Hill Cipher

Tuesday, September 13, 2022 10:01 PM

Last Time: ADFGVX (quite a bit more complex - substitution, and transposition)

Hill is more mathematical. It uses a matrix as a key

key is going to be a n by n matrix, our example I'll use 2 x 2.

$$key = \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \quad n = 2$$

Hill cipher we break the plaintext into n character blocks

Encrypt: "MATH" --> "MA" "TH"

If there is leftover room, add any garbage characters you want to.

To encrypt

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \times \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 3\times12+1\times0 \\ 6\times12+5\times0 \end{pmatrix}$$

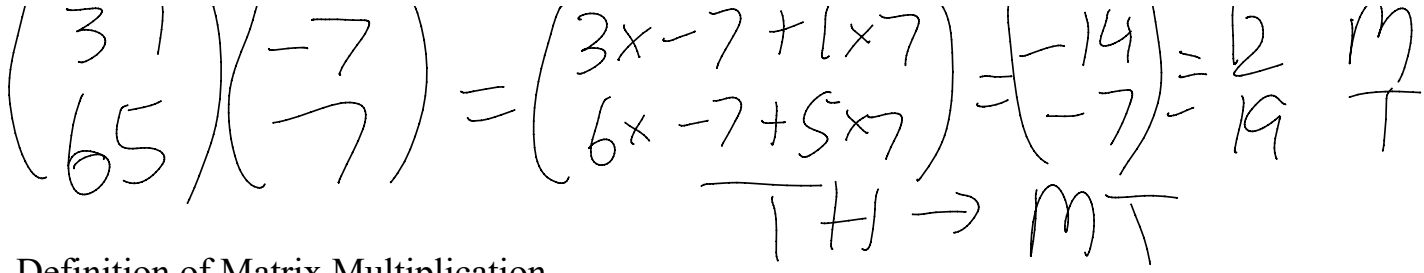
$$= \begin{pmatrix} 36 \\ 72 \end{pmatrix}$$

$$19 \equiv -7 \bmod 26$$

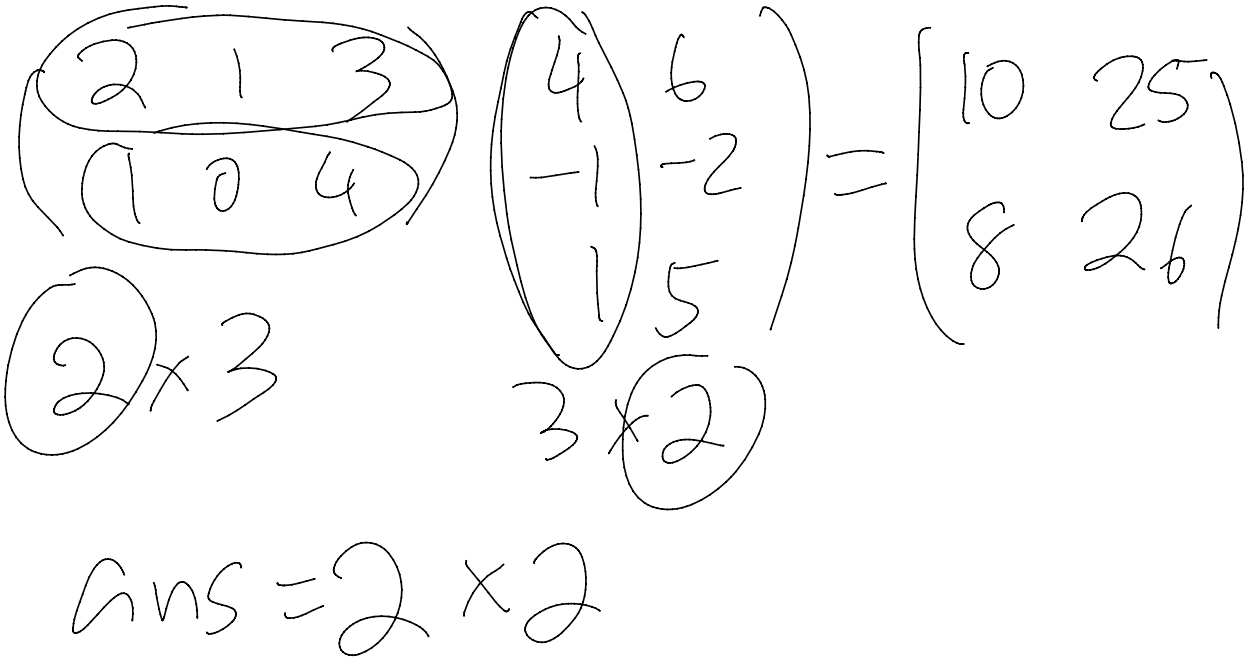
$$\equiv \begin{pmatrix} 10 \\ 20 \end{pmatrix} \bmod 26$$

MA → KU

$$\begin{pmatrix} 3 & 1 \\ -7 & \end{pmatrix} \quad (3\times-7+1\times7) \quad (-14) = 12 \quad M$$



Definition of Matrix Multiplication



entry in row I, column J of the answer is the "dot product"
of row I of the first matrix and column J of the second matrix.

row 1 col1: 2 x 4 + 1 x (-1) + 3 x 1 = 10
row 1 col2: 2 x 6 + 1 x (-2) + 3 x 5 = 25
row 2 col1: 1 x 4 + 0 x (-1) + 4 x 1 = 8
row 2 col 2: 1 x 6 + 0 x (-2) + 4 x 5 = 26

Just did MATH plaintext encrypts to "KUMT"

How to decrypt?

What are our valid keys?

