MATH 314 Sprint 2020 - Class Notes

1/27/20

Scribe: Cameron Crow

Summary: Ceaser Cipher

Ceaser Cipher: The Ceaser or Shift cipher is a symmetric key cryptosystem which adjusts all of the letters of the plain text by a set key length to recieve the cipher text

- The key for Ceasser cipher is the number of letters each plaintext letter will be shifted.
- a key length of 3 will burn the letter a to D, b to E and so forth
- Encryption: $E(x) \equiv x + k(mod 26)$ where k is the key
- Example: let the key length be 7, or k=7 and let the plain text be the word bat.

$$E(b) = 1 + 7 \equiv 8(mod 26)$$

$$E(a) = 0 + 7 \equiv 7(mod 26)$$

$$E(t) = 19 + 7 \equiv 0(mod 26)$$

- taking the values of 8 7 0 we get the ciphertext IHA
- Decryption: $D(y) \equiv y - k(mod 26)$ where k is the key
- Example: let the key length be 7, or k=7 and let the ciphertext be the letters IHA.

$$D(I) = 8 - 7 \equiv 1(mod 26)$$

$$D(H) = 7 - 7 \equiv 0(mod 26)$$

$$D(A) = 0 - 7 \equiv 19(mod 26)$$

- taking the values of 1 0 19 we get the plaintext BAT
- There are 26 possible keys for Ceaser cipher, only 25 being actually useful. This is limited by our modulus 26.

How do you attack the Ceaser Cipher:

- Kerckchoff's Principle: when analyzing the security of a cryptosystem you should assume the attacker knows everything about the system except the key itself
- there are three possible attack types

1. Ciphertext Only: Eve only sees the ciphertext. Goal: get the plaintext or better, the key.
2. Known Plaintext: Eve knows the ciphertext and the corresponding plaintext. Goal: get the key
3. Chosen Plaintext: Eve chooses the plaintext and gets to encrypt using Alice and Bob's cipher. Goal: get the key

- how do you attack the Ceaser cipher specifically

1. Ciphertext Only: Brute force, or use frequency analysis
2. Known Plaintext: suppose that Eve learns the ciphertext character N (13) corresponds to the plaintext character y (24) to find the key Eve uses the formula

$$24 + k \equiv 13(mod 26)$$

   by subtracting 24 from both sides, and using modular arthithmatic Eve finds that the key is 15
3. Chosen Plaintext: Eve simply picks the letter a and finds the shift because a=0 so

$$0 + k \equiv k(mod 26)$$