Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

29 November 2023

Cryptography: Service-Learning Project Final Draft

My team consists of Lou Hodgson, Alan Okinaka, Briana Bonsu, and Hannah Jeffers, and on November 29th, 2023, we presented our introductory lesson about cryptography in Chris Hayden's AP Computer Science Principles class at Upper Dublin High School in Fort Washington, PA. We developed this K-12 lesson with the goal of piquing our students' interest in cybersecurity and the broad umbrella of computing in addition to gaining exposure to teaching at the high school level. Furthermore, we sought to apply certain practices of effective pedagogy through integrating the Understanding by Design (UbD) framework in addition to the principles of the Universal Design for Learning (UDL) into our lesson, setting up our lesson to enhance any student's knowledge, regardless of their prior experience. To do so, we geared our lesson toward students with introductory backgrounds in computer science, such as those enrolled in AP Computer Science Principles, yet provided options to increase the rigor of our activities to engage those with advanced experience in cryptography. Ultimately, our students provided a lot of positive feedback about our lesson, emphasizing that they greatly enjoyed our activities and gained a deeper understanding of cryptography.

Our lesson began by introducing some key terms related to cryptography, explaining the encryption and decryption processes at a high level in addition to providing some practical applications of cryptography. For example, I emphasized how cryptography promotes the privacy of sensitive information such as medical records. We also asked our students to provide some of their own examples of cryptography's real-world applications. Following this, we presented some essential questions: "How does cryptography work? Why is it useful? What are the benefits and costs of using the Caesar Cipher Method? How does the Vigenère method compare to the Caesar Cipher method?" Essentially, these questions served to target our students' curiosity gap, engaging them prior to our activities. We then proceeded to present the Vigenère widget on code.org, explaining how the rows of its matrix are essentially Caesar shifted mutations of the English alphabet, enabling our students to visualize the connection between both cryptographic methods. We then demonstrated a couple examples of how to encrypt and decrypt messages using this method, emphasizing how this method provides quality security of data. Following our online demonstration of the Vigenère method, we conducted an unplugged activity to introduce the Caesar cipher method.

Alan Okinaka developed five "paper ciphers," one of which we distributed to each pair of students in the class. A paper cipher is composed of both an inner an outer circle, with the English alphabet inscribed on the perimeter of both circles, enabling users to align any letter from the inner circle with any letter from the outer circle. Essentially, this enables students to map the original English alphabet to a uniformly shifted variant of the English alphabet, accurately showcasing how the Caesar cipher method works. Each pair of students first investigated this tool to draw this conclusion, and they ultimately enjoyed exploring it. Following this, we provided each pair two messages: an encrypted message to one partner and an English message to the other partner. We additionally instructed each student to hide their message from their partner. Students essentially had to use the tool to either encrypt their message or decrypt their message. Upon finishing, each student communicated to their partner their mutated message, instructing them to use the tool to perform the opposite operation. Hence, each student gained practice with both encryption and decryption through applying the Caesar Cipher method. To conclude this unplugged activity, we asked students to compare both methods and determine which of the two provided higher quality encryption. Students successfully reasoned that due to its matrix structure, the Vigenère method provides greater security than the Caesar Cipher method. Hence, this first unplugged activity aimed to target several levels of Bloom's taxonomy, having students make connections and evaluations.

To allow students to practice encryption with the Vigenère method, we initiated our second unplugged activity, which involved teams working collectively to unlock their respective lock boxes. Mr. Hayden had already assigned the students to groups for previous work, so we leveraged this when creating teams. We provided each team a handout of the Vigenère cipher matrix, a secret key, a cipher text, and a translation key. We asked each team to vote on the difficulty level of this activity, selecting their cipher text based on their choice. Following the distribution of these materials, we tasked each team with encrypting their cipher text through using both the matrix and the secret key. Upon successfully doing so, students then had to use the translation key to convert their result to a four-digit code, which they used to unlock their box, receiving candy as a reward. In the end, this activity excited students, especially after receiving their reward.

The final piece of our lesson was a reflection period, where students discussed what was easy and challenging about the lock box activity. Some students mentioned that it may have been more convenient to conduct this activity following the demonstration on the Vigenère cipher, as it took them some time to recall how to use the matrix and secret key to encrypt the cipher text. This is a consideration for future presentations of this lesson, but it was convenient for the students to be in teams for this reason, as it was much easier to recall the encryption process by working collectively on this challenge. After providing feedback on the activity, we returned to the essential questions of the lesson to reinforce students' understanding about the real-world practicality of cryptography. By the end of this lesson, students took away the importance of cryptography in securing confidential information.

Design thinking was essential in developing this lesson, as we had to consider the optimal way to target students' learning and appeal to students with a broad range of computing experiences. Beyond pedagogy, I can apply design thinking to my other career interests. For example, software engineers must design their applications so that users can seamlessly use them without any difficulties or confusion. Hence, I must apply design thinking when developing my user acceptance tests, which account for all the actions of each user. Furthermore, I must ensure that I am meeting all the requirements of my stakeholders and cater to their diverse needs. Ultimately, design thinking can be applied to a variety of fields, as those in the workforce must prioritize their clients' needs.

To transform this lesson to use guided inquiry and discovery processes, one improvement could be to merge the Vigenère method instruction and the lockbox activity to develop a POGIL activity. To elaborate, in place of the demonstration on encryption with this method, instructors could divide the class into teams and challenge each group to discover how the encryption process works. To facilitate this process, it may be beneficial for instructors to provide an animation of the encryption of a single character. Upon successfully understanding the Vigenère method, teams could begin the lockbox activity. Ultimately, this change may enhance students' understanding of the Vigenère method further and account for the provided feedback as stated previously.

Presenting this lesson in Mr. Hayden's AP Computer Science Principles course gave me direct experience with teaching computing to a K-12 audience, and I am extremely grateful for this opportunity. Furthermore, I am satisfied with the lesson that my team developed and glad that the final product appealed to the students. In the future, I hope to implement the POGIL activity, described previously, to help the lesson flow more naturally. Overall, my biggest takeaway from this experience is the value of the UbD framework and UDL principles, as they truly help in developing a lesson that benefits an audience with varying knowledge backgrounds. The public can access my full portfolio of cryptography lessons that I have developed throughout this course through this hyperlink: William Gillette Biography (williamcgillette.com). In the future, I hope that I receive additional teaching opportunities in extracurricular settings, as delivering this lesson was extremely satisfying.