Page No.
Date

Mod 5

5.1 Prime number generation
Random number generation
Congruences
Solving linear congruences $ax + by = d$.

5.2 Chinese remainder theorem
Fermat's little theorem
Euler's Theorem
Quadratic residue
Legendre & Jacobi symbols.

5.3 Shannon's charc. of good cipher
confusion & diffussion
concepts of encryption & decryption

5.4 Historical background
Transposition : row key & column key
Substitution : Ceaser cipher (additive)
: Affine cipher (additive & multiplicative)
Polyalphabetic & monoalphabetic ciphers : Vignere cipher

Prime number Generation

⇒ Many algorithms use prime no. for encryption
⇒ factoring large prime no. is very hard
⇒ Fast to multiply two prime no.

* In cryptography we have two methods of encryption;
Symmetric where we all share the same key to encrypt & decrypt the msg.
Asymmetric where we have two different keys for encryption & decryption.
  - One key is for writer/sender & one for receiver.
  - sender can encrypt msg with public key from receiver.
  - now receiver uses the private key he has to decrypt the msg.

* now we know, we need to convert our text to numbers
* then a) chose 2 independent prime no. p & q.
  b) $N = p \times q$
  c) $\phi(N) = (p-1) \cdot (q-1)$ // because they are prime.
  d) chose a natural no. e, that is coprime & smaller than $\phi(N)$
  e) calculate multiplicative inverse(k) of
  $e \bmod \phi(N) = k \cdot e \rightarrow d \cdot \phi(N) = 1$

here N & e build our public keys.
k makes our private key.

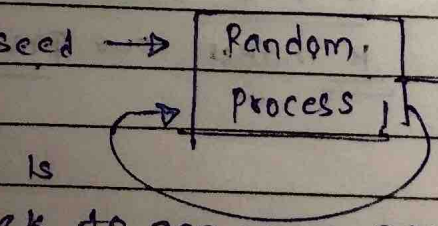
Random no. generators

⇒ Physical device that generates a sequence of random numbers which has no fixed patterns.

⇒ used where we need unpredictable data.

* True Random no. generator:
  - based on observation of random physical process
  - measures some physical phenomenon that is supposed to be random.
  - on that basis the value is generated.
  - they use non-determineable source to generate no.
  - random source called entropy.
  - eg: of, entropy
    a) fan noise
    b) radio active decay.
    c) key board stroke timing
  - entropy source is based on physical phenomenon, thus to be measured.
  - on this basis there is no gurantte the no. will repeat.

* Pseudo Random no generator:
  - here we use short ~~term~~ initial input → key / seed
  - we use computer algo it is not related to any other source
  - just produces long no. of random value using some calc.



- value generated is used as feed back to generate new value.

* most popular algo is congruential generator.

$$x_{n+1} = (a x_n + b) \bmod m.$$

congruences :

* $a \pmod n \equiv 16 \pmod{10} \equiv 6$

(a divided by n)

* a is congruent to b mod n.

$a \equiv b \pmod n$

* it is said that a is congruent to be if (a-b) is multiple of n (- or +ve).

eg: $42 \equiv 7 \pmod 5$

$a \equiv b \pmod n$,

$a = 42$, $b = 7$, $n = 5$

$a - b = 35$ is a multiple of $n = 5$.

42 is congruent to 7 % 5

* $a \equiv b \pmod n \Rightarrow a = b + nk$, k = integer.

eg: $-19 \equiv 37 \pmod 7$

$a = -19$, $b = 37$, $n = 7$

$-19 = 37 + 7(k)$

$k = -8$, thus k = integer. -19 & 37 are congruent

Page No.
Date

* **Properties:**

consider a, b, c, n & $n \neq 0$!

a) $a \equiv 0 \pmod{(n)}$

if and only if $a = a-0$ is a multiple of n.

$(a-b = \text{multiple of } n)$,

b) $a \equiv a \pmod{n}$

$a - a = 0$, $\therefore n = 0$

c) $a \equiv b \pmod{n}$ if & only if

$b \equiv a \pmod{n}$

$a \equiv b \bmod{(n)}$

$a - b = nk$

$b - a = (-k)n$

$b = a \pmod{n}$

d) $a \equiv b$ & $b \equiv c \pmod{n}$

then $a \equiv c \pmod{n}$

* suppose we have 2 no & we want to do add^n.

a) $(a+b) \bmod n = n$, then answer is zero.

or $(a+b) > n-1$ then answer is $n-1$

linear congruence :

linear congruence of $ax \equiv b \pmod{n}$ has

a solution where $= \dfrac{d}{b}$

$d = \gcd(a, n)$, thus it has 'd' mutually incongruent solutions.

