Problem You intercept

GFPYJP_X?UY XSTLADPLW

and you know:

1) 29-letter alphabet was used

A=0, B=1, C=2, ..., Z=25, _=26, ?=27, !=28

2) An enciphering function of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\underline{A}} \begin{pmatrix} x \\ y \end{pmatrix} + \underbrace{\begin{pmatrix} e \\ f \end{pmatrix}}_{\underline{B}}$$

where

$$\underline{B} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

3) The last five letters of plaintext are:

KARLA

Decipher the message.

Soln

GF .... LADPLW (ciphertext)

....KARLA (plaintext)

$\begin{pmatrix} G \\ F \end{pmatrix}$ ..... $\begin{pmatrix} L \\ A \end{pmatrix}$ $\begin{pmatrix} D \\ P \end{pmatrix}$ $\begin{pmatrix} L \\ W \end{pmatrix}$

$\begin{pmatrix} K \end{pmatrix}$ $\begin{pmatrix} A \\ R \end{pmatrix}$ $\begin{pmatrix} L \\ A \end{pmatrix}$

To decipher we need the deciphering function

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \underline{A}^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\underline{A} \begin{pmatrix} A \\ R \end{pmatrix} = \begin{pmatrix} D \\ P \end{pmatrix} \qquad \underline{A} \begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \end{pmatrix}$$

$$\underline{A} \begin{pmatrix} L \\ A \end{pmatrix} = \begin{pmatrix} L \\ W \end{pmatrix} \qquad \underline{A} \begin{pmatrix} 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 11 \\ 22 \end{pmatrix}$$

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

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

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

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

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

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

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

$3\cdot 22 - 15\cdot 11 \pmod{29}$

$= 3(-7) - 15\cdot 11$

$\equiv -21 - 165$

$\equiv 8 - 20$

$\equiv 8 + 9$

$\equiv 17$

need $17^{-1} \pmod{29}$

Need $17^{-1} \mod 29$

$29 = 17 + 12$ ✓

$17 = 12 + 5$ ✓

$12 = 2 \cdot 5 + 2$ ✓

$5 = 2 \cdot 2 + 1$ — gcd(17, 29) ✓

$1 = 5 - 2 \cdot 2$

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

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

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

$\equiv 12 \cdot 17$

$$17^{-1} \equiv 12 \mod 29$$

From (**)

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

$$= \begin{pmatrix} 3 & -16 \\ -6 & 7 \end{pmatrix}$$

$-7 \cdot 12$
$= -84$
$= -26$
$= 3$

From (*)

$$\underline{A}^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & -16 \\ -6 & 7 \end{pmatrix} \mod 29$$

$$\underline{A}^{-1} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}$$

To decipher :

$$\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} G & P & I & - & ? & Y & S & C & D & L \\ F & Y & P & X & U & X & T & A & P & W \end{pmatrix}$$

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

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

= STRIKE - - - - - -

22.6 + 18.5
= -7.6 + -11.5
= -42 - 55
= -13 - 26 = -16 ≡ 19

21.6 + 19.5
-8.6 + -10.5
-48 - 50
-18 - 20 = -38 ≡ -9 ≡ 20