Sagor Roy
IT-21044

1] **Fermet's Little theorem:**

If p is a prime and $a \not\equiv 0 \bmod p$ then,

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

Proof:

Let the set $\{1, 2, \ldots p-1\}$. Each of these number is relatively prime to p. Multiply each by a:

$$\{a \cdot 1, a \cdot 2, \ldots a \cdot (p-1)\} \bmod p$$

Since a is invertible mod p, this is a Permutation. So,

$$a^{p-1} \cdot \{1 \cdot 2 \ldots (p-1)\} \equiv (1 \cdot 2 \ldots (p-1)) \bmod p$$

Cancel out the factorial:

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

Example:

For $a = 7$, $p = 13$,

$$7^{12} \bmod 13 = 1$$

Use in RSA:

Used in modular exponential and in the corectness proof of RSA decryption.

$$m^{ed} \equiv m \bmod n \text{ where, } ed \equiv 1 \bmod \varphi(m)$$

Sagor Roy
IT-21044

Q2| Euler's totient Function $\varphi(n)$

- $\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$
- $\varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5) = (9-3) \cdot 4 = 24$
- $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (4-2)(25-5) = 1$

Euler's theorem
if a and n are coprime,
then $a^{\varphi(n)} \equiv 1 \bmod n$

Q3| Chinese Remainder theorem

Given, $x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 4$
$x \equiv 1 \bmod 5$

- $N = 60, N_1 = 20, N_2 = 15, N_3 = 12$
- $Y_1 = 2, Y_2 = 3, Y_3 = 1$
- Compute inverse:
  - $20^{-1} \bmod 3 = 2$
  - $15^{-1} \bmod 4 = 3$
  - $12^{-1} \bmod 5 = 3$

$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 = 80 + 135$
$= 251$

$x \equiv 251 \bmod 60 = 11$

So, $x \equiv 11 \bmod 60$

Sagor Roy
IT-21044

4] 561 is a Carmichael number

$561 = 3 \times 11 \times 17$ (distinct primes)

Carmichael number test:

1. Composite
2. Square-free
3. $(p-1) \mid (n-1)$ for all divisors
   - $2 \mid 560$
   - $10 \mid 560$
   - $16 \mid 560$

So 561 is a carmichael number

5] Primitive Root of modulo 17

Group: $\mathbb{Z}_{17}^*$ has $\varphi(17) = 16$

Check small numbers:

for $g = 3$ powers are:

$3^1 = 3,\ 3^2 = 9,\ 3^4 = 13,\ 3^8 = 16,\ 3^{16} = 1$

3 generates the full group 3 is a primitive root mod 17.

Sagor Roy
IT 21044

6] Discrete Logarithm: Find x such that

$$3^x \equiv 13 \mod 17$$

Try power of 3 mod 17:

- $3^1 = 3$
- $3^2 = 9$
- $3^3 = 10$
- $3^4 = 13$

So, $x = 4$

7] Role of Discrete Logarithm in Deffie-Hellman

Diffie-Hellman Key exchange uses:

- Public : P, g
- Alice sends $A = g^a \mod p$
- Bob sends $B = g^b \mod p$
- Shared secret = $g^{ab} \mod p$

Security depends on the Discrte log problem (DLP) being hard:

Given g and $g^a \mod p$, its hard to find a

Sagor Roy
IT-21044

8] Cipher comparison

Cipher	Type	Key space	Frequency Vulnerability	Example
Substitution	Substitution	$26! = 2^{88}$	High	A → Q
Transposition	Permutation	Dependson size	Low	"HELLO" → "LOHEL"
Playfair	5x5 matrix, diagraph	25!	Medium	"HE" → "KC"

9] Affine cipher:

Given:

$E(x) = (5x+8) \bmod 26$

Plaintext: "Dept of ICT, MBSTU"

Convert to numbers (A=0, ..., Z=25), ignore space/punctuation:

"DEPTOFICTMBSTU"

→ D=3, E=4, ..., U=20

Encrypt each:

$E(x) = (5x+8) \bmod 26$.

Decrypt:

Find modular inverse of 5 mod 26=2

$D(x) = 21(x-8) \bmod 26$

Sagor Roy
IT-21044

10] Design a Novel cipher:

Cipher idea:

- Combine Affine + Transposition
- Key: affine (a=7, b=3), matrix transposition with key "4312"

Steps:

1. Apply affine : $E(x) = (7x+3) \bmod 26$
2. Write in 4 columns and rearange by key
3. Decrypt : reverse transposition → affine decryption

Cryptanalysis:

- Frequency analysis to break affine part
- Known plaintext to guess permutation