Maths Assignment - I

Name: S. Jaiwanth
Roll No: 12201032501 (12)
Section: B25 CSE (CS)

1) Explain Euclidean Algorithm. Write the g.c.d(1547, 560) as linear combination of 1547 & 560

Sol:

In mathematics, Euclid's algorithm is an efficient method for computing the Greatest common Divisor of two integers, the largest number that divides them both without a remainder. It is named after the ancient Greek mathematician Euclid.

gcd(1547, 560)

$1547 = 2(560) + 427$

$560 = 1(427) + 133$

$427 = 3(133) + 28$

$133 = 4(28) + 21$

$28 = 1(21) + 7$

$\therefore 7 | 21$; $\therefore$ gcd(1547, 560) is 7.

∎

2) Encrypt the message "meet me" using the Hill Cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations & result.

Sol: For the key, choose a 2×2 matrix with entries in Z_{26}

$$A = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

→ Next convert the plaintext into pairs of numbers from Z_{26}

→ me|et|me|at.... cl|oc|kz

→ 13,5|5,20|13,5|1,20|... 3,12|15,3|11,0

→ Now convert the plain text to numbers to cipher text numbers, using key.

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 5 \end{pmatrix} \pmod{26}$$

$$= \begin{bmatrix} 117 + 20 \\ 65 + 35 \end{bmatrix} \pmod{26}$$

$$= \begin{pmatrix} 137 \\ 100 \end{pmatrix} \pmod{26}$$

$$= \begin{pmatrix} 7 \\ 22 \end{pmatrix} \pmod{26}$$

→ Thus, "me" is encrypted as "HW"

$$\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 5 \\ 20 \end{pmatrix} \pmod{26}$$

$$= \begin{bmatrix} 45 + 80 \\ 25 + 140 \end{bmatrix} \pmod{26}$$

$$= \begin{pmatrix} 125 \\ 165 \end{pmatrix} \pmod{26}$$

$$= \begin{pmatrix} 21 \\ 9 \end{pmatrix} \pmod{26}$$

et $= \begin{bmatrix} 4 \\ 19 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \end{bmatrix} \pmod{26}$

$= 8 \begin{bmatrix} 8 \\ 25 \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \end{bmatrix}$

2nd pair = me $= \begin{bmatrix} 12 \\ 4 \end{bmatrix}$

me $= \begin{bmatrix} 4 \\ k \end{bmatrix}$

∴ Cipher text for 'meet me' = 'ik ix ik'

3) Given $\gcd(a, n) = 1$

(a) $x^2 = a \pmod{n}$ has a solution

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a quadratic residue } (\bmod p) \\ -1 & \text{if } a \text{ is a quad non-residue } (\bmod p) \end{cases}$$

If a is a quad residue, then there exists an x, such that $x^2 = a \pmod{n}$

Taking power in $\left[\frac{a}{n}\right) = a^{\frac{n-1}{2}} \bmod(n)$

$$1 = x^{n-1} = a^{\frac{n-1}{2}} \pmod{n} = \frac{a}{n}$$

$$\therefore \left(\frac{a}{n}\right) = 1$$

(b) Since $\left(\frac{a}{n}\right) = 1$

$a^{n-1} = 1$ (by Fermat's Theorem)

So $a^{\frac{n-1}{2}} = \sqrt{1} \pmod{p}$

$a^{\frac{n-1}{2}} = 1 \pmod{p}$ or $(-1) \pmod{p}$

∴ Hence if $\left(\frac{a}{n}\right) = 1$ i.e., $x^2 = a \pmod{n}$ has a solution then it has more than one solution.