Name: Shusmita Ghosh Shoili

ID: IT-21006

Assignment

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 algorithms like RSA.

⟹ **Theorem:**

If p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \bmod (p)$

proof: Consider the integers;

$1, 2, 3, 4, \ldots (p-1)$; they leave the remainders $1, 2, 3, \ldots (p-1)$ when divided by p.

consider an integer a, relatively prime to p,

$a \cdot 1, a \cdot 2, a \cdot 3 \ldots a \cdot p-1$

IT-21006

Observe that if, $a \cdot i \equiv a \cdot j \pmod{p}$, $1 \leq i, j \leq p-1$

then $a(i-j) \equiv 0 \pmod{p}$

which is true if and only if $i = j$

$\therefore ai \not\equiv aj \pmod{p}$, for $1 \leq i, j \leq p-1$, $i \neq j$

$\therefore a \cdot 1, a \cdot 2, a \cdot 3 \ldots a \cdot (p-1)$ leaves $p-1$ numb of different remainders when divided by p, that is $a \cdot 1, a \cdot 2, a \cdot 3 \ldots a(p-1)$ are congruent to $1, 2, 3 \ldots (p-1)$ but in some or

$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot \ldots a \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$

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

$\Rightarrow (p-1)! \{a^{p-1} - 1\} \equiv 0 \pmod{p}$

$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod{p}$

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

Given that, $a = 7$, $p = 13$

we know that, $a^{p-1} \equiv 1 \pmod{p}$

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

$\Rightarrow 7^{13-1} \mod 13 = 1$ IT-21006

or $7^{12} \mod 13 = 1$

Fermat's little theorem plays a vital role in modern cryptography especially in RSA, by enabling secure and efficient modular exp.

Use in RSA algorithm:

RSA encryption and decryption involve raising numbers to large powers modulo n, where $n = p \times q$. Fermat's theorem helps in 2 key ways:

1. Efficiency in computation:

Instead of directly computing $a^k \mod p$, Fermat's theorem simplifies calculations using:

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

This helps reduce the exponent modulo $p-1$, making operations faster.

IT-21066

2. Foundation of reversibility:

RSA ensures that: $(M^e)^d \equiv M \bmod n$

Fermat's theorem guarantees that the decryption operation returns the original message correctly by using properties of mod arithmetic.

Q2 Euler Totient function: Compute $\phi(n)$ for $n = 34, 45, 100$. prove that if a and n are co-prime, then $a^{\phi(n)} \equiv 1 \bmod n$

$\Rightarrow \phi(35) = \phi(7*5)$

$= \phi(7) * \phi(5)$

$= 6 * 4 = 24$

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

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

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

$= 24$

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

$= \phi(2^2) * \phi(5^2)$

$= \phi(2^2 - 2^{2-1}) * (5^2 - 5^{2-1})$

$= 2 * 20$

$= 40$

Statement: If n is a (+ve) integer and a be any integer relatively prime to n, then

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

where φ is the Euler φ function.

proof: Let $[x]$ denote the residue class of the set of integers mod n, let $G = [a]$: a is an integer relatively prime to n.

Then we know that, w.r.t. multiplication of residue classes G is a group of order $\varphi(n)$. The identity element of this group be the residue class $[1]$.

We have, $[a] \in G \Rightarrow [a]^{\varphi(G)} \Rightarrow [a]^{\varphi(n)} = [1]$.

$\Rightarrow [a], [a], [a] \ldots$ up to n times $= [1]$

$\Rightarrow [a \cdot a, \ldots$ upto $\varphi(n)$ times$] = [1]$

$\Rightarrow [a^{\varphi(n)}] = [1]$

$\Rightarrow a^{\varphi(n)} = 1 \pmod{n}$

Q3 Solve the system of congruences using the Chinese remainder Theorem and prove that x congruent to 11 on mod $N = 3 \times 4 \times 5 = 60$

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

⇒ The Chinese remainder theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_n \pmod{m_n}$

CRT states that the above equations have a unique solution of the moduli are relatively prime:

