

## I Spy a Cryptologist

Theresa Guey, Ashley Kaya, Nilasha Krishnamurthy, Pranit Panda, Chisato Ruo | Fall 2022

**Field(s) of Interest:** cryptology, cyber security

### Brief Overview:

Mentees will be learning about cryptology and various ciphers used to communicate securely. The lesson will be structured similar to a scavenger hunt and they will utilize their new knowledge of ciphers to solve puzzles. One mentor holds the “treasure” of the scavenger hunt, and mentees use their decryption skills to find clues to who this is.

### Agenda:

- Introduction (5 min)
- Module 1: Semantic Security! (15 min)
- Module 2: INKredible INKryptions (15 min)
- Module 3: What’s the Password? (20 min)
- Conclusion (5 min)

### Main Teaching Goals/Key Terms:

- **Cipher:** a secret or disguised way of writing
- **Encrypt:** to convert plain text into a cipher or code
- **Decrypt:** to translate or solve a coded message
- **Key:** information used to encrypt or decrypt a cipher

## Background for Mentors

<p><b>Module 1</b></p> <ul style="list-style-type: none"><li>• <b>Cipher</b></li><li>• <b>Caesar Cipher</b></li><li>• <b>Key</b></li><li>• <b>Decrypt</b></li></ul>	<p>A <b>cipher</b> is a secret or disguised way of writing. They have historically been used by the military to transmit encoded messages. Today, complex ciphers are used to secure information across networks, ie. private communication by cell phone.</p> <p>The <b>Caesar cipher</b> is a substitution cipher, where each letter is replaced by another letter located a little further in the alphabet (always shifted forward by a predetermined amount for each cipher). The shift distance is chosen by a number called the <i>offset</i>, which can be right (A to B) or left (B to A).</p>  <p><b>Figure 1:</b> a Caesar cipher decoder</p> <p>To <b>decrypt</b> a message is to translate or solve it in such a way that English speakers can understand. A <b>key</b> gives the information needed to decrypt a message. In the case of a Caesar cipher, it maps the plain alphabet to its corresponding Caesar alphabet representation. It usually comes in the form of two discs that can be rotated to form the correct alignment.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Background for Mentors

<p><b>Module 2</b></p> <ul style="list-style-type: none"><li>• <b>Invisible Ink</b></li><li>• <b>Cryptology</b></li></ul>	<p><b>Cryptology</b> is the science of data communication and storage in a secret form. It uses cryptography and cryptanalysis. This word comes from kryptós and lógos which means hidden word. Cryptology is used around the world as a means of safeguarding the transactions of important information by decoding them so it is not easily accessible. Cryptology ultimately places a major role in information security and data privacy.</p> <p><b>Invisible ink</b>, also known as security ink, is a method used in cryptology to decode a message. It is written in a solvent such as salt water, lemon juice, phenolphthalein etc. The first type of invisible ink was actually made of alum and vinegar. Depending on the type of ink used, the method to decode the message would differ. For example, using lemon juice entails using heat to uncover the message, while baking soda was used to uncover secret messages written in phenolphthalein, which appear pink.</p>  <p><b>Figure 1:</b> A message written in UV invisible ink made visible using a black light.</p>
---------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Background for Mentors

### Module 3

- **Encrypt/  
Encryption**
- **Password**
- **Password  
Security**

**Encryption** helps to further protect user data by converting information into a code to prevent unauthorized access.

One of the ways in which encryption comes into play in our daily lives is through **passwords**. Passwords are a chain of characters that help to protect data for its designated user. Having secure passwords are essential in this day and age where copious hackers strive to crack the code and steal classified information from the rightful owners. Password ‘cracking’ is a method that is used by hackers to try many password combinations until it finds a match. In 2012, a password cracking machine that was able to make 350 billion guesses per second was introduced.



**Figure 1:** A chart depicting how fast it would take a hacker to crack one's password based on what is in their password.

