Hill Cipher
Security in Computing
Ratan Guha

The encryption key is an nxn matrix with an inverse mod 26, where n is the block size.

Example: Assume n=2.
We determine ciphertext for two character at a time

$$K = \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \text{ to encrypt and } K^{-1} \text{ to decrypt}$$

Encrypt a plaintext: MATH.
Group the plaintext in pairs: "MA" and "TH"

Convert each letter to its numerical equivalent, mod 26, and write it in a nx1 matrix as follows:

$$\begin{pmatrix} 12 \\ 0 \end{pmatrix} \text{ stands for "MA"}$$

Multiply the encryption key by the plaintext and reduce mod 26 to get the ciphertext:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 36 \\ 72 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix} \bmod 26$$

Ciphertext: KU.

Here is the encryption of "TH":

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 64 \\ 149 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 19 \end{pmatrix} \bmod 26,$$

Ciphertext: MT.
Hence Plaintext: math Ciphertext: KUMT