RAM PROSAD SARKER
IT-21038

Q. 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.

$$\{1, 2, 3, 4, \ldots, p-1\}$$

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

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

Rompprasad

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:

$a.1, a.2, \ldots\ldots, a.(p-1) \equiv (1.2.\ldots\ldots(p-1) \bmod p$

This simplifies to:

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

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:

$7^{12} \bmod 13$

Ramprasad

By Fermat's little Theorem:

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

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, it is possible to choose a 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 $m^{e.d} \equiv m \bmod n$

RSA relies on the fact that computing $a^b \bmod n$ is easy, but factoring n to find its prime is hard - the assymetry.

Ramprosad

Question 02: Euler Tuotient function: Compute $\phi(n)$ for $n = 35, 45, 100$. Prove that if a and n are coprime then $a^{\phi(n)} \equiv 1 \bmod n$.

Answer:

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

If $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots p_n^{k_n}$ is the prime factorization of n, then

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

Let's compute for:

(i) $n = 35$

prime factorization: ~~35~~ $35 = 5 \times 7$

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

(ii) $n = 45$

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

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

Ramprasad

(iii) $n = 100$

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

$\phi(100) = 100 \cdot (1 - 1/2) \cdot (1 - 1/5) = 100 \cdot 1/2 \cdot 4/5 = 40$

Prove Euler's Theorem:

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

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

Then the set of numbers coprime to n is

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

Multiplying each by a modulo n gives:

$a \cdot r_1, a \cdot r_2, a \cdot r_3, \ldots, a \cdot r_{\phi(n)} \pmod n$

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:

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

Ramprasad

left side becomes:

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

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

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

(proved)

Question: 03 solve the system of congruences using chinese Remainder Theorem and prove that x congruent to 11 on mod $N = 3 \times 4 \times 5 = 60$

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

Answer: Let's solve the system of congruences using the chinese Remainder Theorem (CRT) and proove that;

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

step-1: Express as a system of congruences given:

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

Ramprasad

$x \equiv 11 \pmod{60}$

Let's break 60 into its coprime factors:

$m_1 = 3$

$m_2 = 4$

$m_3 = 5$

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

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

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

$x \equiv 111 \pmod 5 \Rightarrow x \equiv 1 \pmod 5$

solve now, have:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 4$

$x \equiv 1 \pmod 5$

Step 02: Use the Chinese Remainder Theorem

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

$M = 60$

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

$M_2 = 60/4 = 15$

$M_3 = 60/5 = 12$

Now, we need the modular inverses:

Ramprasad

(i) find y_1 such that :

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

(ii) find y_2 such that :

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

(iii) find y_3 such that

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

step 3 ; Construct the solution

The formula is :

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M$$

where ;

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

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

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

Now plug in

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

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

$x \equiv 251 \bmod 60 = 11$

(Ans)

Ramprasad

Q-4

Find whether 561 is a carmichael ~~no~~ number by checking its divisibility and fermats test.

Answer:

A carmichael ~~num~~ number is a composite number n such that:

$$a^n \equiv a \bmod n$$

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

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

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 ~~un~~ number is square-free if no prime factor repeats.

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

Ramprasad

Each prime has exponent 1 → 561 is square-free

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

Let's check weather for each prime factor 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

Rompreesad

Q5)

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,

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

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

Ramprasad

Step 02: Prime factors of 16

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

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

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

Step 03: 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 04: Try $g = 3$

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

Now, let's compute powers of 3 modulo 17

$3^1 \equiv 3 \mod 17$

$3^2 \equiv 9 \mod 17$

$3^2 \equiv 10 \mod 17$

Rimprosad

$3^4 \equiv 13 \bmod 17$

$3^8 \equiv 5 \bmod 17$

$3^6 \equiv 15 \bmod 17$

$3^7 \equiv 11 \bmod 17$

$3^8 \equiv 16 \bmod 17$

$3^9 \equiv 14 \bmod 17$

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

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

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

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

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

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

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

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

$\therefore$ 3 is a primitive root modulo 17.

(Ans:)

Ramprasad

Q.6 Solve the discrete logarithm problem:
find x such that $3^x \equiv 13 \bmod 17$.

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

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

$3^1 \equiv 3 \bmod 17$

$3^2 \equiv 9 \bmod 17$

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

$3^4 \equiv 3 \cdot 10 \equiv 30 \equiv 13 \bmod 17$.

From the calculations, we can see that

$3^4 \equiv 13 \bmod 17$

Therefore $x = 4$.

Rompraasad

Q.7

Discuss the role of discrete logarithm in the Diffi-Hellman key Exchange.

