1 Introduction

In this project, I implement a 3 × 3 Hill Cipher Machine in Python. This machine automatically generates LaTeX reports to decipher user-entered Hill Ciphers step by step.

We will be deciphering: IQCWTM using the key: GYBNQKURP.

Note that the cipher and key in the line above have been entered by the user.

2 Encryption Matrix

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1: Lookup Table for Hill Cipher (Wikipedia)

We use the Lookup Table above and our key GYBNQKURP to create the Encryption Matrix below:

$$\begin{pmatrix} 6.0 & 24.0 & 1.0 \\ 13.0 & 16.0 & 10.0 \\ 20.0 & 17.0 & 15.0 \end{pmatrix}$$

3 Finding the Decryption Matrix (Encryption Matrix Inverse Mod 26)

We now find the modular (26) inverse of the Encryption Matrix to decrypt our message.

We first reduce our Augmented Encryption Matrix (M) to the Identity Matrix:

$$E21 * E31 * M :$$

$$\begin{pmatrix} 1.0 & 0.0 & 0.0 \\ -2.167 & 1.0 & 0.0 \\ -3.333 & 0.0 & 1.0 \end{pmatrix} \begin{pmatrix} 6.0 & 24.0 & 1.0 & 1.0 & 0.0 & 0.0 \\ 13.0 & 16.0 & 10.0 & 0.0 & 1.0 & 0.0 \\ 20.0 & 17.0 & 15.0 & 0.0 & 0.0 & 1.0 \end{pmatrix} = \begin{pmatrix} 6.0 & 24.0 & 1.0 & 1.0 & 0.0 & 0.0 \\ 0.0 & -36.0 & 7.83 & -2.17 & 1.0 & 0.0 \\ 0.0 & -63.0 & 11.67 & -3.33 & 0.0 & 1.0 \end{pmatrix}$$

$$E32 * E21 * E31 * M :$$

$$\begin{pmatrix} 1.0 & 0.0 & 0.0 \\ 0.0 & 1.0 & 0.0 \\ 0.0 & -1.75 & 1.0 \end{pmatrix} \begin{pmatrix} 6.0 & 24.0 & 1.0 & 1.0 & 0.0 & 0.0 \\ 0.0 & -36.0 & 7.83 & -2.17 & 1.0 & 0.0 \\ 0.0 & -63.0 & 11.67 & -3.33 & 0.0 & 1.0 \end{pmatrix} = \begin{pmatrix} 6.0 & 24.0 & 1.0 & 1.0 & 0.0 & 0.0 \\ 0.0 & -36.0 & 7.83 & -2.17 & 1.0 & 0.0 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix}$$

$$E23 * E13 * E32 * E21 * E31 * M :$$

$$\begin{pmatrix} 1.0 & 0.0 & 0.49 \\ 0.0 & 1.0 & 3.84 \\ 0.0 & 0.0 & 1.0 \end{pmatrix} \begin{pmatrix} 6.0 & 24.0 & 1.0 & 1.0 & 0.0 & 0.0 \\ 0.0 & -36.0 & 7.83 & -2.17 & 1.0 & 0.0 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix} = \begin{pmatrix} 6.0 & 24.0 & 0.0 & 1.22 & -0.86 & 0.49 \\ 0.0 & -36.0 & 0.0 & -0.41 & -5.71 & 3.84 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix}$$

$$E12 * E23 * E13 * E32 * E21 * E31 * M :$$

$$\begin{pmatrix} 1.0 & 0.67 & 0.0 \\ 0.0 & 1.0 & 0.0 \\ 0.0 & 0.0 & 1.0 \end{pmatrix} \begin{pmatrix} 6.0 & 24.0 & 0.0 & 1.22 & -0.86 & 0.49 \\ 0.0 & -36.0 & 0.0 & -0.41 & -5.71 & 3.84 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix} = \begin{pmatrix} 6.0 & 0.0 & 0.0 & 0.95 & -4.67 & 3.05 \\ 0.0 & -36.0 & 0.0 & -0.41 & -5.71 & 3.84 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix}$$

$$D * E12 * E23 * E13 * E32 * E21 * E31 * M :$$

$$\begin{pmatrix} 0.17 & 0.0 & 0.0 \\ 0.0 & -0.03 & 0.0 \\ 0.0 & 0.0 & -0.49 \end{pmatrix} \begin{pmatrix} 6.0 & 0.0 & 0.0 & 0.95 & -4.67 & 3.05 \\ 0.0 & -36.0 & 0.0 & -0.41 & -5.71 & 3.84 \\ 0.0 & 0.0 & -2.04 & 0.46 & -1.75 & 1.0 \end{pmatrix} = \begin{pmatrix} 1.0 & 0.0 & 0.0 & 0.16 & -0.78 & 0.51 \\ 0.0 & 1.0 & -0.0 & 0.01 & 0.16 & -0.11 \\ 0.0 & 0.0 & 1.0 & -0.22 & 0.86 & -0.49 \end{pmatrix}$$

Then, in the final step, we multiply the regular inverse with its determinent. Then we multiply it with its detrminent's 'modular (26) inverse'. Then we write the whole matrix mod 26:

$$25 * 441 * \begin{pmatrix} 0.16 & -0.78 & 0.51 \\ 0.01 & 0.16 & -0.11 \\ -0.22 & 0.86 & -0.49 \end{pmatrix} = \begin{pmatrix} 8.0 & 5.0 & 10.0 \\ 21.0 & 8.0 & 21.0 \\ 21.0 & 12.0 & 8.0 \end{pmatrix} (mod 26)$$

4 Matrix Multiplications

Now that we have the inverse/decryption matrix, we will multiply our cipher IQCWTM with the decryption matrix in chunks of 3. For each cipher chunk, we will create a decryption vector to multiply using the Lookup Table shown previously.

$$\begin{pmatrix} 8.0 & 5.0 & 10.0 \\ 21.0 & 8.0 & 21.0 \\ 21.0 & 12.0 & 8.0 \end{pmatrix} \begin{pmatrix} 8.0 \\ 16.0 \\ 2.0 \end{pmatrix} = \begin{pmatrix} 8.0 \\ 0.0 \\ 12.0 \end{pmatrix} (mod 26)$$

Decrypted chunk: IAM

$$\begin{pmatrix} 8.0 & 5.0 & 10.0 \\ 21.0 & 8.0 & 21.0 \\ 21.0 & 12.0 & 8.0 \end{pmatrix} \begin{pmatrix} 22.0 \\ 19.0 \\ 12.0 \end{pmatrix} = \begin{pmatrix} 1.0 \\ 8.0 \\ 6.0 \end{pmatrix} (mod 26)$$

Decrypted chunk: BIG

5 Decryption Result

The final result of the decryption is found by putting together all the chunks above: IAMBIG

6 Final Remarks

The Hill Cipher does not work for keys that result in Encryption Matrices whose determinent is 0 (Non-Invertible Matrices). The cipher also does not work for Encryption Matrices whose determinents are not coprime with 26 because then a unique modular inverse of the determinent does not exist. In both these case, this program will throw an exception. In addition, this program will throw an exception for Encryption Matrices that require row swaps to find their inverse. Future work includes further extending the program to generate 'smarter', step-by-step reports for more linear algebraic algorithms.

MAT-229 Project, Shaamyl Anwar.