Q1) Fermat's little theorem:

Theorem:

If p is a prime and a is an integer such that gcd(a,p) = 1 then $a^{p-1} \equiv 1 \mod p$

Proof:

Consider the set $S = \{a, 2a, 3a \cdots (p-1)a\} \mod p$

since a is coprime to p, multiplication by a permutes the set $\{1, 2 \cdots p-1\}$. So, $a \cdot 2a \cdots$

$(p-1)a \equiv 1 \cdot 2 \cdots (p-1) \mod p$

That is $a^{p-1}(p-1)! \equiv (p-1)! \mod p$

Cancelling $(p-1)!$ $a^{p-1} \equiv 1 \mod p$

Example:

Compute $3^6 \mod 7$ using Fermat's Theorem.

Since 7 is prime and gcd(3,7) = 1,

$$3^{7-1} = 3^6 \equiv 1 \mod 7$$

~~Use in RSA~~:

~~Used in~~

Q2) Euler's Totient Function:

Euler's Function:

$\phi(n)$ = Number of integers $\leq n$ that are coprime to n

compute:

$$\phi(20) = 20\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8$$

Theorem (Multiplicativity):

If m and n are coprime, then

$$\phi(mn) = \phi(m)\,\phi(n)$$

Proof:

→ using Chinese Remainder theorem

→ Bijection between $\mathbb{Z}_{mn}^{*} \cong \mathbb{Z}_{m}^{*} \times \mathbb{Z}_{n}^{*}$

Q3) CRT Example:

$x \equiv 2 \mod 3$
$x \equiv 3 \mod 4$
$x \equiv 1 \mod 5$

Using CRT with $N = 60$, $N_1 = 20$, $N_2 = 15$, $N_3 = 12$

Find inverse:

→ $20^{-1} \mod 3 = 2$
→ $15^{-1} \mod 4 = 3$
→ $12^{-1} \mod 5 = 3$

Then,

$x = (2 \cdot 20 \cdot 2) + (3 \cdot 15 \cdot 3) + (1 \cdot 12 \cdot 3) = 80 + 135 + 36 = 251$

$x \equiv 251 \mod 60 \Rightarrow x \equiv 11 \mod 60$

Q4) Carmichael Numbers:

$561 = 3 \times 11 \times 17$

Check:

→ Square free
→ for each $p \mid 561$, $p - 1 \mid 560$
  → $2 \mid 560$
  → $10 \mid 560$
  → $16 \mid 560$

satisfies Korselt's criterion → 561 is a Carmichael Numbers.

Q5) Primitive Root Modulo 17:

check powers of candidates

Try $g = 3$

$3^1 = 3$, $3^2 = 9$, $3^3 = 10$, $3^4 = 13$, $3^5 = 5$, $3^6 = 15$, $3^7 = 11$

$3^8 = 16$, $3^9 = 14$, . . .

Covers all elements of $Z_{17}^* \Rightarrow 3$ is a Primitive root mod 17

Q6) Discrete Logarithm:

Find x such that $3^x \equiv 13 \mod 17$

Try

→ $3^1 = 3$

→ $3^2 = 9$

→ $3^3 = 16$

. . .

$3^4 = 13$ ✓

So, $x = 4$

Q7) Discrete log in Diffie-Hellman:

→ Uses Difficulty of computing discrete logarithm
→ public: p, g private: a, b
→ Exchange: $A = g^a \bmod p$, $B = g^b \bmod p$
→ shared key: $g^{ab} \bmod p$
→ Security relies on: hardness of computing a from $g^a \bmod p$

Q8) Cipher comparison:

Cipher	Mechanism	Keyspace	Frequency analysis
Substitution	Replace letters	26!	Vulnerable
Transposition	Permute positions	Depends on length	Less vulnerable
Playfair	Digraph substitution	25×25 matrix	Partially resistant

Plaintext: "HELLO"
→ Substitution (Caesar shift 3): "KHOOR"
→ Transposition (block of 5): "OLLEH"
→ playfair (Matrix): Uses digraphs like HE, LL →

Encrypt via matrix rules.

Q9) Affine cipher:

Given $a = 5$, $b = 8$, Plantext: "Dept of ICT, M

a) Convert letters to numbers: D=3, E=4,..

T=19

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

b) Decryption:

Inverse of 5 mod 26 = 21

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

Apply to ciphertext to get original messa

Q16) Design a Novel Ciphers:

Hybrid Cipher:

1) Substitution: Caesar + Vigenere Combinatio

2) permutation: Bit-level transpose

by PRNG (eg. LFSR seed).

Encryption process:

→ Step 1: Apply Caesar with random shift
→ Step 2: Apply Vigenere with fixed keyword
→ Step 3: Transpose using a key-generated matrix

Decryption:

Reverse steps with inverse operations.

Cryptanalysis:

→ Weak PRNG makes permutation predictable
→ Vigenere vulnerable to key length attack
→ Caesar trivially breakable if used alone.