Example Use the enciphering function

$$f_E : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \underbrace{\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}}_{\alpha} \begin{pmatrix} x \\ y \end{pmatrix} + \underbrace{\begin{pmatrix} 0 \\ 0 \end{pmatrix}}_{\beta}$$

to encipher the plaintext

NOANSWER

over a 26-letter alphabet with $A \sim 0, B \sim 1, \ldots, Z \sim 25$.

Soln

plaintext

$$\begin{pmatrix} N \\ O \end{pmatrix} \begin{pmatrix} A \\ N \end{pmatrix} \begin{pmatrix} S \\ W \end{pmatrix} \begin{pmatrix} E \\ R \end{pmatrix}$$

$$\begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

ciphertext

$$\begin{pmatrix} 16 \\ 21 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{pmatrix} \ \\ \ \end{pmatrix} \begin{pmatrix} \ \\ \ \end{pmatrix}$$

$$\begin{pmatrix} Q \\ V \end{pmatrix} \begin{pmatrix} N \\ A \end{pmatrix} \begin{pmatrix} \ \\ \ \end{pmatrix} \begin{pmatrix} \ \\ \ \end{pmatrix}$$

ciphertext: QVNA....

Problem You intercept

GFPYJP_X?UYXSTLADPLW

You know:

1) 24-letter alphabet was used

$A=0, B=1, \ldots, Z=25, \_=26, ?=27, !=28$

2) An enciphering function of the form

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

where

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

3) The last five letters of plaintext are

KARLA

Decipher the message.

GA ..... LADPLW (ciphertext)

KARLA (plaintext)

$\begin{pmatrix} G \\ A \end{pmatrix}\begin{pmatrix} P \\ Y \end{pmatrix}\cdots \quad \begin{pmatrix} L \\ A \end{pmatrix}\begin{pmatrix} D \\ P \end{pmatrix}\begin{pmatrix} L \\ W \end{pmatrix}$

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

To decipher we need the deciphering function

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

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

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

$$\underline{A}\begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \end{pmatrix}$$

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

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

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

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

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

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

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

$$\underline{M}^{-1} = (3.22 - 15.11)^{-1}\begin{pmatrix}22 & -11\\ -15 & 3\end{pmatrix} \quad \text{Mod } 29 \qquad (**)$$

$$3 \cdot 22 - 15 \cdot 11$$

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

$$\equiv -21 - 165$$

$$\equiv 8 - 20$$

$$\equiv 8 + 9$$

$$\equiv 17 \mod 29$$

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

$$29 = 17 + 12$$

$$17 = 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + \textcircled{1} = \gcd(17, 29)$$

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

$$1 = 5 - 2(12 - 2 \cdot 5)$$

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

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

$$= 5 \cdot 17 - 7 \cdot 12$$

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

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

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

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

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

From (*)

$$\underline{A}^{-1} = \begin{pmatrix} 0 & 4 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & -16 \\ -6 & 7 \end{pmatrix}$$

$$\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \quad \text{mod } 29$$

To decypher :

$$\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} G & P & J & - & ? & Y & S & < & D & L \\ A & Y & P & \checkmark & \cup & X & T & A & P & W \end{pmatrix}$$

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

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

Rough work

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 13 \\ 14 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix}$$

13

$8 . 14 \quad 7.2.2.\underline{14}$

2

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 0 \\ 13 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix}$$

116

14 13 0