MATH 314 Spring 2019 - Class Notes

2/7/2019

Scribe: Joseph Case

Summary:A new type of cipher, the Vigenere cipher, was discussed in class. The Cesar/Shift, Affine, and Substitution ciphers (discussed in previous classes)are all classified as monoalphabetic ciphers, which cause one letter of plaintext to correspond to one letter of ciphertext. The Vigenere cipher is not a monoaplhabetic cipher. Different types of attacks on the Vigenere cipher and the encryption method for the Vigenre cipher were the topics discussed in class.

Total keys in the Cesar, Affine, and Substitution Ciphers (Review):

- Cesar - 26 keys. There are 26 possible shifts.
- Affine - 312 keys $(12 * 26)$. There are 12 choices for α, and every α allows 26 choices for β
- Substitution - 26! keys $(26 * 25 * 24...)$. There are 26 choices for a, 25 choices for b, 24 choices for c, ect.

Vigenere Cipher Encryption Mehtod:

- A codeword is chosen to be the key
- Write the plaintext, and then write codeword over and over below the plaintext
- Convert the letters in the plaintext and in the repeated codeword below the plaintext to numbers, and add the numbers modulus 26 vertically
- Change the sum back to letters to get the encrypted message

Vigenere Cipher Excryption Example: Let the codeword be *vector* and the plaintext be `hereishowitworks`

- First write the plaintext, and then write the codeword over and over below the plaintext

$$\begin{array}{cccccccccccccccc} h & e & r & e & i & s & h & o & w & i & t & w & o & r & k & s \\ v & e & c & t & o & r & v & e & c & t & o & r & v & e & c & t \end{array}$$

- Convert the letters to numbers, and them add modulus 26 vertically

$$\begin{array}{rrrrrrrrrrrrrrrrrr} & & 7 & 4 & 17 & 4 & 8 & 18 & 7 & 14 & 22 & 8 & 19 & 22 & 14 & 17 & 10 & 18 \\ (mod 26) & + & 21 & 4 & 2 & 19 & 14 & 17 & 21 & 4 & 2 & 19 & 14 & 17 & 21 & 4 & 2 & 19 \\ \\ & & 2 & 8 & 19 & 23 & 22 & 9 & 2 & 18 & 24 & 1 & 7 & 13 & 9 & 21 & 12 & 11 \end{array}$$

- Change the sum back to letters to get the encrypted message

2	8	19	23	22	9	2	18	24	1	7	13	9	21	12	11
C	I	T	X	W	J	C	S	Y	B	H	N	J	V	M	L

- **Note:** The first `e` in the plaintext `hereishowitworks` was encrpyted to `I` while the second `e` was encrpted to `X`. The Vigenere Cipher does not gurantee a plaintext letter will always map to the same ciphertext letter; however, there is a possibility of a plaintext letter getting mapped to the same ciphertext letter. Observe the first and second `h` in the plaintext `hereishowitworks`. Both are mapped to the ciphertext letter `C`.

Finding the key used by the Vigenere Cipher:

- There are two steps in determining the key used by the Vigenere Cipher
  1. Find the key length
  2. Find the shift associated with each part, or letter, of the key
- Step 1 requires a clever trick, which is based on mathematical dot products (read book to understand the dot product application), and Step 2 requires frequency analysis

Step 1 (Find the key length) Process:

- First, write the ciphertext message
  (Suppose the ciphertext is `AAFFBDGGT`)
- Second, write the ciphertext message shifted one letter to the right below the original ciphertext message

A	A	F	F	B	D	G	G	T
T	A	A	F	F	B	D	G	G

- Third, count the number of matching letters between the original and shifted ciphertext

A	A	F	F	B	D	G	G	T
T	A	A	F	F	B	D	G	G
	*		*				*	

  The starred positions are the positions in which the letters in the original and shifted ciphertext match The starred positions are the positions in which the letters in the original and shifted ciphertext match

- Fourth, repeat the process, and increase the shift amount by one each iteration
- After repeating the process several times, you should notice a spike in the number of matching letters between the original and shifted ciphertext. The spike in the number of matching letters indicates the shift amount is a multiple of the key length.

Step 2 (Find the shift associated with each part, or letter, of the key) Process:

- Assume the key length is discoverd to be n.
- Perform a frequency analysis on letters, in the ciphertext, that are n letters apart. Identify the letter that appears most frequently, and determine the numerical difference between the identified letter and the letter e. The numerical difference is the shift associated with the part of the key.
- Example: Suppose you find the length of the key to be 3, and let the ciphertext be `JFWNPFTRABFP`. Do a frequency analysis on `J,N,T,B` (Every first letter in each group of three). Do a frequency analysis on `F,P,R,F` (Every second letter in each group of three). Do a frequency analysis on `W,F,A,P` (Every thrid letter in each group of three) *The example is not actually big enough to conduct frequency anaylsis on, but the process should be clear*

Attacks on the Vigenere Cipher:

- Known Plaintext Attack: The shift pattern of the key can be identified by computing the difference between the known plaintext and the ciphertext.(assuming the known plaintext is longer than the key)

  Example: Suppose the plaintext is `hellobuddy` and the ciphertext is `QSPUCFDRHG`. Convert the ciphertext and plaintext to numbers and subtract the plaintext from the ciphertext to get the shift pattern.

$$\begin{array}{rrrrrrrrrrrr} & & 16 & 18 & 15 & 20 & 2 & 5 & 3 & 17 & 7 & 6 \\ mod26 & - & 7 & 4 & 11 & 11 & 14 & 1 & 20 & 3 & 3 & 24 \\ & & & & & & & & & & & \\ & & 9 & 14 & 4 & 9 & 14 & 4 & 9 & 14 & 4 & 9 \end{array}$$

  The shift pattern is 9,14,4; therefore, the codeword was `joe`

- Chosen Plaintext Attack: Encrypt the plaintext letter `a` in a string that is longer than the key and the shift pattern of the key can be identified

  Example:Suppose the encrypted plaintext is chosen to be `aaaaaaaa`, and the resulting ciphertext is `JOEJOEJO`. The shift pattern shows the codeword is `joe`.

- Ciphertext Only Attack: Find the length of the key using Step 1 (shifting the ciphertext and finding the shift with the most matching letters) and determine the shift pattern by using Step 2 (applying frequency analysis to ciphertext letters that are separated by the length of the key)