Recall

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -1 & 0 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 5 \\ 3 & -4 \end{pmatrix}$$

2×3 $\quad$ 3×2 $\quad$ 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

2×2 $\quad$ 2×2

$$= (ad-bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So, if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then

$$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (ad-bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

So A^{-1} exists if (and only if) the number

$ad-bc$ is invertible.

Remark Any affine cryptosystem

$$X \longmapsto \alpha X + \beta$$

on single letter message units over an alphabet of N ($=26$) letters is easily broken.

- E is the most frequent letter in English, followed by T. So frequency analysis can be used. E get enciphered as the most frequent letter of ciphertext, T ....

- Also, there are not too many possible enciphering keys. There are

$$N\phi(N)$$ such keys.

All keys could be tried.

Affine matrix cryptosystems

To counter the above two weaknesses we could break plaintext into message units (x, y) of length 2. There are many contenders for the most frequent pair (x, y) in English.

We would encipher using

$$f_E: \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A\begin{pmatrix} x \\ y \end{pmatrix} + B$$

where

A denotes a fixed invertible 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = A$

B denotes a fixed vector, $B = \begin{pmatrix} e \\ t \end{pmatrix}$

and (A, B) is the enciphering key.

A must be invertible mod N,

N = length of alphabet.

The deciphering function is

$$f_D : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A^{-1}\left(\begin{pmatrix} x \\ y \end{pmatrix} - B\right)$$

Example use the enciphering function

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

to encipher the plaintext

NOANSWER

over a 26-letter alphabet

A = 0, ..., Z = 25.

Soln

plaintext

$\binom{N}{O}\binom{A}{N}\binom{S}{W}\binom{E}{R}$

$\binom{13}{14}\binom{0}{13}\binom{18}{22}\binom{4}{17}$

ciphertext

$\binom{16}{21}\binom{13}{0}\binom{\ }{\ }\binom{\ }{\ }$ etc

$\binom{Q}{V}\binom{N}{A}\binom{\ }{\ }\binom{\ }{\ }$

ciphertext

QVNA---- etc

Problem You intercept

GFPY J P_ X ? U Y X S T 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

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

3) Last five letters of plaintext are

K A R L A

Decipher.