Shelu Saha
IT-21009

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.

Answer:

Statement of Fermat's Little Theorem:

If p is a prime number and a is any integer not divisible by p, then:

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

Proof (Using Group Theory/Modular Arithmetic):

Let's consider the set of non-zero integers modulo p:

$$\{1, 2, 3, \ldots, p-1\}$$

Multiplying each element of this set by a modulo p gives a new set:

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

Since a is not divisible by p, it's invertible modulo p, so the new set is just a rearrangement of the original set modulo p.

Hence:

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

This simplifies to:

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

Now, since $(p-1)!$ is not divisible by p (as p is not in the set), we can cancel it from both sides:

$a^{p-1} \equiv 1 \bmod p$ (proved)

given that,

$a = 7$

$p = 13$ (which is prime)

we want to compute: $7^{12} \bmod 13$

By Fermat's Little Theorem:

$7^{13-1} \equiv 7^{12} \bmod 13$

Answer: $7^{12} \equiv 1 \bmod 13$

Importance in Cryptography (RSA example):

Fermat's Little Theorem is a special case of Euler's Theorem and is important in modular arithmetic, especially in RSA.

- In RSA, you choose large prime numbers
- Encryption uses $c \equiv m^e \bmod n$
- Decryption uses $m \equiv c^d \bmod n$
- The values of e and d are chosen such that $m^{e \cdot d} \equiv m \bmod n$

RSA relies on the fact that computing $a^b \bmod n$ is eay but factoring n to find its prime is hard - the asymmetry

Ghatu Saha
IT-21009
Session - 20-21

gives RSA its security.

Question: 2

Euler Tuotient Function : Compute $\phi(n)$ for $n = 35, 45, 100$. Prove that if a and n are coprime, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Answer:

The Euler Totient function $\varphi(n)$ counts how many numbers from 1 to n are coprime with n. If

If $n = p_1^{K1} \cdot p_2^{K2} \cdots p_r^{Kr}$ is the prime factorization of n, then:

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

Let's compute for :

(i) $n = 35$

Prime factorization : $35 = 5 \times 7$

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

(ii) $n = 45$

Prime factorization: $45 = 3^2 \times 5$

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

(iii) $n = 100$

Prime factorization $100 = 2^2 \times 5^2$

$$\varphi(100) = 100 \cdot \left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

Prove Euler's Theorem:

Theorem Statement: If a and n are coprime, then

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Let a be an integer such that gcd $(a,n)=1$.

Then the set of numbers coprime to n is:

$$R = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$$

Multiplying each by a modulo n gives:

$$a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(n)} \pmod n$$

This new set is a permutation of the original set R, because multiplication by a doesn't change the coprimality (since a is coprime to n).

So: $a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \bmod n$

Left side becomes:

$$a^{\varphi(n)} \cdot (r_1 \cdot r_2 \cdots r_{\varphi(n)}) \equiv (r_1 \cdot r_2 \cdots r_{\varphi(n)}) \bmod n$$

Divide both sides (since product is non-zero mod n):

$$a^{\varphi(n)} \equiv 1 \bmod n \quad \text{(Proved)}$$

Shetu Saha
IT-21009

Question: 3

Solve the system of congruences using the Chinese Reminder Theorem and prove that x congruent to 11 on mod $N = 3 \times 4 \times 5 = 60$.

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

Answer: Let's solve the system of congruences using the Chinese Remainder Theorem (CRT) and prove that:

$x \equiv 11 \pmod{60}$, where $N = 3 \times 4 \times 5 = 60$

Step-1: Express as a system of congruences we are given:

$$x \equiv 11 \pmod{60}$$

Let's break 60 into its coprime factors:

$m_1 = 3$

$m_2 = 4$

$m_3 = 5$

Now compute $x \bmod m_1, m_2, m_3$:

