Assignment

Afsana Akter Mim
ID: IT-21004

Q1) Prove Fermat's Little Theorem and use it to compute $a^{p-1} \bmod p$ for given values of $a = 7$, $p = 13$. Then, discuss how this theorem is useful in cryptographic algorithm like RSA.

Farmat's Little Theorem:

If p is a prime number and a is any integer such that $\gcd(a, p) = 1$, then:

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

Proof:-

The set $\{a, 2a, 3a, \ldots (p-1)a\} \bmod p$ produces a permutation of the set $\{1, 2, \ldots (p-1)\} \bmod p$. multiplying all elements gives.

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

Afsana
IT-21004

Since $\gcd(a,p)=1$, we can cancel $(p-1)!$ on both sides and we get:

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

Example: compute $7^{12} \bmod 13$

Here, $a=7$, $p=13$. Since 13 is prime and $\gcd(7,13)=1$ we can apply FLT:

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

Use in cryptography (RSA):

Farmars Little Theorem is fundamental in RSA encryption, where the security depen on modular exponentiation and properties of prime numbers. It helps in computed modular inverses and ensures correct encryption and decryption under modula arithmetic.

Afsana
IT-21004

Q2) Eular Tuotient Function: compute $\varphi(n)$ for $n = 35, 45, 100$. Prove that if a and n are coprime, then $a^{\varphi(n)} \equiv 1 \mod \{n\}$.

Euler's Totient Function $\phi(n)$ gives the count of numbers less than or equal to n that are coprime with n.

Formula:

if $n = p_1^{k_1} \cdot p_2^{k_2} \cdots\cdots p_m^{k_m}$ (Prime factorizati

then,

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

Compute:

(i) $\phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$

(ii) $\phi(45) = 45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 24$

(iii) $\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{1}{5} = 40$

IT-21004

Euler's Theorem:

If $\gcd(a,n)=1$ then

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

Q3) Solve the system of congruences using the Chinese Remainder Theorem and prove that x congruent to 11 on mod $N = 3\times4\times5$

$$x \equiv 2 \bmod 3 \quad x \equiv 3 \bmod 4 \quad x \equiv 1 \bmod 5$$

System of congruences:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{5} \end{cases}$$

We know,

$$N = 3.4.5 = 60$$

Let's solve step-by-step using CRT:

Afsana
IT-21004

Let:

$N_1 = 60/3 = 20,$

$N_2 = 60/4 = 15$

$N_3 = 60/5 = 12$

Find modular inverse of N_1, N_2, N_3 modulo their respective moduli:

$20y_1 \equiv 1 \mod 3 \Rightarrow y_1 = 2$

$15y_2 \equiv 1 \mod 4 \Rightarrow y_2 = 3$

$12y_3 \equiv 1 \mod 5 \Rightarrow y_3 = 3$

Now use the formula:

$$x = a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3$$

$$x = 2.20.2 + 3.15.3 + 1.12.3$$

$$= 80 + 135 + 36$$

$$= 251$$

So,

$x \equiv 251 \mod 60$

$\Rightarrow x \equiv 11 \mod 60$

Afsana
IT-21004

Q4) Find whether 561 is a Carmichael number by checking its divisibility and Fermat's test.

A number n is charmichael if -

→ n is composit

→ For all integers a such that $\gcd(a,n) = 1$ we have $a^{n-1} \equiv 1 \mod n$.

check if,

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

→ Satisfied Korselt's criterion : $p-1 \mid n-1$ for all primes p dividing n.

Check;

- $2 \mid 560$, $10 \mid 560$, $16 \mid 560$ → all hold

So, 561 is a Carmichael number.

Afsana
IT-21004

Q5) Find a generator (Primitive root) of the multiplicative group modulo 17.

To find a primitive root, it must satisfy:

$$g^k \not\equiv 1 \mod 17 \text{ for any } k < \phi(17) = 16$$

$g = 3$: check powers of 3 modulo 17

→ gives all residues mod 17

primitive root: 3.

Q6) Solve the Discrete Logarithm Problem:

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

Find x such that:

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

Try powers:

$3^1 = 3 \mod 17$

$3^2 = 9 \mod 17$

$3^3 = 10 \mod 17$

$3^4 = 13 \mod 17$

So, $x = 4 \mod 17$.

