Last week:

Frequency analysis can be used to break affine cryptosystems with single letter message units. This is because we know the most frequent letter in English is E, followed next by T.

Affine matrix cryptosystems

To counter frequency analysis we could break the plaintext into message units (x, y) of length 2, and then use an enciphering function

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

where

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

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

$$\underline{A}^{-1} = 12 \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 22 & -11 \\ -15 & 3 \end{pmatrix} \mod 29$$

$$= \begin{pmatrix} 21 & 19 \\ 22 & 13 \end{pmatrix}.$$

Plaintext is

$$\begin{pmatrix} 21 & 19 \\ 22 & 13 \end{pmatrix} \begin{pmatrix} 6 & 15 & 4 & \cdots \\ 5 & 24 & 15 & \end{pmatrix}$$

etc.

Example Use the enciphering function

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

to encipher the plaintext

NO ANSWER

over the 26-letter alphabet

A = 0, B = 1, ..., Z = 25.

Soln

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

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

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

B denotes a fixed vector

(A, B) is the enciphering key.

A must be invertible mod N where N = length of alphabet.

The deciphering function is

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

Let's now find $21^{-1} \bmod 26$.

Note: $\gcd(21, 26) = 1$

$$26 = 1 \cdot 21 + 5$$

$$21 = 4 \cdot 5 + 1$$

So

$$1 = 21 - 4 \cdot 5$$

$$= 21 - 4(26 - 21)$$

$$= 5 \cdot 21 - 4 \cdot 26$$

$$\equiv 5 \cdot 21 \pmod{26}$$

Then $21^{-1} = 5 \pmod{26}$.

So

$$A^{-1} = 5 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}$$