Hill cipher

Wednesday, September 16, 2020 11:36 AM

Matrix based.

A matrix is just a grid of numbers with some number of rows and some columns.

Operations such as addition, subtraction and multiplication are defined for matrices.

$$\begin{pmatrix} 2 & 3 & 1 \\ 6 & -1 & 5 \end{pmatrix} + \begin{pmatrix} 6 & 9 & 2 \\ 1 & 5 & 7 \end{pmatrix} = \begin{pmatrix} 8 & 12 & 3 \\ 7 & 4 & 12 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 & 1 \\ 6 & -1 & 5 \end{pmatrix} - \begin{pmatrix} 6 & 9 & 2 \\ 1 & 5 & 7 \end{pmatrix} = \begin{pmatrix} -4 & -6 & -1 \\ 5 & -6 & -2 \end{pmatrix}$$

For multiplication, the number of columns in the first matrix must equal the number of rows in the second matrix.

For the Hill cipher, we always use n by n matrices, which are called square matrices. Naturally you can always multiply together two square matrices.

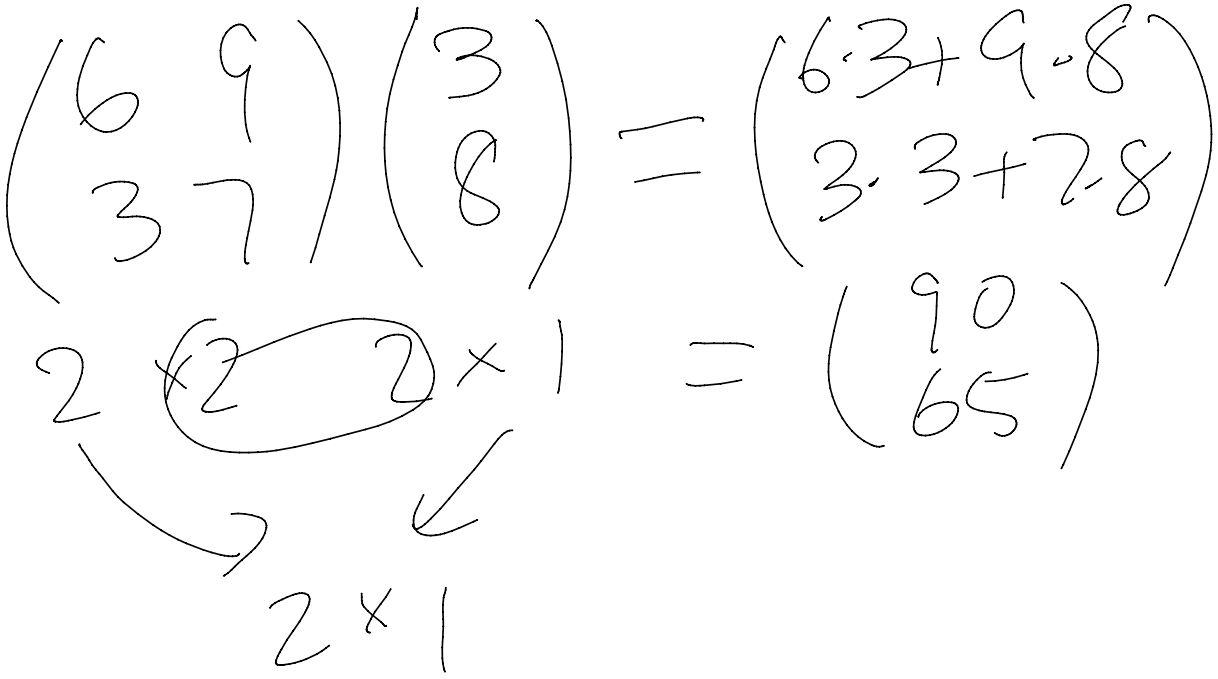
$$\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 8 & 2 \end{pmatrix} = \begin{pmatrix} 2\cdot 4 + 6\cdot 8 & 2\cdot 1 + 6\cdot 2 \\ 3\cdot 4 + 5\cdot 8 & 3\cdot 1 + 5\cdot 2 \end{pmatrix} = \begin{pmatrix} 56 & 14 \\ 52 & 13 \end{pmatrix}$$

$2\times 2 \quad 2\times 2 \quad 2\times 2$

row i in the first matrix times column j in the second matrix equals the

entry in the result in row i column j.

