Q1. Answer: (IT-21046)

Proof of Fermat's Little Theorem:

Fermat's Little theorem states that if p is a prime number and a is an integer not divisible by p, then:

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

Proof: Consider that the set $S = \{1, 2, \ldots, p-1\}$.

Multiply each element by a modulo p to get S,

$S' = \{a \cdot 1 \mod p, a \cdot 2 \mod p, \ldots a \cdot (p-1) \mod p\}$

Since a and p are coprime, the elements of S' are distinct and nonzero, hence a permutation of S.

Taking the product of all elements in S and S':

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

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

(IT-21046)

since $(p-1)$ and p are coprime, we can cancel

$(p-1)!$:

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

Computation for $a=7,\ p=13$:

By Ferat's Little Theoram:

$$7^{12} \equiv 1 \mod 13$$

Usefulness in RSA: Fermat's Little theorem is used in RSA to ensure that for a prime p and an integer e copprime to $p-1$, the decryption exponent d can be found such that $e \cdot d \equiv 1 \mod (p-1)$.

This guarantees that $(m^e)^d \equiv m \mod p$, enabling secure encryption and decryption.

(IT-21046)

Q2: Ans: Computation:

\# $\phi(35)$: $35 = 5\times7$, so $\phi(35) = (5-1)(7-1) = 24$

\# $\phi(45)$: $45 = 3^2\times5$, so $\phi(45) = 45\times(1-1/3)(1-1/5) = 24$

\# $\phi(100)$: $2^2\times5^2$, so $\phi(100) = 100\times(1-1/2)(1-1/5) = 40$

proof of Euler's Theorem:

If a and n are coprime, then: $a^{\phi(n)} \equiv 1 \mod n$

The proof is analogous to Fermat's Little Theorem, using multiplicative group of integers modulo n.

CamScanner

(IT-21046)

Q3: Ans:

$$x \equiv 2 \bmod 3$$

$$x \equiv 3 \bmod 4$$

$$x \equiv 1 \bmod 5$$

Let $N = 60 = 3 \cdot 4 \cdot 5$

using CRT:

Let $N_1 = 60/3 = 20$, $m_1 = 2$ (since $20 \cdot 2 \equiv 1 \bmod 3$)

$N_2 = 15$, $m_2 = 3$

$N_3 = 12$, $m_3 = 3$

$$x = (2)(20)(2) + (3)(15)(3) + (1)(12)(3)$$

$$= 80 + 135 + 36$$

$$= 251$$

$$x \equiv 251 \bmod 60 = 11$$

$\therefore \quad x \equiv 11 \bmod 60$

CS CamScanner

Q4 Ans: (IT-21046)

~~A Chu~~

Q3 Ans:

A Carmichael number satisfies $a^{n-1} \equiv 1 \mod n$

for all a coprime to n but is not prime.

→ $561 = 3 \cdot 11 \cdot 17$ – all primes

→ Passes Fermat's test for small a values: Yes

∴ 561 is a Carmichael number.

Q5: Ans: We need g such that $g^k \mod 17$ gives

all 1 to 16. try $g = 3$

$3^1 = 3,\ 3^2 = 9,\ 3^3 = 10, \cdots 3^{16} \equiv 1 \mod 17$

∴ 3 is a generator modulo 17.

CS CamScanner

(IT-21046)

Q6 : Ans :

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

successive powers :

$3^1 = 3$

$3^2 = 9$

$3^4 = 81 \mod 17 = 13$

$\therefore x = 4$

Q7 : Ans :

→ The security of Diffie-Hellman relies on the hardness of the DLP. Two parties exchange public keys $g^a \mod p$ and $g^b \mod p$, and compute the shared secret $g^{ab} \mod p$. An attacker can't compute g^{ab} without solving the DLP for eighter a or b.

CamScanner

Q8) Ans: (IT-21046)

Substitution Cipher : Replaces each letter with another. · Key space : 26! · Vulnerable to frequency analysis.

Transposition Cipher: Rearranges letters. Key space depends on block size · Vulnerable to anagramming.

Playfair Cipher : Encrypts digraph using 5×5 Key matrix · Key space 25! · Resists single letter frequency analysis.

Example : Plaintext "HELLO"

Substitution : Replace H→K, E→Q, L→W, O→R→ KQWWR

Transposition : Revers → "OLLEH"

Playfair : "HE→ "DM", "LL"→ "QR", "O"→ "X"→ "DMQRX"

(IT-21046)

Q9: **Ans:** Given $E(x) = (5x+8) \bmod 26$:

⇒ Encryption "Dept. of ICT, MBSTU"

convert to numbers (A=0, -- Z=25):

$D=3, E=4, \ldots, U=20$

Encrypt each: $E(3) = 23$, $E(4) = 28 \bmod 26 = 2$ etc.

~~Ciphertext : " XW...~~

Encrypted letters: X, C, F, Z, A, H, W, S, Z, Q, N, U, Z, E

∴ ciphertex: "XCFZAHWSZQNUZE (Encrypted)

Decryption function: $D(y) = 21 \cdot (y-8) \bmod 26$

∴ Decrypted plaintex: " Dept of ICT, MBSTU "

CS CamScanner

Q10: Ans: (IT-21046)

Cipher: Combine Caesar shift (shift by K) and columner transposition.

Encryption: shift letters by K, then write in rows and read columns.

Decryption: Revers transposition, then revers shift.

Valnerablities: Knaon plain text attacks can reveal K and transposition pattern.

Frequency analysis may still apply.

Example: Plaintex: "HELLO", K = 3

→ shift "KHOOR

→ Transpose (2 column) KHOOR ~~read~~

read column: "KHOOR".

Ciphertext: "KHOOR".

CS CamScanner