Afsana Akter Mitu
ID: IT-21053

Assignment - 5

Q-1: Prove Fermat's Little Theorem and use it to compute a^{p-1} mod p for given value $a=7$, $p=13$.

Answer:

Statement: Fermat's Little theorem state that If p is a prime number and a is any integer not divisible by p then, $a^{p-1} \equiv 1 \mod p$.

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

consider the set:

$$S = \{a, 2a, 3a, \ldots (p-1)a\} \mod p$$

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

So, $a, 2a, 3a \ldots (p-1)a \equiv 1, 2, 3 \ldots (p-1) \mod p$

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

AJ IT21053

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

$\rightarrow 7^2 = 49 \bmod 13 = 10$

$\rightarrow 7^4 = (7^2)^2 \bmod 13 = 100 \bmod 13 = 9$

$\rightarrow 7^8 = (7^4)^2 \bmod 13 = 81 \bmod 13 = 3$

$\rightarrow 7^{12} = 7^8 \cdot 7^4 \bmod 13 = 3 \cdot 9 \bmod 13 = 1$

verified $7^{12} \equiv 1 \bmod 13$.

Use in cryptography (RSA): Fermat's Little theorem ensures that if

$e \cdot d = 1 \bmod \phi(n)$ then

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

$\rightarrow$ This property is used in RSA decryption to recover the original message after encryption.

$\rightarrow$ Ensure correct decryption.

$\rightarrow$ Used in key generation.

IT-21053

Q-2: Euler Tuotient Function - compute $\phi(n)$ for $n=35, 45, 100$; Prove that if a and n are co-prime, than

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

Answer: Euler's Totient Function $\phi(n)$ is the number of integer less than or equal to n that are co-prime to n their gcd with n is 1

Formula: If n has a prime ~~functio~~ factorization $n = p_1^{k_1}, p_2^{k_2}, \dots p_r^{k_r}$

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

Example:

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

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

ii) $\phi(35)$: prime factor $= 5 \times 7$

$$\phi(35) = (p-1)(q-1)$$
$$= (5-1)(7-1)$$
$$= 24$$

IT-21053

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

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

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

$$= 40$$

Theorem: If a and n are co-prime then

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

This is known as Eulers 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 co-prime to n be.

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

multiply each element by a modulo n,

$$S = \{ar_1, ar_2 \cdots ar_{\phi n}\} \mod n.$$

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

$$a^{\phi(n)} \cdot r_1 \cdot r_2 \cdots r_{\phi(n)} = r_1 r_2 \cdots r_{\phi(n)} \mod n$$

cancelling both sides,

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

IT-21053

Q-3: Chinese Remainder Theorem (CRT).

Answer: Given system,

$$x \equiv 2 \bmod 3 \quad | \quad a = 2$$
$$x \equiv 3 \bmod 4 \quad | \quad a = 3$$
$$x \equiv 1 \bmod 5 \quad | \quad a = 1$$

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

Step-1: Find individual modulo,

$$m_1 = \frac{60}{3} = 20$$
$$m_2 = \frac{60}{4} = 15$$
$$m_3 = \frac{60}{5} = 12$$

Step-2: Find modular 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, $20 \cdot 2 = 1 \bmod 3$

$\therefore m_1^{-1} = 2$

and, $m_2 \times m_2^{-1} = 1 \bmod m_2$

$\Rightarrow 15 \times 3 = 1 \bmod 4$

$\therefore m_2^{-1} = 3$

and, $m_3 \times m_3^{-1} = 1 \bmod m_3$

$\Rightarrow 12 \times 3 = 1 \bmod 5 \therefore m_3^{-1} = 3$

IT-21053

Step-3: CRT Formula

$$x = a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + a_3 m_3 m_3^{-1}$$

$$= 2\times20\times2 + 3\times15\times3 + 1\times12\times3$$

$\therefore x \equiv 251 \mod 60$

or, $x = 11 \mod 60$.

