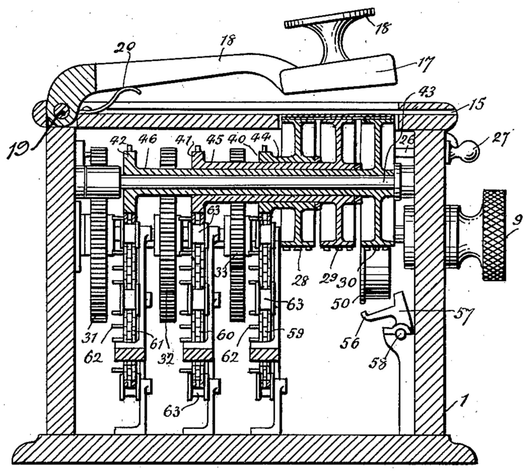
Hill Cipher

Josephine Lee, Shuprovo Sikder

So What is the Hill Cipher?

- Invented by Lester S. Hill
- It's the first polygraphic substitution cipher that could operate on more than three characters at the same time
- It's heavily rooted in linear algebra (matrix algebra) which makes it difficult (especially at higher dimensions) to compute by hand but fast for computers
- Considered the bridge between classical and modern cryptography



Hill's 6-dimensional encrypting/decrypting machine

Matrices

N-Component Matrix:

$$\begin{array}{lc} & \textit{1 column} \\ A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} & \textit{n rows} \end{array}$$

(Just a matrix with one column and any number of rows)

Square Matrix:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(Notice how the number of rows and columns are the same!)

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Matrices cont.

Matrix Multiplication (Dot Product):

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

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

cuemath
THE MATH EXPERT

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

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: Encryption Example

Let's encrypt the message "CIPHER" with the following key: BELL

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

Thus, the key can be represented as the following matrix:

$$\begin{pmatrix} B & L \\ E & L \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix}$$

Hill Cipher: Encryption Example

The message “CIPHER” can be represented as the following matrix:

$$\begin{pmatrix} C \\ I \end{pmatrix}\begin{pmatrix} P \\ H \end{pmatrix}\begin{pmatrix} E \\ R \end{pmatrix} \longrightarrow \begin{pmatrix} 2 \\ 8 \end{pmatrix}\begin{pmatrix} 15 \\ 7 \end{pmatrix}\begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

Next, we take the key matrix and multiply it by the first vector. Then we take the modulo 26 of the resulting matrix.

$$\begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix}\begin{pmatrix} 2 \\ 8 \end{pmatrix} = \begin{pmatrix} 1\cdot\ 2 + 11\cdot\ 8 \\ 4\cdot\ 2 + 11\cdot\ 8 \end{pmatrix} = \begin{pmatrix} 90 \\ 96 \end{pmatrix}$$

$$\begin{pmatrix} 90 \\ 96 \end{pmatrix} mod\, 26 = \begin{pmatrix} 12 \\ 18 \end{pmatrix}$$

Hill Cipher: Encryption Example

We continue this process with the rest of the 2x1 matrices.

$$\begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix}\begin{pmatrix} 15 \\ 7 \end{pmatrix} = \begin{pmatrix} 92 \\ 137 \end{pmatrix} = \begin{pmatrix} 14 \\ 7 \end{pmatrix} mod\ 26$$

$$\begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix}\begin{pmatrix} 4 \\ 17 \end{pmatrix} = \begin{pmatrix} 191 \\ 203 \end{pmatrix} = \begin{pmatrix} 9 \\ 21 \end{pmatrix} mod\ 26$$

Hill Cipher: Encryption Example

We convert these matrices composed of numbers into matrices composed of letters.

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

$$\begin{pmatrix} 12 \\ 18 \end{pmatrix}\begin{pmatrix} 14 \\ 7 \end{pmatrix}\begin{pmatrix} 9 \\ 21 \end{pmatrix} \longrightarrow \begin{pmatrix} M \\ S \end{pmatrix}\begin{pmatrix} O \\ H \end{pmatrix}\begin{pmatrix} J \\ V \end{pmatrix}$$

Thus, our encrypted message is “**MSOHJV**”.

Hill Cipher: Decoding Example

So we just encrypted CIPHER with the key BELL and got MSOHJV.

Let's try working backwards and decrypting this.

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

$$\begin{pmatrix} M \\ S \end{pmatrix}\begin{pmatrix} O \\ H \end{pmatrix}\begin{pmatrix} J \\ V \end{pmatrix} \longrightarrow \begin{pmatrix} 12 \\ 18 \end{pmatrix}\begin{pmatrix} 14 \\ 7 \end{pmatrix}\begin{pmatrix} 9 \\ 21 \end{pmatrix}$$

Hill Cipher: Decoding Example

When we encoded, we had to do matrix multiplication with the key, but to undo multiplication, we must find an **inverse matrix** of the key (specifically modulo 26).

Key:

$$\begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix}$$

$$K^{-1} = d^{-1} * \text{adj}(K)$$

$$d * d^{-1} = 1 \mod 26$$

Inverse Determinant:

$$det \begin{pmatrix} 1 & 11 \\ 4 & 11 \end{pmatrix} \mod 26 = 19$$

$$(19 * 1) \mod 26 = 19$$

$$(19 * 2) \mod 26 = 12$$

$$(19 * 3) \mod 26 = 3$$

$$\dots$$

$$(19 * 11) \mod 26 = 1$$

Adjugate Matrix:

$$\text{adj} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\text{adj}(K) = \begin{pmatrix} 11 & -11 \\ -4 & 1 \end{pmatrix}$$

$$\text{adj}(K) \mod 26 = \begin{pmatrix} 11 & 15 \\ 22 & 1 \end{pmatrix}$$

Hill Cipher: Decoding Example

So we find the inverse of our key BELL. Now we just multiply our enciphered text with this inverted key and we should have our plaintext!

$$K^{-1} = 11 * \begin{pmatrix} 11 & 15 \\ 22 & 1 \end{pmatrix} \mod 26 = \begin{pmatrix} 17 & 8 \\ 9 & 11 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 8 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 18 \end{pmatrix} = \begin{pmatrix} 366 \\ 294 \end{pmatrix} \mod 26 = \begin{pmatrix} 2 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 8 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 366 \\ 294 \end{pmatrix} \mod 26 = \begin{pmatrix} 15 \\ 7 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 8 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 21 \end{pmatrix} = \begin{pmatrix} 366 \\ 294 \end{pmatrix} \mod 26 = \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 8 \end{pmatrix} \begin{pmatrix} 15 \\ 7 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} \mathrm{C} \\ \mathrm{I} \end{pmatrix} \begin{pmatrix} \mathrm{I} \\ \mathrm{P} \end{pmatrix} \begin{pmatrix} \mathrm{E} \\ \mathrm{R} \end{pmatrix}$$

Hill Cipher: Weakness/How to Break it

- Since the Hill cipher is based on linear algebra, you can treat problems like a system of equations
- If you know the full plaintext or even just a piece of the plaintext and know the ciphertext, you can reasonably figure out the key!
- The partial plaintext must be of size n^2 (n being the number of rows/columns in the key matrix)

Hill Cipher: Challenges

1. Encrypt the following (by hand): HATS with the key: FINE
2. Encrypt the following: CHALLENGES with the key: WORD
3. Encrypt the text file “challenge3.txt” with the key:
4. Decrypt the following:
5. Break the following:

4.

5.

Solutions to Challenges

1. Encrypted message: **JERQ**
2. Encrypted message: **HXFHYKYSEG**
3. Decrypted message: