Cryptography & Cyber Law
Assignment-05
Sadia Chowdhury
IT-21062

Ans of 01:

If p is a prime number and a is any integer such that gcd(a,p) = 1, then:

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

proof: Let $S = \{1, 2, 3, \ldots, p-1\}$ be the set of integers modulo p, excluding 0. Multiplying each element by a, where gcd(a,p) = 1 to form a new set:

$$S' = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \bmod p$$

Since, a has an inverse modulo p. all elements in S' are distinct modulo p, and S' is must a rearrangement of S.

Thus:

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

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

Cancelling (p-1)! from both sides (allowed since gcd((p-1)!, p) = 1):

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

This proves Fermat's Theorem.

Using the theorem to compute $a^{P-1} \bmod p$:

Given: $a = 7, P = 13$

since 13 is a prime and gcd(7,13) = 1, by Fermat's Little Theorem:

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

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

Importance of cryptographic Algorithms like RSA:-

Fermat's Little Theorem is foundational in number theory and crucial for cryptography, especially in the RSA algorithm. Here's how:

- RSA Encryption / Decryption uses modular exponentiation:

$$c = m^e \bmod n, \quad m = c^d \bmod n$$

The ~~corresp~~ correctness relies on the fact that:

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

When $ed \equiv 1 \bmod \phi(n)$, where $\phi(n)$ is Euler's totient function.

- Fermat's Theorem (as a special case of Euler's theorem) helps ensure that:

$$m^{P-1} \equiv 1 \bmod P$$

- Which is used when n is a product of two primes p and q.
- Key Generation & Modular inverses : The theorem helps in computing modular inverses which are required to find the decryption key d.

Fermat's Little Theorem simplifies exponentiation in modular arithmetic and forms the mathematical backbone of public-key cryptographic algorithms like RSA ensuring secure data transmission.

Answer of ques 02:

Given that, $n=35$, $n=45$, $n=100$

and prove that if a and n are co-prime then:

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

Step 01 : compute Euler's Totient Function $\phi(n)$

Euler's totient function for:

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

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

For $n=35$:

Prime factorization : $35 = 5 \cdot 7$

$$\phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$$

For $n=45$

prime factorization:

$$45 = 3^2 \cdot 5$$

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

For $n=100$

Prime factorization: $100 = 2^2 \cdot 5^2$

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

Step 2: Proof of Euler's theorem

Theorem: If $\gcd(a,n)=1$, then:

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

Let $A = \{x \in \mathbb{Z}_n^* \mid \gcd(x,n)=1\}$ be the group of units modulo n

Then A has $\phi(n)$ elements.

Since $a \in A$, the function $f(x) = ax \bmod n$ is a bijection on A

So, the product $\prod_{x \in A} x \equiv \prod_{x \in A} ax \bmod n$

$$\prod_{x \in A} ax = a^{\phi(n)} \prod_{x \in A} x$$

cancel $\prod x$ from both sides (it's invertible mod n):

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

Solution of ques 03:

Given that, $x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 4$

$x \equiv 1 \bmod 5$

Let, $n_1 = 3$, $n_2 = 4$, $n_3 = 5$

$N = n_1 \cdot n_2 \cdot n_3 = 3.4.5 = 60$

Step 01: Compute $N_i = \frac{N}{n_i}$

$N_1 = \frac{60}{3} = 20$

$N_2 = \frac{60}{4} = 15$

$N_3 = \frac{60}{5} = 12$

Step 02: Find y_i such that,

$N_i \cdot y_i \equiv 1 \bmod n_i$

- $20 \cdot y_1 \equiv 1 \bmod 3 \rightarrow 20 \equiv 2 \bmod 3$, So solve

  $2y_1 \equiv 1 \bmod 3 \rightarrow y_1 = 2$

- $15 \cdot y_2 = 1 \bmod 4 \rightarrow 15 \equiv 3 \bmod 4$, So solve

  $3y_2 \equiv 1 \bmod 4 \rightarrow y_2 = 3$

- $12 y_3 \equiv 1 \bmod 5 \rightarrow 12 \equiv 2 \bmod 5$, So solve $2y_3 \equiv 1 \bmod 5 \rightarrow y_3 = 3$

