MATH 314 - Class Notes

8/29/2017

Scribe: Yitzi Turnianski

Summary: Overview of cryptography and an introduction to the Caesar Cipher.

Notes: Definitions:

- Cryptology - the study of secure communication
- Cryptography - writing secure messages
- Cryptanalysis - trying to read secure messages

Alice wants to send a secure message to **Bob**, and **Eve** wants to eavesdrop.

The original message is called the *plaintext* and then Alice encrypts it with some method. The encrypted message is called the *ciphertext*, which Bob must decrypt to read. Eve may want to: a) read Alice's message, b) corrupt Alice's message, or c) pretend to be Alice.

It is the goal of cryptographers to ensure four things:

- Confidentiality- only Bob may read the message
- Data Integrity- the message isn't altered
- Authentication- Alice is the only one who could have sent the message
- Non-repudiation- Alice can't deny having sent the message

Many encryption methods have been used throughout history to send messages. The ancient Greeks used steganography, such as invisible ink, which were methods to hide the existence of a secret message. This contrasts with cryptography, where the *content* of the message is obscured, but the existence of the message is known to Eve.

Eventually, people started using primitive encryption methods, such as *scytales* (a message wound around a stick of a known radius) and *ciphers* (a message written in an alphabet that is shifted over). In response to these methods, cryptanalysts started thinking of ways to beat these methods, such as *frequency analysis*- ie, guessing the cipher based on how commonly letters are used. More ciphers were developed, oftentimes abandoning the one-to-one correspondence of old ciphers, but still more ways to crack them were developed, eventually leading to the use of early computers assisting in the job.

This pattern of developing a new encryption method, calling it "unbreakable", using it for sensitive communication, and then someone cracking it will be a repeating pattern throughout history.

We can analyze encryption methods mathematically to determine how difficult they are to break. For example, we can start with a Caesar Cipher, which shifts the alphabet by κ (originally shifting

the alphabet by $\kappa = 3$). To encrypt, we will assign to each letter of the alphabet an index, i, from 0 through 25, and then map each letter to the letter of index $(i + \kappa) \mod 26$.

Example:

`helloworld`

becomes

7 4 11 11 14 22 14 17 11 3.

Shift it by $\kappa = 3$ and you get

10 7 14 14 17 25 17 20 14 6

which, turned back into letters, becomes

`khoorzruog`.