Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

16 November 2023

Cryptography: Service-Learning Project Draft #1

My project group comprises of Lou Hodgson, Alan Okinaka, Briana Bonsu, and Hannah Jeffers, and our goal is to collectively present a lesson about introductory cryptography to a K-12 audience, ultimately piquing their interest in both cybersecurity and the broad umbrella of computing. Another benefit of this experience is that the exposure to teaching may inspire one or more of us to pursue it professionally. Thus, we plan to integrate both the Understanding by Design (UbD) framework and the principles of the Universal Design for Learning (UDL) to craft a lesson that targets certain learning goals and appeals to people of all knowledge backgrounds. Finally, it is important to note that our lesson is primarily geared toward students with introductory backgrounds in computer science, such as those enrolled in AP Computer Science Principles, but there are ways to adjust the rigor of the activities to challenge students with prior knowledge.

Our lesson will begin by introducing some key terms related to cryptography, such as the significance of the words cryptography, encryption, decryption, and cipher. Students will make connections between these terms to then answer the essential questions, “How does cryptography work? Why is it effective? Why is it useful?” It is important for students to understand the practical applications of cryptography so that the lesson is purposeful. Before moving on to direct instruction, we must ensure that students have a strong grasp on the fundamental concepts of cryptography.

We will then proceed to introduce the Vigenère cipher widget on code.org, exposing students to one of the most secure cryptographic methods. To aid our explanation, we plan to demonstrate a few examples of the encryption and decryption processes using the provided matrix in the widget. We may also utilize the blackboard to present examples by hand if some students are having trouble following along with the widget. Our presentation of the Vigenère cipher is a segue into our unplugged activities, which will expose students to the Caesar cipher method, a less secure cryptographic method.

The first unplugged activity involves a circular “paper cipher,” which is composed of both an inner and outer circle. The English alphabet is written on the perimeter of both circles, allowing students to rotate the inner circle to align with different letters in the outer circle. Essentially, this enables students to map the original English alphabet to a uniformly shifted variant of the English alphabet, showcasing how the Caesar cipher works. Hence, students will investigate this tool and draw conclusions about how the Caesar cipher shift works. Following this, students will compare the Caesar cipher method to the Vigenère cipher, making connections and evaluating which method leads to more secure encryption. Therefore, this unplugged activity targets several levels of Bloom’s taxonomy.

Our second unplugged activity is challenging yet rewarding, involving groups working collectively to unlock a lock box. To create teams, we will ideally group people based on their confidence with decryption. To elaborate, students will freely choose whether they would like to complete the activity on its easy difficulty, medium difficulty, or challenging difficulty. Following the formation of teams, the instructors will provide each team with a lock box, a "cipher worksheet," and an encrypted message. Teams must use the paper cipher tool to decrypt their respective messages and then reference the cipher worksheet to record the number associated with each character of their decrypted message. The resulting number is the code required to unlock the box. Upon successful completion, students will discover treats and stickers inside the box, which they can divide among themselves.

Given that there is still time remaining, the final piece of our lesson will include a reflection period, having students discuss what was easy and challenging about the lock box activity. Finally, the instructors will return to the essential questions presented at the beginning of the lesson, having students answer them. Thus, this last phase of the lesson brings everything full circle, reinforcing understanding about how cryptography is practical in the real world. Ultimately, our goal is that students will take away from this lesson the importance of cryptography in securing confidential information and gain inspiration to explore more topics in cybersecurity during their leisure time.