Nazibur Rahman

(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.

Fermat's Little theorem: If p is a Prime number and a is an integer not divisible by p, then

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

Proof: Multiply set $1, 2, \ldots, P-1$ by a: $a, 2a, \ldots (P-1)a$ mod p is a permutation of Z_p^*.

So, $a^{P-1} \cdot (P-1)! \equiv (P-1)! \bmod P$

$\Rightarrow a^{P-1} \equiv 1 \bmod P$

(Proved)

Given that,

$a=7$

$p=13$

We know that, $a^{P-1} = 1 \pmod{P}$

$\Rightarrow 7^{13-1} = 1 \pmod{13}$

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

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

Use in RSA algorithm:

RSA encryption and decryption involve raising numbers to large powers modulo n, where $n = p \times q$.

Fermat's little theorem helps to the mathematic backbone of RSA, ensuring

⇒ Correctness of encryption/decreption

⇒ Efficient computation

⇒ Resistance to brute force attacks due to large number handling.

(Q2) Euler totient function: Compute $\phi(n)$ for $n = 35, 45, 100$. Prove that if a and n are Co-Prime, then $a^{\phi(n)} \equiv 1 \mod n$.

$$\phi(35) = \phi(7 * 5)$$
$$= \phi(7) * \phi(5)$$
$$= 6 * 4$$
$$= 24$$

$\phi(45) = \phi(3^2 \times 5)$

$= \phi(3^2) \times \phi(5)$

$= (3^2 - 3^{2-1}) \times 4$

$= (9-3) \times 4$

$= 24$

$\phi(100) = \phi(2^2 \times 5^2)$

$= 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 100 \times \frac{1}{2} \times \frac{4}{5}$

$= 40$

Euler's Theorem Statement:

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

then, $a^{\phi(n)} \equiv 1 \mod n$

Proof:

Let,

$R = \{r_1, r_2, r_3 \ldots r_{\phi(n)}\}$ be the set of all integers in $[1, n)$ that are coprime to n.

Since $\gcd(a,n) = 1$, multiplication by a modulo n permutes the elements of R.

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

is just a reordering of R, because multiplication by a coprime number is a bijection modulo n.

Hence:

$$r_1 r_2 \cdots r_{\phi(n)} \equiv (ar_1)(ar_2)\cdots(ar_{\phi(n)}) \pmod{n}$$

$$\Rightarrow r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} \cdots r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

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

(Q3) Solve the system of congruences using the chinese remainder theorem and Prove that x congruent to 11 on mod $N = 3\times4\times5 = 60$.

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

Given,

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 4$

$x \equiv 1 \bmod 5$

$N = 3\times4\times5 = 60$

Step-1:

Compute components

Let,

$N_1 = 60/3 = 20$

$N_2 = 60/4 = 15$

$N_3 = 60/5 = 12$

Find inerse's y_i such that,

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

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

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

Now applying Chinese remainder theorem,

$$x \equiv a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 \mod 60$$

$$\Rightarrow x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \mod 60$$

$$\Rightarrow x \equiv 80 + 35 + 36 \mod 60$$

$$\therefore x \equiv 11 \mod 60$$

(Proved)

(Q4) Find whether 561 is a carmichael number, by checking its divisibility and fermet's test.

The composite number n is a carmichael number if, whenever a is relatively prime to n, we have,

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

561 is a composite number.

$$561 = 3 \times 11 \times 17$$

Korselt's criterion:

Check if for each prime p, $p-1 \mid 561-1$

Here,

$3-1 = 2 \mid 560$

$11-1 = 10 \mid 560$

$17-1 = 16 \mid 560$

All conditions satisfied.

Fermat's test:

3 is a prime with $(3, a) = 1$

$\Rightarrow a^2 \equiv 1 \pmod{3}$

$\Rightarrow (a^2)^{280} \equiv 1 \pmod{3}$

$\Rightarrow a^{560} \equiv 1 \pmod{3}$ ——①

Similarly, 11 is a Prime with $(11, a) = 1$

$\Rightarrow a^{10} \equiv 1 \pmod{11}$

$\Rightarrow a^{560} \equiv 1 \pmod{11}$ —— (ii)

Again,

$a^{16} \equiv 1 \pmod{17}$

$\Rightarrow (a^{16})^{35} \equiv 1 \pmod{17}$

$\Rightarrow a^{560} \equiv 1 \pmod{17}$ —— (iii)

From equation (i), (ii), (iii)

$a^{560} \equiv 1 \bmod (3 \cdot 11 \cdot 17)$

$\Rightarrow a^{560} = 1 \pmod{(561)}$.