∴ linear eqn. $ax + by = c$,
this has a solution if & only if.
$(d|c)$ & $gcd(a,c) = d$

⇒ $ax \equiv b \pmod n$

$ax - b = ny$

$ax - ny = b$ ← this has a soln if & only if $d|b$, $d = GCD(a,n)$

Chinese Remainder Theorem:

⇒ CRT is used to solve different congruent equations with one variable but different moduli which are prime.

⇒
$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_n \pmod{m_n}$$

} set of equations, with one variable and different modulus val.

⇒ CRT states that above equation have a unique solution of the moduli are relatively prime.

meaning

⇒ when $m_1, m_2, \cdots, m_n$ are relatively prime, then there exists a unique solution $= x$.

m_1, m_2 & m_3 should be prime

⇒ $$X = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}] \pmod M$$

$M = m_1 \times m_2 \times m_3$ $\quad M_1 = \frac{M}{m_1}$ $\quad m \neq M$ $\quad M_2 = \frac{M}{m_2}$ $\quad M_3 = \frac{M}{m_3}$

m_1, m_2, m_3 needs to be prime

Chinese R.T

$\Rightarrow x = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}] \bmod M$

($M \neq$ quests m) | $M = m_1 \times m_2 \times m_3$

Page No.
Date

$x = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}] \bmod M$

$M = m_1 \times m_2 \times m_3$ | $M_1 \times M_1^{-1} = 1 \pmod{m_1}$

$X = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}] \bmod M$

Q) $x \equiv 2 \bmod 3$ $\quad x = a_1 \bmod m_1$ $\quad a_1 = 2, a_2 = 3, a_3 = 2$

$x \equiv 3 \bmod 5$ $\quad x = a_2 \bmod m_2$ $\quad m_1 = 3, m_2 = 5, m_3 = 7$

$x \equiv 2 \bmod 7$ $\quad x = a_3 \bmod m_3$

$x = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}] \bmod M$

→ $\because m_1, m_2$ & m_3 should be prime, they are

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105 = M$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

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

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

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$M_1 \times M_1^{-1} = 1 \bmod m_1$ | $M_2 \times M_2^{-1} = 1 \bmod m_2$ | $M_3 \times M_3^{-1} = 1 \bmod m_3$

$35 \times M_1^{-1} = 1 \bmod 3$ | $= 21 \times M_2^{-1} = 1 \bmod 5$ | $15 \times M_3^{-1} = 1 \bmod 7$

$\frac{35}{3} \times M_1^{-1} = 1$ | $= \frac{21 \times M_2^{-1}}{5} = 1$ | $\frac{15 \times M_3^{-1}}{7} = 1$

$\frac{35 \times 2}{3} = 1$ | $M_2^{-1} = 1$ | $M_3^{-1} = 1$

$M_1^{-1} = 2$

Page No.
Date

* $X = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}] \bmod M$

* $M = m_1 \times m_2 \times m_3$

* $M_1 = \frac{M}{m_1}$ $M_2 = \frac{M}{m_2}$ $M_3 = \frac{M}{m_3}$

* $M_1 \times M_1^{-1} = 1 \bmod m_1$; $M_2 \times M_2^{-1} = 1 \bmod m_2$; $M_3 \times M_3^{-1} = 1 \bmod m_3$

$\Rightarrow [2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$\Rightarrow 233 \bmod 105$

$= \underline{\underline{23}}$.

Q2) $4X = 5 \bmod 9$ using CRT.
$2X = 6 \bmod 20$

$X = a_1 \bmod m_1$

$X = a_2 \bmod m_2$

$4X = 5 \pmod 9$.

multiply 4^{-1} on both sides

$X = 4^{-1} \times 5 \pmod 9$

proper $X = 4^{-1} \pmod 9 \times 5 \pmod 9$

$X = 7 \times 5 \pmod 9$

$X = 35 \pmod 9$

$35/9 \Rightarrow$ rem $= 8$.

