MATH 314 Spring 2018 - Class Notes

8/27/2018

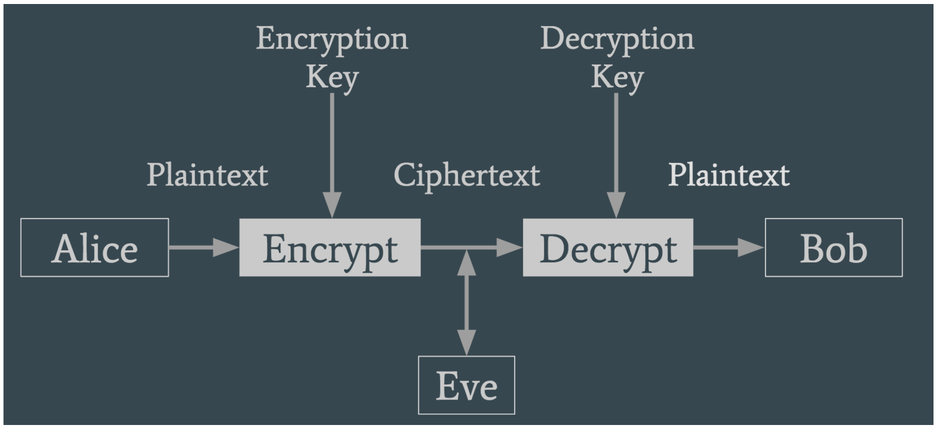
Scribe: Carleigh Duncan

Summary: History of cryptography was covered, but will not be revisited. The Caesar Cipher was covered in detail.

Notes:

Cryptography: the act of writing messages securely. Related fields include:

- **Cryptology**: the study of communicating securely over insecure channels
- **Cryptanalysis**: the study of methods to analyze and break hidden messages



The above image illustrates the purpose of cryptography. Assume Alice and Bob are communicating, and Eve is eavesdropping on the ”secure” conversation. If Alice **encrypts** her plaintext message into Ciphertext, using an encryption key, only those who have the decryption key can **decrypt** the message, returning it to plaintext. This would make eavesdropping nearly impossible.

There are two types of keys. The **symmetric key** method (**symmetric cryptography**), as shown above, only allows those who have the decryption key to read the message. This presents a problem, as the two entities communicating over this secure connection must have ”met” before, in order to swap keys and establish the secure connection.

The second type of key was introduced in the 1970’s, and is the **public key** method, or **asymmetric cryptography**. Using this method, any entity can encrypt a message using the receiver’s public key, but the encrypted message can only be decrypted with the receiver’s private key.

Why It Matters

In terms of the above example, here are some reasons why encryption matter:

Confidentiality: Only Bob should be able to read Alice's messages, otherwise Eve could not only read the messages, but corrupt the messages.
Data Integrity: Alice's messages 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

History

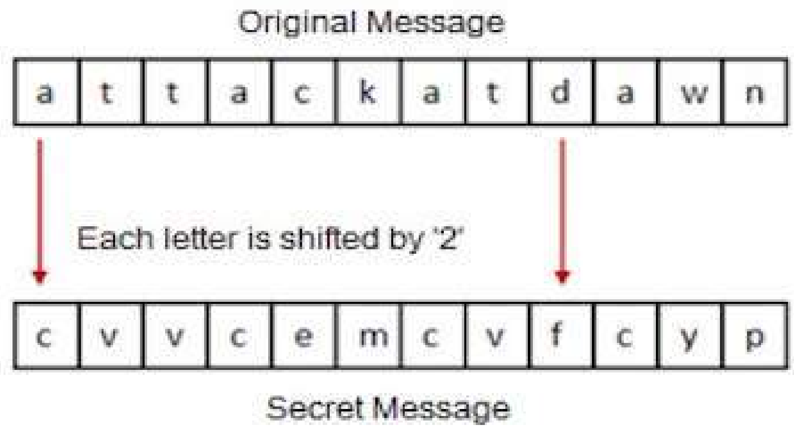
In the 5th century BC, hidden writing, or **steganography**, was widely utilized. Unlike cryptography, which is the act of writing messages securely, steganography is the act of *hiding the existence of a message.*
The first (loose) example of cryptography was the scytale.
The first *practical* example of cryptography arose during the 1st century BC, and was created by Julius Caesar, hence its name the **Caesar Cipher**.

The Caesar Cipher

The Caesar cipher works by shifting the letters in a message by k spaces in the alphabet. Mathematically, the formula is

$$E(x) = k + x \pmod{26} \tag{1}$$

where x is the numerical representation of the letter being encrypted (A=0, B=1, C=2 ...), and k is the **key** by which the message is being shifted.
For example, k=2 in the below graphic.



To **decrypt** the message, each letter is shifted by k in the opposite direction. The formula for decryption is as follows

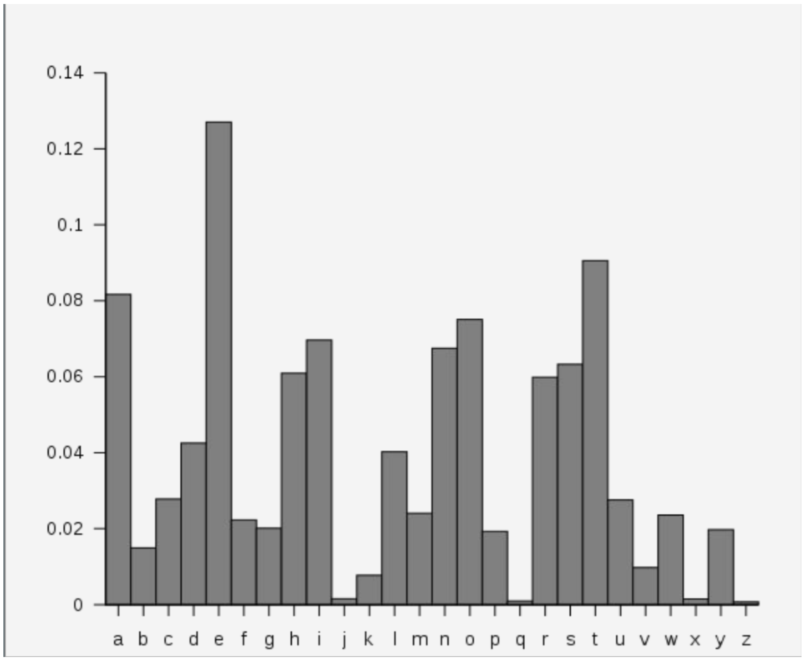
$$E(x) = k - x \pmod{26} \tag{2}$$

It should be noted that in this class the convention for encrypted/decrypted messages is as follows:

An encrypted message, or **ciphertext** is represented as UPPERCASE, and the decrypted message, or **plaintext** is represented as lowercase.

Frequency Analysis

During the 9th-10th century, the Arabs invented **cryptanalysis**, the systemic study of ways of deciphering a code without a key. The most notable method was known as frequency analysis. This examines the frequency at which letters tend to appear in messages, and uses this information to decipher code



There is a recurring theme in the realm of cryptography:

- A secret code is invented
- Typically called "unbreakable" by inventor
- Used by spies, ambassadors, kings, and generals for crucial tasks
- Eventually broken by enemy using cryptanalysis