Q-4: Find whether 561 is a carmicheal number by checking its divisibility and Fermat's test.

Answer: Step-1: checking if 561 is composite and square-free.

Factorize 561: $561 = 3\times11\times17$

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.

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

for every integer a co-prime to n.

Test with some value a coprime to 561.

For a=2, compute $2^{560} \mod 561$

IT-21053

For $a = 3$, compute $3^{560} \bmod 561$

For $a = 4$, compute $4^{560} \bmod 561$

All these computation show :

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

This means 561 passes Fermats test for these bases.

So, 561 is a carmichael number.

Q-5: Find a Generator (primitive Root) of the multiplicative Group modulo 17.

Answer: Step-1: The multiplicative group modulo 17 denoted as :

$$Z_{17} = \{1, 2, 3 \cdots 16\}$$

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 co-prime 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 Z^*_{17} that is

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

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

Step-3: we check power 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.

Q-6: Solve the Discrete Logarithm Problem

Answer: Find x such that,

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

Let's try successive power's of 3 mod 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 $x=4$

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

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

Q:-7 : Role of discrete logarithm in DiffieHellman key exchange ?

Answer: The discrete logarithm problem is the mathmetical 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 (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 : $S = B^a \bmod P$

user2 : $S = A^b \bmod P$

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

→ The security depends on the difficulty of solving:

IT-21053

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.

Advantage: 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.

Q-8: Compare of substitution, Transposition and play fair ciphers.

Answer:

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

IT-21053

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:

Lets 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 diagraph "HE" "LX" "LO"

Encrypt using playfair rules: HE → 'CF'

LX → 'SU'

LO → 'PM'

So, the ciphertext = 'CFSUPM'

IT-21053

Q-9: Affine Cipher Encryption and Decryption.

Answer:

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	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

plain Text → Dept of ICT, MBSTU.

Formula:

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

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

For, D

$$E(D) = \{(5\times3)+8\} \bmod 26$$
$$= 23(X)$$

For (F)

$$E(E) = \{(5\times4)+8\} \bmod 26 = 2(C)$$

For (P)

$$E(P) = \{(5\times15)+8\} \bmod 26$$
$$= 83 \bmod 26 = 5(F)$$

CamScanner

IT-21053

For T

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

$= 103 \bmod 26$

$= 25 (Z)$

For O

$E(O) = \{(5\times14)+8\} \bmod 26$

$= 0 (A)$

For F

$E(F) = \{(5\times5)+8\} \bmod 26$

$= 7 (H)$

For I

$E(I) = \{(5\times8)+8\} \bmod 26$

$= 22 (W)$

For C

$E(C) = ((5\times2)+8) \bmod 26 = 18 (S)$

For M

$E(M) = \{(5\times12)+68\} \bmod 26$

$= 16 (Q)$

IT-21053

For B

$E(B) = \{(5\times1)+8\} \bmod 26$

$= 13\ (N)$

For S

$E(S) = \{(5\times18)+8\} \bmod 26$

$= 20\ (U)$

For U

$E(U) = \{(5\times20)+8\} \bmod 26$

$= 4\ (E)$

So, the Encrypted ciphertext

= "XCFZAHWSZQNUZE"

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, $ax \bmod 26 = 1$

or, $5\times21 \bmod 26 = 1$

IT-21053

So, $a^{-1} = 21$.

For x

$D(X) = 21 \cdot (23-8) \bmod 26$
$= 3\ (D)$

$D(C) = 21\ (2-8) \bmod 26$
$= -21 + 26 = 4(E)$

$D(F) = 21\ (5-8) \bmod 26$
$= -11 + 26 = 15(P)$

$\cancel{B}(Z) = 21\ (25-8) \bmod 26$
$= 19\ (T)$

$D(E) = 21\ (4-8) \bmod 26$
$= 0\ (14)$

$D(H) = 21\ (7-8) \bmod 26$
$= 5\ (P)$

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

Decrypted msg = Dept of ICT, MBSTU.