Step 03: Compute the solution:

$$x \equiv a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 \bmod N$$

Where:

$$a_1 = 2,\ a_2 = 3,\ a_3 = 1$$

$$x \equiv (2)(20)(2) + (3)(15)(3) + (1)(12)(3) \bmod 60$$

$$x \equiv 80 + 135 + 36 = 251 \bmod 60$$

$$x \equiv 251 \bmod 60 \Rightarrow x \equiv 11 \bmod 60$$

$11 \bmod 3 = 2$

$11 \bmod 4 = 3$

$11 \bmod 5 = 1$

$\therefore x \equiv 11 \bmod 60$

Solution of Ques 04:

A carmichael number is a composite number n such that:

$$a^n \equiv a \bmod n$$

for all integers a such that $\gcd(a, n) = 1$. It passes Fermat's Little Theorem for all such a, even through it is not prime.

Step 01 : Check if 561 is square free. A number is square-free if no prime factor repeats.

$561 = 3^1 \cdot 11^1 \cdot 17^1$

Each prime has exponent $1 \rightarrow 561$ is square-free

Step 02 : Apply Fermat's Test for each prime factor:

$(p-1) \mid (561-1 = 560)$

- For $p=3$, $p-1=2 \Rightarrow 2 \mid 560$
- For $p=11$, $p-1=10 \Rightarrow 10 \mid 560$
- For $p=17$, $p-1=16 \Rightarrow 16 \mid 560$

All prime divisors satisfy $(p-1) \mid 560$.

For each prime p dividing 561, $p-1 \mid 560$

Therefore, 561 is a carmichael number

Solution of Ques 05:

We want to find a primitive root modulo 17, that is, a number g such that :

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

produces all numbers from 1 to 16 without repetition.

Step 1: Euler's Totient Function:

Since, 17 is a prime number,

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

So, the order of any primitive root modulo 17 must be 16

Step 2: Prime factors of 16

$16 = 2^4 \Rightarrow$ Prime factor is 2

To test whether a number g is a primitive root modulo 17, check:

$$g^{16/2} = g^8 \not\equiv 1 \bmod 17$$

Step 03: Try $g = 2$

$2^8 = 256 \Rightarrow 256 \bmod 17 = 1$

So, $g = 2$ is not a primitive root because it's order is 8

Step 04: Try $g = 3$

$3^8 = 6561 = 3^8 \bmod 17 = 16 \neq 1$

Now Let's compute all powers of 3 modulo 17:

$3^1 \equiv 3 \bmod 17$

$3^2 \equiv 9 \bmod 17$

$3^3 \equiv 10 \bmod 17$

$3^4 \equiv 13 \bmod 17$

$3^5 \equiv 5 \bmod 17$

$3^6 \equiv 15 \bmod 17$

$3^7 \equiv 11 \bmod 17$

$3^8 \equiv 16 \bmod 17$

$3^9 = 14 \bmod 17$

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

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

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

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

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

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

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

All $\{1, 2, \ldots, 16\}$ appeared once $\Rightarrow$ order is 16.

$\therefore$ 3 is a primitive root modulo 17

Solution of Ques 06:

To solve the discrete logarithm problem $3^x \equiv 13 \mod 17$, we need to find the value of x.

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

$3^1 \equiv 3 \mod 17$

$3^2 \equiv 9 \mod 17$

$3^3 \equiv 3.9 \equiv 27 \equiv 10 \mod 17$

$3^4 \equiv 3.10 \equiv 30 \equiv 13 \mod 17$

From the calculations, we can see that $3^4 \equiv 13 \mod 17$.

Therefore, $x = 4$

Solution of Ques 07:

Role of Discrete Logarithm in Diffiere Heltman Key Exchange -

1. Public Parameters : Large prime p, generation g.
2. Key Exchange :
   - Alice sends $A = g^a \mod p$
   - Bob sends $B = g^b \mod p$
   - Shared key : $g = g^{ab} \mod p$

3. Discrete Logarithm Problem (DLP):

- Hard to find a from $A = g^a \bmod P$
- This difficulty ensures security

4. Attacker's challenge:

- cannot compute shared key without solving DLP
- DLP is computationalty hard for large P

Solution of Ques 08:

Substitution cipher:

Encryption Mechanism: Each Letter is replaced by another letter.