$X = 8 \pmod 9$

$M_1^{-1} \times M_1 = 1 \bmod m_1$

$\frac{20}{180} \times M_1^{-1} = 1$ $M_1^{-1} = 5$

$= \frac{20 \times M_1^{-1}}{9} = 1$ $\frac{m_1}{}$

$2X = 6 \pmod{20}$

$2X = 2 \times 3 \pmod{20}$

$X = \underline{\underline{3 \bmod 20}}$

$a_1 = 8$ $m_1 = 9$

$a_2 = 3$ $m_2 = 20$

$M = m_1 \times m_2 = 9 \times 20 = 180 = M$

$M_1 = \frac{M}{m_1} = \frac{180}{9} = 20$

$M_2 = \frac{M}{m_2} = \frac{180}{20} = 9$

$M_2^{-1} \times M_2 = 1 \bmod m_2$

$\frac{9 \times M_2^{-1}}{20} = 1$ $M_2^{-1} = 9$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$$
$$= (80 \times 20 \times 5 + 3 \times 9 \times 9) \bmod 180$$
$$= (800 + 243) \bmod 180$$
$$= 1043 \bmod 180 = 143$$

Fermat's little theorem:

If 'p' is a prime no and 'a' is positive integer not divisible by p. then,

(*) $$a^{p-1} \equiv 1 \pmod p$$

a) check if a is divisible by p, it should not be
b) p is prime number.

eg: for a=2 4 p=5 check fermats theorem.

$$\Rightarrow a^{p-1} \equiv 1 \pmod p$$

a) is p prime - true
b) is a not divisible by p = true.

$$2^{5-1} \equiv 1 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$
$$16 = 1 \bmod 5$$
$$16/5 = 1 \quad \text{true.}$$

Fermats ⇒ $a^{p-1} \equiv 1 \bmod p$ | a shld not be divisible by p | p = prime no.

Eulers ⇒ $a^{\phi(n)} \equiv 1 \bmod n$

Page No. Date

b) for $a = 11$ & $p = 13$

a) p is prime b) a is not divisible by p.

$\therefore a^{p-1} \equiv 1 \pmod p$

$11^{13-1} \equiv 1 \pmod{13}$

$11^{12} \equiv 1 \pmod{13}$

$-2^{12} \equiv 1 \bmod 13$

$-2^4 \cdot 2^3 \equiv 1 \bmod 13$

$3^3 \equiv 1 \bmod 13$

$27 \equiv 1 \bmod 13$

$27/13 = 1$ true

c) does not hold for $p = 6$, because, p is not prime.

Eulers Theorem:

For every positive integer 'a' & 'n', which are relatively prime, then

$$a^{\phi(n)} \equiv 1 \pmod n$$

∴ For $\phi(n)$ we have euler totient theorem = ϕ function $\phi(n)$

⇒ $\phi(n)$ = no. of positive integers that are less than n. that are relatively prime to n.

eg: find $\phi(5)$, $n = 5$ here.

∴ no. of numbers that are less than n & coprime.

no. less than $n = 5$ ⇒ 1, 2, 3, 4.

∴ no. which are relatively prime to n ⇒ 1, 2, 3, 4 (4 nos)

↳ GCD = 1

∴ $\phi(5) = 4$

* $\phi(n)$ → all no. less than n, which are relatively prime to n, count

+ If n is prime, $\phi(n) = (n-1)$

* $n = a \times b$ composite $= \phi(n) = n \times \left(\frac{P_1-1}{P_1}\right)\left(\frac{P_2-1}{P_2}\right)\cdots$ P_1, P_2 are prime factors.

Page No.
Date

eg: $\phi(11)$, here $\phi(n)$, $n=11$

∴ no. less than 11 ⇒ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

∴ no. that are relatively prime to 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

∴ 10 numbers.

∴ $\phi(11) = 10$

* for $\phi(n)$ If n is a prime number,

$\phi(n) = n-1$

eg.. $\phi(8)$, here $\phi(n)$, $n=8$.

no. less than n = 1, 2, 3, 4, 5, 6, 7.

∴ no. that are relatively prime → 1, 3, 5, 7

= 4 no.s.

$\phi(8) = 4$

If n is prime no. in $\phi(n)$

∴ $\boxed{\phi(n) = n-1}$

* If $n = p \times q$, and value of p, q which are prime.

then

$$\boxed{\phi(n) = (p-1) \times (q-1)}$$

* If $n = a \times b$, where a or b OR a & b are composite.

then.

