Notes from 9/8/2016

Sidney Heier

September 10, 2016

Recall: Vigener Cipher

-polyalphabetic cipher (frequency analysis no longer works)

-Steps to encrypt using cipher:

1. choose key word
2. write plaintext
3. convert plaintext to number
4. convert key word to number
5. write key word number under plaintext number
6. add numbers together (if ¿26, do mod 26 to get ¡26)
7. convert numbers back to letters

```
EXAMPLE:
    -key word: cat (2, 0, 19)
    -plaintext: Wednesday

        W    E    D    N    E    S    D    A    Y          18+19 = 37 mod 26 = 9
        22   4    3   14    4   18    3    0   24          24+19 = 43 mod 26 = 17
    +   2    0   19    2    0   19    2    0   19
    ---------------------------------------------
        24   4   22   16    4    9    5    0   17
        Y    E    W    Q    E    J    F    A    R

        Cipher text: YEWQEJFAR
```

-Steps to decrypt vigener cipher:

-subtract key word from cipher text

-Steps for finding the key word

1. Write out cipher text on one line
2. write it out again, but shift each letter one to the right by one place directly below the first line
3. Count how many times the same letter in the shifted row matches the letter in the same column in the original cipher text.

**COINCIDENCES = SHIFTED LETTER IS THE SAME AS LETTER IN COLUMN OF CIPHER TEXT

4. Keep repeating the shift until letters do not line up anymore.

**Line with most coincidences is most likely the length of the key word or a multiple of the key word length.

```
EXAMPLE: (from textbook)
 cipher text:  V    V    H    Q    W    V    V    R    H    M    U    S    G    J    G
 shift 1:           V    V    H    Q    W    V    V    R    H    M    U    S    G    J...
 shift 2:                V    V    H    Q    W    V    V    R    H    M    U    S    G...

 Displacement    1    2    3    4    5    6...      **NOTICE: 5 has the most coincidences
 Coincidences   14   14   16   14   24    12            therefore most likely key length
```

-More steps to finding key

5. Break cipher text into groups. Each nth goes into a group

Hill Cipher

-Polyalphabetic

-block cipher (blocks of letters incripted at the same time changing the output of the whole block)

-1st cipher to use algebra fundamentally

-Steps to the Hill Cipher:

1. Pick a block length, m
2. Break the plaintext into blocks of length, m

```
EXAMPLE:
    plaintext:  |----------|----------|----------|----------|----------|
                      m          m          m          m          m
               **key: m x m matrix of integers 0-25.
```

Encryption Step

-Treat each block of letters as a vector and multiply the vector times the key matrix.

-cipher text = vector we get out

-we need the determinant of the key matrix to have gcd 1 with 26.

EXAMPLE:

m=2

k= $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} -> determinant(k) = 77 - 24 = 53 \equiv 1(mod 26)$

$**crossmultiplymatrix$

```
We want to encrypt the word "JULY" = |JU| |LY|
                                     <9,20><11,24>


          <9, 20>
```