MATH 314 Fall 2019 - Class Notes

9/9/2019

Scribe: Nick Taormino

Summary: Starting the Hill Cipher.

Notes: First quiz today.

Hill Cipher: a block cipher(like the playfair cipher). Entire blocks of plain text are encrypted at the same time, one plain text letter could equate to multiple cipher text letters.

Block length: number of letters encrypted at the same time is a "block", this can be any integer

$$m >= 2$$

for the Hill Cipher.

We will use linear algebra to encrypt and decrypt messages.
Key: mxm matrix K of integers $mod(26)$

represent each block of plain text as a vector $\vec{v}$

Encryption Method

$$E(\vec{x}) = \vec{v} * K$$

Multiplication = rows * columns

Example:

$$m = 2$$

`plain text :  "june"` $= 9, 20, 13, 4$

$$K = \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$$

Encrypt each block $ju =< 9, 20 > ne =< 13, 4 >$

$$E(< 9, 20 >) =< 9, 20 > * \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$$

$$E(< 9, 20 >) =< 9 * 3 + 20 * 2, 9 * 9 + 20 * 7 >$$

$$E(< 9, 20 >) \equiv< 67, 221 > (mod 26)$$

$$E(< 9, 20 >) \equiv< 15, 13 > (mod 26) \equiv< P, N >$$

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

$$E(<13,4>) =<13*3+4*2, 13*9+4*7>$$

$$E(<13,4>) \equiv <47,145> (mod 26)$$

$$E(<13,4>) \equiv <21,15> (mod 26) \equiv <V,P>$$

`plain text :  "june"` $\equiv PNVP$

change 1 letter of plain text: June to Dune `plain text :  "dune"` $= 3,20,13,4$

$$E(<3,20>) \equiv <23,11> \equiv XL$$

`plain text :  "june"` $\equiv XLVP$

Hill cipher is reasonably secure against cipher text only attacks, but not against know plain text attacks.

$$E(\vec{x}) = \vec{v} * K$$

$$\vec{x} K K^{-1} = \vec{y} * K^{-1}$$

$$\vec{x} = \vec{y} * K^{-1}$$

Decryption Method

$$D(\vec{y}) = \vec{y} K^{-1} (mod 26)$$

$$K K^{-1} = I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

all 1s running along the main diagonal

In order to decrypt K, it must have an inverse K^{-1}