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

here, $P_1, P_2 \ldots$ are distinct prime no

Page No.
Date

1) Find $\phi(5)$,

we know n = prime no.

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

$\phi(5) = 4$

2) Find $\phi(31)$

we know n = prime no.

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

$\phi(31) = 30$

3) Find $\phi(35)$

we know $\phi(n) = n = p \times q$

p = prime, q = prime.

$\phi(35) = \phi(5 \times 7)$

$= (p-1)(q-1)$

$= 4 \times 6$

$\phi(35) = 24$

5) Find $\phi(1000)$

$\therefore n = 1000$

we can write this as.

$n = a \times b = 2^3 \times 5^3$ ⇒ got by factoring 1000.

Distinct prime no. are 2 & 5 $p_1 = 2$ & $p_2 = 5$

$2^3 \times 5^3$

2	1000
2	500
2	250
5	125
5	25
5	5
	1

$$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

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

$\phi(1000) = 400$

Eulers theorem :

For every positive integer a & n, which are said to be relatively prime, then

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

here a & n should ~~have~~ be relatively prime

$\gcd(a, n) = 1$

*. for euers, a & n should be relatively prime

Page No.
Date

1) a=3 & n=10

gcd(a,n) = 1, then only apply euers

$a^{\phi(n)} \equiv 1 \pmod n$

$3^{\phi(10)} \equiv 1 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$

$81 \equiv 1 \bmod 10$

$81/10$ = rem = 1 true.

$\phi(10) = \phi(2) \times \phi(5)$

$= (2-1)(5-1)$

$\phi(10) = 1 \times 4 = 4$

2) a=2 & n=10,

gcd(a,n) ≠ 1, thus no euers

3) a=10 & n=11

gcd(9,n) = 1

$a^{(\phi(n))} \equiv 1 \pmod n$

$10^{10} \equiv 1 \pmod{11}$

$(-1)^{10} = 1 \bmod 11$

$+1 = 1 \bmod 11$

1/11 = 1 erem.

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

$\phi(11) = 10^1 - 1 = 10$

Quadratic Residue :

If a & n are natural no. and are relatively prime i.e. gcd(a,n) = 1, then a is said to be quadratic residue of modulo if.

$x^2 \equiv a \bmod n$ is solvable,

else it is non-quadratic residue.

Page No.
Date

eg $n=7$ (odd prime)

$\Rightarrow 1^2 \equiv 1 \pmod 7$ ($x^2 \equiv a$) value of a is identified by putting all values that are less than n in x^2.

$2^2 \equiv 4 \pmod 7$

$3^2 \equiv 9 \pmod 7 \equiv 2 \pmod 7$

16/7 = 2 $4^2 \equiv 16 \pmod 7 \equiv 2 \pmod 7$

$5^2 \equiv 25 \pmod 7 \equiv 4 \pmod 7$

36/7 = 1 $6^2 \equiv 36 \pmod 7 \equiv 1 \pmod 7$

so, 1, 2 & 4 = values of a are quadratic residues of (mod 7).

thus 3, 5, 6 are non-residues.

eg: $n = 8$ → not a odd prime, but this won't be relatively prime with all values of a.

$\Rightarrow$ (1, 3, 5, 7) values less than n, that are relatively prime to n.

$\therefore 1^2 \equiv 1 \pmod 8$

9/8 = 1 $3^2 \equiv 9 \pmod 8 = 1 \bmod 8$ ∴ 1 is only quad. residue.

$5^2 \equiv 25 \pmod 8 \equiv 1 \bmod 8$ 1, 3, 5, 7 are non-quad residues.

$7^2 \equiv 49 \pmod 8 \equiv 1 \bmod 8$

. Let p be an odd prime, then there are $\left(\frac{p-1}{2}\right)$ incongruent quadratic residues and non-quad residues of mod p.

Legendre and Jacobi Symbol

→ based on quadratic residue,

~~a and P are prime no,~~

$y^2 \equiv a \pmod P$,

then for all values that are less than P and relatively prime to P are considered.

and solved as $y^2 \equiv a$.

→ fermats.

$a^{(P-1)} \equiv 1 \bmod P$

a should no be divisible by P ∴ P is a prime no.