$x \equiv 11 \pmod 3 \Rightarrow x \equiv 2 \pmod 3$

$x \equiv 11 \pmod 4 \Rightarrow x \equiv 3 \pmod 4$

$x \equiv 11 \pmod 5 \Rightarrow x \equiv 1 \pmod 5$

So, we now have:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 4$

$x \equiv 1 \pmod 5$

Shetu Saha
IT-21009

Step 2: Use the Chinese Remainder Theorem

Shetu Saha
IT-21009

Let
$m_1 = 3,\ m_2 = 4,\ m_3 = 5$

$M = 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{60}{4} = 15$

$M_3 = \frac{60}{5} = 12$

Now we need the modular inverses:

(i) Find y_1 such that:

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

(ii) Find y_2 such that:

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

(iii) Find y_3 such that:

$$12y_3 \equiv 1 \pmod 5 \Rightarrow 2y_3 \equiv 1 \pmod 5 \Rightarrow y_3 = 3$$

Step3: Construct the solution

The formula is:

$$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod M$$

where:

$a_1 = 2,\ a_2 = 3,\ a_3 = 1$

$M_1 = 20,\ M_2 = 15,\ M_3 = 12$

$y_1 = 2,\ y_2 = 3,\ y_3 = 3$

Now plug in:

$$x \equiv (2)(20)(2) + (3)(15)(3) + (1)(12)(3) \pmod{60}$$

$$x \equiv 80 + 135 + 36 = 251 \pmod{60}$$

$$x \equiv 251 \bmod 60 = 11 \quad \text{(Ans:)}$$

Question: 4

Find Whether 561 is a Carmichael number by checking its divisibility and fermats test.

Answer:

A carmichael number is a composite number n such that:

$$a^n \equiv a \mod n$$

for all integers a such that gcd(a, n) = 1

It passes fermet's Little Theorem for all such a, even though it is not prime.

Shefu Saha
IT-21009

Step-1: Check if 561 is composite

we factor 561:

$$561 = 3 * 11 * 17$$

So, 561 is composite

Step-2: Check if 561 is square-free

A number is square-free if no prime factor repeats.

$$561 = 3^1 \cdot 11^1 \cdot 17^1$$

Each prime has exponent 1 → 561 is square-free

Step-3: Apply fermat's Test for Each Prime factor:

Let's check whether for each prime factor p of 561

$$(p-1) \mid (561-1 = 560)$$

for $p = 3$, $p-1 = 2 \Rightarrow 2 \mid 560$

for $p = 11$, $p-1 = 10 \Rightarrow 10 \mid 560$

for $p = 17$, $p-1 = 16 \Rightarrow 16 \mid 560$

All prime divisors satisfy $(p-1) \mid 560$

for each prime p dividing 561, $p-1 \mid 560$

Therefore, 561 is a carmichael number.

Question-5:

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

Answer:

We want to find a primitive root modulo 17, that is, a number g such that:

$$\{g^1, g^2, g^3, \ldots g^{16}\} \bmod 17$$

produces all numbers from 1 to 16 without repetition

Step: 1- Euler's Totient function

Since 17 is prime number,

$$\varphi(17) = 17-1 = 16$$

So, the order of any primitive root modulo 17 must be 16.

Step: 2- Prime factors of 16

$16 = 2^4 \Rightarrow$ Prime factor is 2

To test whether a number g is a primitive root modulo 17, check:

$$g^{16/2} = g^8 \not\equiv 1 \mod 17$$

Step-3: Try $g=2$

$2^8 = 256 \Rightarrow 256 \mod 17 = 1$

So, $g = 2$ is not a primitive root because its order is 8.

Step-4: Try $g=3$

$3^8 = 6561 = 3^8 \mod 17 = 16 \neq 1$

Now, let's compute all powers of 3 modulo 17:

$3^1 \equiv 3 \mod 17$

$3^2 \equiv 9 \mod 17$

$3^3 \equiv 10 \mod 17$

$3^4 \equiv 13 \mod 17$

$3^5 \equiv 5 \mod 17$

$3^6 \equiv 15 \mod 17$

$3^7 \equiv 11 \mod 17$

$3^8 \equiv 16 \mod 17$

$3^9 \equiv 14 \mod 17$

$3^{10} \equiv 8 \mod 17$

$3^{11} \equiv 7 \mod 17$

$3^{12} \equiv 4 \mod 17$

$3^{13} \equiv 12 \mod 17$

$3^{14} \equiv 2 \mod 17$

$3^{15} \equiv 6 \mod 17$

$3^{16} \equiv 1 \mod 17$

Shetu Saha
IT-21009

All $\{1, 2, \ldots\ldots 16\}$ appeared once order is 16.

