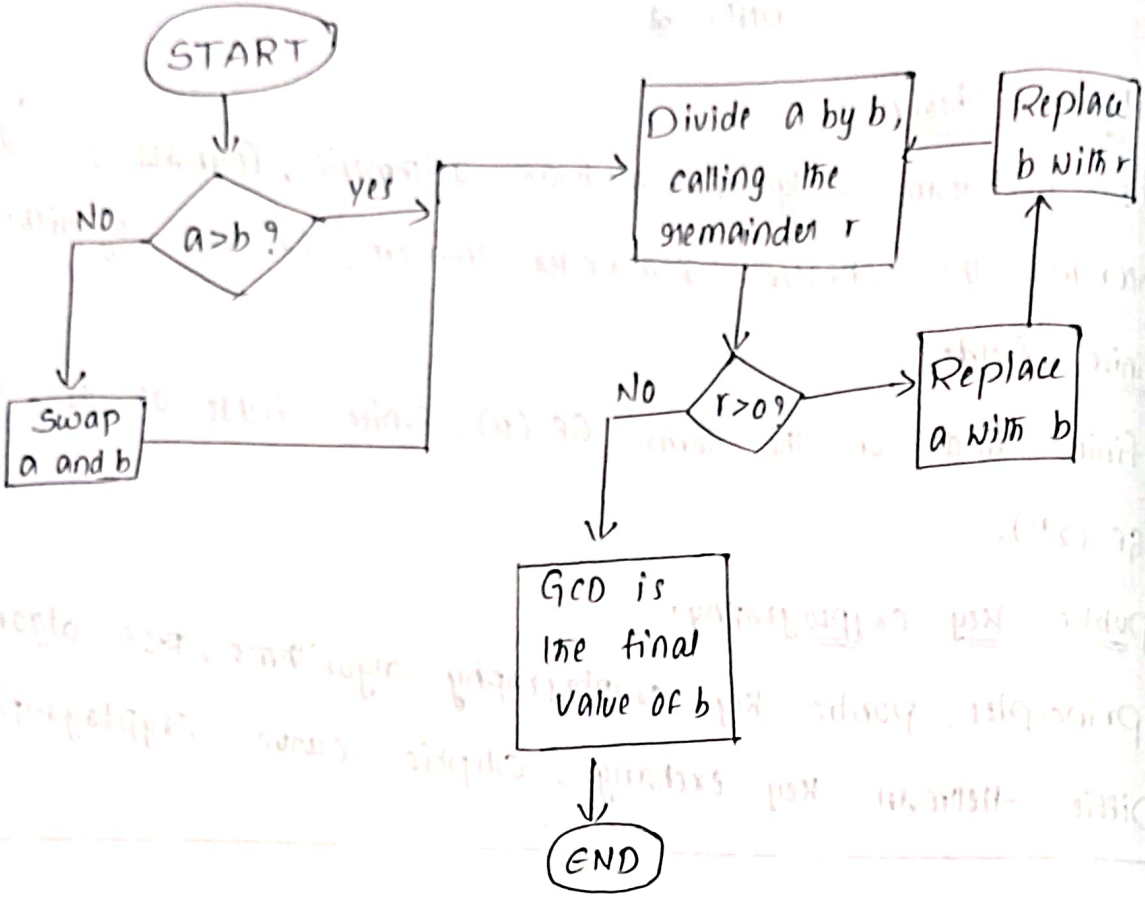


fig:- Euclidean Algorithm

Steps :-

(i) Let a, b be two numbers

(ii) a mod b = R (remainder)

(iii) Let a = b & b = R

(iv) Repeat steps (ii) & (iii) until a mod b is greater than 0.

(v) GCD = b

(vi) END

Example :- 300 and 42

↳ GCD (300, 42)

→ a = 300, b = 42

→ a mod b = R

300 mod 42 = 6

∴ R (remainder) = 6

→ a = b & b = R

∴ a = 42 & b = 6

→ a mod b = R

42 mod 6 = 0

If R = 0 (stop)

→ GCD = b

∴ GCD = 6

```
   7
42 | 300
     294
   ------
     6 (R)
     ↓
   remainder
```

```
   7
6 | 42
    42
   ----
    0 (R)
    ↓
  remainder
```

② Modular arithmetic :-

If 'a' is an integer & 'n' is a positive integer, then a mod n to the remainder when a is divided by n. The integer 'n' is called "modulus".

Eg :- 11 mod 7 = 4

$$7 \overline{)\,11\,(1} \quad 7 \quad \Rightarrow 4 \text{ remainder}$$

* Two integers 'a' and 'b' are said to be "congruent modulo n", if (a mod n) = (b mod n). This will be written as $a \equiv b \pmod n$.

($\equiv$: congruent (equal))

Eg :- $73 \equiv 4 \pmod{23}$ ↗ 73 is congruent to 4 (mod 23)

$$23 \overline{)\,73\,(3} \quad 69 \quad \Rightarrow 4$$

(or) $a \bmod n = b \bmod n$

$73 \bmod 23 = 4 \bmod 23$

Note :- $a \equiv 0 \pmod n$, then n / a. (n divides a)

Properties of congruences :-

(i) $a \equiv b \pmod n$ if $n / (a-b)$ (n divides (a-b))

(ii) $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

(iii) if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then, $a \equiv c \pmod n$.