Simple and commonly used passwords like 123456789, qwertyuiop, or even names are easily cracked. In order to ensure data safety, **password security** has been emphasized these last few decades. This includes the use of capital letters, numbers, and special characters as well as password managers which help to generate unique passwords and store them securely.



```
0x300, 0xef51ef00, 0x6b7c  
0x500, 0x19a3c400, 0xa5a  
0x00, 0x10c2a100, 0xb0c  
0x00, 0xPassword, 0x5f  
0x10, 0x656ef500, 0x9  
0x7, 0xac121200, 0x7  
0xb2b1c100, 0x7
```

**Figure 2:** A screen showing different password combinations, which include a mix of letters and numbers.

## Introduction

<p><b>Concepts to Introduce</b></p> <ul style="list-style-type: none"><li>Ask mentees to think about an instance in which they wanted to communicate a secret with another person. What were some things or methods of delivery that ensured its security? Ex. walkie talkie, code word, gestures, using a lock, invisible ink etc.</li><li>Mentees might already know some ciphering, but ask if they can recall any other existing forms of conveying messages that certain people used/continue to use today. Ex. hieroglyphics (ancient Egyptians), braille, street signs.<ul style="list-style-type: none"><li>Emphasize how in order to make meanings out of these, you have to understand the rules of each language. In this lesson, we will use a cipher to explore this concept.</li></ul></li></ul>	<p><b>Questions to Pique Interest</b></p> <ul style="list-style-type: none"><li>What are some ways we can protect vital messages from being stolen?</li><li>How can we make our own invisible ink?</li><li>Why is it important to have a strong password?</li><li>What makes a strong password?</li><li>Have you ever used secret code names or ways of communicating something secretly?</li></ul>
<p><b>Scientists, Current and Past Events</b></p> <ul style="list-style-type: none"><li><a href="#">In 2016</a> there was an Uber data breach in which secure information of about 57 million drivers and customers were leaked.</li><li><a href="#">Julia Parsons</a> was a member of Women Accepted for Volunteer Emergency Service, or WAVES and intercepted and decrypted messages from Nazi armies. WAVES helped to communicate with Allied armies to help them locate enemy submarines - a key influencer during WW2.</li><li>Recently, amongst some teenagers codes using <a href="#">emojis</a> have been developed to convey hidden messages about trading drugs.<ul style="list-style-type: none"><li> “mail drugs”</li><li> “marijuana”</li><li> “large batch”</li></ul></li></ul>	<p><b>Careers and Applications</b></p> <ul style="list-style-type: none"><li>Cryptologist: someone who analyzes and interprets data or patterns to decipher messages</li><li>Computer/Cybersecurity: protection of computer systems and software from information theft or exposure</li></ul>

## Module 1: Semantic Security!

Mentees will be learning about ciphers, specifically the Caesar Cipher, by an interactive activity where they attempt to decode a secret message that will give them a clue to who has the treasure!

Teaching Goals	Materials
<ol style="list-style-type: none"><li><b>Cipher:</b> secret or disguised way of writing. A mapping between an original message and an encrypted message.</li><li><b>Caesar Cipher:</b> A cipher where each letter is offset by a fixed amount. If it goes longer than the alphabet it wraps around.</li><li><b>Decrypt:</b> To convert a message from its secret form to a form that can be understood.</li><li><b>Key:</b> The mapping of input messages to output messages that allows you to decrypt.</li></ol>	<ul style="list-style-type: none"><li>Cipher <a href="#">printouts</a> (1 per group)</li><li>Split brass paper fastener (1 per group)</li></ul>

### Procedure

- Break mentees up into groups of 3-4 (groups of 4-5 for bigger sites). These will be their teams for the scavenger hunt.
- Pass out the pre-constructed cipher decoder.
- On the board write out the first clue for the scavenger hunt that describes the mentor that has the treasure. For example, if the mentor is wearing glasses, the clue that the mentees will decode can be “glasses” and we can write on the board the encrypted message of “ejyqqcp.”
  - Use this link to encode your message:  
<https://www.dcode.fr/caesar-cipher>
- The encrypted message needs to be shifted to the right 2 times (this part will be kept a secret from the mentees). First, have the mentees start by matching up the A's on both wheels. The inside circle represents the secret message and the outside circle represents the translation.
- Have mentees experiment by rotating the cipher to different positions and try decoding the message with this new pairing.

