Day 1 Notes

Emily Vogel

January 28, 2020

1 Introduction to Cryptography

1.1 Name Origins

The name comes from Greek roots, the first meaning 'hidden or secret' and the second meaning 'writing'.

Cryptology refers to the study of communication securely over insecure channels.
Cryptography refers to writing messages securely.
Cryptanalysis refers to the study and analysis to break hidden messages.

1.2 The Types of Keys

Symmetric Key Alice and Bob use a pre-shared secret key.
Public Key Bob makes one key *public* so that Alice can encrypt a message. However, Bob can only decrypt it using his *private* key.

1.3 Why it Matters

Confidentiality - Only Bob should be able to read Alice's message.
Data Integrity - Alice's message shouldn't be altered in any way.
Authentication - Bob wants to make sure Alice actually sent the message.
Non-Repudiation - Alice cannot claim she didn't send the message.

1.4 History

1.4.1 5th Century BC

Steganography hides the existence of a message. This could be in the form of invisible ink or a shaved head or something else.

NOTE: This is different from ***Cryptography*** *because cryptography hides the meaning of a message, not it's existence.*

Scytale was a way to encrypt a message by wrapping a piece of leather around a cylinder. Used by Lysander of Sparta.

1.4.2 1st Century BC

Caesar Cipher was used by Rome. See next section for more details.

1.4.3 9th - 10th Century

Cryptanalysis, created by Arabs, invented a systematic study of ways of deciphering a code without a key. This was detailed in the *The Secretaries' Manual*.
Frequency Analysis uses frequently used letters to decipher the code.

1.4.4 15th Century

Nulls were used to confuse frequency analysis by inserting random characters like * into the plaintext. Used in Babington plot to assassinate Queen Elizabeth and led to the trial and execution of Mary, Queen of Scots.

1.4.5 1586

Vigenère Cipher uses multiple caesar ciphers to encode a piece of text. Using a plaintext message and a chosen key (like 'lemon'), encrypt each letter with a different caesar cipher key.

1.4.6 1854

Charles Babbage found a solution to the Vigenère Cipher. Created the analytical engine and herald as the 'father of the computer', along with **Ada Lovelace**.

1.4.7 1920s - 1940's

Enigma Machines were used in WWII by the Germans to encode messages. The Polish Cipher Bureau, along with Alan Turing, found a way to break the German Enigma.

2 Caesar Cipher

2.1 Introduction

Note: as a common convention, plaintext is in lowercase (a-z) and ciphertext is in uppercase (A-Z).

It is also called the **Shift Cipher**. This cipher *maps letters to numbers*:

- a = 0
- b = 1
- c = 2

A **Key** is defined, specifying how many letters to shift. I.e. k = 7.

2.2 Equations

2.2.1 Encrypting

$$E_k(x) \equiv x + k \pmod{26}$$

2.2.2 Decrypting

$$D(y) \equiv y - k \pmod{26}$$

2.3 Example

k = 7, plaintext = 'bat' or 1 0 19.

$$E(1) = 1 + 7 = 8 \pmod{26} = 8$$

$$E(0) = 0 + 7 = 7 \pmod{26} = 7$$

$$E(19) = 19 + 7 = 26 \pmod{26} = 0$$

ciphertext= IHA

2.4 Kerckhoff's Principle and Types of Attack

Kerckhoff's Principle refers to when analyzing the security of a cryptosystem, assume Eve knows everything about the system except the key.

Ciphertext only Attack Eve only knows the ciphertext being sent, she wants to find plaintext or the key being used.

Known Plaintext Attack Eve has a ciphertext as well as its decrypted plaintext. She wasnt to determine the key.

Chosen Plaintext Attack Eve chooses a plaintext and encrypts it using the encryption function to see the cipher text. She wants to determine the key.

2.5 Attacking the Caesar Cipher

2.5.1 Cipher Only Attack

You can use *Frequency Analysis* or *Brute Force* (try all 26 shifts).

2.5.2 Known Plaintext Attack

Suppose we know the plaintext y(24) encryptes to ciphertext N(13), then

$$24 + k \equiv 13 \pmod{26}$$

$$k \equiv 13 - 24 \equiv -11 \equiv 15 \pmod{26}$$

2.5.3 Chosen Plaintext Attack

Choose the easiest letter to see the key. In this case, it would be 'a' since it maps to 0.