Modular arithmetic operations :-

Modular arithmetic operations exhibits the following properties :-

1. $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
2. $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
3. $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Eg :- Let a = 11, b = 15, n = 8

$\therefore (a \times b) \bmod n = (11 \times 15) \bmod 8$
$= 165 \bmod 8 = 5$

$[(a \bmod n) \times (b \bmod n)] \bmod n =$
$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8$
$= (3 \times 7) \bmod 8 = 21 \bmod 8 = 5$
$\therefore 5 = 5$

4) if $x \equiv y \bmod n$, $a \equiv b \bmod n$ then,

$$\boxed{(x+a) \equiv (y+b) \bmod n}$$

Eg:- $17 \equiv 4 \bmod 13$, $42 \equiv 3 \bmod 13$

$\rightarrow (17+42) \equiv (4+3) \bmod 13$

$\rightarrow 59 \equiv 7 \bmod 13$ (True). ✓ (7 → remainder)

$$13 \overline{)\begin{array}{l} 59 \\ 52 \\ \hline 7 \end{array}}\ 4$$

5) if $x \equiv y \pmod n$ and $a \equiv b \bmod n$ then,

$$\boxed{(x-a) \equiv (y-b) \bmod n}$$

Eg:- $42 \equiv 3 \bmod 13$, $14 \equiv 1 \bmod 13$

$\rightarrow (42-14) \equiv (3-1) \bmod 13$

$\rightarrow 28 \equiv 2 \bmod 13$ (True) ✓ (2 → remainder)

$$13 \overline{)\begin{array}{l} 28 \\ 26 \\ \hline 2 \end{array}}\ 2$$

Set of residues (or) residue classes modulo n :-

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

Eg:- $Z_6 = \{0, 1, 2, 3, 4, 5\}$

each integer in Z_n represents a residue class.

③ Fermat's & Euler's Theorems :-

Fermat's theorem states the following : If 'p' is prime and 'a' is a positive integer not divisible by p, then

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$, where p = prime, a = positive integer

Eg:- $a = 3$, $p = 5$ - prime

$\rightarrow 3^{5-1} = 3^4 = 81$

$\therefore 81 \equiv 1 \bmod 5$

$$5 \overline{)\begin{array}{l} 81 \\ 80 \\ \hline 1 \rightarrow \text{remainder} \end{array}}\ 16$$

Note : remainder must be 1 in fermat's theorem when 'p' is prime

Another form of fermat's theorem :-

* 'p' is prime and 'a' is a positive integer then,

$$a^p \equiv a \pmod p$$

Eg :- $p = 5$ - prime, $a = 3$

$\rightarrow a^p = 3^5$

$= 243$

$\therefore$ $243 \equiv 3 \pmod 5$

$a^p \equiv a \pmod p$

$$5 \overline{)243} \quad 48$$
$$240$$
$$3$$

Eulers Totient function :-

* Denoted as $\phi(n)$.

* $\phi(n)$ = Number of positive integers less than 'n' that are relatively prime to n.

Eg :- $\phi(5)$

Here $n = 5$

Numbers less than 5 are 1, 2, 3 and 4.

$\therefore$ 1, 2, 3 and 4 are relatively prime to 5.

$\therefore$ GCD (1,5) = 1
GCD (2,5) = 1
GCD (3,5) = 1
GCD (4,5) = 1

If GCD (a,b) = 1; then they are relatively prime

$\therefore \phi(5) = 4$ - Total 4 numbers (1,2,3,4) are relatively prime to 5.

2) $\phi(6)$

GCD (1,6) = 1 $\rightarrow$ $1 \Rightarrow (1)$, $6 \Rightarrow (1)$, 2, 3, 6 } = 1.
GCD (5,6) = 1

$\phi(6) = \{1, 2, 3, 4, 5\}$

$\phi(6) = \{1, 5\}$

$\therefore \phi(6) = 2$

Suppose, we have two integers,

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

Eg:- $\phi(21)$

$$\phi(21) = \phi(\overset{p}{3}) \times \phi(\overset{q}{7})$$
$$= (\overset{p-1}{3-1}) \times (\overset{q-1}{7-1})$$
$$= 2 \times 6$$
$$= 12$$

$\therefore \phi(21) = 12$

Euler's Theorem :-

-Euler's theorem states that if 'a' and 'n' are relatively prime, then

$a^{\phi(n)} \equiv 1 \bmod n$, where $\phi(n) \rightarrow$ euler's toitient function

* It is the generalized version of fermat's theorem.