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$

IT-21006

$x \equiv 2 \bmod 3 \quad x \equiv a_1 \pmod{m_1}$

$x \equiv 3 \bmod 4 \quad x \equiv a_2 \pmod{m_2}$

$x \equiv 1 \bmod 5 \quad x \equiv a_3 \pmod{m_3}$

$a_1 = 2,\ a_2 = 3,\ a_3 = 1 \quad m_1 = 3,\ m_2 = 4,\ m_3 = 5$

$M = m_1 \times m_2 \times m_3$

$= 3 \times 4 \times 5 = 60$

$M_1 = \frac{M}{m_1}$

$= \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2}$

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

$M_3 = \frac{M}{m_3}$

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

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$20 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$15 \times 3 = 1 \bmod 4$

$M_2^{-1} = 3$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$12 \times 8 = 1 \bmod 5$

$M_3^{-1} = 8$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 20 \times 2 + 3 \times 15 \times 3 + 12 \times 12 \times 8) \bmod 60$

$= (80 + 135 + 96) \bmod 60 = 311 \bmod 60$

$= 11$

I7-21006

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

$x = 11$ satisfies all three congruences

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

⇒ The composite number ~~if~~ 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 carmichael number.

(i) The prime factorization of 561 is

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

So, 561 is composite

(ii) $a^{560} \equiv 1 \pmod{561}$, if $(a, 561) = 1$

we have, $561 = 3 \times 11 \times 17$

$(a, 561) = 1 \Rightarrow 3 \nmid a$

similarly, $11 \nmid a \rightarrow (11, a) = 1$ and

$17 \nmid a \rightarrow (17, a) = 1$

Now by Fermat's theorem,

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

$\rightarrow a^2 = 1 \pmod 3$

$\therefore a^{560} = 1 \pmod 3$ ---(i)

Similarly, 11 is a prime with $(11, a) = 1$.

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

$\rightarrow (a^{10})^{56} \equiv 1 \pmod{11}$

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

17 is a prime with $(17, a) = 1$

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

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

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

Since 3, 11 and 17 are distinct prime and are relatively prime to another,

from (i), (ii) and (iii)

$a^{560} \equiv 1 \bmod (3.11.17)$

$a^{560} \equiv 1 \pmod{561}$

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 co-prime to n is congruent to a power of a modulo n. In a simple sentence, a is said to be a primitive root of prime number 'p', if 'a' mod p, a^2 mod p, a^3 mod p, a^{p-1} mod p are distinct.

2 is not a primitive root of modulo 17.

Because, $2^1 = 2 \bmod 17$

$= 2$

$2^9 = 512 \bmod 17$

$= 2$

Here, 2 is not distinct value, so 2 is not a primitive root.

$3^1 = 3 \bmod 17$
$= 3$

$3^2 = 9 \bmod 17$
$= 9$

$3^3 = 27 \bmod 17$
$= 10$

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

$3^5 = 243 \bmod 17$
$= 5$

$3^6 = 729 \bmod 17$
$= 15$

$3^7 = 2187 \bmod 17$
$= 11$

$3^8 = 6561 \bmod 17$
$= 16$

$3^9 = 19683 \bmod 17$
$= 14$

$3^{10} = 59049 \bmod 17$
$= 8$

$3^{11} = 177147 \bmod 17$
$= 7$

$3^{12} = 531441 \bmod 17$
$= 4$

$3^{13} = 1594323 \bmod 17$
$= 12$

$3^{14} = 4782969 \bmod 17$
$= 2$

$3^{15} = 14348907 \bmod 17$
$= 6$

$3^{16} = 43046721 \bmod 17$
$= 1$

So, 3 is a primitive root of modulo 17.

Q6 Solve the discrete logarithm problem. Find x such that $3^x = 13 \bmod 17$

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

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

$3^2 = 9 \bmod 17 = 9$

$3^3 = 27 \bmod 17 = 10$

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

From the calculations, we can see that,

$3^4 \equiv 13 \bmod 17$.

Therefore, $x = 4$

Q7 Discuss the role of the discrete logarithm in the Diffie-Hellman key exchange.

