Crypto Notes-Feb9th

Keenan Starstrom

March 9, 2017

Topic Covered: Hill Cipher

Hill Cipher, a poly-alphabetic block cipher created by Lester Hill in 1929

Characteristics of a block cipher: breaks the plain-text into blocks of a set length
i.e. take the word June and put it into blocks of 2 Ju ne
Then encrypt block by block

Hill Cipher Encryption:
Step 1: Choose block size -> m
Step 2: Treat the blocks as vectors -> Ju = (9,20) ne = (13,4)
The key will be a m * m matrix called K, this matrix must have a determinate that is relatively prime to 26
Note: The determinate of a 2 by 2 matrix is found by multiplying diagonally and subtracting the two products
Step 3: Multiply each vector by the key K

Decryption of a Hill Cipher:
Need the inverse matrix K^{-1}
For a matrix

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

$$[K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

* (ab - bc)
Break the cipher text into blocks of length m like in the encryption steps
Multiple the blocks by the inverse K matrix
The cipher-text should decrypt to the plain-text

Attacking the Hill Cipher: There are three general ways a cipher can usually be attacked:
Cipher-text only

Known Plain-text
Chosen Plain-text

The Hill Cipher is secure against a cipher-text only attack, however, if the block length can be determined certain known plain-texts and a Chosen plain-text can be used to break the cipher.

A Chosen plain-text attack for m=2 would use ABBA, which in vectors is (0,1) and (1,0) these identity vectors when multiplied by the key will return the values of the key, breaking the cipher.

Certain known plain-texts can also be used to break the cipher by using them to create a 4-equation system and find the key

i.e (1,1) and (1, -1) when multiplied by a matrix

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

return (5,6) and (1, -4) you can determine that the series of equations is:
a+c=5
b+d=6
a-c=1
b-d=-4

This attack does not work with every possible cipher-text however as certain vector combinations will return systems with multiple instances of variables making the system unsolvable
It is important to note that both of these attacks require some other method of learning the block length of the key.