Eg:- Let $a = 11$, $n = 10$; both are relatively prime

$\therefore$ We can represent them as

$$11^{\phi(10)} \equiv 1 \bmod 10$$

$$11^{4} \equiv 1 \bmod 10$$

$\therefore 14641 \equiv 1 \bmod 10$; which is true.

```
    406
10 | 14641
     140
     ----
      641
      600
      ---
        1
```

Where,

$$\phi(10) = \phi(2) * \phi(5)$$
$$= 1 * 4$$
$$= 4$$

$\phi(2)$

$= \phi(2) = (1,2)$

GCD $(1,2) = 1$ ✓

GCD $(2,2) = 2$; not relatively prime

$\therefore \phi(2) = 1$

$\phi(5)$

$\Rightarrow \phi(5) = \{1,2,3,4\}$

$\phi(5) = 4$

(ii) The chinese remainder Theorem :-

chinese remainder theorem states that there always exists an "x" that satisfies the given congruences.

$$x \equiv rem[0] \pmod{num[0]}$$
$$x \equiv rem[1] \pmod{num[1]}$$
$$\text{------}$$

and (num[0], num[1] ... num[n-1]) ; are co-primes (or) relatively prime to one another.

Eg :- $x \equiv 1 \pmod 5$, $x \equiv 3 \pmod 7$ } 5 & 7 are relatively prime.

We have to find the value of 'x' = ? (That's y chinese remainder theorem can be used).

Steps :-

i) if $x \equiv a_i \pmod{m_i}$

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

(ii) $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$ (i.e, all are co-prim (or) relatively prime)

(iii) $x = (H_1 x_1 a_1 + H_2 x_2 a_2 + H_3 x_3 a_3 \text{ ------} + H_n x_n a_n) \bmod H$

$H = m_1 * m_2 + m_3 \text{ ----} m_n$

$H_i = \frac{H}{m_i} \Rightarrow$ eg :- $H_1 = \frac{H}{m_1} = \frac{m_1 m_2 m_3}{m_1} = m_2 m_3$

$\therefore H_1 = m_2 m_3$

Similarly, $H_2 = m_1 m_3$

$H_3 = m_1 m_2$

To calculate x_i :-(i.e, $x_1, x_2, x_3 \ldots$)

$H_i x_i \equiv 1 \pmod{m_i} \Rightarrow$ eg :- $H_1 x_1 \equiv 1 \pmod{m_1}$

Eg :- $x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$
$x \equiv 3 \pmod{11}$

$\longrightarrow$ $x \equiv a_i \bmod (m_i)$

So, $a_1 = 1$, $a_2 = 1$, $a_3 = 3$

$m_1 = 5$, $m_2 = 7$, $m_3 = 11$

Since 5, 7 and 11 are relatively prime to one another.

So, we can find 'x'.

i.e, $\gcd(5,7) = \gcd(7,11) = \gcd(11,5) = 1$.

$M = m_1 * m_2 * m_3 = 5 * 7 * 11 = 385$

$\therefore M = 385$

$M_1 = \frac{M}{m_1} = m_2 \cdot m_3 = 7 * 11$

$M_1 = 77$

; $M_2 = m_1 m_3 = 5 * 11$

$M_2 = 55$

; $M_3 = m_1 m_2 = 5 * 7$

$M_3 = 35$

Now we will calculate x_i value :-

$M_1 x_1 \equiv 1 \pmod{m_1}$ -> i.e, ~~$M_1 x_1 \equiv 1 \bmod m_1$~~ $M_1 x_1 \pmod{m_1} = 1$

$77 \cdot x_1 \pmod 5 = 1$

$2 \cdot x_1 \pmod 5 = 1$

$\therefore x_1 = 3$ -> if $2 \times 3 \bmod 5 = 1$ (x_1)
$6 \bmod 5 = 1$
then $x_1 = 3$

$5 \overline{)77}\ 65\ \overline{12}\ 10\ \overline{2}$ ✓ (132)

Similarly,

$M_2 x_2 \equiv 1 \pmod{m_2}$

$55 \cdot x_2 \bmod 7 = 1$

$6 \cdot x_2 \pmod 7 = 1$

$x_2 = 6$ -> 6×6 (x_2) $\bmod 7 = 1$
$36 \bmod 7 = 1$
$\therefore x_2 = 6$

; $M_3 x_3 = 1 \pmod{m_3}$

$35 \cdot x_3 = 1 \bmod 11$

$35 \cdot x_3 \bmod 11 = 1$

$2 \cdot x_3 \bmod 11 = 1$

$\therefore x_3 = 6$

$11 \overline{)35}\ 33\ \overline{2}$ ✓ (3)

2×6 (x_3) $\bmod 11 = 1$
$12 \bmod 11 = 1$ ✓

NOW, $a_1 = 1$, $a_2 = 1$, $a_3 = 3$

$m_1 = 5$, $m_2 = 7$, $m_3 = 11$

$M_1 = 77$, $M_2 = 55$, $M_3 = 35$; $x_1 = 3$; $x_2 = 6$; $x_3 = 6$; $M = 385$

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \text{ Mod } M$

$x = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3) \text{ Mod } 385$

$= (231 + 330 + 630) \text{ mod } 385$

$= 1191 \text{ mod } 385$

$\therefore x = 36$

$\therefore$ verify, $36 \text{ mod } 5 = 1$ ✓

$36 \text{ mod } 7 = 1$ ✓

$36 \text{ mod } 11 = 3$ ✓

⑤ Discrete logarithms :-

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the DSA.

we make use of "primitive root".

