Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

11 October 2023

Cryptography Assessment Plan

Lesson Topic: Introduction to Cryptography: General Overview and Applications, Study of Caesar Cipher, Random Substitution, and Vigenère Cipher Cryptographic Methods

Learning Objectives:

- *Students will understand that…*
    1. Cryptography is the process of encoding information so that only exclusive people or groups can decipher it and has many practical applications in the technical world.
    2. 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.
    3. 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.
    4. The Vigenère cryptographic method is the most secure method relative to the Caesar Cipher and random substitution methods due to the incorporation of a

private key that substantially increases the number of possible combinations for character mappings.

- *Students will be able to independently use their learning to…*
    1. Analyze practical scenarios in which cryptography may be applicable and understand how its incorporation can promote the security of classified information.
    2. Evaluate the strengths and weaknesses of three cryptographic methods: the Caesar cipher, random substitution, and the Vigenère cipher, understanding when it would be practical to apply one compared to the other.
    3. Detect instances in which others are actively using cryptography to encrypt data.
- *Students will be skilled at…*
    1. Using the code.org widgets to encode their own messages using all three methods.
    2. Understanding how to accurately shift the alphabet by a certain increment without the use of Code.org widgets.

<u>Formative Assessments (Lesson Checkpoints):</u>

- Distribution of the first formative assessment will occur after instructors introduce students to the Caesar Cipher cryptographic method and walk them through using the Frequency Analysis Widget on code.org. Students will utilize this widget to decrypt an encrypted message using the Caesar Cipher method, and then encrypt the decrypted message back using the Random Substitution method. Thus, this evaluates progress at Learning Goals 1.1, 1.2, 1.3, 2.3, 3.1, and 3.2:
    - ➢ 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 and

complete the communicated task: **“Ghp, xgvhwx mabl fxlltzx nlbgz max ktgwhf lnulmbmnmbhg, tgw kxihkm rhnk kxlnem.”**

- Students will receive the second formative assessment after instructors discuss how the Vigenère Cipher method compares to the Random Substitution and Caesar Cipher methods. Instructors will additionally explain how the Vigenère Cipher works to promote more secure encryption. This assessment targets the application of the Vigenère Cipher method, ensuring students understand how to utilize the widget for encryption and decryption. Thus, this evaluates progress at Learning Goals 1.1, 1.4, 2.2, 2.3, and 3.1:
  - Using the Vigenère Cipher widget, decode this question and answer it.
    - **SECRET_KEY:** PASSWORD
    - **Message:** SORPJHQNBONRWAOCTNUITCJLCNRD_GYRSS?

Summative Assessment (Post-Lesson Assignment):

- Students will be evaluated on how they believe cryptography can contribute to the business world and evaluate its significance in the modern world. The primary objective of this assessment is to target the transfer learning objectives to ensure that students understand the application of these tools in the real world. Specifically, this assessment targets learning objectives 1.1, 1.2, 1.3, 1.4, 2.1, 2.3, and 3.2:
  - Submit a report recalling instances in which you have witnessed cryptography firsthand. What was the context, and why was it necessary? To elaborate, without cryptography, what problems would the respective business likely encounter? Which of the three cryptographic methods described does it relate to the most, and why? If you are unable to recall a situation in which you have noticed the usage of

cryptography, think about scenarios in which it would be favorable for companies to incorporate concepts from cryptography.

Summative Assessment Rubric:

Description	Pre-Emerging (<50%)	Beginning (50%)	Progressing (85%)	Proficient (100%)
Relevant Situation/Scenario Identified and Described Thoroughly	Student does not clearly define a scenario relevant to cryptography or describes one that has trivial significance.	Student identifies a relevant scenario but does not elaborate upon it enough to demonstrate connections to specific concepts from cryptography.	Student describes the context of their relevant scenario and makes connections with specific concepts from cryptography but does not describe the significance of the scenario or why cryptography was necessary.	Student demonstrates full understanding and knowledge about how their significant scenario encompasses several specific concepts from cryptography and makes an argument for why cryptography is necessary for their respective scenario.
Discussion of Potential Issues without Cryptography Usage	Student does not make any considerations about how their scenario could have changed without the presence of cryptography.	Student makes some considerations about how a lack of cryptography could have made their scenario different but does not elaborate enough to demonstrate understanding of the specific roles of cryptography.	Student includes a meaningful reflection to present understanding of how cryptography's presence promotes security in a general sense but does not elaborate on this enough to address specific roles of cryptography.	Student demonstrates that they have identified all the specific roles that cryptography ties into their scenario and discusses what specific issues could arise if there were no cryptography usage during their scenario.
Description of Connection to at least one Cryptographic Method	Student does not connect their specific scenario to any of the three cryptographic methods described during the lesson.	Student describes how cryptography applies to their scenario in a general sense but does not identify which of the three cryptographic method is most relevant in their scenario.	Student identifies at least one cryptographic method that ties into their scenario but does not elaborate enough about the respective method's relevance to the scenario.	Student makes a connection to at least one of the three cryptographic methods described during the lesson and makes a meaningful argument as per why they believe that respective method is the

				most relevant compared to the other two methods.

Summative Assessment Contract Grading:

- To receive an A…:
    - Describe why the chosen method is the most relevant in this scenario compared to the other two methods and make a compelling argument if another method would be more applicable to the respective scenario.
    - Explain at least two reasons as per why cryptography is necessary for the respective scenario in a general sense and tie this reasoning into the reported potential issue that would exist without cryptography.
    - All requirements for a B are met.
- To receive a B…:
    - Describe how the potential issue identified relates to at least two specific roles of cryptography.
    - Form a connection between either the Caesar Cipher, Random Substitution, or Vigenère Cipher method and the respective scenario. Explain why it is relevant.
    - All requirements for a C are met.
- To receive a C…:
    - Describe at least one potential issue that could arise in your respective scenario if there were no usage of cryptographic methods.
    - All requirements for a D are met.
- To receive a D…:

- Describe a scenario in which you have witnessed the application of cryptography or explain a situation in which a business would benefit from implementing cryptographic methods.