Notes 2/3

Seth Graham

February 10, 2020

Summary: In today's class, we finished discussing the **affine cipher** and started discussing the **substitution cipher** and **Vigenere cipher**.

Notes:

- Chosen plaintext attack against affine cipher: ("it"[8,19] encrypts "OH"[14,7])

(a= alpha, b = beta)
a(8)+b=14(mod26)
-(a(19)+b=7(mod26))
a(-11)=7(mod26)
solving this gives you a= 23. which you plug back into an equation to get b=12
thus, the key is (a,b)=(23,13)

- **Substitution table**

1. The key is a table listing all plaintext letters(a-z) along with corresponding CIPHERTEXT letters

Example: a b c d e f ... z
Example: L R D Y M Q ... E
-Notice how there is not any distinct shift, it is chosen randomly.
-To be a valid table, each letter must show up once in the bottom row
How do we attack the substitution cipher?

- Ciphertext only attack:

  It is not possible to brute force this cipher,as the amount of combinations is around $4.03 * 10^(26)$

  However, Frequency analysis still will let us analyze the text based on the amount of letter appearences.

- Known plaintext attack:

  Literally just lets us fill out the table with the known letters.

- Chosen plaintext attack:

  You could just choose the whole alphabet or a sentence that has all the letters and it gives you the entire key table.

The ciphers discussed before this have all been **Mono-Alphabetic**, this means that they always encrypt single letters of plaintext to single letters of CIPHERTEXT.

The first **Poly-Alphabetic** cipher was the Vigenere cipher.

To encrypt a Vigenere cipher, you convert a key to a list of numbers(vectors). Then you convert the plaintext to a string of numbers as well. You write out the plaintext numbers and repeat the key over and over below. You then add the two numbers and mod26 to get your CIPHERTEXT number.

Example: Key= "key" [10,4,24]

Encrypting plaintext = "message" [12,4,18,18,0,6,4]

12,4,18,18,0,6, 4

+10,4,24,10,4,24,10

(mod26)22,8,16,2,4,4,14

ciphertext=WIQCEEO

By doing this, we break brute force and standard frequency analysis.

To decrypt this, you just take the CIPHERTEXT and subtract the key (mod26)

This cipher is stil weak if you know the plaintext and cipher or can chose the plaintext.

- Known plaintext attack:

  You just text the ciphertext and subtract the plaintext, then (mod26) to get the key.

- Chosen plaintext attack:

  You can choose the letter "a" over and over again to get the key out directly.

- If we wanted to attack this cipher text only, we must do two things.

  1. Figure out the length of the key
  2. Use frequency analysis to figure out the letters in the key.

- Bababges idea to find the key length goes like this. You write out the ciphertext on one line. Then below it you write the letters shifted 1 time. then go one more line down and shift 2 times. Repeat.

  Cipher: 3 2 1 V I R I Q Q L M R....

  Shift 1: 3 2 V I R I Q Q L M R ....

  Shift 2: 3 V I R I Q Q L M R ....

  Shift 3: V I R I Q Q L M R ....

  You then count the number of times the same letter occurs in each line as in the same postition of the orignal cipher.

  Tally the total number of coincidences in each line. There are more coincidences in lines where the shift is a multiple of the key length.