Answers:

Role of Discrete Logarithem 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 or from $A = g^a \bmod p$
   - This difficulty ensures security.
4. Attacker's challenge:
   - cannot compute shared key without solving DLP

Ramprasad

- DLP is computationally hard for large p

Q-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)

Ramprasad

Transposition ciphers:

- Method : Rearrange letters, don't change them.
- key space : Depends on length (eg, 5! for 5 letters)
- Frequency Attack : Harder
- Example :

  HELLO → LHOEL (3-1-4-2-5 pattern)

Playfair ciphers:

- Method : Encrypt letter pairs using 5x5 grid
- key space : Very large ($\sim 10^{40}$)
- Frequency Attack : Medium
- Example :

  HELLO → DIMUZUP (pairs : HE, LX, LO)

Ramprasad

Cipher	Method	Key Size	Freq. Attack	Example
Substitution	Letter swap	Huge	Easy	KHOOR
Transposition	Letter-shuffle	Medium	Harder	EHOEL
Playfair	Pair swap	very big	Medium	DIMUZUP

Q-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:

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

Where,

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

Ramprosad

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) → $(5\times3+8) \bmod 26 = 23 \rightarrow x$

E(4) → $(5\times4+8) \bmod 26 = 2 \rightarrow C$

P(15) → $(5\times15+8) \bmod 26 = 5 \rightarrow F$

T(19) → $(5\times19+8) \bmod 26 = 23 \rightarrow Z$

O(14) → $(5\times14+8) \bmod 26 = 0 \rightarrow A$

F(5) → $(5\times5+8) \bmod 26 = 7 \rightarrow H$

I(8) → $(5\times8+8) \bmod 26 = 22 \rightarrow W$

C(2) → $(5\times2+8) \bmod 26 = 18 \rightarrow S$

T(19) → $(5\times19+8) \bmod 26 = 25 \rightarrow Z$

M(12) → $(5\times12+8) \bmod 26 = 16 \rightarrow Q$

Assignment 1

Rampraasad

B(1) → (5x1 + 8) mod 26 = 13 → N

S(18) → (5x18 + 8) mod 26 = 20 → U

T(19) → (5x19 + 8) mod 26 = 25 → Z

U(20) → (5x20 + 8) mod 26 = 4 → E

Encrypted Text :

XCFZAHWSZQNUZE

Steb b

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

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

Pamprasad

4. Decrypt XCFZAHMSZQNUZE :

X(23) : 21(23-8) = 21×15 mod 26 = 3 → D

C(2) : 21(2-8) = 21×(-6) mod 26 = 4 → E

F(5) : 21(5-8) = 21×(-3) mod 26 = 15 → P

Z(25) : 21(25-8) = 21×17 mod 26 = 19 → T

A(0) : 21×(-8) = -168 mod 26 = 14 → O

H(7) : 21×(7-8) = -21 mod 26 = 5 → F

W(22) : 21×14 = 294 mod 26 = 8 → I

S(18) : 21(18-8) = 210 mod 26 = 2 → C

Z(25) : 21(25-8) = 357 mod 26 = 19 → T

Q(16) : 21×8 = 168 mod 26 = 12 → M

N(13) : 21×5 = 105 mod 26 = 11 → 3

U(20) : 21×12 = 252 mod 26 = 18 → S

Z(25) : T

E(4) : 21×(-4) = -84 mod 26 = 20 → U

Decrypted text:

DEPTOFICTMSTU

Ramprasad

Q-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.

Ramprasad

Example PRNG:

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

2. Permutation:

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

Decryption steps:

1. Reverse Permutation:

Reverse back each (4-letters) block

2. Reverse Substitution:

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

Example:

plaintext: "HELLOWORLD"

seed: 3

PRNG sequence: 3, 16, 23, 0, 7, 4, 19, 6, 1, 10

Rompraasad

Step 1: substitution

H(7) + 3 = 10(K)

E(4) + 16 = 20(U)

L(11) + 0 = 11(L)

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) + 18 = 13(N)

→ KUKLVAHXMN

Step 2: Permutation (block size = 4)

split : KUKL | VAHX | MN → Reverse each b

→ LKUK | XHAV | NM

Ciphertext : LKUKXHAVNM

Basic cryptanalysis:

Strengths:

- Randomized shifts make frequency analysis harder
- ~~Rep~~ Permutation breaks patterns.

Weaknesses:

- IF PRNG is predictable or seed is leaked → cipher breaks.
- Block permutation pattern may be guessed ~~wh~~ with enough ciphertext.