A primitive root of prime number n is one whose power modulo generate all the integers from 1 to n-1.

Eg :-

$\alpha = 3, q = 7 = (1,2,3,4,5,6)$ upto 6. because $q-1$, $7-1=6$.

$\alpha^1 \text{ mod } q$

$\alpha^2 \text{ mod } q$

$\alpha^3 \text{ mod } q$

⋮

$\alpha^{q-1} \text{ mod } q$ should have values $\{1, 2 \cdots q-1\}$.

$\Rightarrow$ $3^1 \text{ mod } 7 = 3$

$3^2 \text{ mod } 7 = 2$

$3^3 \text{ mod } 7 = 6$

$3^4 \text{ mod } 7 = 4$

$3^5 \text{ mod } 7 = 5$

$3^6 \text{ mod } 7 = 1$

$(1,2,3,4,5,6)$

$\Rightarrow$ So, 3 is primitive root of 7.

All numbers should exist from 1 to 6.

Discrete logarithm problem :-

Eg :- solve $\log_2 9 \bmod 11$

Sol :- Here p (prime) $= 11$, g (base) $= 2$, $x = 9$

Equation = $\log_g x = n \pmod p$

$$\log_g x \equiv n \pmod p$$

$$x \equiv g^n \pmod p$$

$$9 \equiv 2^n \pmod{11}$$

Try $'n' = 1, 2, 3 \text{----}$

If we take '6' then it is congruent to '9'.

$$9 \equiv 2^6 \pmod{11} \checkmark$$

$\therefore n = 6$

part-B

① Finite fields of the form GF (p) :-

For a given prime p, we define the finite field of order p, GF (p) as the set Z_p of integers $\{0, 1 \text{----} p-1\}$ together with the arithmetic operations modulo p.

Where,

$Z_p = \{0, 1, \text{----} p-1\}$

GF (p)

↳ Galois field

p = prime

if $n = 1$, then the finite field is GF (p).

