Hill Ciphers

Olivia Delffs

Traditional Ciphers

Each letter is swapped with a different 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
Q	Y	F	H	I	R	U	T	C	J	Z	E	P	L	K	N	D	V	M	O	A	X	W	B	S	G

"The dog runs fast outside" —> "Oti hku valm rqmo kaomchi"
"It is hot in the sun" —> "Co cm tko cl oti mal"
"Smell the roses" —> "Mpiee oti vkim"

Problem with Traditional Ciphers

Easy to find patterns with common words:

“**The** dog runs fast outside” —> “**Oti** hku valm rqmo kaomchi”

“It is hot in **the** sun” —> “Co cm tko cl **oti** mal”

“Smell **the** roses” —> “Mpiee **oti** vkim”

Recognize “the” = “oti”, uncover other letters

O = T	T = H	I = E

“~~Oti~~ hku valm rqm~~o~~ ka~~o~~mch~~i~~” —> “**The** hku valm rqm**t** ka**t**mch**e**”

“C~~o~~ cm ~~tko~~ cl ~~oti~~ mal” —> “C**t** cm **hkt** cl **the** mal”

“Mp~~i~~ee ~~oti~~ vk~~i~~m” —> “Mp**e**ee **the** vk**e**m”

Find more patterns

Numeric Conversion

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
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

"The dog runs fast outside" —> $\begin{bmatrix} 19 & 3 & 17 & 18 & 18 & 20 & 8 \\ 7 & 14 & 20 & 5 & 19 & 19 & 3 \\ 4 & 6 & 13 & 0 & 14 & 18 & 4 \end{bmatrix}$

Conversion to numbers allows for linear algebra to be used, which is a huge component of hill cyphers

Modular Arithmetic

- 26 letters in the alphabet —> keep values in matrices from 0-25
- Mod symbol (%) calculates remainder
- Ex.
  - $(32)\ \%\ 26 = 6$ because $(26 \cdot 1) + 6 = 32$
  - $\left(4 \cdot \begin{bmatrix} 7 \\ 4 \\ 1 \end{bmatrix} + 3 \cdot \begin{bmatrix} 12 \\ 3 \\ 17 \end{bmatrix}\right) \%\ 26 = \begin{bmatrix} 12 \\ 25 \\ 3 \end{bmatrix}$
    - $(4 \cdot 7) + (3 \cdot 12) = 64, (2 \cdot 26) + 12 = 64$
    - $(4 \cdot 4) + (3 \cdot 3) = 25, (0 \cdot 26) + 25 = 25$
    - $(4 \cdot 1) + (3 \cdot 17) = 55, (2 \cdot 26) + 3 = 55$

Key Matrix

- Messages converted to numbers are put into matrices and multiplied by a key matrix to become encoded
- We will explore 3x3 matrices
- Key matrix requirements:
  - Must be in the set Z_3^{26}, which is spanned by all vectors with 3 elements in the range of 0 through 25.
    - Multiplying a vector in this set yields another vector, also in Z_3^{26}, serving as an encoded version.
  - All calculations must be modded by 26
  - Must be invertible modulo 26, it's inverse serves as a decoding matrix
    - Determinant can not be a multiple of 2, 13, or 26

Encoding and Decoding

Encoding:

- Message is converted to a numeric matrix

- Key matrix is multiplied by message matrix and modded by 26

- Product of the two is converted back to letters and is now a secret message

Decoding:

- Inverse of key matrix is multiplied by product of key matrix and message matrix

- Value found above is converted back to letters, revealing the original message

Example:

Encode the phrase "Hill Cipher v Classic Cipher" using key matrix: $\begin{bmatrix} 21 & 23 & 7 \\ 4 & 25 & 2 \\ 9 & 11 & 12 \end{bmatrix}$

Step 1: Convert phrase to numeric matrix

$$\begin{bmatrix} 7 & 11 & 15 & 17 & 11 & 18 & 2 & 7 \\ 8 & 2 & 7 & 21 & 0 & 8 & 8 & 4 \\ 11 & 8 & 4 & 2 & 18 & 2 & 15 & 17 \end{bmatrix}$$

Step 2: Multiply key by message

$$\begin{bmatrix} 21 & 23 & 7 \\ 4 & 25 & 2 \\ 9 & 11 & 12 \end{bmatrix} \times \begin{bmatrix} 7 & 11 & 15 & 17 & 11 & 18 & 2 & 7 \\ 8 & 2 & 7 & 21 & 0 & 8 & 8 & 4 \\ 11 & 8 & 4 & 2 & 18 & 2 & 15 & 17 \end{bmatrix} \% \ 26$$

$$\begin{bmatrix} 18 & 21 & 10 & 22 & 19 & 14 & 2 & 7 \\ 16 & 6 & 9 & 25 & 2 & 8 & 8 & 4 \\ 23 & 9 & 0 & 18 & 3 & 2 & 15 & 17 \end{bmatrix}$$

Step 3: Convert back to letters

Encoded message: "sqxvgjkjawzstcdeqoteaugz"

Example:

Decode the phrase "sqxvgjkjawzstcdeqoteaugz" using key matrix: $\begin{bmatrix} 21 & 23 & 7 \\ 4 & 25 & 2 \\ 9 & 11 & 12 \end{bmatrix}$

Step 1: Convert phrase to numeric matrix

$$\begin{bmatrix} 18 & 21 & 10 & 22 & 19 & 14 & 2 & 7 \\ 16 & 6 & 9 & 25 & 2 & 8 & 8 & 4 \\ 23 & 9 & 0 & 18 & 3 & 2 & 15 & 17 \end{bmatrix}$$

Step 2: Multiply inverse of key by above

$$\begin{bmatrix} 10 & 5 & 15 \\ 18 & 1 & 24 \\ 15 & 4 & 21 \end{bmatrix} \times \begin{bmatrix} 18 & 21 & 10 & 22 & 19 & 14 & 2 & 7 \\ 16 & 6 & 9 & 25 & 2 & 8 & 8 & 4 \\ 23 & 9 & 0 & 18 & 3 & 2 & 15 & 17 \end{bmatrix} \% \ 26$$

$$\begin{bmatrix} 7 & 11 & 15 & 17 & 11 & 18 & 2 & 7 \\ 8 & 2 & 7 & 21 & 0 & 8 & 8 & 4 \\ 11 & 8 & 4 & 2 & 18 & 2 & 15 & 17 \end{bmatrix}$$

Step 3: Convert back to letters

Decoded message: "hillciphervclassiccipher"

Classic Cipher vs Hill Cipher

- Average run time when computing in R
- Hill Cipher takes a significant amount longer to encode and decode
- Hill Cipher is harder to crack and may be a better choice for encryption