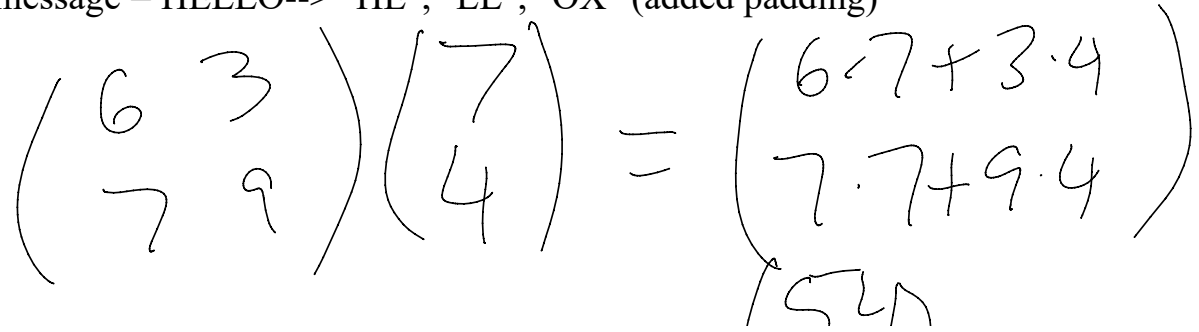
Multiplying an "array of numbers" by another same sized "array of numbers" is more formally called a dot product and by this I mean you multiply corresponding pairs of numbers and add all of these products.



Hill cipher

Key is a n by n matrix of values from 0 to 25.
Method of encryption is to separate the plaintext into blocks of size n, and if the last block isn't filled, add some padding characters to it (doesn't really matter what).
Encrypt each block by multiplying by the key and then modding the contents by 26.

message = HELLO--> "HE", "LL", "OX" (added padding)



$$= \begin{pmatrix} 54 \\ 85 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 2 \\ 7 \end{pmatrix} \mod 26$$

CH

$$\begin{pmatrix} 6 & 3 \\ 7 & 9 \end{pmatrix}\begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 6\cdot 11 + 3\cdot 11 \\ 7\cdot 11 + 9\cdot 11 \end{pmatrix}$$

$$= \begin{pmatrix} 99 \\ 176 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 21 \\ 20 \end{pmatrix}$$

VU

$$\begin{pmatrix} 6 & 3 \\ 7 & 9 \end{pmatrix}\begin{pmatrix} 14 \\ 23 \end{pmatrix} \equiv$$

$$\begin{pmatrix} 6 & 3 \\ 7 & 9 \end{pmatrix}\begin{pmatrix} 14 \\ -3 \end{pmatrix} = \begin{pmatrix} 6\cdot 14 + 3(-3) \\ 7\cdot 14 + 9(-3) \end{pmatrix}$$

$$= \begin{pmatrix} 84 - 9 \\ 98 - 27 \end{pmatrix}$$

$$= \begin{pmatrix} 98 \\ -211 \end{pmatrix}$$

$$= \begin{pmatrix} 75 \\ 71 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 23 \\ 19 \end{pmatrix}$$

XT

CHVUXT

1) How do we go backwards??? (How do we decrypt?)
2) Are all possible 2 by 2 matrices valid keys?
3) If the answer to #2 is no, how can I tell if a matrix is a valid key?

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

M $\quad$ M^{-1} $\quad$ Identity matrix

If we can find M^{-1} that satisfies this property, then we can definitely "UNDO" the operation of M.