$\therefore$ 3 is a primitive root modulo 17 (Ans:)

Question-6:

Solve the discrete logarithm problem:

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

Answer: To solve the discrete logarithm problem $3^x \equiv 13 \mod 17$, we need to find the value of x.

We can do this by computing the powers of 3 modulo 17 until we reach 13.

$3^1 \equiv 3 \mod 17$

$3^2 \equiv 9 \mod 17$

$3^3 \equiv 3 \cdot 9 \equiv 27 \equiv 10 \mod 17$

$3^4 \equiv 3 \cdot 10 \equiv 30 \equiv 13 \mod 17$

From the calculations, we can see that $3^4 \equiv 13 \mod 17$.

Therefore, $x = 4$ (Ans:)

Shetu Saha
IT:21009

Question-7:
Discuss the role of the discrete logarithm in the Diffie-Hellman Key Exchange.

Answer:
Role of Discrete Logarithm in Diffie-Hellman Key Exchange-

1. Public Parameters: Large prime p, generator g.
2. Key Exchange:
   - Alice sends $A = g^a \bmod p$
   - Bob sends $B = g^b \bmod p$
   - shared key: $g^{ab} \bmod p$
3. Discrete Logarithm Problem (DLP):
   - Hard to find a from $A = g^a \bmod p$
   - This difficulty ensures security
4. Attacker's challenge:
   - Cannot compute shared key without solving DLP
   - DLP is computationally hard for large p

Shetu Saha
ID: IT21009

Question-8: Compare and contrast the substitution cipher, Transposition cipher, and playfair cipher in terms of encryption mechanism, key space, and vulnerability to frequency analysis. provide an example plain text and show how each cipher transforms it.

Answer: Here's a simple and short comparison of substitution cipher, Transposition cipher and playfair cipher

including encryption mechanism, key space, frequency analysis and examples:

Substitution Cipher:

- Method: Replace each letter with another
- Key space: 26!
- Frequency Attack: Easy
- Example:
  HELLO → KHOOR (Caesar+3).

Shetu Saha
ID:- IT-21009

Transposition Cipher:

- Method: Rearrange letters, don't change them.
- Key Space: Depends on length (e.g., 5! for 5 letters)
- Frequency Attack: Harder
- Example:
  HELLO → LHOEL (3-1-4-2-5 pattern)

Playfair Cipher:

- Method: Encrypt letter pairs using 5×5 grid
- Key Space: very large ($\sim 10^{40}$)
- Frequency Attack: Medium
- Example:
  HELLO → DMUZUP (Pairs: HE, LX, LO)

Cipher	Method	Key Size	Freq. Attack	Example
Substitution	Letter Swap	Huge	Easy	KHOOR
Transposition	Letter Shuffle	Medium	Harder	LHOEL
Playfair	Pair swap	very big	Medium	DMUZUP

Question-9:

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.

Answer:

Given

Encryption function:

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

Shetu Saha
ID: IT-21009

where:

- $a=5, b=8$
- a and 26 must be coprime → 5 and 26 are coprime

Step a) Encrypt "Dept of ICT, MBSTU"

1. Remove spaces/punctuation: DEPTOFICTMBSTU
2. 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

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

D(3) → (5×3+8) mod 26 = 23 → X
E(4) ⇒ (5×4+8) mod 26 = 2 → C
P(15) → (5×15+8) mod 26 = 5 → F
T(19) → (5×19+8) mod 26 = 25 → Z
O(14) → (5×14+8) mod 26 = 0 → A
F(5) → (5×5+8) mod 26 = 7 → H
I(8) → (5×8+8) mod 26 = 22 → W
C(2) → (5×2+8) mod 26 = 18 → S
T(19) → (5×19+8) mod 26 = 25 → Z
M(12) → (5×12+8) mod 26 = 16 → Q
B(1) → (5×1+8) mod 26 = 13 → N
S(18) → (5×18+8) mod 26 = 20 → U
T(19) → (5×19+8) mod 26 = 25 → Z
U(20) → (5×20+8) mod 26 = 4 → E

