Eid Holiday Assignment

Bindu (21003)

Q1) Prove Fermat's Little Theorem and use it to compute $a^{p-1} \bmod p$ for given value

$a = 7, p = 13$

Ans:-

Statement:-

Fermat's Little theorem States:-

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

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

proof:-

Let a be an integer such that $\gcd(a,p) = 1$ and p is prime.

Consider the set:-

$$S = \{a, 2a, 3a, \cdots (p-1)a\} \bmod p$$

All the elements of S are distinct modulo p and are just a rearrange of $\{1, 2, \cdots p-1\}$ modulo p.

So,

$a, 2a, 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$

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

Since $(p-1)!$ is not divisible by p, we can cancel it.

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

Example:-

Let, $a = 7$, $p = 13$

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

Compute $7^{12} \bmod 13$ (using successive squaring)

- $7^2 = 49 \bmod 13 = 10$
- $7^4 = (7^2)^2 \bmod 13 = 100 \bmod 13 = 9$
- $7^8 = (7^4)^2 \bmod 13 = 81 \bmod 13 = 3$
- $7^{12} = 7^8 \cdot 7^4 \bmod 13 = 3 \cdot 9 \bmod 13 = 1$

verified $7^{12} \equiv 1 \mod 13$

- Use in Cryptography (RSA)

Fermat's Little Theorem ensures that if $e \cdot d = 1 \mod \phi(n)$ then

$$m^{ed} \equiv m \mod n$$

- This property is used in RSA decryption to recover the original message after encryption.
- Ensure correct decryption.
- used in key generation.

Bindu (21003)

Q2) Euler Tuotient Function :- Compute $\phi(n)$ for $n = 35, 45, 100$. Prove that if a and n are coprime, than,

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

Definition :-

Euler's Totient Function $\phi(n)$ is the number of integers less than or equal to n that are co-prime to n. their greatest common divisor with n is 1.

Formula

If n has a prime factorization,

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots p_r^{k_r}$$

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

Example :-

(i) $\phi(45) =$

$45 = 3^2 \times 5$ (prime factor)

$\frac{3-1}{3} \cdot \frac{1}{5}$

prime factor :

45.

~~$\phi(45) = 9 \times 5$~~

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

$= 45 \cdot \frac{2}{3} \cdot \frac{4}{5}$

$= 24$

(ii) $\phi(35)$

prime factor $= 5 \times 7$

$\phi(35) = (p-1)(q-1)$

$= (5-1)\times(7-1)$

$= 24$

(iii) $\phi(100)$

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

$\frac{1}{2} \times \frac{4}{5}$ $\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

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

$= 40$

Theorem:-

If a and n are coprime then,

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

This is known as Euler's Theorem, which generalized Fermat's Little Theorem.

Proof

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

Let the set of integers less than n and coprime to n be

$$R = \{r_1, r_2 \cdots r_{\varphi n}\}$$

multiply each element by a modulo n.

$$S = \{a \cdot r_1, a \cdot r_2 \cdots a r_{\varphi n}\} \bmod n$$

Since multiplication by a is a bijection the product of the two sets is the same modulo n:

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

Cancelling both sides,

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

Q3) Chinese Remainder Theorem (CRT)

Given system,

$x \equiv 2 \bmod 3$ | $a_1 = 2$

$x \equiv 3 \bmod 4$ | $a_2 = 3$

$x \equiv 1 \bmod 5$ | $a_3 = 1$

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

Step-1 Find individual moduli.

$\therefore M_1 = \frac{60}{3} = 20$

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

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

Step-2 : Find modulan inverse,

Find m_1^{-1}, m_2^{-1}, m_3^{-1}

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

or, $20 \cdot M_1^{-1} = 1 \bmod 3$

or, $20 \cdot (2) = 1 \bmod 3$

$M_1^{-1} = 2$

and,

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

or, $15 \times (3) = 1 \bmod 4$ ⇒

$M_2^{-1} = 3$

and,

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

or, $12 \times (3) = 1 \bmod 5$

$M_3^{-1} = 3$

Step-3

CRT Formula

$x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}$

$= 2 \times 20 \times 2 + 3 \times 15 \times 3 + 1 \times 12 \times 3$

$\therefore x = 251 \bmod 60$ ~~or x = 11~~ or $x = 11 \bmod 60$

Eid Holiday Assignment

Bindu
It-21003

187

Qy :- Find whether 561 is a Carmichael number by checking its divisibility and Fermat's test.

Answer:-

Step: 1

Checking if 561 is composite and Square-free.

- Factorize 561:-

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

- Since 561 has three prime factors and no repeated prime factors, it is composite and square-free.

Step-2

Fermat's Little Theorem test:-

- For a number n to be a Carmichael number, it must satisfy the condition:-

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

for every integen a coprime to n.

Test with some valve a coprime to 561 :-

- For $a=2$, compute $2^{560} \bmod 561$.
- For $a=3$, compute $3^{560} \bmod 561$
- For $a=4$, compute $4^{560} \bmod 561$

All these computations show:-

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

This means 561 passes Fermat's test for these bases.