finite fields of order p :-

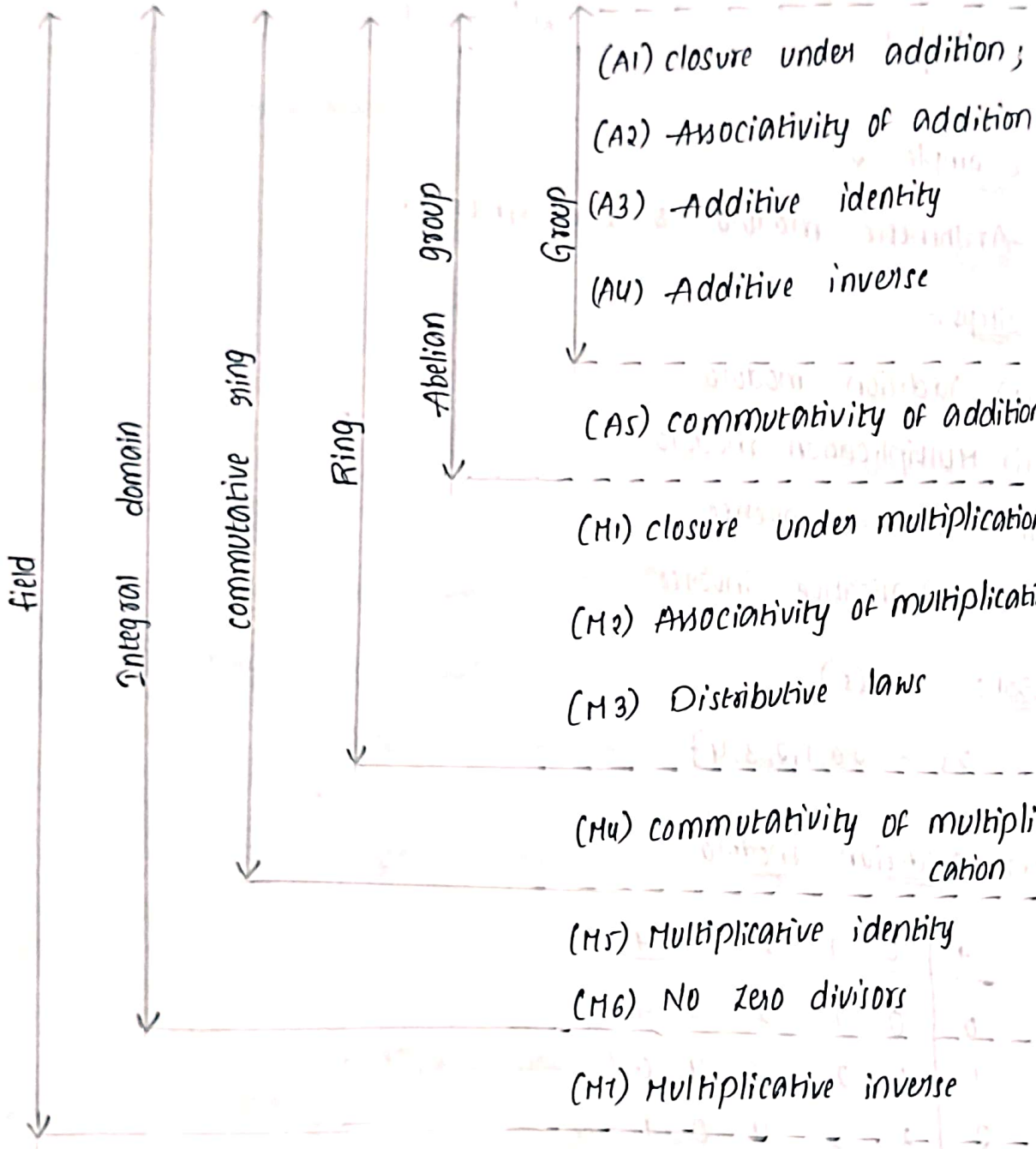


fig:- properties of groups, rings & fields

Example :-

The simplest finite field is GF(2).

Arithmetic operation {+, *}
↳ because the field contains +, *

GF(2) = {0,1} because {0,1 ---- p-1}
↳ elements {0,1 ---- 2-1} = {0,1}

a)

+	0	1
0	0	1
1	1	0 (1+1=2 ; if it equal to 2, keep '0')

b)

*	0	1
0	0	0
1	0	1

c) Additive inverse

N	0	1
-N	1	0

(elements)

d) Multiplicative inverse

N	0	1
N^{-1}	-	1

Example 2 :-

Arithmetic modulo 5. (i.e, GF(5)).

Steps :-

(i) Addition modulo

(ii) Multiplication modulo

(iii) Aditive inverse

(iv) Multiplicative inverse

Sol :- $GF(5)^P$

$Z_5 = \{0,1,2,3,4\}$ ($Z = \{0,1 \ldots p-1\}$)

$= \{0,1,2,3,4,5-1\}$

$= \{0,1,2,3,4\}$

(elements)

(i) Addition modulo :-

+	0	1	2	3	4
→ 0	0	1	2	3	4
1	1	2	3	4	0 (because it equal to 5, so keep '0')
2	2	3	4	0	1 (2+4=6 → 6 mod 5 = 1)
3	3	4	0	1	2 (3+4=7 → 7 mod 5 = 2)
→ 4	4	0	1	2	3 → 8 mod 5 = 3

$5 \overline{)6}$ (1, remainder 1)

(ii) Multiplication modulo :-

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$5 \overline{)6}$ (1, remainder 1)

6 mod 5 = 1

(iii) Additive inverse

→ In A.2, consider addition modulo table i.e, remainder = 0.

W	0	1	2	3	4 } elements
-W	0	4	3	2	1

→ consider remainder = 1 in mul table.

(iv) Multiplicative inverse

W	0	1	2	3	4 } elements
W^{-1}	-	1	3	2	4

↳ we get remainder 1 in 1 value in mul table

② Finite fields of the form $GF(2^n)$:-

→ A Galois field is introduced by - Galois.

→ In Galois field,

No. of elements in the field = [prime number] positive integer

→ Example :- $GF(2^3)$

$GF(2^n) = GF(p^n)$

$GF(2^3) = 8, (0, 1, 2, 3, 4, 5, 6, 7) \rightarrow Z = \{0, 1, \ldots p-1\}$, $8-1=7$

$= \{000, 001, 010, 011, 100, 101, 110, 111\}$

(a)

+	0	1	2	3	4	5	6	7 (x^2+x+1)
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

$6 \Rightarrow x^2+x+1+1$
$\Rightarrow x^2+x = 6$

$5 \Rightarrow x^2+x+1+x$
$\Rightarrow x^2+1 = 5$

$4 \Rightarrow x^2+x+1+x+1$
$\Rightarrow x^2 = 4$

See table $GF(2^3)$ in next page and then substitute these values

(a) Addition

(b)

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	[1]	2	3	4	5	6	7
2	0	2	4	6	3	[1]	7	5
3	0	3	6	5	7	4	[1]	2
4	0	4	3	7	6	2	5	[1]
5	0	5	[1]	4	2	7	3	6
6	0	6	7	[1]	5	3	2	4
7	0	7	5	2	[1]	6	4	3

(b) Multiplication

(c) Additive and multiplicative inverse

w	-w	w^{-1}
0	0	-
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

↳ consider '1' in multiplication table
↳ consider '0' in addition table

Modular Polynomial arithmetic :-

eg:- consider 8-bit binary stream

1	0	0	1	0	1	0	1
x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0

$\Rightarrow x^0 + x^2 + x^4 + x^7$; $x^1 + x^3 + x^5 + x^6$

$\rightarrow \boxed{x^7 + x^4 + x^2 + 1}$ $(x^0 = 1)$ $\Rightarrow \boxed{x^6 + x^5 + x^3 + x}$ $(x^1 = x)$