To solve in general, we can multiply the LHS and set it equal to the right hand side, and solve the system of four equations in four variables. (Recall that a, b, c, d are known, so they aren't variables.)

ae+bg = 1 mod 26
af + bh = 0 mod 26
ce+dg = 0 mod 26
cf+dh = 1 mod 26

$\begin{pmatrix} a & b \end{pmatrix}$

ce+dg = 0 mod 26
cf+dh = 1 mod 26

Given a 2 by 2 matrix M $= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

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

In regular math

So with real numbers as entries, the inverse exists if and only if ad-bc is non-zero. This quantity is so important in linear algebra, it has a name, it's called the determinant of the matrix.

Are we allowed to divide in mod math?
What can we do instead???
We can multiply by the modular inverse.

For us the formula is:

$$M^{-1} = \left((ad-bc)^{-1} \bmod 26\right)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} 6 & 3 \\ 7 & 9 \end{pmatrix}^{-1} = \left((54-21)^{-1} \bmod 26\right)\begin{pmatrix} 9 & -3 \\ -7 & 6 \end{pmatrix}$$

$$= (33^{-1} \bmod 26)\begin{pmatrix} 9 & -3 \\ -7 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 7^{-1} \bmod 26 \end{pmatrix} \begin{pmatrix} 9 & -3 \\ -7 & 6 \end{pmatrix}$$

$$\equiv 15 \begin{pmatrix} 9 & -3 \\ -7 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 135 & -45 \\ -105 & 90 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 5 & 7 \\ 25 & 12 \end{pmatrix} \bmod 26$$