So, 561 is a carmichael numben.

(Eid Holiday Assignment)

Bindu (IT-21003

Q5) Find a Generator (primitive Root) of the multiplicative Group modulo 17

Step-1:-

The multiplicative group modulo 17 denoted as;-

$$\mathbb{Z}_{17} = \{1, 2, 3, \ldots, 16\}$$

This group contains all integers from 1 to 16 that are co-prime to 17. Since 17 is a prime number, so all numbers from 1 to 16 automatically coprime to it.

Size of the group is

$$\phi(17) = 16.$$

Step-2:-

A number g is a primitive Root modulo 17 if the powers of g generate all elements of $\mathbb{Z}^*_{17}$ that is,

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

So, all numbers from 1 to 16 ~~whit~~ without repeating before $g^{16} \equiv 1$

Step-3 :- $g = 3$

we check powers of 3 module 17

$3^1 \bmod 17 = 3$

$3^2 \bmod 17 = 9$

$3^3 \bmod 17 = 10$

$3^4 \bmod 17 = 13$

$3^5 \bmod 17 = 5$

$3^6 \bmod 17 = 15$

$3^7 \bmod 17 = 11$

$3^8 \bmod 17 = 16$

$3^9 \bmod 17 = 14$

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

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

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

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

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

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

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

So, The number 3 is the primitive Root modulo 17.

Bindu (IT-21003)

Q6) Solve the Discrete Logarithm Problem:

Find x such that,

$3^x \equiv 13 \pmod{17}$

· Let's try successive powers of 3 modulo 17

x	$3^x \bmod 17$
1	3
2	9
3	$27 \equiv 10 \bmod 17$
4	$81 \equiv 13 \bmod 17$
5	$243 \equiv 5 \bmod 17$

we get $x = 4$,

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

$\log_3(13) \equiv 4 \bmod 17$

Bindu (IT-21003)

Q7) Role of discrete logarithm in Diffie-Hellman key exchange?

Answer:-

The discrete logarithm problem is the mathematical foundation of the Diffie-Hellman key exchange.

In this method:-

- Two users agree on a prime number P and a primitive root g
- Each user selects a private key ~~Sayf~~ (Say a, b) and computes their public key as $A = g^a \bmod P$ and $B = g^b \bmod P$
- They exchange public keys and compute the shared secret.

user 1: $S = B^a \bmod P$

user 2: $S = A^b \bmod P$

Both values are equal $S = g^{ab} \bmod p$

- The security depends on the difficulty of solving :.

  Given $g, p, g^a \bmod p \Rightarrow$ find a

This is the discrete logarithm problem which is computationally hard, making the key exchange secure.

Advantages-

→ The discrete logarithm ensures that even if an attacker sees the public values, they can't easily compute the private key or the shared secret, making the system safe for secure communication.

Bindu (21IT-003)

Qs) Compare of substitution, Transposition and playfair ciphers.

Aspect	Substitution Cipher	Transposition Cipher	Playfair Cipher.
Encryption mechanism	1) Replace each letter with another letter.	1) Rearranges the positions of letters.	1) Encryption - pairs of letters using a 5x5 grid.
key space	2) 26! (very Large)	2) Depends on length of key (factorial)	2) 5x5 matrix of letters (based on keyword)
Frequency Analysis	3) Vulnerable (letter frequencies preserved)	3) Less vulnerable (frequencies changed)	3) Hard (diagraph frequency needed)

Example Transformation

plaintext → HELLO

Substitution Cipher:-

Suppose we use a caesar cipher (shift by 3):-

H → K , E → H, L → O, L → O

O → R

Ciphertext :- "KHOOR"

Transposition Cipher:-

Using a simple permutation (reverse the text):-

Plaintext :- HELLO

Reversed :- OLLEH

Ciphertext :- "OLLEH"

Playfair cipher:

Let's assume the key = "MONARCHY".

(5×5) matrix

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Y

Break "HELLO" into digraph

"HE" , "LX" "LO"

Encrypt using playfair rules:-

- HE → "CF"
- "LX" → "SU"
- LO → "PM"

So, the ciphertext = "CFSUPM"

Bindu (IT-21003)

Q9) Affine Cipher Encryption and Decryption.

Ans:-

Encryption

D	E	P	T	O	F	I	C	T	M	B	S	T	U
3	4	15	19	14	5	8	2	19	12	1	18	19	20
X	C	F	2	A	14	W	S	2	Q	N	U	2	E
23	2	5	25	0	7	22	18	25	16	13	20	25	4

Plain Text → Dept of. ICT, MBSTU

Formula

$E(x) = (ax + b) \bmod 26$

key $(a, b) = (5, 8)$

For D

$E(D) = (5 \times 3 + 8) \bmod 26$

$= 23 (X)$

For (E)

$E(E) = (5 \times 4 + 8) \bmod 26 = 2 (C)$

For (P)