Example of GF (2^3) :- (0, 1, 2, 3, 4, 5, 6, 7)

u 2 1	
000	0
001	1
010 ($x^2\ x^1\ x^0$)	x
011	x+1
100	x^2
101	x^2+1
110	x^2+x
111	x^2+x+1

$\Rightarrow$ 0 0 1 ($x^0 = 1$)

$\Rightarrow$ 0 1 0 ($x^1 = x$)

$\Rightarrow$ 0 1 1 ($x+1$)

$\Rightarrow$ 1 0 0 (x^2)

$\Rightarrow$ 1 0 1 ($x^2 + x^0 = 1$)

$\Rightarrow$ 1 1 0 ($x^2\ x^1$)

$\Rightarrow$ 1 1 1 ($x^2\ x^1\ x^0$, $x^0 \downarrow 1$)

Addition

Part-C

① Principles of public key cryptography :-

⇒ public key cryptography is also called as "Asymmetric key cryptography".

⇒ It uses two different keys for encryption & decryption.

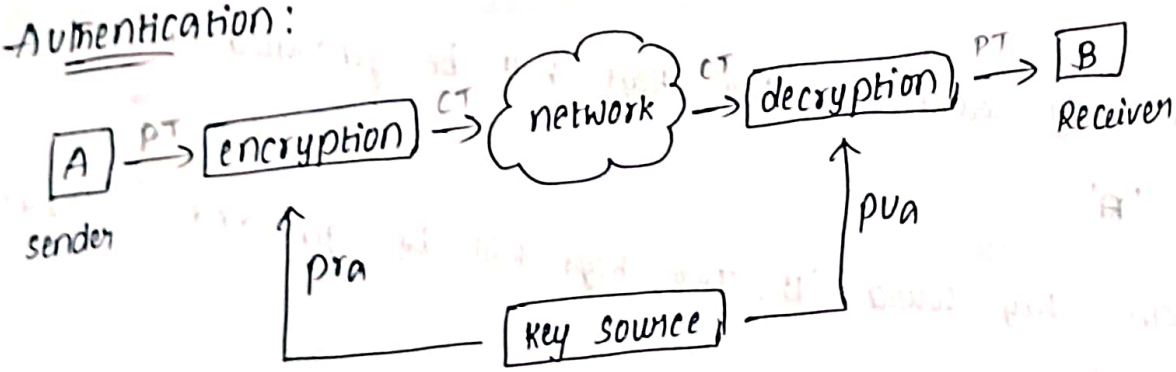
public key → known to everyone

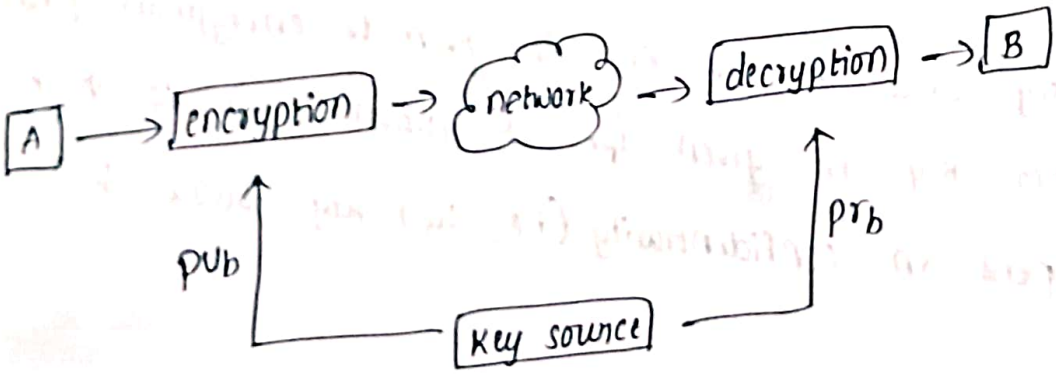
private key → known to only particular person

⇒ There are two principles :

1. Authentication
2. confidentiality

Authentication :