⇒ Role of discrete logarithm in Diffie-

IT-21006

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.
4. Attacker challange:
   - → can not ~~complete~~ compute shared key w/o solving DLP.
   - → DLP is computationally hard for large p.

Q8. Compare and contrast the substitution cipher, Transposition cipher and playfair cipher.

⇒ 1. Substitution cipher:

↳ Encryption mechanism: Each letter is replaced by another letter.

↳ Example: Ceaser cipher shifts each letter by a number.

key space: For monoalphabetic: $26! \approx 4 \times 10^{26}$

2. Transposition cipher:

→ Encryption mechanism:

(i) Letters are rearranged based on a pattern or key.

(ii) No change to actual letters.

3. Playfair cipher:

Encryption mechanism:

⇒ Encrypt digraphs (pairs of letters)

→ Use rules: same row, column or rectangle.

99 $E(x) = (ax+b) \bmod 26$, $a = 5, b = 8$

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

⇒ **Step A:** Encryption

1. Preprocessing the plaintext:

Remove punctuation and spaces, convert to uppercase

plaintext = "DEPTOFICTMBSTU"

2. Convert letters to numbers:

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

3.

Letter	X	E(X)	Cipher
D	3	$(5\times3+8) \% 26 = 23$	X
E	4	$(5\times4+8) \% 26 = 2$	C
P	15	$(5\times15+8) \% 26 = 1$	B

IT-21006

Letter	X	E(x)	Cipher
T	19	$(5\times19+8) \% 26 = 21$	V
O	14	$(5\times14+8) \% 26 = 0$	A
F	5	$(5\times5+8) \% 26 = 7$	H
I	8	$(5\times8+8) \% 26 = 22$	W
C	2	$(5\times2+8) \% 26 = 18$	S
T	19	$(5\times19+8) \% 26 = 21$	V
M	12	$(5\times12+8) \% 26 = 16$	Q
B	1	$(5\times1+8) \% 26 = 13$	N
S	18	$(5\times18+8) \% 26 = 20$	U
T	19	$(5\times19+8) \% 26 = 21$	V
U	20	$(5\times20+8) \% 26 = 6$	G

Step B: 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, $5 \cdot 21 \equiv 105 \equiv 1 \bmod 26 \Rightarrow a^{-1} = 21$

So, the decryption fuction becomes

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

2. Apply decryption on ciphertext:

Ciphen text : XCBVAHWSVQNQUVG

Converts letters to numbers:

X = 23, C = 2, B = 1, V = 21, A = 0, H = 7, W = 22,

S = 18, Q = 16, N = 13, ~~A = 16~~ U = 20, V = 21, G = 6

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

IT-21006

Letter	y	D(y)	plaintext
X	23	21 x (23-8) % 26 = 3	D
C	2	21 x (2-8) % 26 = 4	E
B	1	21 x (1-8) % 26 = 15	P
V	21	21 x (21-8) % 26 = 19	T
A	0	21 (0-8) % 26 = 14	O
H	7	21 (7-8) % 26 = 5	F

Similarly,

W ≈ I, S ≈ C, V ≈ T, Q ≈ M, N ≈ B, U ≈ S, V ≈ T,

G ≈ U

∴ Ciphertext: XCBVAHWSVQNUVG

Plaintext: DEPTOFICTMBSTU

IT-21006

Q10 Design a simple novel cipher.

⇒ **Substitution:** Each character is substitution using a keyed caeser shift.

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

PRNG: Custom linear congruential generator.

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

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

Example: Inputs:

plaintext : "Hello"

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

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

H → H(7) + 5 + 3 = 15 → P

E → E(4) + 12 + 3 = 19 → T

L → L(11) + 7 + 3 = 21 → V

L → L(11) + 19 + 3 = 33 → H (mod 26)

O → O(14) + 2 + 3 = 19 → T

Substituted : "PTVHT"

Step 2: Permutation (Block size 2)

split: [PT] [VH] [T-]

Final ciphertext : "TPHV_T"