Cryptograpy 3/9

Reagan Shirk

March 9, 2020

Ciphers and Attacks

- Caesar - exhaustive
- Substitution - frequency
- Affine Linear Block - linear analysis
  - Vigenere
  - Hill
    - Permutation
- There are ways beyong mathematical attacks such as side channel analysis and social engineering

Advanced Encryption Standard (AES)

- Before AES, people used something called DES
  - "Dumb encryption standard" - Jake Crampton
  - The keyspace for DES is very small
- 1997 came with the creation of NIST/NSA
  - Supposed to design an encryption standard
  - It was called NIST but it was basically the NSA
  - Goal was to replace DES
  - Open competition rather than designing in your house. . . ?
- AES was actually founded by two people in Europe
  - Rijmen and Daemen
  - Rijndael Cipher
- 2001 came with. . . something?
- Different kinds of attacks:
  - ciphertext only
  - known ciphertext attack
  - chosen plaintext attack
  - chosen ciphertext attach (CCA)
- In the AES standard, the last round has three transformations, every other round has four transformations.
  - Do I know what this means? Not even a little bit.