Hill Cipher

Josephine Lee, Shuprovo Sikder

A Quick Refresher on Pre-Calc Math

Matrices

Matrix Multiplication (Dot Product):

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \begin{bmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ b_7 & b_8 & b_9 \end{bmatrix} = \begin{bmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{bmatrix}$$

Matrix Inverse:

Inverse of a Matrix

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\quad$ $A' = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ $\quad$ $AA' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

inverse of A

determinant

Identity matrix

Inverse of a Matrix

$$A^{-1} = \frac{1}{|A|} \cdot \text{Adj } A$$

Hill Cipher: Encoding

- The Hill cipher is a polygraphic substitution cipher based on linear algebra
- To encrypt a message:
  - each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26.
- To decrypt the message:
  - each block is multiplied by the inverse of the key matrix used for encryption.
- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26).

Hill Cipher: Example

Let’s encrypt the message “cipher” with the following key:

Hill Cipher: Decoding

<What it is>

Hill Cipher: Weakness/How to Break it

If you know a partial part of the decoded message, you can test each possibility.

Hill Cipher: Challenges

1. Encrypt the following:
2. Decrypt the following:
3.
4.
5.