Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

23 October 2023

Cryptography Unplugged Activity: One Student at a Time

Lesson Topic:

For my lesson topic, I wish to continue building on teaching concepts within the realm of cryptography, developing lesson activities that enable students to understand basic information hiding techniques and ultimately be able to apply the Caesar Cipher method for encoding and decoding messages. My unplugged activity hopes to engage students of all learning backgrounds, enabling students without prior experience to see the practicality of these methods and to challenge those who are experienced. Thus, I hope to incorporate various ideas from the Universal Design for Learning (UDL). This activity comprises of two parts: one introducing information hiding protocols (heavily inspired from the CS Unplugged Book), and another involving the entire class working together to decrypt an encoded message by applying several iterations of the Caesar Cipher method.

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.

- *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. Detect instances in which others are actively using cryptography to encrypt data.

Prerequisite Skills/Knowledge:

- *Students will be skilled at…*
    1. Computing the sum and product of two integers.
    2. Understanding how to accurately shift the alphabet by a certain increment without the use of Code.org widgets.

Materials Needed:

- Writing Utensil
- Deck of Flash Cards

Activity 1: Computing Average Height

1. The instructor writes down a random two-digit number discretely and reports it to a random student. This two-digit number is the "secret key."
2. The random student then computes their height in inches (12*ft. + inches) and adds this number to the instructor's secret key, writing it down on a piece of paper.

3. The first student then reports this new number to the student adjacent to them, having them repeat the same process as described in the second step. The only difference with this step is that the student will be computing the sum of their height in inches and the previous student's computed number.
4. This process repeats until accounting for every student in the class. The last student hands their paper with their number to the instructor, who subtracts the secret key from it. By dividing by the number of people in the class, the instructor displays the average height in inches and converts it back to feet.
5. The instructor reveals the process of the fourth step to the class, noting that it is impossible for any outsider to figure out any individual's height without the cooperation of at least two students.

Activity 2: Incremental Caesar Cipher Shifting:

1. The instructor chooses a short phrase as a "secret key" and applies a random Caesar Cipher shift to that phrase, remembering the increment of the random shift before writing down the encrypted phrase on a sheet of paper and handing it off to the nearest student.
2. The first student applies a second layer of encryption to this phrase using a Caesar Cipher shift with an increment of one. This student then writes down this new phrase on a different sheet of paper and hands it off to the student adjacent to them.
3. The process described in step two repeats until accounting for each student. Essentially, each student adds an additional layer of encryption to the original message.
4. Now, each student plays a role in decrypting the message. This process begins when the last student hands the final encrypted message to the first student. The first student

applies a reverse Caesar Cipher shift with an increment of one, recording the result on a new sheet of paper before handing it off to the student adjacent to them.

5. Step four's process repeats until accounting for each student. Now, like at the end of the encryption process, the last student hands the final resulting phrase to the first student. Step four's process repeats for a certain number of students to account for the instructor's initial random Caesar Cipher shift at the start of this activity. Ultimately, one student will have bypassed the final layer of encryption, resulting in the instructor's original phrase.

Accessibility:

- In both activities, the instructor must play a key role in verifying each student's result to ensure that no errors are present. This is essential as one student's mistake can affect the result of other student's as the activity progresses. Therefore, the instructor is also able to oversee students and ensure that they are understanding how to compute the next result (either by adding their height in inches to the previous number or by applying a forward or backward Caesar Cipher shift of one to the previous message). To elaborate, if a student is struggling, the instructor could guide them through the necessary steps to achieve their result, making the activity more accessible for students of all learning backgrounds.

Formative Assessments:

1. The first activity primarily serves as an introduction to information hiding as a preview of the second activity, so for instructors to formatively assess students, they should have them answer at least one transfer question, allowing students to brainstorm the applications of cryptography in the real world.

2. To bounce off the point on accessibility, the instructor's role as the "verifier" additionally enables them to determine whether each student understands the process and calculations. This is primarily relevant in the second activity, which directly examines students' ability to apply forward and backward Caesar Cipher shifts to a phrase. Essentially, if the instructor correctly verifies the student's result, then it becomes clear that the respective student understands the material. On the contrary, if the student reaches an incorrect result, the instructor can provide feedback and guide the student to the correct result.

Alignment to Learning Standards:

1. The first activity accounts for learning objectives 1.1 and 2.1, which both encompass students' understanding of the fundamentals of cryptography and its applications in the real world. Essentially, the simple example of starting with a numerical secret key and then adding the sum of each student's height in inches sets students up to brainstorm about how this process can provide layers of security to valuable information in the real world.
2. The second activity directly aligns with learning objectives 1.2 and 2.2, which cover students' ability to recognize encrypted messages and perform both encryption and decryption using the Caesar Cipher method. Recall that each student plays an active role in both the encryption and decryption processes, receiving an encrypted message and either adding or removing a layer of encryption from it.

Reflection:

I chose cryptography as my topic because it plays a key role in the world by enhancing the security of all kinds of valuable information. Thus, it is important for students to have familiarity with it, especially as it relates to computer science. I crafted these activities with the intention of having the first activity prepare students for the second activity, which makes logical sense as the second activity follows a similar process to the first but with greater complexity. Thus, my hope is that when conducting these activities, they run smoothly, and students gain significantly more knowledge from the second activity as opposed to the first one. Furthermore, one of the goals of kinesthetic learning is to keep students engaged, and in these activities, each student is playing at least one active role in achieving the final results. With plugged activities, it is much more challenging to keep students engaged, as the internet can be distracting. The goal of the second activity, however, is to present an encrypted message and keep students on edge until they finally decrypt it, helping them stay actively engaged throughout the entire activity. Ultimately, incorporating kinesthetic learning in computer science allows newcomers to learn the fundamental concepts more effectively because these activities present them in a way such that people of all experience levels can make connections.

One challenge I faced when designing the second activity was that I was unsure how feasible it would be for students to finally remove the last layer of encryption. To elaborate, I was unsure about how long this process would take, and I considered that even if only one student makes a mistake, it would throw off the results of the remaining students. To remedy the first problem, I decided to have students use the Caesar Cipher method with a shift of only one, allowing them to encrypt or decrypt their message more efficiently. As per the second problem, I considered having the instructor act as a “verifier,” with the duty of ensuring that each student’s

respective result is accurate. Ultimately, my goal is that these two solutions help the activity remain smooth and efficient, retaining the engagement of all students.

To enhance the second activity in the future, I could incorporate the random substitution method as well, having some students use random substitution for encryption and decryption while others use the Caesar Cipher method. My logic behind choosing not to include this immediately was that I imagined that it would become challenging to verify each student's result or correct an error when both these methods are playing significant roles in the final result. However, if I were to figure out a concise way to incorporate random substitution, it would allow students to compare both cryptographic methods and consider which one provides the strongest security to information. After initially conducting these activities, I hope to refine them using feedback from my peers and consider ways to assess the random substitution method.