Encrypted Text:

XCFZAHWSZQNUZE

Shetu Saha
ID: IT-21009

Step 2) Decrypt

1. Decryption function:

$D(y) = a^{-1}(y-b) \bmod 26$

2. Find modular inverse of $a = 5 \bmod 26$:

$5 \cdot 21 \bmod 26 = 1 \rightarrow a^{-1} = 21$

3. Use :

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

4. Decrypt XQFZAHMSZQNUZE :

$X(23): 21(23-8) = 21 \times 15 \bmod 26 = 3 \rightarrow D$

$Q(2): 21(2-8) = 21 \times (-6) \bmod 26 = 4 \rightarrow E$

$F(5): 21(5-8) = 21 \times (-3) \bmod 26 = 15 \rightarrow P$

$Z(25): 21(25-8) = 21 \times 17 \bmod 26 = 19 \rightarrow T$

$A(0): 21 \times (-8) = -168 \bmod 26 = 14 \rightarrow O$

$H(7): 21 \times (7-8) = -21 \bmod 26 = 5 \rightarrow F$

$W(22): 21 \times 14 = 294 \bmod 26 = 8 \rightarrow I$

$S(18): 21(18-8) = 210 \bmod 26 = 2 \rightarrow C$

$Z(25): 21(25-8) = 357 \bmod 26 = 19 \rightarrow T$

$Q(16): 21 \times 8 = 168 \bmod 26 = 12 \rightarrow M$

$N(13): 21 \times 5 = 105 \bmod 26 = 1 \rightarrow B$

$U(20): 21 \times (12) = 252 \bmod 26 = 18 \rightarrow S$

$Z(25): T$

$E(4): 21 \times (-4) = -84 \bmod 26 = 20 \rightarrow U$

Decrypted text :

DEPTOFICTMBSTU

Shetu Saha
ID: IT-21009

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

Answer: Here's a simple novel cipher using substitution and permutation with a custom PRNG:

Cipher Name: SubPerm Cipher

Encryption Steps:

1. Substitution:

Shift each letter by a pseudo-random number generated from a seed key.

Example PRNG:

$x_i = (x_{i-1} \times 3 + 7) \bmod 26$

2. Permutation:

Reverse the blocks of 4 letters (you can change block size)

Shetu Saha
ID: IT21009

Decryption Steps:

1. Reverse Permutation:

Reverse back each 4-letter block

2. Reverse Substitution:

Use the same PRNG to subtract the shift from each letter.

Example:

Plaintext: HELLOWORLD

Seed: 3

PRNG Sequence: 3, 16, 25, 0, 7, 4, 19, 6, 1, 10

Step1: Substitution

H(7) + 3 = 10 (K)

E(4) + 16 = 20 (U)

L(11) + 0) = 11 (K)

L(11) + 0 = 11 (L)

O(14) + 7 = 21 (V)

W(22) + 4 = 0 (A)

O(14) + 19 = 7 (H)

R(17) + 6 = 23 (X)

L(11) + 1) = 12 (M)

D(3) + 10 = 13 (N)

→ KUKLVAHXMN

Shetu Saha
IT21009

Step 2 : Permutation (block size = 4)

Split: KUKL|VAHx|MN → Reverse each block

→ LKUK|XHAV|NM

Ciphertext : LKUKXHAVNM

Sheta Saha
IT 21009

Basic Cryptanalysis :

Strengths:

- Randomized shifts make frequency analysis harder
- Permutation breaks patterns

Weaknesses:

- If PRNG is predictable or seed is leaked → cipher breaks.
- Block permutation pattern maybe guessed with enough ciphertext.