Q-(8)

Cipher Comparison :

Cipher	Type	Key space	Freq. Vulnerability	Example
Substitution	Sub	$26! \approx 2^{88}$	High	A→a
Transposition	Permutation	Depends on size	Low	"Hello"→"Hlelo"
Playfair	5×5 matrix di	25!	Medium	"HE"→"KC"

Q-10

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

Plaintext : "Dept of ICT, MBSTU"

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

"DEPT OF ICT MBSTU" → D = 3, E = 4, ...

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

Decrypt : Find modular inverse of 5 mod 26 ⇒ 21

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

Q6

Discrete Logarithm : Find x such that

$3^x \equiv 13 \mod 17$

$3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 10 \quad 3^4 = 13.$

so $x = 4$

Q7

Role of Discrete Logarithm in Diffie-Hellman:

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

Security depends on the discrete log Problem (DLP) being hard:

Given g and $g^a \mod p$, it's hard to find a

$x = 2 \cdot 20 \cdot 22 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 = 251$

$x \equiv 251 \mod 60 = 11$

So, $x \equiv 11 \mod 60$

Q4) Check 561 is a carmichael number

$561 = 3 \times 11 \times 17$

Carmichael number test:

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

- $2 \mid 560$
- $10 \mid 560$
- $16 \mid 560$

So, 561 is a Carmichael number.

Q5) Primitive root of modulo 17

Group: $\mathbb{Z}_{17}$ has $\phi(17) = 16$

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 full group → 3 is primitive root mod 17

Q2

Eulers Totient function $\phi(n)$

- $\phi(35) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24$
- $\phi(45) = 3 \cdot 4 = 24$
- $\phi(100) = \phi(2^2 \cdot 5^2) = 2 \cdot 20 = 40$

Eulers Theorem :

If a and n are coprime then,

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

Q3

Given,

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 4$

$x \equiv 1 \mod 5$

Solu :

- $N = 60$, $N_1 = 20$, $N_2 = 15$, $N_3 = 12$
- $y_1 = 2$, $y_2 = 3$, $y_3 = 1$
- Compute inverses :

$20^{-1} \mod 3 = 2$

$15^{-1} \mod 4 = 3$

$12^{-1} \mod 5 = 3$

Q.1

Fermat's Little Theorem and Its use in RSA:

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

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

Proof:

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

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

since a is invertible mod p, this is a permutation. So,

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

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

Use in RSA:

Used in modular exponentiation and in the correctness proof of RSA decryption:

$m^{ed} \equiv m \bmod n$ where $ed \equiv 1 \bmod \phi(n)$