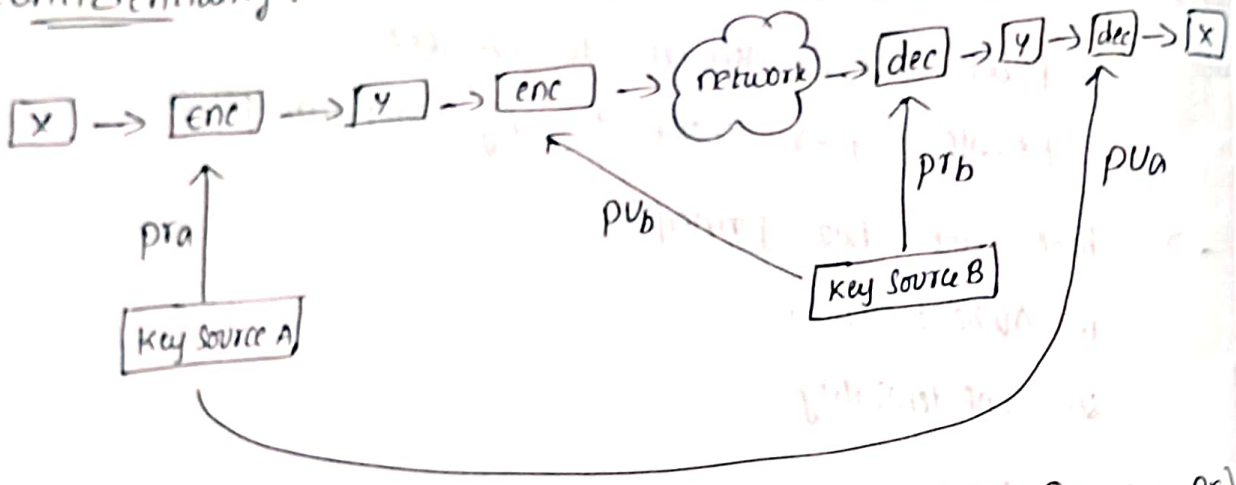
Where, pr - private key
pu - public key

⇒ A (sender) will encrypt the message and carried through network then ciphu-text (CT) will decrypt to plain text (PT) and message passes to receiver. for both encryption & decryption key will be needed. The key is generated by

Key source. Here both of the keys (pra, pua) are from same source 'a'.

→ from fig (ii) also both of the keys (prb, pub) are from same source 'b'.

Confidentiality :-



* from key source 'A', two keys will be generated (i.e, pua, pra) say 'A'.

* from key source 'B', two keys will be generated (i.e, pub, prb) say 'B'.

* from key source 'A', one key is given to encryption (pra) and another key is given for decryption (pua). so these will happens in confidentiality (i.e, two key sources will be used).

Advantages :-

* separate key is used for encryption & decryption, even if encrypted msg is stolen by attacker cannot decrypt the msg.
* Easy to use for user

Disadvantage :-

* It uses more resource compare to symmetric key cryptography

Application of Public key cryptography:-

It can be classified into three categories:

1. Encryption / Decryption: During this process the sender encrypts the msg with the receiver's public key.

2. Digital signature: During this process the sender "signs" a msg with his/her private key.

3. key exchange: Both sender & receiver cooperate to exchange a session key, typically for conventional encryption.

② RSA algorithm :-

→ RSA stands for "Rivest - Shamir - Adleman".

→ It is a "Asymmetric key" algorithm and "Block cipher" algorithm.

→ It has 3 steps :

1. key generation
2. Encryption
3. Decryption

key generation :-

1. Select two large numbers p and q.
   (↳ for more security)

   Eg:- $p = 3$, $q = 11$

2. calculate $n = p * q \Rightarrow n = 3 \times 11 = 33$

   $\therefore n = 33$

3. calculate $\phi(n) = (p-1)(q-1)$

   $\phi(n) = (3-1)(11-1)$

   $= 2 \times 10 = 20$

   $\therefore \phi(n) = 20$

4. choose the value of 'e' (encryption) such that,

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$.

Let,

consider $e = 7 \Rightarrow 1 < 7 < 20$ and $\gcd(20, 7) = 1$

$\therefore e = 7$

5. calculate $d = e^{-1} \bmod \phi(n)$

$ed = \bmod \phi(n)$

$ed \bmod \phi(n) = 1 \Rightarrow ed \bmod \phi(n) = 1$

$7 \times d \bmod 20 = 1$

$7 \times 3 \bmod 20 = 1$

$21 \bmod 20 = 1$

$\therefore d = 3$

6. public key = $\{e, n\} \Rightarrow \{7, 33\}$

7. private key = $\{d, n\} \Rightarrow \{3, 33\}$

2) Encryption :-

formula for encryption, $C = M^e \bmod n$

M = no. of digits in plain text

C = cipher text

Again, assume the value of 'M' i.e, $M < n$ (M should be less than n. Here $n = 33$, so take $M = 31$).

Let $M = 31$

$C = (31)^7 \bmod 33$

$= 4$ $\therefore C = 4$

3) Decryption :-

$M = C^d \bmod n$

$= (4)^3 \bmod 33 = 64 \bmod 33 = 31$ so $M = 31$ is true.

$\therefore M = 31$

③ Diffie Hellman Key exchange :-

→ It is not an encryption / decryption algorithm.

→ used to exchange keys between sender and receiver.

→ It follows "Asymmetric key cryptography".

Procedure :

1. consider a prime number 'q'.

   Let $q = 7$

2. select 'α' such that $\boxed{\alpha < q}$ and 'α' is primitive root of q.

   Primitive root - ?

