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 algorithm like RSA.

Ans: Fermat's Little Theorem states that if p is a prime number and a is an integer such that a is not ~~divide~~ divisible by p then $a^{p-1} \equiv 1 \pmod p$.

This also can be written by $a^p \equiv a \pmod p$

Proof: Let p be a prime number and a be an integer such that a is not divisible by p. consider the set of numbers formed by multiplying a with integers from 1 to p-1 :

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

Assume that for two numbers i and j such that $1 \le i, j < p$, the products $ia \equiv ja \pmod p$

→ if $ia \equiv ja \pmod p$ then $(i-j)a \equiv 0 \pmod p$

→ Since p is prime and a is not divisible by p, this implies that p must divide $i-j$.

→ However $1 \le i, j < p$ means that $i-j$ can not be divisible by p unless $i=j$.

Thus, all the products, $a, 2a, \cdots (p-1)a$ are distinct modulo p.

The product of all the element in S is

$$a \cdot 2a \cdot 3a \cdots (p-1)a = a^{p-1} \cdot [1 \cdot 2 \cdot 3 \cdots (p-1)] = a \cdot (p-1)!^{p-1}$$

By wilson's theorem we know that

$$(p-1)! \equiv -1 \pmod p.$$

Thus the equation (1) becomes

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

Since $(p-1)! \equiv -1 \pmod p$, we can rewrite the equation as:

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

multiply both sides by -1, we get

$$a^{p-1} \equiv 1 \cdot (\text{mod } p)$$

which is the fermet's little theorem.

Given that,

$a=2, p=13$

$2^{12} \bmod 13 = 1$

we calculate $2^{12} \bmod 13$ and if equals 1. So the theorem holds.

Use in RSA

→ It helps find the modular inverse in RSA

→ It is a foundation for Euler's theorem which is used in RSA decryption.

Q2:- Euler Totient function: compute $\phi(n)$ for $n=35, 45, 100$. prove that if a and n are coprime, then $a^{\phi(n)} \equiv 1 \bmod n$

The Euler Totient function $\phi(n)$ counts the number of integers from 1 to n that are coprime with n.

formula:

→ If n is prime $\phi(n) = n-1$

→ If $n = p^k$: $\phi(p^k) = p^k - p^{k-1}$

→ If $n = p \times q$ (product of distinct primes) : $\phi(n) = (p-1)(q-1)$

① compute $\phi(35)$

prime factorization $35 = 5 \times 7$

$$\phi(35) = (5-1)(7-1)$$
$$= 4 \times 6 = 24$$

Numbers coprime to 35 are

{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34}

② compute $\phi(45)$

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

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

③ compute $\phi(100)$

prime factorization $= 2^2 \times 5^2$

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$= 100 \times \frac{1}{2} \times \frac{4}{5} = 40$$

Proof:

If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

→ Let, $\{r_1, r_2, \cdots r_{\phi(n)}\}$ be the residues coprimes to n.

→ multiply each residue by $a \bmod n$. Since $\gcd(a,n) = 1$, the resulting set $\{ar_1, ar_2, \cdots ar_{\phi(n)}\}$ is a

permutation of the original residues (all are distinct and coprime to n)

→ Take product of both sides sets:

$$\prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} (ar_i) \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i \mod n.$$

→ cancel $\prod r_i$ (since it is coprime to n)

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

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

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 4$

$x \equiv 1 \mod 5$

Given		To find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 20$	$M_1^{-1} = 2$	$M = 60$
$a_2 = 3$	$m_2 = 4$	$M_2 = 15$	$M_2^{-1} = 3$	
$a_3 = 1$	$m_3 = 5$	$M_3 = 12$	$M_3^{-1} = 3$	

$M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

$M_1 \times M_1^{-1} \equiv 1 \mod 3$

$20 \times 2 \equiv 1 \mod 3$

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$
$$= (2 \times 20 \times 2 + 3 \times 15 \times 3 + 1 \times 5 \times 12) \bmod 60.$$
$$= 251 \bmod 60$$
$$= 11$$

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

Step-1: A carmichael number is a composite integer n that satisfies fermat's Little Theorem for all integers a coprime to n. Specifically:

$$a^{n-1} \equiv 1 \bmod n \text{ for all } \gcd(a,n) = 1$$

These numbers are also called absolute pseudoprimes because they pass fermat's test despite being composite.

Step-2: Check Divisibility or composite test.

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

Step-3: Apply fermat's test

To confirm 561 is carmichael, check $a^{560} \equiv 1 \bmod 561$ for all a coprime to 561.

