MATH 314 - Class Notes

9/5/2017

Scribe: Amber Jenkins

Summary: In class on Tuesday, 9/5, we reviewed monoalphabetic ciphers and and introduced the Vigenere Cipher.

Notes:

- Monoalphabetic: one letter of plain text always maps to the same letter of cipher text
- Monoalphabetic Ciphers include:
  - Ceasar Cipher:26 possible keys
  - Affine Cipher: 312 possible keys
  - Subsitution Cipher: 26! (or approximately $4 * 10^{28}$)possible keys
- Substitution Cipher
  - Creates a cipher by mixing the 26 letters of the alphabet is some other (random) order
  - Example
    `Plain Text` : A B C ...
    `Cipher Text`: R Q D...
  - Cannot use brute force to solve a substitution cipher
  - Suppose your computer can check 1 million keys every second-using the brute force method it would take the computer the age of the universe to crack
  - Attack Substitution Cipher:
    Known Plain Text: is easy to figure out the key if the message has a lot of letters
    Cipher Text Only: can use frequency analysis and intelligent guessing
  - This is not a secure cipher
- Vigenere's Cipher
  - Not a monoalphabetic cipher
  - Steps to Encrypt using Vigenere's Cipher:
    1. Pick a key that is a word
    2. Write your `Plain Text` and convert the letters in `Plain Text` to numbers (mod 26)
    3. Below the `Plain Text`, and the corresponding numbers,write the word that you picked as your key repeatedly
    4. Convert the letters from your repeated key word into numbers (mod 26)
    5. Add the line of numbers from your `Plain Text` and the line of numbers from your key and than reduce by (mod 26)

6. Convert the new line of numbers into the corresponding letters-now you have your `Cipher Text`

- Example:
  `Key`: CAT
  `Plain Text`: WEDNESDAY

  Plain Text
  W E D N E S D A Y
  22 4 3 14 4 18 3 0 24
  Key
  C A T C A T C A T
  2 0 19 2 0 19 2 0 19
  Addition of Plain Text and Key
  24 4 22 16 4 37 5 0 43
  (mod 26)
  24 4 22 16 4 11 5 0 17
  Cipher Text
  Y E W Q E L F A R

  * Note: The First "D" in the `Plain Text` became a "W" in the `Cipher Text` and the Second "D" became a "F"

- Frequency Analysis doe not work on the Vigenere Cipher since it is not monoaplhabetic
- People thought this cipher was secure (atleast against Cipher Text only attacks)
- Attack Vigenere Cipher
  Known Plain Text: `Cipher Text-Plain Text` will recover the key repeated
  Cipher Text Only(Broken by Charles Babbage):Can not use Brute force-Suppose the key has at least 20 letters, that means there is 26^{20} possible keys and this is impossible to solve using brute force
  In a Cipher Text only attack we need to:
  1. Figure out the lenght of the key
  2. Figure out the key (one letter at a time)

  Use the Displacement Method for cipher text only attacks
  The Goal of the Displacement Method is to find the lenght of the key
  Steps for the Displacement Method:
  1. Write down the `Cipher Text` in a single line
  2. Below write down the `Cipher Text` again, but this time shift it one letter to right
  3. Write `Cipher Text` again, and shift it two letters to the right (of the original `Cipher Text`)
  4. Count Coincidences by counting how often the letter in the `Shifted Ciphers` match the letter of the original `Cipher Text`
  5. Look for a spike in the table of the number of displacements/ number of coincidences- where there is a spike in the table, this corresponds to the lenght of the key or a multiple of the lenght of the key

6. After you determine the lenght of the key you can try to figure out the key word by using frequency analysis and intelligent guessing

Example (This is only a small section of the example; the full example used in class is on CoCalc, or can be found in the text book): `Cipher Text`:
V V H Q W V V R H M
`Cipher Text- 1st Shift`
- V V H Q W V V R H
`Cipher Text- 2nd Shift`
- - V V H Q W V V R
Counting Coincides(Data came from the Text Book)
Displacement: 1 2 3 4 5 6
Coincidences: 12 14 16 14 **24** 12
The Spike in the table occurs at displacement 5
We can conclude the key word is 5 letters long, than use frequency alaysis and intelligent guessing to figure out the key word