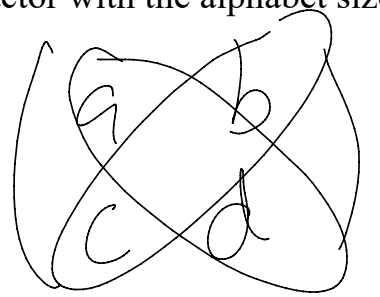
To decrypt, we'll have to use the inverse of the matrix (under mod).
A key is valid if and only if the inverse of the matrix exists.

All square matrices have something called a determinant.

In real numbers, a matrix is invertible, if and only if the determinant is
NOT 0.

In our case, a matrix is invertible, if and only if the determinant does NOT share a common factor with the alphabet size. (Really similar to affine cipher.)

2×2



$$\text{determinant} = ad - bc$$

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

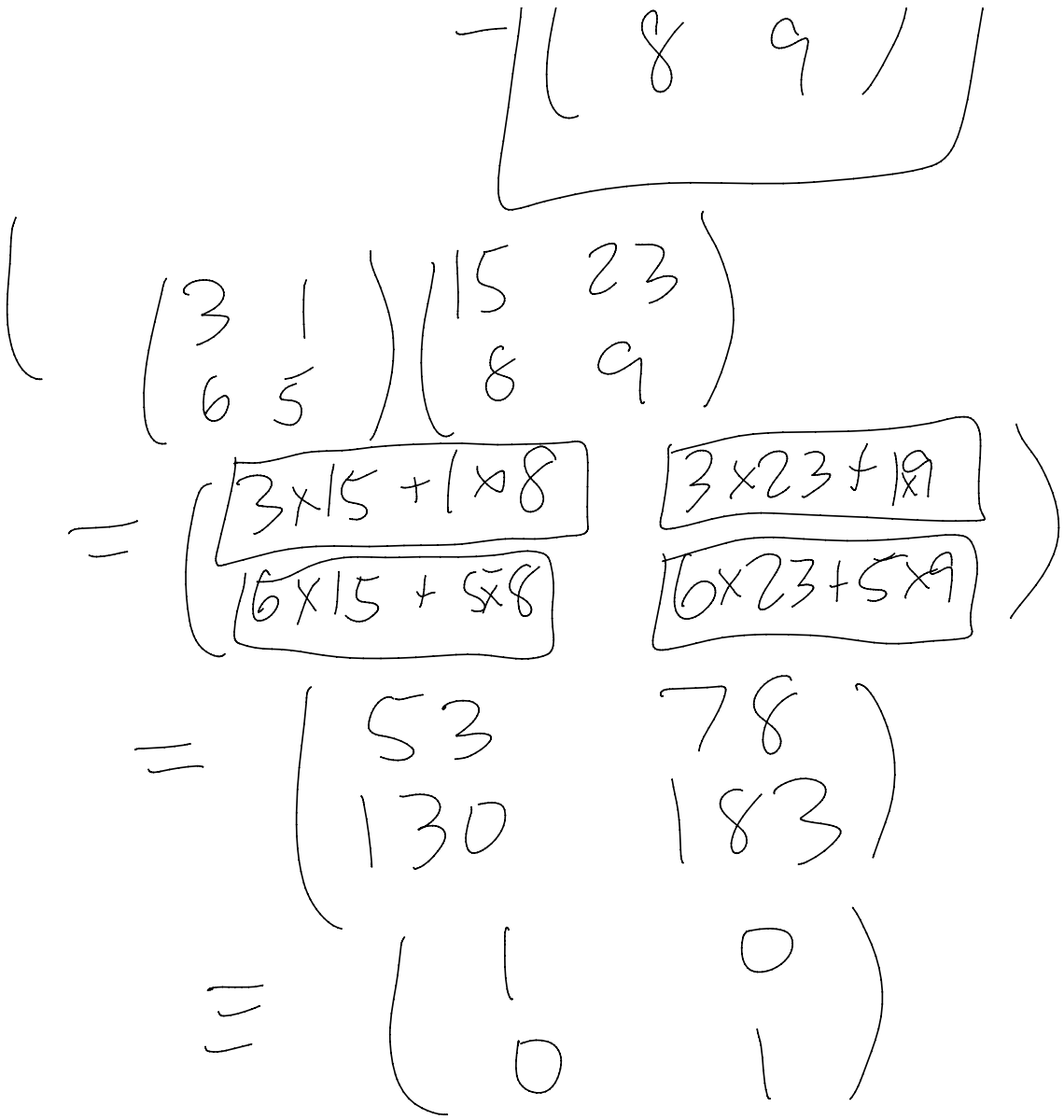
$$\begin{pmatrix} 9 & 1 \\ 6 & 5 \end{pmatrix}^{-1} = (15-6)^{-1} \begin{pmatrix} 5 & -1 \\ -6 & 3 \end{pmatrix}$$

$$= (9^{-1} \bmod 26) \begin{pmatrix} 5 & -1 \\ -6 & 3 \end{pmatrix}$$

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

$$= \begin{pmatrix} 15 & -3 \\ -18 & 9 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}$$



To decrypt, take the ciphertext, in this case, "KUMT", break it into pairs (since n = 2), and multiply the decryption key (inverse matrix) by each pair.

$$\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 10 \\ 20 \end{pmatrix} =$$

$$\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 12 \\ 19 \end{pmatrix} =$$

Left as exercise for you to verify that you get "MATH" back.

What's happening is that each block of n characters maps to a different block of n characters, so it's substitution of blocks, so to speak. If you think about the process of matrix multiplication, a single letter in the plaintext affects multiple letters in the ciphertext.

Cryptanalysis

If you have some matching plaintext ciphertext pairs, you can set up equations…so if we knew that MA --> KU

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$$

$$\begin{aligned} a12 &= 10 \mod 26 \\ c12 &= 20 \mod 26 \end{aligned}$$

reduces possible values we need to search through.