SI110
Symmetric Encryption

Major Brian Hawkins, USMC

U.S. Naval Academy

Fall AY 2018

Outline

What is Cryptography?

The study and practice of *hiding secret information*.

In this course.....

...we'll look at:

1. Encryption
   - Scrambling a message so that only the intended recipient can unscramble it.
   - A method of encryption is called a *cipher*.
2. Hashing (hash functions)
   - Creating a number from a file or string that's hard to reverse.
   - Two different files or strings should almost never *hash* to the same number.
3. Steganography
   - Hiding even the existence of a message in some other medium

Caesar Cipher

- Alice wants to send Bob a secret message (juicy!)
- Beforehand, they agree on some value k, as a shift value. We call k the "key".
- To encrypt her message – called the plaintext or PT, Alice shifts each letter k spots to the right (mod 26).
- Alice sends the encrypted message – the ciphertext or CT – to Bob.
- Bob receives the CT, shifts each letter to the left k spots, and recovers the PT
- Question – if Eve, a nefarious individual overhears this, will she have any way to reconstruct the message without the key k?

Enter frequency analysis!

The English language (and nearly all others) are highly non-random.
What's the most commonly used letter?
Second most?

The Vigenere Cipher

How could we address some of the flaws of the Caesar Cipher?

Frequency Analysis of the Vigenere Cipher

Can we use frequency analysis on the Vigenere Cipher?

Chosen Plaintext Attack

If we could pick a message (or part of a message) to be encrypted, could we then discover the key?

Questions

Questions?