Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

9 November 2023

Cryptography: POGIL Activity

Central Problem:

- A local firm has hired your group as a cybersecurity team to develop security solutions to safeguard data and classified information from outsiders. Your supervisor is aware of the Caesar Cipher and Random Substitution methods but does not have sufficient knowledge about them. Therefore, they have tasked you with either implementing the Caesar Cipher method or the Random Substitution cryptographic method for the encryption and justifying your decision.

Roles:

1. Manager: The manager is responsible for keeping the team cohesive. They must ensure active participation from all group members so that everyone can collaborate by providing their knowledge and opinions.
2. Presenter: The presenter must share the team's findings with the supervisor, discussing the benefits and drawbacks of using each method to ultimately justify the team's collective decision about which encryption method to use.

3. Reflector: The reflector's duty is to ponder the advantages and disadvantages of using each method to provide some considerations to the team. In doing so, the reflector must ask key questions to promote inquiry.
4. Recorder: The recorder's mission is to document all findings so that the presenter communicates all facts accurately to the supervisor. Essentially, the recorder's goal is to organize all the thoughts and ideas of the team.

Guiding Questions:

1. What is the purpose of cryptography in computer science? Why is it necessary in the modern world?
2. What is the Caesar Cipher method, and how does it work? Can you illustrate how shifting letters can encrypt and decrypt a message?
3. What are the differences between the Random Substitution method and Caesar Cipher method? Which of the two methods are more beneficial to implement?
4. When might one method be preferred over the other in real world applications?

Models:

Figure 1: Caesar Cipher Wheel: Examine how one can use the tool below to encrypt and decrypt messages through the Caesar Cipher method.

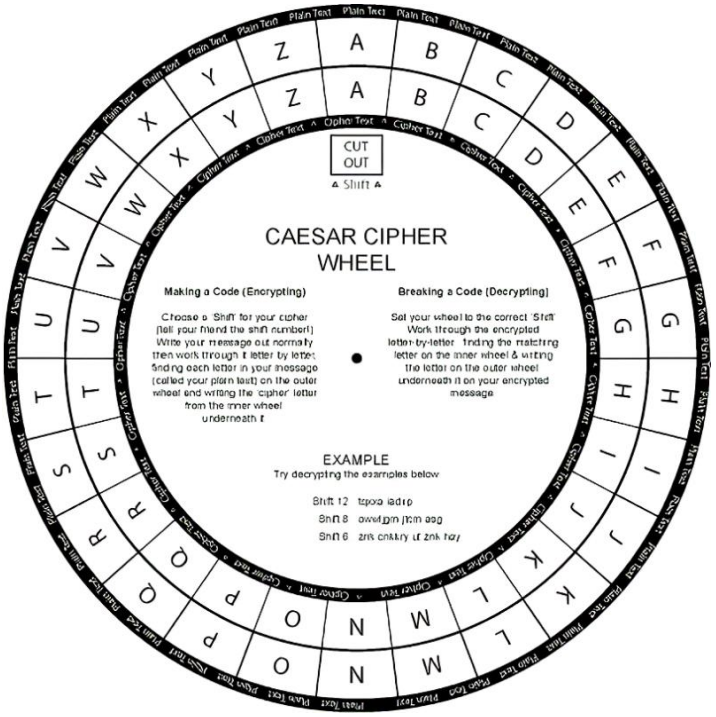
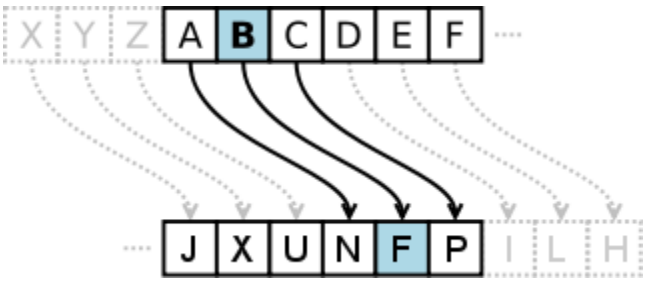


Figure 2: Random Substitution Diagram: Explore how this representation of the random substitution method differs from Figure 1.



Summative Assessment Questions:

1. Reflect on the importance of cryptography in real world applications.
2. Evaluate the benefits and costs of using both methods. Are there scenarios in which one is more beneficial to use than the other?
3. The following message was encoded using the Caesar Cipher method with a shift of 7 characters. Visit code.org and 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.”**

Goals and Integration of CS Principles:

Through this activity, students will use the models provided to make inferences about which cryptographic method is appropriate for this scenario. Being partitioned into teams, students must collaborate and share their thoughts and ideas with the group, enhancing everyone’s overall understanding. Finally, the presenters of each team must “lead with concepts” by communicating the team’s ideas to the supervisor through both technical and nontechnical lenses.

Facilitator’s Guide:

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.

- *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 two cryptographic methods: the Caesar cipher and random substitution, understanding when it would be practical to apply one compared to the other.

