Lesson 7: Simple Encryption

Adapted from code.org curriculum

Objectives: You will be able too…

- Explain why encryption is an important need for everyday life on the Internet
- Crack a message encrypted with a Caeser cipher using a Caeser Cipher Widget
- Crack a message encrypted with random substitution using Frequency Analysis
- Explain the weaknesses and security flaws of substitution ciphers

Getting Started: The critical role of encryption in everyday life

- 5 minutes – What do you know about encryption?

Getting Started: The critical role of encryption in everyday life

- In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?

Getting Started: The critical role of encryption in everyday life

- In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?
  - Surprise birthday party
  - A play in a sports game, your hand in a card game
  - PIN numbers, SSN
  - Business and government negotiations
  - Military activity

Getting Started: The critical role of encryption in everyday life

- Secrecy is a critical part of our lives, in ways big and small
- As our lives increasingly are conducted on the Internet, we want to be sure we can maintain the privacy of our information and control who has access to privileged information
- As we saw in the Internet Unit, the internet is NOT secure…
  - Packets traveling across the Internet move through many routers, each of which is owned by different people/orgs
  - So we should assume all information is public, as if written on a postcard and sent through the mail

Getting Started: Classic Encryption – The Caeser Cipher

- Many of the ideas we use to keep secrets in the digital age are far older than the Internet. The process of encoding a plain text message in some secret way is called Encryption
- For example in Roman times Julius Caesar is reported to have encrypted messages to his soldiers and generals by using a simple alphabetic shift - every character was encrypted by substituting it with a character that was some fixed number of letters away in the alphabet.
- As a result an alphabetic shift is often referred to as the Caesar Cipher.

Getting Started: Classic Encryption – The Caeser Cipher

- Prompt:
  - This message was encrypted using a Caesar Cipher (an "alphabetic shift").
  - Let's see how long it takes you to decode this message (remember it's just a shifting of the alphabet):

serr cvmmn va gur pnsrgrevn

Getting Started: Classic Encryption – The Caeser Cipher

- With this simple encryption technique it only took a few minutes to decode a small message.
- What if the message were longer BUT you had a computational tool to help you?!

Activity: Cracking Substitution Ciphers

- We will be using Code Studio Unit 4 - Stage 5
- Part 1 – Crack a Caeser Cipher
- Part 2 – Crack a Random Substitution Cipher

Wrap-up

- Encryption is essential for every day life and activity
- The "strength" of encryption is related to how easy it is to crack a message, assuming adversary knows the technique but not the exact "key"
- A random substitution cipher is very crackable by hand though it might take some time, trial and error.
- However, when aided with computational tools, a random substitution cipher can be cracked by a novice in a matter of minutes.
- Simple substitution ciphers give insight into encryption algorithms, but as we've seen fall way short when a potential adversary is aided with computational tools…our understanding must become more sophisticated.
- If we are to create a secure Internet, we will need to develop tools and protocols which can resist the enormous computational power of modern computers.

Wrap-up:

- How much easier is it to crack a Caesar cipher than a random substitution cipher? Can you put a number on it?
- Was it difficult to crack a Random Substitution cipher? Did it take longer than you thought? shorter? Why?
- Any encryption cipher is an algorithm for transforming plaintext into ciphertext. What about the other way around? Can you write out an algorithm for cracking a Ceasar cipher? What about a random substitution cipher?

Wrap-up:

- Recall that in RFC 3271, “The Internet is for Everyone” Vint Cerf wrote the following. What did he mean by “cryptographic technology?” What does it mean?

Vocabulary:

- Caeser Cipher – a technique for encryption that shifts the alphabet by some number of characters
- Cipher – the generic term for a technique (or algorithm) that performs encryption
- Cracking encryption – when you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to "crack" the encryption.

Vocabulary:

- Decryption – a process that reverses encryption, taking a secret message and reproducing the original plan text
- Encryption – a process of encoding messages to keep them secret, so only "authorized" parties can read it
- Random Substitution Cipher – an encryption technique that maps each letter of the alphabet to a randomly chosen other letter of the alphabet