Decrypt

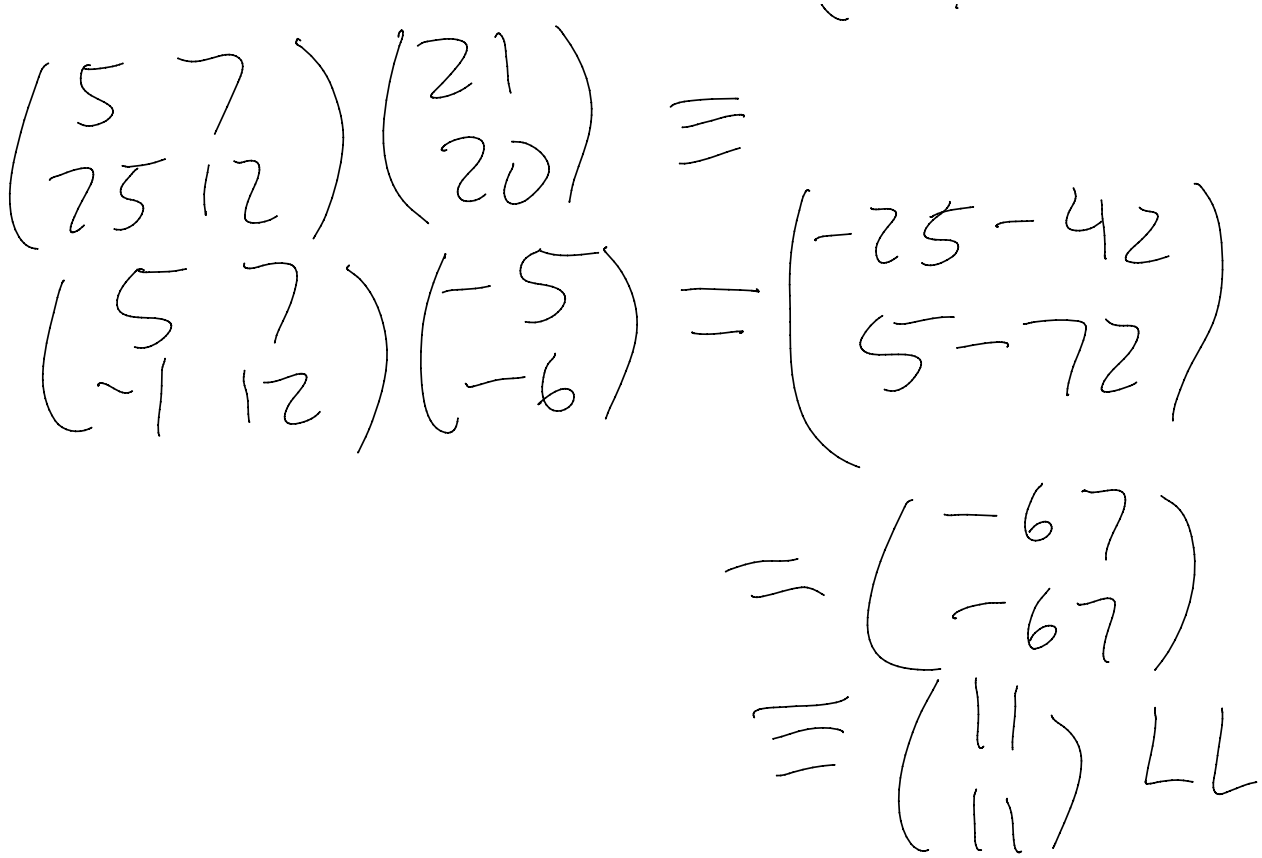
Cipher: CHIVUXT

$$\begin{pmatrix} 5 & 7 \\ 25 & 12 \end{pmatrix} \begin{pmatrix} 2 \\ 7 \end{pmatrix} = \begin{pmatrix} 10+49 \\ 50+84 \end{pmatrix}$$

$$= \begin{pmatrix} 59 \\ 134 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \text{HE}$$

(5 7 \ 12 1) =



The Hill cipher is the precursor to the block cipher. A block cipher splits the plaintext up into equal sized blocks, where a block is multiple characters/symbols (or in modern crypto bits), and then encrypts each block one by one. A block itself, does both confusion and diffusion as each input letter in a block affects each output letter in the block.

Although this is 2 by 2 like Playfair, you can use larger matrices, though by hand it is really horrible to do so.

Matrix Multiplication Code

```
// Assume we have a matrix result which is all 0s and size n by n.
// Assume we have matrices A and B which have set values in them
// Let's say that A.rows is the number of rows in matrix A, A.cols is the
// number of columns in matrix A, and same convention for B.

for (int i=0; i<A.rows; i++)
   for(int j=0; j<B.cols; j++)
      for(int k=0; k<A.cols; k++)
         res[i][j] = (res[i][j] + A[i][k]*B[k][j])%26
```

When is a key valid?

Ans: When ad-bc (the determinant) is relatively prime with 26.

Breaking Hill

For 2 by 2, you can probably do brute force since there are only 150,000 keys, roughly.
Past 2 by 2, brute force will be harder…

Known plaintext attack would work like this…
Say you knew that the plaintext HELL mapped to the ciphertext CHVU.
You can set up some equations to solve for the decrypt matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 \\ 7 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 21 \\ 20 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$$

$$2a+7b \equiv 7 \mod 26$$
$$2c+7d \equiv 4 \mod 26$$
$$21a+20b \equiv 11 \mod 26$$
$$21c+20d \equiv 11 \mod 26$$

$$2 \quad -5a-6b \equiv 11 \mod 26$$
$$5 \quad 2a+7b \equiv 7 \mod 26$$

5

$-10a - 12b \equiv 22 \pmod{26}$

$10a + 35b \equiv 35 \pmod{26}$

$23b \equiv 57 \pmod{26}$

$9(-3b) \equiv 9 \cdot 5 \pmod{26}$

$-27b \equiv 45 \pmod{26}$

$-b \equiv 45 \pmod{26}$

$b \equiv -45 \pmod{26}$

$b \equiv 7 \pmod{26}$

$2a + 7b \equiv 7 \pmod{26}$

$2a + 49 \equiv 7 \pmod{26}$

$2a \equiv -42 \pmod{26}$

$2a = -42 + 26n \quad n \in \mathbb{Z}$

$a = -21 + 13n$

$a \equiv -21 \pmod{13}$

$1a \equiv 5 \pmod{13}$

$$a \equiv 5 \pmod{13}$$

$\hookrightarrow$ $a = 5$ or $a = 18$