IT-21004

Q7) Discuss the role of the discrete logarithm in the Diffie-Hellman Key Exchange.

The security of Diffie-Hellman Key Exchange relies on the hardness of computing the discrete log.

Given, $g, p, g^a \bmod p$, it is hard to find a

- Users exchange $g^a \bmod p$ and $g^b \bmod p$
- Final shared key: $(g^b)^a \bmod p = (g^a)^b \bmod p$

$= g^{ab} \bmod p$.

nly Alice and Bob know, a,b attacker
n't compute shared key without solving
crete log.

Afsana
IT-21004

Q8) Compare and contrast the substitution Chipher, Transposition chipher, and Playfair Cipher in terms of encryption mechanism, key space, and vulnerability to frequency analysis. Provide an example plaintext and show how each cipher transforms it.

Feature	Substitution Cipher	Transposition Cipher	Playfair Cipher
Encryption Mechanism	Replaces each letter with another letter	Rearranges letters without changing them	Replaces pairs of letters using a 5x5 letter grid.
key Space	26!	Depends on rule	pattern recognition
Vulnerability	frequency analysis	Pattern recognition	Still vulnerable if known bigram used.
Frequency preservation	Yes	No	Less.

Afsana
IT-21004

Example :-

plaintext : "HELLO"

→ substitution : "IFMMP"

→ Transposition : (e.g. reverse) . "OLLEH"

→ playfair (e.g. "HE" → "KC", "LL" → "ZX" etc)

Q9) Given the Affine Cipher encryption function $E(x) = (ax+b) \bmod 26$, where $a = 5$ and $b = 8$

a) Encrypt the plaintext "Dept of ICT, MBSTU"

b) Derive the decryption function and decrypt the ciphertext.

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

a) Encrypt "Dept of ICT, MBSTU"

Convert letters to numbers (A=0, ... Z=25);

• D=3, E=4, P=15, T=19, O=14, F=5, I=8, C=2, M=12, B=1, S=18, U=20.

Apply:

• $E(3) = (5 \times 3 + 8) \bmod 26 = 23 \rightarrow X$

• Continue this for each letter.

Afsana
IT-21004

Encrypted text: "XCIH SL ZWM, KTQIJ"

b) Decryption:

- $a^{-1} = 21$ Since, $5 \cdot 21 \equiv 1 \mod 26$.
- $D(x) = 21(x-8) \mod 26$

use this formula to recover original text.

Q 10) Design a simple novel cipher (using a combination of substitution and permutation techniques) Describe it's encryption and decryption processes. Then, perform a basic cryptanalysis on your cipher to identity its potential vulnerabilities. You may use your own PRNG technique.

A Novel cipher - Sub-Perm Stream Cipher.

Cipher Design Overview

This cipher consists of three layers.

1. Substitution Layer
2. Transposition Layer
3. Stream XOR Layer

Afsana
IT-21004

Key Components

- Main key: A 5-character keyword (e.g. HELLO)
- Seed for PRNG: Derived for from the sum of ASCII values
- PRNG - A custom psedu-random number generator using seed = (seed * a + c) % m

Encryption Steps:

Let's say the plaintext is: SECRETMESSAGE
And the key is: HELLO

Step 1: Substitution Layer

1. Generate a randomized alphabet by shuffling A-Z based on the key.

~~Example~~

2. Substitude each letter in the plaitext with its mapped value.

plaintext: SECRETMESSAGE
Substitude: LTERTCDTLLQUT

Afsana
IT-21004

Step 2: Transposition Layer (PRNG Position Swapping)

1. Seed = sum of ASCII of "HELLO" = 72+69+76+76+79 = 372
2. Use PRNG:

   Seed = (Seed * 1664525 + 1013904223) % 2^32

3. Generate swap indices and swap adjacent positions using PRNG.

Example swap (for 13-character message).

- Swap position 1 ↔ 4
- Swap position 2 ↔ 7
- Final result after swaps: LCELTRDTQLTUT

Step 3: XOR Layer (for added stream cipher security)

- Convert final string to ASCII
- Generate PRNG stream of same length
- XOR each character with stream value

Afsana
IT-21004

Decryption Process :-

1. Reverse the XOR
2. Reverse the transpositions using the same PRNG swap sequence.
3. Use the reversed substitution alphabet to map ciphertext back to original plaintext.