example:

$$A = \begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix} \to A^{-1} = (1\cdot 7 - 5\cdot 4)^{-1} \begin{pmatrix} 7 & -4 \\ -5 & 1 \end{pmatrix} = -\frac{1}{13}\begin{pmatrix} 7 & -4 \\ -5 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -\frac{7}{13} & \frac{4}{13} \\ \frac{5}{13} & -\frac{1}{13} \end{pmatrix}$$

APPLICATION:

Affine matrix cryptosystems

Suppose we wish to encipher the following → HELLO_WORLD_

→ 2-letter message units

$\begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ L \end{pmatrix}, \begin{pmatrix} O \\ \_ \end{pmatrix}, \begin{pmatrix} W \\ O \end{pmatrix}, \begin{pmatrix} R \\ L \end{pmatrix}, \begin{pmatrix} D \\ \_ \end{pmatrix}$ ← column matrices

using a correspondance between letters and numbers where $A \leftrightarrow 0$, $B \leftrightarrow 1$, … $Z \leftrightarrow 25$, $\_ \leftrightarrow 26$

$\begin{pmatrix} 4 \\ 5 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix} \begin{pmatrix} \; \end{pmatrix} \begin{pmatrix} \; \end{pmatrix} \begin{pmatrix} \; \end{pmatrix} \begin{pmatrix} \; \end{pmatrix}$ sequence of matrices.

For an enciphering program, we could choose some matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries $a, b, c, d \in \mathbb{Z}_{27}$

and $B = \begin{pmatrix} e \\ f \end{pmatrix}$, with $e, f \in \mathbb{Z}_{27}$

We could then use the following:

$$f_E : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A\begin{pmatrix} x \\ y \end{pmatrix} + B, \qquad f_D : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A^{-1}\left(\begin{pmatrix} x \\ y \end{pmatrix} - B\right) = A^{-1}\begin{pmatrix} x \\ y \end{pmatrix} - A^{-1}B$$

→ A must be invertible

PROBLEM:

You intercept

GFPYJP_X?UVXSTLADPLW

And you know:

1) 29-letter alphabet was used

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

2) Affine enciphering function was used, of the form

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

// 2-letter message units.

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

3) The last five letters of plaintext are the user's name, KARLA

DECIPHER

Sol^{n}

GFPY ... S $\underline{\text{TLADPLW}}$

$\uparrow\ \uparrow\ \uparrow\ \uparrow\ \uparrow$

K A R L A

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

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

To decipher, we need f_D

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A^{-1} \begin{pmatrix} x \\ y \end{pmatrix} + A^{-1} B \rightarrow A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

// cause $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, so $A^{-1} B$ = zero matrix

$$A \begin{pmatrix} L \\ A \end{pmatrix} = \begin{pmatrix} L \\ W \end{pmatrix} \quad \Bigg\| \quad A \begin{pmatrix} 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 11 \\ 22 \end{pmatrix}$$

$$A \begin{pmatrix} A \\ R \end{pmatrix} = \begin{pmatrix} D \\ P \end{pmatrix} \quad \Bigg\| \quad A \begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \end{pmatrix}$$

$$\left[A \begin{pmatrix} 11 & 0 \\ 0 & 17 \end{pmatrix} = \begin{pmatrix} 11 & 3 \\ 22 & 15 \end{pmatrix} \mod 29 \right]$$

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

// $A^{-1} A$ = identity

identity · anything = that matrix

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

$$\left[\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} = A^{-1} \mod 29 \right] \ (*)$$

// multiply both sides by the inverse of $\begin{pmatrix} 11 & 3 \\ 22 & 15 \end{pmatrix}$

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

$$m^{-1} = (3 \cdot 22 - 11 \cdot 15)^{-1} \begin{pmatrix} 22 & -11 \\ -15 & 3 \end{pmatrix}$$

$= 3 \cdot 22 - 11 \cdot 15 \mod 29$

$= 3(-7) - 165 \mod 29$

$= -21 - 165 \mod 29$

$= 8 - 20 \mod 29$

$= 8 + 9 \mod 29$

$= 17 \mod 29$

$17^{-1} = 12 \mod 29$ (euclidean)

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

$$m^{-1} = \begin{pmatrix} 3 & -16 \\ -6 & 7 \end{pmatrix}$$

from $(*)$

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & -16 \\ -6 & 7 \end{pmatrix} = \left[A^{-1} = \begin{pmatrix} -8 & 19 \\ 22 & 18 \end{pmatrix} \right]$$

$$A^{-1} \begin{pmatrix} G \\ F \end{pmatrix} = A^{-1} \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} G & P & J & \_ & ? & V & S & L & D & L \\ F & Y & P & X & U & X & T & A & P & W \end{pmatrix}$$

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