Cryptography - Day 1: Introduction and the Caesar Cipher

MA 111: Intro to Contemporary Math

September 27, 2013
Definition: Cryptography

In the most general sense, **Cryptography** is the process (and mathematical underpinnings) of changing a message that is written plainly in some language (i.e. English) to make it appear unreadable to everyone except the intended recipient.

The process of changing the message from readable to unreadable is called **Encryption**. In order to do so, we require something called an **Encryption Key**.

Before an encrypted message can be read, it must undergo **Decryption**, the process of changing from unreadable back to readable. We will require a **Decryption Key** to do this.
Cryptography Notation: □ and ⊠

**Plaintext** is used to describe unencrypted/decrypted, readable language. We will use □ to describe numbers associated with plaintext.

**Ciphertext** is used to describe encrypted, unreadable language. We will use ⊠ to describe numbers associated with ciphertext.

For example, with the standard alphabetic encryption key, a plaintext message “F” is □ = 6.

Whereas, a ciphertext “T” is ⊠ = 20.
Congratulations, You Are Now A Spy 1

Your first mission is to intercept communications from an enemy agent, code named GOOFUS. Unfortunately, all enemy agents use some method to disguise their messages from being read. Fortunately, Agent GOOFUS is known to use a relatively simple method for doing this.

Enemy agents are after one of several (code named) targets:

   DOG, MAN, BOY, DAD, MOM, BIT, BOT

- If you intercept the message “PRP”, who is the target?
- Using the enemy agents’ method above, how would the word “ZOD” be sent?
Encryption Method: Caesar Cipher

The **Caesar Cipher** is a code that encrypts a letter by moving it 3 units to the right (with respect to alphabetic order).

For the letters A–W, this encryption can be described using the rule

\[ \square + 3 = \bigotimes. \]

What about the letters X, Y, and Z?

They are encrypted as A, B, and C respectively.

Encryption for the Caesar Cipher can be described completely using *modular arithmetic* as

\[ \square + 3 (\text{mod } 26) = \bigotimes. \]
Julius Caesar has been surrounded during the battle of Alesia! He needs you to respond to two questions posed by one of his lieutenants. Unfortunately, those filthy Gauls are everywhere!

You will need to encrypt Caesar’s answers:

▶ Question: What do you need?

Caesar’s Answer: WATER

▶ Question: Do we attack tomorrow?

Caesar’s Answer: YES
A Caesar Cipher can be decrypted by moving 3 units to the left (against alphabetic order).

For the letters D–Z, this decryption can be described using the rule

\[ \text{⊠} - 3 = \Box. \]

The letters A, B, and C are decrypted by wrapping back around the alphabet to X, Y, and Z respectively.

Decryption for the Caesar Cipher can be described completely using modular arithmetic as

\[ \text{⊠} - 3 (\text{mod } 26) = \Box. \]
You return to Caesar with a message from a Lieutenant.

- The message gives the time of the next attack. It is encrypted as the following:
  
  GDZQ

- Like all Romans, Caesar is extremely superstitious and avoids making actions on the left. If you were to decrypt the message above by *only moving to the right*, how much would you have to move by?
Hail Caesar 3

One last exchange message before the attack:

- Caesar asks you to encrypt and deliver the following message:
  
  FORTUNA
  
- You return with the following encrypted message. Decrypt it for Caesar:
  
  YLFWRULDL
Related Idea: Frequency Analysis

The Caesar Cipher disguises letters, but does not disguise the natural frequency of letters!

Given a Caesar Cipher, the most frequent symbol used in the ciphertext will most often correspond to “E” in the plaintext.
We will talk about several different types of codes during the next few weeks and it will be good to keep a summary for each. The ideas behind Encryption Key and Decryption Key for the Caesar Cipher will be applicable to all codes. Additionally, Key Secrecy (how secret the decryption key must be) and Letter Frequency (how much a cipher changes the nature of how often letters appear) will become increasingly important.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>Key Secrecy</th>
<th>Letter Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caesar</td>
<td>+3</td>
<td>-3 or +23</td>
<td>Private</td>
<td>Normal</td>
</tr>
</tbody>
</table>
Related Idea: Modular Arithmetic

We will often say things like “$b$ is equal to $a$ modulo $n$”. This means the following:
We write $b = 0 \pmod{n}$ if $n$ divides (no remainder) into $b$.
We write $b = 1 \pmod{n}$ if $n$ divides perfectly into $b - 1$.
We write $b = 2 \pmod{n}$ if $n$ divides perfectly into $b - 2$.
We write $b = 3 \pmod{n}$ if $n$ divides perfectly into $b - 3$.
\[ \vdots \]
We write $b = a \pmod{n}$ if $n$ divides perfectly into $b - a$.

This is a simple mathematical idea to describe, but it takes some practice to get used to. We’re most comfortable with the idea of “mod 12” because it describes an analog clock.

Amazingly, this idea is the basis for many different types of codes, both ancient and modern.
Homework Assignments

1. read pp. 387-391 on Substitution Ciphers (Cryptography Section)
2. HW 5 - Cryptography 1 may become available?