Name: Md. shahidul Islam

ID : IT-21024

Session: 2020-21

Assignment on: Eid Holiday Course Review

Q1. Prove fermat's little theorem and use it to compute a^{p-1} mod p for given values of a = 7, p = 13. Then discuss how this theorem is useful in cryptographic algorithm like RSA.

Ans:

If p is a prime and $a \not\equiv 0 \pmod{p}$ then

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

Given that, a = 7, p = 13.

$$\therefore 7^{12} \bmod 13 = ?$$

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

$7^4 = 10^2 = 100 \bmod 13 = 9$

$7^8 = 9^2 = 81 \bmod 13 = 3$

Then, $7^{12} = 7^8 \cdot 7^4 = 3 \cdot 9 = 27 \bmod 13 = 1.$

$\therefore 7^{12} \equiv 1 \pmod{13}$.

Usefulness in cryptography:

It allows efficient computation of modular inverse and powers.

Q2. Euler totient function: compute $\phi(n) = 35, 45, 100$. Prove that if a and n are coprime then $a^{\phi(n)} \equiv 1 \pmod{n}$

Ans:

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

$\phi(45) = \phi(3^2 \cdot 5) = (3^2-3)(5-1) = 6 \cdot 4 = 24$

$\phi(100) = \phi(2^2 \cdot 5^2) = (4-2)(25-5) = 2 \cdot 20 = 40$

Prove: we get from fermat's little theorm $a^{n-1} \equiv 1 \pmod{n}$ when $\gcd(a,n) = 1$

when $\gcd(a,n) = 1$ then all the numbers less than n will be coprime with n and

$$\varphi(n) = n-1$$

So we can write that,

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

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

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 1 \pmod{5}$$

Ans:

Let $N = 60$ and compute:

$N_1 = 60/3 = 20,\ m_1 = 2$ such that $20 m_1 \equiv 1 \pmod{3}$
$\Rightarrow m_1 = 2$

$N_2 = 15,\ m_2 = 3 \Rightarrow 15 m_2 \equiv 1 \bmod 4 \Rightarrow m_2 = 3$

$N_3 = 12,\ m_3 = 3 \Rightarrow 12 m_3 \equiv 1 \bmod 5 \Rightarrow m_3 = 3$

$\therefore x \equiv (2 \cdot 20 \cdot 2) + (3 \cdot 15 \cdot 3) + (1 \cdot 12 \cdot 3)$

$= 251 \ \% \ 60$

$= 11$

$\therefore x \equiv 11 \pmod{60}$

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

Ans:

$561 = 3 \cdot 11 \cdot 17$ (product of distinct prime)

For each prime $p \mid 561$, check $a^{p-1} \equiv 1 \bmod p$ for $a \not\equiv 0 \bmod p$

Also, if $a^{560} \equiv 1 \mod 561$ for all $\gcd(a, 561) = 1$,

then 561 is carmichael.

∴ 561 is a carmichael number.

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

Ans: Try $g = 3$:

Compute $3^k \mod 17$ for $k = 1$ to 16.

values : 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1

covers all nonzero mod 17.

So, 3 is a primitive root mod 17.

p.t.o.

Q 6. Solve the discrete logarithm Problem:

Find x such that $3^x \equiv 13 \mod 17$.

Ans:

compute:

$3^1 = 3$

$3^2 = 9$

$3^3 = 10$

$3^4 = 13$

$\therefore$ Answer $x = 4$

Q 7. Discuss the role of discrete logarithm in the Diffie-Hellman key exchange.

Ans: role:

→ DH is secure because computing $g^{ab} \mod p$ is easy if you know a or b, but hard to compute if only g^a, g^b are known – the discrete Log problem

→ Security depends on infeasibility of computing logs in modular arithmatic.

Q8.

Ans: cipher comparison:

Cipher	key space	Mechanism	Weakness
Substitution	26!	Replace letters	frequency attack
Transposition	factorial of len	Permute order	still freq. same
playfair	25×25 digraph key	Bigram replace	Bigram analysis

Plaintext : "HEllO"

→ Substitution : H → X, E → D

→ Transposition : Swap position, e.g. "HLOEL"

→ Playfair : Use 5×5 grid, encrypt pairs:

HE, LL, OX---.

Q9. Ans:

Given : $a=5$, $b=8$, $E(x)=(5x+8) \bmod 26$

a) Encrypt: "Dept of ICT, MBSTU"

map letters to numbers:

→ $D=3$, $E=4$, ---. $T=19$ etc

Encrypt each letter x :

$$y=(5x+8) \bmod 26$$

b) Decrypt: need $a^{-1} \bmod 26=21$, since $5 \cdot 21=105 \equiv 1 \% 26$

Decryption :

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

Q10. Ans: Design a Novel ciphen.

Example: Substitution + Penmutation

1. Substitution: caesan shift by 3
2. Penmutation: Reverse blocks of 4 letters.

Encrypt "HEllo WORLD"

1. caesan shift: "KHOOR ZRUOG"
2. Bneak into blocks: KHOO RZRU OG
3. Reverse blocks: OOHK URZR GO

Decrypt: Reverse steps

cryptanalysis:

→ Frequency test
→ Block length test
→ known plaintext attack

We can make it mone secune using a PRNG for Caesan key pen block.