Prerequisite Skills:

- An understanding of how to shift or substitute letters in the English alphabet to craft a new message.
- General knowledge of computer science vocabulary to communicate thoughts through a technical lens.
- Some introductory knowledge about encryption and decryption and how they are essentially inverse operations.

Instructions for Forming Teams:

- Divide students into groups of four, ideally grouping those with similar knowledge levels so that everyone feels comfortable and confident sharing their ideas.
- Ensure that each group has assigned a role to each member, accounting for the four roles: manager, presenter, reflector, and recorder.

Facilitating the Activity:

- It is the primary duty of the manager of each team to ensure that all group members remain on task. However, when the manager becomes off task, this becomes problematic.

For this reason, the instructor must play a role in visiting each team periodically to ensure that everyone understands the tasks and answer any questions that students may have.

- At the end of the discussion, the instructor will ask the presenter from each team to communicate their ideas.

Answer Key:

Guiding Questions:

1. Cryptography essentially serves to secure information and data using codes. Computer scientists implement cryptographic methods to ensure data integrity and confidentiality. In the modern world, most information is stored digitally, making it easy for hackers to steal data that is not encrypted.
2. The Caesar Cipher performs a uniform shift on the English alphabet to encrypt and decrypt messages. Consider the message “abc” with a shift of one and observe that the resulting message would be “bcd.” The decryption process is essentially a reverse uniform shift.
3. The Caesar Cipher performs a uniform shift, while the random substitution method replaces each letter with a randomly assigned letter. Generally, random substitution provides more security than the Caesar cipher for this reason.
4. It may be beneficial to use the Caesar Cipher method when security is not a significant concern, such as for data that is not confidential. On the contrary, it is suggested to use the random substitution method when security is a priority, such as with banking.

Summative Assessment Questions:

1. Same as guiding question #1 but rephrased to promote reinforcement.

2. Same as guiding question #2 but rephrased to promote reinforcement.
3. The decrypted message is: “Now, encode this message using the random substitution method, and report your result.” One possible result of this would be: “Uqk, eusqge vbrw iewwzne lwrun vbe czugqi wltwvrvlvrqu, zug cehqcv pqlc cewlyv.”

Accessibility for all Students:

- As mentioned previously, it is ideal for students of similar knowledge levels to work together to promote an inclusive environment in which everyone feels comfortable sharing their ideas and valued.
- Some students without much background knowledge may struggle with understanding how to shift the English alphabet, but the instructor can provide as much guidance as necessary for these students.
- The students who have a lot of background knowledge can brainstorm about cryptographic methods that may be more powerful than the Caesar Cipher or random substitution.

Links to Standards Addressed:

- This activity serves as an introduction to the Caesar Cipher and random substitution methods, allowing students to brainstorm and explore about where these methods are applicable in the real world. Thus, this activity encourages collaboration and communication of ideas.

Reflection:

Cryptography has been my primary topic for this semester, so I decided to continue being consistent by developing a POGIL activity related to it. Essentially, my goal was to design an

activity that introduces people to the Caesar Cipher and Random Substitution methods, serving as a prerequisite to my unplugged activity. This activity incorporates POGIL principles by emphasizing collaboration and inquiry. To elaborate, the goal of the manager of each team is to ensure that students remain on task and to promote the sharing of thoughts and ideas. Furthermore, the reflector of each team asks engaging questions to encourage team members to ponder deeply. Essentially, because each student has an important role, they have a responsibility to remain actively involved in the activity, aligning with POGIL principles.

Similarly, this activity incorporates principles of computer science pedagogy by promoting inclusivity and building a supportive classroom environment. To elaborate, the instructor's duty is to group students based on prior knowledge, allowing each student to feel valued within their team. Initially, I did not mind groupings of some people with lots of knowledge and others without much knowledge, but I realized the flaw in that certain group members would not feel comfortable sharing thoughts out of fear of criticism. Thus, I revised my lesson in this way.

One challenge that I faced was ensuring that the activity was interesting to all students. For example, some students with lots of background knowledge may already understand the fundamentals of these cryptographic methods. In this scenario, however, these students can work on developing cryptographic methods that are stronger than both the random substitution and Caesar Cipher. During the presentation, these students can then explain their algorithm and justify its strength. In the future, I can create instructions more formally for this, incorporating the principles of UDL more explicitly, ultimately improving this activity.

Initially learning computer science comes with a series of challenges such as understanding abstract concepts, overcoming syntax errors, and seeing the big picture of

concepts. Collaborative inquiry allows people to gain a deeper understanding of certain concepts by learning from their peers. Furthermore, in careers related to computer science, students will need to collaborate with their coworkers to complete projects, and it can be difficult for a team to become a cohesive unit. Thus, it is essential to incorporate POGIL activities in the early stages to prepare students for the workforce. Essentially, collaborative inquiry exposes students to diverse ideas, promotes a deeper understanding of concepts, and models careers in the technical world, making it substantially beneficial to integrate POGIL activities in the classroom.