Computer Security

Reagan Shirk

September 3, 2020

Attacking Mono-Alphabetic Ciphers

- Known plaintext attacks
- Different letters appear at different frequencies in the English language
  - E appears very often, followed by T and A.
- This means that if we write some text and change every letter with some unknown characters, we can compare the frequencies of the characters against the frequencies of letters used in the English language to decrypt the message
- This is called frequency analysis
- You can also look at frequencies of three letter words if you notice patterns in the ciphertext (like two letters next to each other)

Vigenere Cipher

- Aims to break the ability to do frequency analysis
- Mono-Alphabetic is one-to-one mapping, we should now introduce one-to-many or many-to-one mapping to avoid issues with frequency
- A Vigenere Cipher uses a *set* of mono-alphabetic substitution rules
  - the key determines what the sequence of rules is, this is called poly-alphabetic
- Take a plaintext of BANDBAD
  - You shift these letters 3153153, respectively
  - This means the ciphertext message is EBSGCFG

Hill Ciphers

- This encrypts m letters of plaintext at each step
  - plaintext is processed in blocks of size m
- For this cipher, $c = Kp$
  - the matrix $m \times m$ is the key (K)
  - decryption is multiplication by the inverse $p = K^{-1}c$
- He's moving too fast for me rn but I have cryptography notes from last semester about this stuff so I'll try to fill in gaps with those later