# MATH 314 Sprint 2020 - Class Notes

2/3/20

Scribe: Cameron Crow

**Summary:** Substitution and Vigenere Ciphers

## Substitution Cipher

- The goal of a Substitution Cipher is to increase the number of keys possible
- For a substitution cipher, map any letter of the alphabet to any other letter of the alphabet, so any character a-z can be any other letter a-z
- The possible number of keys for the substitution is 26! that is $4.03x10^26$ keys. You can not brute force this.

## How do you attack the Substitution Cipher:

- Ciphertext Only: Can be solved using frequency analysis of common word patterns.
- Known Plaintext: Read the key. If you know the plaintext match it to letters of the ciphertext.
- Chosen Plaintext: Use the alphabet or any sentence which contains all of the letters of the alphabet

## Vigenere Cipher

- The vigenere cipher is the 1st poly alphabetic cipher. This means a single letter can be encrypted into multiple different letters.
- Pick a key word or phrase adn write it as numbers or vectors.
- to encrypt a message we write the plaintext as numbers and repeat the key to the plaintext length. Then encrypt the same way you would Ceaser cipher.
- let our key be: key this encrypts to 10,4,24. Let our PT message be: Message
- repeat the key till it has the same character length as our message, in this case seven characters.
- The new key should look like keykeyk which numerically is 10,4,24,10,4,24,10.
- Encrypt each letter of message by adding its corresponding key letter.
- Decryption is done by subtracting the key from the ciphertext.

## How do you attack the Vigenere Cipher:

- Known Plaintext: Check the shift for each letter working down the plaintext until the key has been completed.
- Chosen Plaintext: Use a series of A's greater then or equal too the key length.
- Ciphertext Only: First we need to find the key length. Then we can use frequency analysis on letters in each position.

## How do you find the key length:

- Start by writing out the ciphertext, then proceed to shift the ciphertext letters one to the left wrapping around the fist letter to the last position.
- The Ciphertext: phiauszdhgbnpa on a first shift becomes: hiauszdhgbnpap then becomes: iauszdhgbnpaph on shift two.
- repeat this shift a large number of times, then count the coincidences where a letter of the original CT and a letter of the shifted CT line up.
- If you shift by a number equal to the key length the frequency of coincidences will nearly double.