* $a^{(p-1)/2} \equiv 1 \pmod P$, p is prime, a is integer. then a is a quad. residued mod P.

means, $x^2 \equiv a \pmod P$ has a solution if and only if $a^{(p-1)/2} \equiv 1 \pmod P$

~~* let P be the prime number,~~

legendre and Jacobi symbols give a simple method to determine if a number is sqr. mod P.

consider an odd prime no. P & let $a \not\equiv 0 \pmod P$ (quad residue)

then legendre ⇒ $\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod P \text{ has sol}^n \\ -1 & \text{if } x^2 \equiv a \pmod P \text{ has no sol}^n. \end{cases}$

$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod P \text{ has sol}^n \\ -1 & \text{if } x^2 \equiv a \pmod P \text{ has no sol}^n. \end{cases}$

Page No.
Date

* **Properties of legendre**

a) If $a \equiv b \not\equiv 0 \pmod{p}$,
then, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

b) If $a \cdot b \not\equiv 0 \pmod{p}$
then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

c) $a \not\equiv 0 \pmod{p}$ then,
$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

d) $(-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$

\# the Jacobi symbol is based on legendre,

consider an (odd) positive integer n, and 'a' non zero integer, such that $\gcd(a,n) = 1$

then prime factors of n are,

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1} \cdot \left(\frac{a}{p_2}\right)^{b_2} \cdot \left(\frac{a}{p_3}\right)^{b_3} \cdots\cdots$$

the rhs represents legendre symbol, but if $n=p$,
if $n=p$, then in rhs we get only one symbol
= Jacobi symbol

Page No.
Date

* Properties Jacobi:

a) when $a \equiv b \pmod n$ & gcd of $(a,n) = 1$

$$\left(\frac{a}{b}\right) = \left(\frac{b}{n}\right)$$

b) if $\gcd(ab, n) = 1$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

c) $\left(\frac{2}{n}\right) = \begin{cases} +1 & \text{if } n \equiv 1 \\ -1 & \text{if } n = 3 \end{cases}$

d) $(-1)^{(n-1)/2} = (-1/n)$

e) consider q = odd no, with $\gcd(n, q) = 1$

$$\left(\frac{q}{n}\right) = \begin{cases} (-n/q) & \text{if } q = n = 3 \pmod 4 \\ +\left(\frac{n}{q}\right) & \text{otherwise} \end{cases}$$

law of quadratic reciprocarity.

---

* legendre $\Rightarrow \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quad. residue of mod } p. \\ -1 & \text{if } a \text{ is non quad residue of mod } p \end{cases}$

is a a quad residue of mod p = (a/p)

p = odd prime, $x^2 \equiv a \pmod p$

Page No.
Date

g) ∴ using legendre symbol solving $x^2 \equiv a \bmod p$,
where $p \geq 7$, = odd prime

∴ consider all no. less than 7 that are coprime to 7.

$1^2 \equiv 1 \bmod 7$ $\quad x^2 \equiv a$

$2^2 \equiv 4 \bmod 7$ $\quad (2, 4, 1) \rightarrow$ quad residue.

9/7 = 2 $\quad 3^3 \equiv 9 \bmod 7 = 2 \bmod 7$

$4^2 \equiv 16 \bmod 7 = 2 \bmod 7$. $\Rightarrow \left(\frac{a}{p}\right)$

$5^2 \equiv 25 \bmod 7 = 4 \bmod 7$.

$6^2 \equiv 36 \bmod 7 = 1 \bmod 7$.

quad residue $\quad$ quad non residue.

$\left(\frac{a}{b}\right)$, $\left(\frac{2}{7}\right) = 1 \quad \left(\frac{3}{7}\right) = -1$

$\left(\frac{4}{7}\right) = 1 \quad \left(\frac{5}{7}\right) = -1$

$\left(\frac{1}{7}\right) = 1 \quad \left(\frac{6}{7}\right) = -1$

* Eulers criterion :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

eg) $p \geq 7$ and $a = 5$ ∴ a = quad non residue mod 5.

$(1 \cdot 5) = 5 \bmod 7$.

$(2 \cdot 6) = 12 \bmod 7 = 5 \bmod 7$.

$(3 \cdot 4) = 12 \bmod 7 \equiv 5 \bmod 7$.