Example: Caesar cipher shifts each letter by a fixed number.

Key Space: For monoalphabetic : $26! \approx 4 \times 10^2$

Frequency Analysis vulnerability:

Highly vulnerable: Letter frequencies remain unchanged.

Example: Plaintext: Hello

Key: Caesar shift by 3

Ciphertext: KHOOK

2. Transposition cipher:

Encryption Mechanism:

- Letters are rearranged based on a platform or key.
- No change to actual letters.

Key Space:

- depends on message/block length: for length n, key space is n!

Frequency Analysis Vulnerability:

less vulnerable: Frequencies preserved, but letter positions change.

Example:

plaintext: Hello

key: Rearranged as 3-1-4-2-5

→ Rearranged to LHOEL

3. PlayFair Cipher:

Encryption Mechanism: Encrypt digraphs (pairs of letters) using a 5X5 matrix.

Key Space : Based on 5×5 grid of letters (excluding 'j') → $25! \approx 1.55 \times 10^{25}$

Example : HELLO → digraphs : HE, LX, LO key : Matrix from keyword. MONARCHY

Solution of Ques 09 :

Given,

Affine Cipher encryption function :

$$E(x) = (a \cdot x + b) \bmod 26$$

Where,

$a = 5$

$b = 8$

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 (A=0 to Z=25)

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. Apply the encryption function $E(x) = (5x+8) \bmod 26$

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
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	$(5\times1+8)\%26 = 26$	N
S	18	$(5\times18+8)\%26 = 16$	Q
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 function becomes:

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

2. Apply decryption on ciphertext:

ciphertext: XCBVAHWSVQNQVG

converts letters to numbers:

X=23, C=2, B=1, V=21, A=0, H=7, W=22, S=18, V=21, Q=16, N=13, Q=16, V=21, G=6

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

Letter	y	D(y)	plain
X	2^3	$21 \times (23-8) \% 26 = 3$	D
C	2	$21 \times (2-8) \% 26 = 4$	E
B	1	$21 \times (1-8) \% 26 = 15$	P
V	21	$21 \times (21-8) \% 26 = 19$	T
A	0	$21 \times (0-8) \% 26 = 14$	O

H	7	$21 \times (7-8) \% 26 = 5$	F
W	22	$21 \times (22-8) \% 26 = 8$	I
S	18	$21 \times (18-8) \% 26 = 2$	C
V	21	$21 \times (21-8) \% 26 = 19$	T
Q	16	$21 \times (16-8) \% 26 = 12$	M
N	13	$21 \times (13-8) \% 26 = 1$	B
Q	16	$21 \times (16-8) \% 26 = 12$	S
V	21	$21 \times (21-8) \% 26 = 19$	T
G	6	$21 \times (6-8) \% 26 = 20$	U

Solution of Ques 10:

Here's a simple novel cipher that uses a combination of substitution and permutation techniques. It also uses a custom pseudo-random number generation (PRNG) for added complexity.

Cipher Name: Sub-Perm cipher (SPC)

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

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

RRNG: Custom linear congruential generator (LCG)

Key:

k_1: Integer (used for caesar shift)

k_2: Seed value for PRNG

Block Size: Fixed Block Size

Encryption Process:

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

parameters: $a = 17, c = 43, m = 256$

For each character C_i, compute:

$Shift_i = PRNG(k2) \bmod 26$

$C_i = (C_i + Shift_i + k_1) \bmod 26$

Step 2 : Permutation :

Split the substituted ciphertext into blocks of size N.

Decryption Process :

Step 01: Reverse Permutation

Using the same PRNG and Block size, rearrange the permutation Pattern and reverse it for each block.

Step 02: Reverse Substitution

$Shift_i = PRNG(K_2) \bmod 26$

$C_i = (C_i' - Shift_i - K1 + 26) \bmod 26$

Example:

Input :

plaintext : "HELLO"

K1 = 3 K2 = 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 → 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 02: Permutation (Block size 2)

Split : [PT] [VH] [T_]

Permutation generated : [1, 0]

[PT] → [TP]

[VH] → [HV]

[T_] → [_T] (padding with _)

Final cipherText : "TPHV_T"