IT-21014

Q.1 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 cryptographic algorithms like RSA.

Soln:

If p is prime and $\gcd(a,p)=1$, then

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

proof:

multiply set $1, 2, \ldots, p-1$ by a: $a, 2a, \ldots$

$(p-1)a \bmod p$ is a permutation of Z_p^*

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

$\Rightarrow a^{p-1} \equiv 1 \bmod p$ (proved)

Computing $a^{p-1} \equiv 1 \bmod p$ where $p=13$ and $a=7$.

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

Ans: 1

IT-21014

Use in RSA:

- RSA used : $c = m^e \bmod n$,
  $m = c^d \bmod n$
- Correctness relies on:
  $m^{\phi(n)} \equiv 1 \bmod n$

Fermat's Little theorem underpins RSA encryption decryption by ensuring modular exponentiation behaves predictably

Q.2 Euler Totient Function: Compute $\phi(n)$ for $n = 35, 45, 100$ prove that if a and n are co-prime then $a^{\phi(n)} \equiv 1 \bmod n$.

Soln:

i) $n = 35 = 5 * 7$

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

(ii) $n = 45 = 3^2 * 5$

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

(iii) $n = 100 = 2^2 * 5^2$

$\therefore \phi(100) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 100 * \frac{1}{2} * \frac{4}{5} = 40$

IT-21014

Euler's Theorem - statement and proof:

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

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

proof idea:

- Let $Z_n^* =$ set of integers $< n$ and co-prime to n
- multiply each by $a \Rightarrow$ permutation
- product of elements stays the same.

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

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

(proved)

Q:3

Solve the system of congruences using the CRT and prove that x congruent to n on mod $N = 3 \times 4 \times 6 = 60$

$x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 4$, $x \equiv 1 \bmod 6$

Soln: Given,

$$x \equiv 2 \bmod 3$$

$$x \equiv 3 \bmod 4$$

IT-21014

$x \equiv 1 \mod 5$ $\quad N = 3 \times 4 \times 5 = 60$

Step-1: Compute components

Let: $N_1 = 60/3 = 20$

$N_2 = 60/4 = 15$

$N_3 = 60/5 = 12$

Now find modular inverse:

$20y \equiv 1 \mod 3 \Rightarrow y = 2$

$15y \equiv 1 \mod 4 \Rightarrow y = 3$

$12y \equiv 1 \mod 5 \Rightarrow y = 3$

Step-2: Now apply CRT formula

$x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \mod 60$

$\Rightarrow x = 80 + 135 + 144$

$\Rightarrow x = 359 \mod 60$

$\therefore x = 59 \mod 60$

Ans.

IT-21014

Q:4:

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

Korselt's criterion:

check if for each prime p, $p-1 \mid 561-1$

$\rightarrow 3-1 = 2 \mid 560$

$\rightarrow 11-1 = 10 \mid 560$

$\rightarrow 17-1 = 16 \mid 560$

all conditions satisfied

Fermates Test

check $a^{560} \equiv 1 \bmod 561$ for some $\gcd(a, 561) = 1$.

Try $a = 2$,

$2^{560} \equiv 1 \bmod 561$ which is true.

This holds for many bases a, so, 561 passes Fermat's test.

Thus, 561 is a carmichael number.

IT-21014

Q.5: $\phi(17) = 16 \rightarrow$ we want g such that:

$g^k \not\equiv 1 \bmod 17$ for any $k < 16$

Let's try: $g = 3$, test orders via prime divisors of 16: 2, 4, 8

$\rightarrow 3^2 = 9 \not\equiv 1 \bmod 17$

$\rightarrow 3^4 = 81 \equiv 13 \not\equiv 1 \bmod 17$

$\rightarrow 3^8 = 13^2 = 169 \equiv -1 \bmod 17$

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

$\therefore$ it passes all. so, 3 is a primitive root of modulo 17.