$E(P) = \{(5 \times 15) + 8\} \bmod 26$

$= 83 \bmod 26$

$= 5 (F)$

For T

$E(T) = \{(5 \times 19) + 8\} \bmod 26$

$= 103 \bmod 26$

$= 25 (Z)$

For O

$E(O) = \{(5 \times 14) + 8\} \bmod 26$

$= 0 (A)$

For F

$E(F) = \{(5 \times 5) + 8\} \bmod 26$

$= 7 (H)$

For I

$E(I) = \{(5 \times 8) + 8\} \bmod 26$

$= 22 (W)$

For C

$E(C) = \{(5 \times 2) + 8\} \bmod 26 = 18 (S)$

For m

$E(m) = \{(5 \times 12) + 8\} \bmod 26$

$= 16 (Q)$

For B

$E(B) = \{(5 \times 1) + 8\} \bmod 26$

$= 13 (N)$

For S

~~For~~ $E(S) = \{(5 \times 18) + 8\} \bmod 26$

$= 20 (U)$

For U

~~For~~ $E(U) = \{(5 \times 20) + 8\} \bmod 26$

$= ~~18~~ \; 4 (E).$

So, the Encrypted ~~cy~~ ciphertext

= "XQF2AHWS2QNUZE"

Decryption

1. Decryption function of Affine cipher :-

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

To find the a^{-1}

Let $a^{-1} = x$

or $a \cdot x \bmod 26 = 1$

or $5 \times 21 \bmod 26 = 1$

$(26 \times 4) + 1 = 105/5 = 21$

so, $a^{-1} = 21$

x	C	F	Z	A	H	W	S	Z	Q	N	U	Z	E
23	2	5	25	0	7	22	18	25	16	13	20	25	4
D	E	P	T	O	F	I	C	T	M	B	S	T	U
3	4	15	19	14	5	8	2	19	12	1	18	19	20

For (x)

$D(x) = 21(23-8) \bmod 26$

$= 3(D)$

$D(c) = 21(2-8) \bmod 26$

$= -22 + 26 = 4(E)$

$D(F) = 21(5-8) \bmod 26$

$= -11 + 26 = 15 (P)$

$D(Z) = 21(25-8) \bmod 26$

$= 19 (T)$

$D(E) = 21(4-8) \bmod 26$

$= 20 (U)$

$D(A) = 21(0-8) \bmod 26$

$= 10 (K)$

$D(H) = 21(7-8) \bmod 26$

$= 5 (F)$

$D(W) = 21(22-8) \bmod 26$

$= 8 (I)$

$D(S) = 21(18-8) \bmod 26$

$= 2 (C)$

$D(Q) = 21(16-8) \bmod 26$

$= 12 (M)$

$D(N) = 21(13-8) \bmod 26$

$= 1 (B)$

$D(U) = 21(20-8) \bmod 26$

$= 18 (S)$

Decrypted msg

= "Dept of ICT, MBSTU"

Bindu (IT-21003)

Q10) own cipher creation.

Name → Bindu cipher.

→ A simple cipher using substitution + permutation with a PRNG-based key.

Encryption process

Step -1 :- Substitution (Random Shift)

use a LCG to generate random shifts for each character.

The LCG Formula is,

$$R_{n+1} = (a \cdot R_n + c) \bmod m$$

we'll use :-

- $a = 5$, $c = 3$, $m = 26$
- Initial se key : $R_0 = 7$

use each generated number to shift a character in the plaintext

Step-2 :- permutation (block shuffling)

After substitution, divide text into blocks of 4 letters.

In each block swap positions.

→ position $1 \leftrightarrow 3$ and $2 \leftrightarrow 4$.

Example:-

"HELLOWORLD"

Step-1 :- Substitution using PRNG

Step	Formula
R_0	key
R_1	$(5 \times 7 + 3) \bmod 26 = 38 \bmod 26$
R_2	$(5 \times 12 + 3) \bmod 26 = 63 \bmod 26$
R_3	$(5 \times 11 + 3) \bmod 26 = 58 \bmod 26$
R_4	$(5 \times 6 + 3) \bmod 26 = 33 \bmod 26$
R_5	$(5 \times 7 + 3) \bmod 26 = 38 \bmod 26$
....	...

Now shift each letter by the generated number.

H → +12 → T

E → +11 → P

L → +6 → R

L → +7 → S

O → +12 → A

W → +11 → H

O → +6 → U

R → +7 → Y

L → +12 → X

D → +11 → O

Substitution Result : "TPRSAHUYXO"

Step-2 : permutation (swap inside each block of 4)

Break into block of 4 :-

TPRS AHUY XO

Swap position

- Block 1: T P R S → R S T P
  1 2 3 4
- Block 2: AHUY → UYAH
- Block 3: XO → XO
  1 2

Final ciphertext: "RSTPUYAHXO"

Decryption process

1. Reverse permutation (swap 1↔3 2↔4 in each block)

2. Reverse substitution: use same PRNG and Subtract shifts.

Cryptanalysis (weakness):-

1) PRNG is predictable.
2) Fixed block permutation.
3) No strong key management.

4) Letter frequency partially hidden.

It's potentiality

- Mixes substitution and permutation.
- uses a custom PRNG (my own!)
- Simple to implement and explain.
- Looks different from other.