Notes 2/5

Seth Graham

February 27, 2020

Summary: In today's class,we started discussing block ciphers and more specifically the **Hill cipher**.

Block Ciphers

- Most modern cryptosystems are block ciphers. This means that they encrypt "blocks" or a set of letter all at one time.
- This means that by changing on letter could affect the whole block of cipher text.
- Block length is an important factor.

  The first real block cipher was the **Hill Cipher**:
- This encryption uses matrices with a fixed block length, m.
- The key is an m by m matrix(mod26) *(k).

  To encrypt, we take a block and write it out as a row or vector.

  E(v)=vk

  v= block from plaintext.

  k= key matrix

  Example:

  m= 2 and the matrix key k is:

$$k = \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix}$$

  Say we want to encrypt the plaintext, "rows". To do this, we convert the word rows to its letter equivilant. 17,14,22,18. Then divide them into two blocks being (17,14) and (22,18).

  Next we follow the encryption formula and multiply the vectors by the key matrix.

  E(<17,14>)=<17,14>*k

  <17*10+14*5,17*3+14*0> = <6,25>

This encrypts the first block as GZ.

E(<22,18>)=<22,18>*k

<22*10+18*5,22*3+18*0> = <24,14>

The second block encrypts to YO.

Decrypting the hill cipher:

- To decrypt it, we want to find the matrix $k^{(} - 1)$, so the $k * k^{(} - 1) = I$ t(The identity matrix)

  To start, we call the cipher text,w.(Important note, when multiplying matrices, order matters. If you multiply b=a by a vector x, you must do b*x=a*x or x*b=x*a.)

  w=v*k(mod26), multiply by k inverse.

  $w * k^{-1} = v * k * k^{-1}(mod 26)$, this simplifies to $w * k^{-1}$=v(mod26)

  This means the decryption is $D(w) = w * k^{-1}$(mod26).

  If m=2 and

  $$k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

  Then k inverse = (ad-bc)$^{-1} * r(mod 26)$

  $$r = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

If (ad-bc) does not have an inverse, then k is not a valid matrix for the hill cipher.