Problem You intercept

GFPY J P_ X ? U Y X ST L A D P L W

you know:

1) 29-letter alphabet was used

A = 0, B = 1, ..., Z = 25, _ = 26, ? = 27, ! = 28

2) An enciphering function of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{mod } 29$$

3) Last five letters of plaintext are

KARLA

Decipher.

Soln Need to find the matrix $\underline{A}$. (2×2)

$$\begin{pmatrix} A \\ R \end{pmatrix} \longmapsto \underline{A}\begin{pmatrix} A \\ R \end{pmatrix} = \begin{pmatrix} D \\ P \end{pmatrix}$$

$$\begin{pmatrix} L \\ A \end{pmatrix} \longmapsto \underline{A}\begin{pmatrix} L \\ A \end{pmatrix} = \begin{pmatrix} L \\ W \end{pmatrix}$$

$$\underline{A}\begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \end{pmatrix} \quad \text{mod } 29$$

$$\underline{A}\begin{pmatrix} 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 11 \\ 22 \end{pmatrix} \quad \text{mod } 29$$

$$\underline{A}\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix} \quad \text{mod } 29$$

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} = \underline{A}^{-1}\begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix}\begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} = \underline{A}^{-1} \quad \text{mod } 29$$

$$\underline{X} = \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}$$

$$\underline{X}^{-1} = (3 \cdot 22 - 15 \cdot 11)^{-1} \begin{pmatrix} 22 & -11 \\ -15 & 3 \end{pmatrix} \mod 29 \quad (*)$$

$$\det(x) = 3 \cdot 22 - 15 \cdot 11 \mod 29$$

$$\equiv -3 \cdot 7 - 165 \mod 29$$

$$\equiv -21 - 165 \mod 29$$

$$\equiv 8 - 165 \mod 29$$

$$\equiv -157 \mod 29$$

$$\equiv -12 \mod 29$$

$$\equiv 17$$

$17^{-1} = ? \mod 29$

$29 = 17 + 12$

$17 = 12 + 5$

$12 = 2 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$$1 = 5 - 2 \cdot 2$$

$$= 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12$$

$$= 5(17 - 12) - 2 \cdot 12 = 5 \cdot 17 - 7 \cdot 12$$

$$= 5 \cdot 17 - 7(29 - 17) = 12 \cdot 17 - 7 \cdot 29$$

$$\equiv 12 \cdot 17 \pmod{29}$$

So $\underline{17^{-1} \equiv 12 \pmod{29}}$

So from (*)

$$\underline{X}^{-1} = 12 \begin{pmatrix} 22 & -11 \\ -15 & 3 \end{pmatrix} \pmod{29}$$

$$\underline{A}^{-1} = 12 \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 22 & -11 \\ -15 & 3 \end{pmatrix} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \pmod{29}$$

Plaintext:

$$\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15 & 9 & \cdots \\ 5 & 24 & 15 & \end{pmatrix}$$

$$= \begin{pmatrix} S & R & K & \\ T & I & E & \cdots \end{pmatrix}$$

= STRIKE! AT NOON, KARLA