Cryptography 2/26

Reagan Shirk

February 26, 2020

Caesar Cipher

- Encryption:

$$\begin{aligned} \Sigma &\to \Sigma \\ \Sigma &= \mathbb{Z}/26\mathbb{Z} \\ x &\to x + k \\ \text{Affine Linear Cipher: } x &\to k_1 x + k_2 \\ k_1, k_2 &\in \mathbb{Z}/26 \\ \forall\ x,\ D(E(x)) &= x \end{aligned}$$

- Math is important for security

Substitution Cipher

- Random permutation of the alphabet
- key space: $26! \approx \left(\frac{26}{e}\right)^{26} \approx 10^{26} \approx 2^{\frac{26}{3} \times 10} \approx 2^{85}$
  - This is Stirling's formula...?
- The Codebook: An example
  - The Cipher was chosen at random by 26 students in the class

Alphabet	Cipher
A	G
B	S
C	O
D	K
E	Z
F	F
G	P
H	Y
I	U
J	D
K	A
L	B
M	X
N	Q
O	J
P	W
Q	N
R	T
S	H
T	C
U	I

Alphabet	Cipher
V	L
W	E
X	V
Y	R
Z	M

- COLORADO = OJBJTGKJ
- UTAH = ICGY

The Frequency Attack "This is very very important"

- Almost 1000 years after Caesar's Cipher
- Problem with English language is that it is a... boring language? I didn't catch what he said
- Letters occur in different frequencies
  - e is the most frequent, followed by t then a
  - z is the least frequent
- You can break the subsitution cipher by getting a buuuuuuuunch of messages and comparing the letter frequencies of the encrypted messages to the letter frequencies of the English language
  - You may have a couple wrong letters but that doesn't really matter
- If your plaintext space is small, you will have a frequency problem
  - How do you increase your plaintext space? Block Cipher

Block Cipher

- Instead of encrypting character by character, we're going to encrypt entire character blocks
  - The frequency of information is getting smaller and smaller because your plaintext space is large
- For a two character block, your codebook is 26^2, it's 26^3 for a three character block, etc.
- Random codebook could lead to issues because the codebook would be too large, you want a small codebook
  - You need to strike a balance, you need some type of rule that won't end up being easy to solve (like Caesar's Cipher)

Permutation Cipher

- Since you're going to be counting characters anyways, we won't change characters. But we will permutate their positions...?
- Example:
  - Given a list [1, 2, 3, 4, 5, 6, 7, 8], your encryption would be [3, 5, 1, 8, 6, 7, 2, 4]
  - Oh wait I think this is just like scrambling the words, I don't think it'd be very effective?
  - [C, O, L, O, R, A, D, O] = [L, R, C, O, A, D, O, O]
- Your keyspace size is 8!
- Your plaintext space is 26^8
- You can combine permutation and substitution
  - First permutate, then substitute, then permutate, then substitute but it's still not very safe