$5^{(7-1/2)} = 5^3$

$5 \cdot 5 \cdot 5 \pmod p$

$= (1 \cdot 5)(2 \cdot 6)(3 \cdot 4)$

$= 1 (5 \cdot 3)(2 \cdot 4 \cdot 6) \cdot 6$

$= 6 \equiv -1 \bmod 7$

Page No.
Date

g) $(8/13)$ →

$$\left(\frac{8\times2\times2}{13}\right) = \left(\frac{2^2\cdot 2}{13}\right) = \left(\frac{2^2}{13}\right)\left(\frac{2}{13}\right)$$

$$\frac{a\cdot b}{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$= 1 \times \left(\frac{2}{13}\right) = \left(\frac{2}{13}\right)$$

$\frac{4}{13}$ $\sqrt{13} = 1$.

now $\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)$

$\left(\frac{a}{p}\right) = a^{(p-1)/2} \cdot \text{mod } p$ · $\left(\frac{8}{13}\right) = -1$

$\frac{2}{13}$ $= 2^6 \cdot (\text{mod } 13)$

$= 64 \ (\text{mod } 13)$

$= 12 \ (\text{mod } 13)$

$= -1 \ (\text{mod } 13)$

q $\left(\frac{10}{13}\right) \Rightarrow \frac{2\times5}{13} = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

for $(2/13) = 2^{(13-1)/2} \cdot \text{mod } 13$

$= 2^6 \text{ mod } 13$

$= 64 \text{ mod } 13$

$= 12 \text{ mod } 13$

$= -1 \text{ mod } 13$

$\frac{2}{13} = -1$

$(5/13) = 5^{(12/2)} \text{ mod } 13$

$= 15625 \ (\text{mod } 13)$

$= 12 \text{ mod } 13$

$(5/13) = -1$

but $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -1\times-1 = 1$

$2^2/13 = 1$ legendre property

Page No.
Date

Q) $\left(\frac{12}{13}\right) = 6 \times 2 = \frac{2^2 \times 3}{13} = \left(\frac{2^2}{13}\right) \times \left(\frac{3}{13}\right)$

$\frac{2^2}{13} = a^{(p-1)/2} = 1 \quad \frac{3}{13} = a^{(p-1)/2} \cdot \text{mod } p$

$= 3^6 \cdot \text{mod } 13$

$= 729 \text{ mod } 13$

$= 1 \text{ mod } 13$

$= 1$

Shannon's characteristic of good cipher

1) **security** : a good cipher should provide high level sec. and resist cryptographic attacks.

2) **key dependency** ⇒ the security of cipher should heavily depend on secrecy and randomness of encryption key The ciphertext should provide no info regarding the key.

3) **Resistance to attack** ⇒ cipher should be designed to resist various types of cryptographic attacks, also including brute-force attacks

4) **Flexibility** ⇒ a good cipher should flexible to adapt to different encryption scenarios. It should have various key sizes, block sizes & mode of operation.

Page No.
Date

* Diffusion and confusion:

- Introduced by Claude Shannon.
- Shannon's concern was to prevent cryptanalysis [attack] based on statistical analysis.
  → Assume attacker has some knowledge of statistical charac. of plain text.
  (eg: freq. of various letters is known).
  → If these statistics are anywhere reflected in cipher text, the attacker may be able to deduce encryption key. & change data.

Thus Shannon suggested 2 methods for solving this.
∴ confusion & diffusion are properties of creating the secure cipher.

* Diffusion ⇒

→ In simple words, if we change any small thing in simple plain text, then all the elements of cipher text will change.

→ Idea of diffusion is to hide the relationship between ciphertext & plain text

* hide relationship of ciphertext & plain text. because any change in plain text changes the cipher thus, cipher can be guessed.
→ If we change cipher text, plain bit also change.

Page No.
Date

each bit of CT dependent on PT

⇒ Diffusion tells that each symbol of cipher text is dependent on plain text.
∴ cipher text & plain text have relationship which diffusion hides.

* Confusion ⇒ Hides the relationship between ciphertext and key
→ the relation is maintained as complex as possible.

each bit of CT dependent on key

→ if a single bit of key is changed, most or all ciphertext also changes

→ each bit of ciphertext should depend on several part of key. making an unclear connectn between them.

Cryptograph :-

- converting plaintext to cipher text & plain text again.

* encryption ⇒ convert data in some format that only other device coould understand.

* decryption ⇒ @ sender sends encrypted data, and ~~send that to us~~. decrypts.

- @ key is most imp. of encryption
- Private key - encrytion - only one key is used. for both encrypt & decrypt, thus we needs to send key with data.
- one key is used to encrypt data & one to decrypt (Private key) which only receiver has the key, thus no data harm. [2 keys required].

symmetric.