Example Use the encipherment function

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

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

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

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

Ciphertext: QVNA....

Problem You intercept

GFPYJP_X?UYXSTLADPLW

you know:

1) 29-letter alphabet was used

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

2) An enciphering function of the form

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

where

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

3) The last five letter of plaintext are

KARLA

Decipher the message.

GF ..... LADPLW (ciphertext)

KARLA (plaintext)

$\binom{G}{F}, \binom{P}{Y} \cdots \binom{L}{A}, \binom{D}{P}, \binom{L}{W}$

$\binom{K}{\ } \binom{A}{R} \binom{L}{A}$

To decipher we need the deciphering function

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

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

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

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

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

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

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

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

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

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

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

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

(4)

$3.22 - 15.11$

$\equiv 3(-7) - 15.11$

$\equiv -21 - 165$

$\equiv 8 - 20$

$\equiv 8 + 9$

$\equiv 17$

Need to find $17^{-1} \bmod 29$.

$29 = 1.17 + 12$

$17 = 1.12 + 5$

$12 = 2.5 + 2$

$5 = 2.2 + 1$ $= \gcd(17, 29)$

(5)

$$1 = 5 - 2.2$$

$$= 5 - 2(12 - 2.5)$$

$$= 5.5 - 2.12$$

$$= 5(17 - 12) - 2.12$$

$$= 5.17 - 7.12$$

$$= 5.17 - 7(29 - 17)$$

$$= 12.17 - 7.29$$

$$\equiv 12.17 \pmod{29}$$

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

From (**)

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

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

From (*)

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

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

To decipher

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

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

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

$$\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 18 \\ 19 \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$$

$-40 - 50 \quad = \quad -98$

$= -11$

$= 18$

$-42 - 55 \quad = \quad -97$

$= -10$

$= 19$

Rough work