Will Gillette, Alan Okinaka

Dr. Mongan

CS-471: CS Pedagogy

8 September 2023

Lightning Talk #2: Crytography

Introducing the Widgets (2 min.):

Students will understand:

- That cryptography is the process of encoding information so that only exclusive people or groups can decipher it and has many applications in the technical world.
- That the Caesar cipher cryptographic method involves shifting the English alphabet by a certain increment to scramble the characters in a message. The message can be easily decrypted since there are only 26 letters in the alphabet.
- That the random substitution cryptographic method involves arbitrarily shuffling the characters of the English alphabet. Using this method makes it significantly more challenging for external parties to decrypt messages compared to the Caesar cipher because the resulting alphabet is not in any specific order.

Main Idea Questions:

1.) What is cryptography, and why does society use it?

2.) How can corporations and businesses use cryptography to secure classified information?

3.) How did the Caesar Cipher cryptographic method originate? How does it encode information? What are the benefits and costs of using it?

4.) How does the Random Substitution method work to encrypt data? How does it compare to the Caesar Cipher method?

5.) How can individuals examine character frequencies as a tool for decryption?

Exploring the Widgets (5 min.):

- Students will explore the code.org Frequency Analysis Widget, exploring how they can analyze character frequencies to facilitate the decryption process.
- Within the same widget, students will use both the Caesar Cipher and random substitution methods to encrypt their own messages.
- Activity: The following message was encoded using the Caesar Cipher method with a shift of 7 characters. Use the Frequency Analysis Widget to decrypt the message: **"Ghp, xgvhwx mabl fxlltzx nlbgz max ktgwhf lnulmbmnmbhg, tgw kxihkm rhnk kxlnem."**

Discussing Key Takeaways (1 min.):

- Instructors will review the main idea questions conveyed during the beginning of the lesson and have students attempt to answer them.
- **Take-Home Question:** Use either the Caesar cipher or random substitution method to encode a message to give to a partner. Have the partner decode the message without informing them of which method you used.