We Test $a = 2, 5$ (none divide 561)

1. Test $a = 2$:

$$2^{560} \bmod 561$$

Breaking down using the Chinese Remainder Theorem (CRT) modulo 3, 11, and 17.

i. $2^{560} \bmod 3$

Since $\phi(3) = 2$ and $560 \equiv 0 \bmod 2$

$$2^{560} \equiv (2^2)^{280} \equiv 1^{280} \equiv 1 \bmod 3$$

ii. $2^{560} \bmod 11$

$\phi(11) = 10$ and $560 \equiv 0 \bmod 10$

$$2^{560} \equiv (2^{10})^{56} \equiv 1^{56} \equiv 1 \bmod 11.$$

iii. $2^{560} \bmod 17$

$\phi(17) = 16$, and $560 \equiv 0 \bmod 16$

$$2^{560} \equiv (2^{16})^{35} = 1^{35} \bmod 17$$

By CRT: $2^{560} \equiv 1 \bmod 561$

Step-4 = Korselt's criterion (Alternative verification)

A number n is Carmichael if and only if

1. n is square-free (no repeated prime factors)
2. for every prime p dividing n, $p-1$ divides $n-1$

check for 561 = 3 × 11 × 17

① square-free : yes (primes 3, 11, 17 are distinct)

② Divisibility :

3 − 1 = 2 divides 560 (560/2 = 280)

11 − 1 = 10 divides 560 (560/10 = 56)

17 − 1 = 16 divides 560 (560/16 = 35)

561 is satisfies Korselt's criterion.

Q5:- Find a generator (primitive root) of the multiplicative group modulo 17.

Given that, p = 17

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

prime factorization of $\phi(p)$

$\phi(p) = p_1 \times p_2 \times p_3 \cdots p_n$

$16 = 2 \times 2 \times 2 \times 2$

$= 2^4$

2	16
2	8
2	4
	2

Now, we calculate $n = \frac{\phi(p)}{p}$

$= \frac{16}{2}$

$= 8$

→ If any of the residues is 1 then 'a' is not a primitive root, else it is a primitive root.

Try 2: $2^8 \bmod 12 = 1$

2 is not a primitive root.

Try 3: $3^8 \bmod 12 = 16$

3 is a primitive root of 12.

Try 4: $4^8 \bmod 12 = 1$

4 is not a primitive root of 12.

Q6: Solve the discrete logarithm problem: find n such that $3^n \equiv 13 \bmod 17$.

We need to find the smallest integer n such that, $3^n \equiv 13 \bmod 17$

Brute-force search (Trial and Error) compute successive power of 3 modulo 17 until we find 13.

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

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

$3^3 \equiv 22 \bmod 17 = 10$

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

The smallest solution is $n = 4$.

Q2: Discuss the role of the discrete logarithm in the Diffie-Hellman key Exchange.

Ans The Discrete Logarithm problem (DLP) is at the heart of the Security of the Diffie-Hellman key Exchange (DHKE)

→ The Diffie-Hellman key Exchange is a cryptographic protocol that allow ~~to~~ two parties (Alice and Bob) to Securely share a secret key over an insecure channel - without transmitting the key itself.

Alice does:

→ chooses a private key a
→ computes her public key $A = g^a \bmod p$
→ Sends A to Bob

Bob does:

→ chose a private key b
→ computes her public key $B = g^b \bmod p$
→ Sends B to Alice.

→ Alice computes $K = B^a \bmod p = g^{ba} \bmod p$

→ Bob computes $K = A^b \bmod p = g^{ab} \bmod p$

Since $g^{ab} = g^{ba}$, they now share same secret key.

To find a,

$g^a \bmod p = A$.

This is called Discrete Logarithm problem (DLP)

Example

$q = 13$, $p = 6$

Bob

$SK = a = 3$

$A = 6^3 \bmod 13$

$= 8$ (public key)

Alice

$SK = b = 10$

$B = 6^{10} \bmod 13$

$= 4$ (public key)

Sent A →

← Sent B

Bob

$S = B^a \bmod 13$

$= 4^3 \bmod 13$

$= 12$ (private key)

$A = 8$

$S = A^b \bmod 13$

$= 8^{10} \bmod 13$

$= 12$ (private key)

Q8: 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 plaintext and show how each cipher transform it.

Ans:

Feature	Substitution cipher	Transposition cipher	playfair cipher
Encryption mechanism	Replace each letter with another	Rearrange letters in a block	Replace pairs of letters using a matrix
Key Space	26! possible keys (monoalphabetic)	Depends on block size and permutation	5×5 matrix: 25 letters → 25! layouts.
Frequency analysis	Highly vulnerable	partially vulnerable	more resistant due to digraphs
Type	Monoalphabetic	permutation based	polygraphic substitution

Example plaintext:-

HELLO WORLD

Substitution cipher (caesar cipher with sift=3)

mechanism $E(x) = (x+3) \bmod 26$

Plaintext

H E L L O W O R L D

positions:

7 4 11 11 14 22 14 17 11 3

Add 3

10 7 14 14 17 25 17 20 14 6

Back to letters

K H O O R Z R U O G

Transposition cipher (block size = 5, reverse block)

mechanism: Rearrange characters → "block-level shuffling"

Remove Space:

HELLOWORLD

Split into blocks of 5:

HELLO

WORLD

Reverse each block:

OLLEH

DLROW

cipher text : OLLEHDLROW

Playfair cipher

mechanism: Encrypt pairs of letters using 5x5 grid.

plaintext : HELLO

HE LX LO

key : PLAYFAIREXAMPLE

HE	LX	LO
DM	YR	AN

Grid

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

ciphertext: DMYRAN

Q9: 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.