   $\alpha^1 \bmod q$

   $\alpha^2 \bmod q$

   $\alpha^3 \bmod q$

   ⋮

   $\alpha^{q-1} \bmod q$ should have values $\{1, 2, 3, \ldots, q-1\}$

   ⇒ Ex: $\alpha = 3$ and $q = 7$ $(1, 2, 3, 4, 5, 6)$

   $3^1 \bmod 7 = 3$

   $3^2 \bmod 7 = 2$

   $3^3 \bmod 7 = 6$

   $3^4 \bmod 7 = 4$

   $3^5 \bmod 7 = 5$

   $3^6 \bmod 7 = 1$

   ↳ upto '6' because $q-1$, $7-1=6$

   All numbers exists from 1 to 6. so 3 is primitive root of 7.

3. Assume X_A (private key of A) and $\boxed{X_A < q}$

   calculate $Y_A = \alpha^{X_A} \bmod q$.

Ex: $q = 7$ and $\alpha = 5$ - check with '5' also (or) '3'

assume, $X_A = 3$

$Y_A = (5)^3 \bmod 7$

$= 125 \bmod 7 = 6$

$\boxed{\therefore Y_A = 6}$

4. Assume x_B and $x_B < q$; x_B - private key of B.

calculate $y_B = \alpha^{x_B} \bmod q$

Let, $x_B = 4$

$y_B = (5)^4 \bmod 7$

$= 625 \bmod 7 = 2$

$\therefore y_B = 2$

$x_A, x_B = (3,4)$

$y_A, y_B = (6,2)$

5. calculate secret keys K_1 and K_2

$K_1 \Rightarrow$ person A $\quad K_2 \Rightarrow$ person B

$K_1 = (y_B)^{x_A} \bmod q$

$K_1 = (2)^3 \bmod 7$

$\Rightarrow 8 \bmod 7 = 1$

$\therefore K_1 = 1$

$K_2 = (y_A)^{x_B} \bmod q$

$K_2 = (6)^4 \bmod 7$

$\Rightarrow 1296 \bmod 7 = 1$

$\therefore K_2 = 1$

If both $K_1 = K_2$ then key is exchanging between persons are successfully done.

$\therefore$ key exchanged successfully.

So, the purpose of these algorithm is to exchange the keys between sender & receiver successfully.

④ Elliptic curve cryptography :- (ECC)

→ It follows "Asymetric key" cryptography.

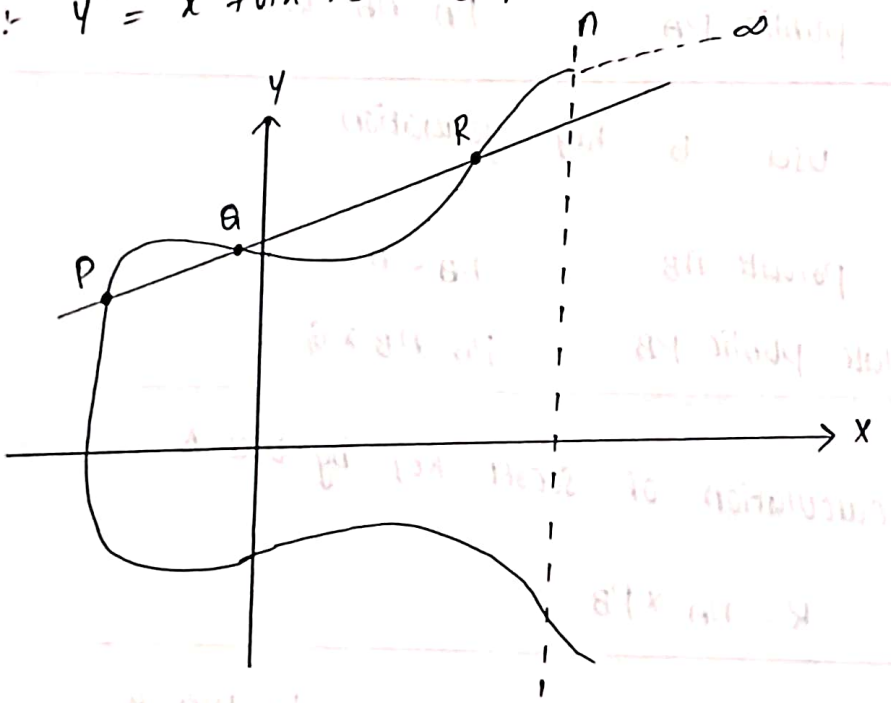
→ It provides equal security with smaller key size as compared to non ECC algorithms.

i.e, small key size and high security

→ It makes use of Elliptic curves.

→ Elliptic curves are defined by some mathematical functions - cubic functions.

Eg :- $y^2 = x^3 + ax + b$ (equation for degree 3).



→ symmetric to x-axis.

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

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

consider the equation $\boxed{Q = kP}$

Where Q, P → point on curve and $k < n$.

	Global public element
$E_q(a,b)$	elliptic curve with parameters a, b and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n.
	user A key Generation
Select private n_A	$n_A < n$
calculate public P_A	$P_A = n_A \times G$
	user B key generation
Select private n_B	$n_B < n$
calculate public P_B	$P_B = n_B \times G$
	calculation of secret key by user A
	$K = n_A \times P_B$
	calculation of secret key by user B
	$K = n_B \times P_A$

fig:- ECC key exchange

×