MATH 314 Fall 2019 - Class Notes

Scribe: Druv Narain

September 9, 2019

Summary: Introduction to the Hill Cipher

Background:

A block cipher encrypts groups of letters called blocks at the same time. Changing one letter of plaintext can change an entire block of ciphertext.

Anytime
we have a block cipher, we have a block length that specifies the number of letters in a block.

The Hill Cipher

The Hill Cipher uses linear algebra (specifically Matrices) to encrypt and decrypt messages.

To encrypt a message we take a block of letters and write them as a vector $\vec{v}$

$$E(\vec{v}) \equiv \vec{v}k \bmod(26)$$

Where k is the key matrix, block length is $M \geq 2$ where M is an integer.

The key is an m x m matrix of numbers (mod 26)

Notes:

- The vector comes before the k, order matters in linear algebra!
- Hill Cipher is secure against Ciphertext-Only attacks if the block size is sufficiently large

When multiplying vectors or matrices we do so by pairing rows and columns
(Assume block size remains the same)

Example of Encryption:

Let block size $m = 2, k = \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$ Encrypt "june" (9, 20, 13, 4)

$$E(< 9, 20 >) \equiv < 9, 20 > \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix} \pmod{26}$$

$$\equiv < 9 \times 3 + 20 \times 2, 9 \times 9 + 20 \times 7 > \pmod{26}$$

$$\equiv < 1 + 14, 3 + 10 > \pmod{26} \equiv < 15, 13 > \pmod{26}$$

"ju" encrypts to PN

$$E(< 13, 4 >) \equiv < 13, 4 > \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix} \pmod{26}$$

$$\equiv < 13 \times 3 + 4 \times 2, 13 \times 9 + 4 \times 7 > \pmod{26}$$

$$\equiv < 13 + 8, 13 + 2 > \pmod{26} \equiv < 21, 15 > \pmod{26}$$

"ne" encrypts to VP. The complete ciphertext of "june" is PNVP.

To Decrypt a Hill Cipher

Start with $E(\vec{v}) \equiv \vec{v}k \text{ mod}(26) \equiv \vec{c}$ and multiply both sides by the inverse matrix k^{-1}

$k^{-1} \times k \equiv I$: I is the Identity Matrix

$$\vec{v}k^{-1}k \equiv \vec{c}k^{-1} \pmod{26}$$

$$D(\vec{c}) \equiv \vec{c}k^{-1} \pmod{26}$$

Notes:

- This only works if k has an inverse.
- A valid key matrix k must have an inverse matrix k^{-1}