Cryptography 3/6

Reagan Shirk

March 6, 2020

Encryption

- Caesar Cipher
- Substitution Cipher
  - Hill Cipher
    - Permutation Cipher
    - Vigenere Cipher
- Block Cipher

Vigenere Cipher

- plaintext + key = ciphertext
- You have your plaintext and your key. You list out the alphabet as $\{A, \cdots, Z\} \to \frac{\mathbb{Z}}{26\mathbb{Z}}$ with $A \to 0$ and $Z\ to 25$
  - You add the number for the plaintext letter with the number for the key letter and that is your ciphertext
- Not very safe... what can you do instead? Affine Linear Block Cipher

Affine Linear Block Cipher

- Combination of block cipher and vigenere cipher

Attacks

- There are lots of different types of cipher attacks but I was distracted and missed their descriptions, not sure I would've understood even if I had been paying attention though
- Ciphertext only attack
- Known plaintext attack
  - Linear analysis
- Chosen plaintext attack
- If you have the plaintext and a key, it's *easy* to compute the ciphertext (encryption)
- If you have the ciphertext and a key, it's *easy* to compute the plaintext (decryption)
- If you have the plaintext and ciphertext, it's *hard* to compute the key