Thus by definition of carmichael number, 561 is a Carmichael number.

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

Primitive root: A number α is a primitive root modulo n if every number coprime to n is congruent to a power of a modulo n.

In a simple sentence,
a said to be a Primitive root of Prime number 'p', if 'a^1' mod P, 'a^2' mod P, 'a^3' mod p, .. a^p mod P are distinct.

Let's try $g=3$. test orders via Prime divisors of 16 : 2, 4, 8

- $3^2 = 9 \not\equiv 1 \mod 17$

$3^4 = 81 \not\equiv 1 \mod 17$

$3^8 = 6561 \not\equiv 1 \mod 17$

$3^{16} = 43046721 \equiv 1 \mod 17$.

It passes all.
So, 3 is a Primitive root of modulo 17.
3 is a generator of Z_{17}^*.

Nazibur Rahman

(Q.6) Solve the Discrete Logarithm problem:

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

Ans:

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

$3^1 \equiv 3 \mod 17 = 3$

$3^2 \equiv 9 \mod 17 = 9$

$3^3 \equiv 27 \mod 17 = 10$

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

$\therefore 3^4 = 13 \mod 17$.

Therefore $x = 4$. (Ans:)

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

Ans:

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: $g = g^{ab} \bmod p$
3. Discrete logarithm Problem (DLP):
   - → Hard to find a from $A = g^a \bmod p$
   - → This difficulty ensures security.

Nazibur Rahman

(Q8) Compare and contrast the substitution cipher, Transportation cipher and playfair cipher.

Ans:

1. Substitution Cipher:
   - ⇒ Each letter is replaced by another letter.
   - ⇒ Example: Caesar cipher shifts each letter by fixed number.

2. Transposition Cipher:
   - ⇒ Letters are rearranged based on a pattern or key.
   - ⇒ No change to actual letters.

3. Playfair Cipher:
   - ⇒ Encrypt digraphs (pairs of letters)
   - ⇒ Use rules: Same row, Same column or rectangle.

(Q9) $E(n) = (an+b) \bmod 26$, $a=5$, $b=8$

Encrypt the plaintext "Dept of ICT, MBSTU".

Ans:

Plain text: DEPTOFICTMBSTU

Numeric: 3 4 15 19 14 5 8

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

Plain text	3	4	15	19	14	5	8	2	19	12	1	18	19	20
5n+8	23	28→2	83→5	103→25	78→0	33→7	48→22	18	103→25	68→16	13	98→20	103→25	108→4
Cipher	X	C	F	Z	A	H	W	S	Z	Q	N	U	Z	E

∴ Cipher text: XCFZAHWSZQNUZE

Decryption:

The decryption function of Affine cipher is

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

where a^{-1} is the modular inverse of $a=5$ modulo 26.

Since:

$5.21 \equiv 105 \equiv 1 \bmod 26$

$\Rightarrow a^{-1} = 21$

So, the decryption function becomes

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

Nazibur Rahman

Applying to each cipher letter recovers:

Ciphery	23	2	5	25	0	7	22	18	25	16	13	20	25	4
y-8	15	-6 →20	-3 →13	17	-8 →18	-1 →25	14	10	17	8	5	12	17	-4 →22
24(y-8) mod 26	3	4	15	19	14	5	8	2	19	12	1	18	19	20
Plain	D	B	P	T	O	F	I	C	T	M	B	S	T	V

Recovered: DEPTOFICTMBSTU

Cie: Dept of ICT, MBSTU

(Q10) Design a simple novel cipher.

Ans:

Substitution: Each character is substitution using a keyed caesar shift.

Permutation: Blocks of text are permuted using a PRNG-based skuffle.

Key:

K1: Integer

K2: Seed value for PRNG

Block size: Fixed block size.

Encryption Process:

Step-1: Substitution

Each character c in plaintext is shifted forward

Nazibur Rahman

using a caesar-like method with a varying shift based on the PRNG.

PRNG: $X_{n+1} = (a x_n + c) \bmod m$

Example: Inputs

Plaintext: "Hello"

$k_1 = 3$, $k_2 = 7$, Block size = 2

Step-1: Substitution

Let's say PRNG gives, shift = [5, 12, 7, 19, 2]

H → H(7) + 5 + 3 = 15 → P

E → E(4) + 12 + 3 = 19 → 7

L → L(11) + 19 + 3 = 33 → H

O → O(14) + 2 + 3 = 19 → T

Substitude: "PJVHT"

Step-2: Permutation (Block size 2)

Split: [PJ] [VH] [T_]

Final ciphertext: "TPHV_T"