Ans: 3 is a generator of $\mathbb{Z}_{17}^*$

IT-21014

Q.6:

Soln: lets try sucessive powers 3 modulo 17

if $x=1$, $3^1 \bmod 17 = 3 \bmod 17 = 3$

if $x=2$, $3^2 \bmod 17 = 9 \bmod 17 = 9$

if $x=3$, $3^3 \bmod 17 = 27 \bmod 17 = 10$

if $x=4$, $3^4 \bmod 17 = 81 \bmod 17 = 13$

$\therefore 3^4 \equiv 13 \bmod 17$

Ans: $x=4$

Q.7:

Soln:

The Diffie-Hellmen key Exchange lets two people share a secret key over a public channel.

It works like this.

IT-21014

→ Each person chooses a private number.

→ They use a shared base (g) and prime (p) to compute their public values.

→ They exchange public values and use them to calculate the same secret key.

Security depends on the Discrete Logarithm problem:

It's very hard to find a if you only know g, p and $g^a \bmod p$.

That's why ~~attackers~~ can't find the the secret key, even if they see the public values.

IT-21014

Q:8:

1. **Substitution cipher**

→ Encryption Method Replaces each letter with another letter

→ Key Space very large

Example:

Suppose key : A→D, B→E, ----, H→K, E→H, L→O, O→R

HELLO → KHOOR

2. **Transposition cipher:**

→ Encryption method Rearranges the letters positions

→ Key space depends on block size

Example:

Swap position in pair (block size = 2)

HELLO → EHLLO → EOLLH

IT-21014

3. <u>playfair cipher</u>

key square (5x5) with no repeating letter.

- pair up: HELLO → HE LX LO
- use playfair rules to encrypt each pair.
- Example: HE → MP , LX → ZB

LO → QR

HELLO → MPZBQR

IT-21014

Q.9: Encryption:

Pain text : DEPT OF ICT MBSTU

Numeric : 3 4 15 19 14 5 8 2 19 12 1 18 19 20

Encrypt $E(x) = (5x+8) \bmod 26$

plain x	3	4	15	19	14	5	8	2	19	12	1	18	19	20
5x+8	23	28→2	83→5	103→25	78→20	33→7	48→22	18	103→25	68→16	13	98→20	103→25	208→4
cipher	X	C	F	Z	A	H	W	S	Z	Q	N	V	Z	E

∴ cipher text : XCFZAHWSZQNVZE

Decryption:

Compute $a^{-1} \bmod 26$ since

$5 \cdot 21 = 105 \equiv 1$, $a^{-1} = 21$

IT-21014

→ Decrypt $D(y) = 21 \cdot (y-8) \bmod 26$.
Applying to each cipher letter recovers:

Cipher	23	2	5	25	0	7	22	18	25	16	13	20	25	4
y-8	15	-6→20	-3→23	17	-8→18	-1→25	14	10	17	8	5	12	17	-4→22
26 mod	3	4	15	19	14	5	8	2	19	12	1	18	19	20
plain	D	E	P	T	O	F	I	C	T	M	B	S	T	U

Recovered: DEPT OF ICT MBSTU

IT-21014

Q.10

Prime Mix cipher (Substitution + permutation)

Encryption process:

Step: 1: substitution

- Use prime numbers [2, 3, 5, 7] cyclically.
- Shift each letter forward by the corresponding prime.

Step: 2

→ After substitution, reverse every block of 4 letters (or full text if less than 4)

Example:

plain text : HELLO

primes : 2, 3, 5, 7, 2

- After substitution:

H+2 = J , E+3 = H , L+5 = Q

L+7 = S , O+2 = Q

→ JHQSQ

- After permutation - (reverse 4-letter block) : SQHJQ

Ciphere text : SQHJQ

Decryption:

Step-1 : Reverse the permutation

Reverse back the block of 4 letters

IT-21014

Step-2:

- Use the same prime sequence to shift letters backward.

Analysis:

→ It stronger than ~~caser~~ caeser

→ Still vulnerable to frequency analysis if message is long

→ PRNG is simple and predictable if known.