Ans: Encryption function: $E(x) = (5x+8) \bmod 26$

plaintext: "Dept of ICT, MBSTU"

Step 1: convert Letters to number

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

Step 2: Apply the Affine Encryption function

x	$E(x) = (5x+8) \bmod 26$	Letter
3	$(5\times3+8) = 23$	X
4	$(5\times4+8) = 28 \to 2$	C
15	$(15\times5+8) = 83 \to 5$	F
19	$(5\times19+8) = 103 \to 25$	Z
14	$(5\times14+8) = 78 \to 0$	A
5	$(5\times5+8) = 33 \to 7$	H
8	$(5\times8+8) = 48 \to 22$	W
2	$(5\times2+8) = 18$	S
19	$(5\times19+8) = 103 \to 25$	Z
12	$(5\times12+8) = 68 \to 16$	Q
1	$(5\times1+8) = 13$	N

x	$E(x) = (5x+8) \bmod 26$	Letter
18	20	U
19	25	Z
20	9	E

Encrypted Text: XCFZAHWSZQNUZE

(b) We need to find modular inverse of

$a = 5$ modulo 26

Find a^{-1} such that $5a^{-1} \equiv 1 \bmod 26$

Try values:

$5 \times 21 = 105 \bmod 26 = 1$

So, $5^{-1} = 21$

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

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

Decrypt ciphertext XCFZAHWSZQNUZE

Letter	X	C	F	Z	A	H	W	S	Z	Q	N	U	Z	E
number	23	2	5	25	0	7	22	18	25	16	13	20	25	9

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

y	y-8	$21 \times (y-8) \bmod 26$	x
23	15	$315 \rightarrow 315 \bmod 26 = 3$	D
2	-6	$21 \times 20 = 420 \bmod 26 = 4$	E
5	-3	$21 \times 23 = 483 \bmod 26 = 15$	P
25	17	19	T
0	-8	14	O
7	-1	5	F
22	14	8	I
18	10	2	C
25	17	19	T
16	8	12	M
13	5	1	B
20	12	18	S
25	17	19	T
4	-4	20	U

Decrypted plaintext: DEPTOFICT MBSTU

Q10: 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 techniques.

Ans: cipher Name : Subperm-X cipher

A block based cipher that:

① Substitute each character using a generated key

② Applies a fixed permutation pattern within blocks.

Step 1:

→ Block size 4 (each block = 4 letters)

→ Substitution key: A random shift value $s \in [1, 25]$

→ permutation key: A fixed permutation pattern

[3, 1, 4, 2] means

1st → 3rd
2nd → 1st
3rd → 4th
4th → 2nd

Encryption process:

Let assume

Block size = 4

Substitution shift S = 5 (caesar shift by 5)

permutation pattern [3, 1, 4, 2]

plaintext : "saveEarth"

→ Break the plaintext into blocks of 4

save EART HXXX

→ Substitution (caesar shift by 5)

	S	a	v	e	E	a	r	t	H	X	X	X
	18	0	21	4	4	0	17	19	7	23	23	23
+5 =	23	5	0	9	9	5	22	24	12	2	2	2
	X	F	A	J	J	F	W	Y	M	C	C	C

using permutation using [3, 1, 4, 2]

A X J F W J Y F C M C

ciphertext: AXJFWJYFCCMC

Decryption process:

ciphertext: AXJFWJYFCmCC

Break down cipher text into 3 blocks

AXJF WJYF CmCC

A X J F W J Y F C m C C

Inverse permutation [2,4,1,3] is used.

X F A J J F W Y m C C C

23 5 0 9 9 5 22 24 12 2 2 2

Reverse caesar shift (-5)

18 0 21 4 4 0 17 19 7 23 23 23

S A V E E A R T H X X X

final plaintext: SAVE EARTH

cryptanalysis (weakness):

Strengths:

→ combines both substitution + permutation

→ Block shuffling increase confusion.

→ padding hides exact message length.

Weakness :

1. caesar Substitution is weak.
2. permutation is static
3. Block size is small.
4. No key variation per block.

How to improve :

1. use a strong substitution.
2. change shift/key per block using a PRNG.
3. use dynamic permutation.
4. Increase block size to 8+.