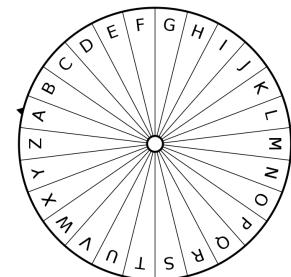
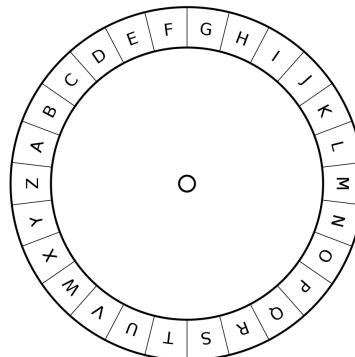


Figure 1: The Caesar Cipher Cutout

- a. Practice trial and error until they decode the entire message successfully. Walk around helping the teams to ensure they don't get stuck.

**Classroom Notes**

Be sure to walk around explaining the concepts to the teams and guiding them conceptually, especially for the difference between the two circle wheels.

## Module 2: INKredible INKryptions

Mentees will learn about invisible ink and how it is used in cryptology. In this activity, they will be making invisible ink messages and decrypting a secret message prepared by the mentors.

Teaching Goals	Materials
<ul style="list-style-type: none"><li>● <b>Invisible Ink:</b> a type of ink that is not visible or cannot be seen unless it is heated or treated with something else</li><li>● <b>Cryptology:</b> science that deals with the communication of data in a secure and usually secret form</li></ul>	<ul style="list-style-type: none"><li>● Crayons</li><li>● Salt</li><li>● Container with water (1 per group)</li><li>● Paper (1 per group)</li><li>● Paper with secret message (1 per group)</li><li>● Spoon (1 per group)</li><li>● Cotton swabs (3 per group)</li></ul>

### Procedure

1. Keep mentees in groups of 3-4 (groups of 4-5 for bigger sites).
2. Add salt to the container of water until the solution becomes saturated with salt (until salt does not dissolve in the water).
3. Stir the solution with the spoon for 1 minute.
4. Take a cotton swab and scoop up the solution. Write a message on the paper with the solution.
5. Allow the paper to dry **completely**.
6. While the paper is drying, pass out the paper with the premade secret message to the mentees. This will have the second clue for the scavenger hunt that gives another description of the mentor with the treasure.
7. Rub the crayons back and forth across the paper to reveal the clue.
8. Once the first paper has dried completely, brush off all the remaining salt stuck to it.
9. Repeat step 7 and use the crayons to reveal the mentees' secret messages.



*Figure 1: Mentees will dip the cotton swab in the salt water solution and write their secret messages.*



*Figure 2: This is what the revealed messages should look like after using the crayons.*

### **Classroom Notes**

This activity can get a little messy so it is good for mentors to be aware of things that could spill, like the rackwater container, or salt getting everywhere. Additionally, when making the solution of salt water, use a small amount of water and a larger amount of salt. Results work best when there is a lot of salt scooped up on the cotton swab when writing the invisible messages.

## Module 3: What's the Password?

Mentees will learn how to keep their private information safe with a strong password. The activity allows them to make their own passwords and test their strength.

Teaching Goals	Materials
<ul style="list-style-type: none"><li>● <b>Encrypt:</b> concealing data in a safe place by converting it into a code</li><li>● <b>Password:</b> a string of characters used to protect information in the authentication process from unauthorized users</li><li>● <b>Password Security:</b> a combination of characters that help to create a more secure protective code</li></ul>	<ul style="list-style-type: none"><li>● The secret message students obtained to access the hidden treasures</li><li>● Scissors</li><li>● Pencil</li><li>● Paper (1 per group)</li><li>● Envelope (to store secret message in)</li><li>● Tape</li></ul>

### Procedure

1. The secret message in the previous module is a clue to which mentor has the “treasure.” Mentees write down the name of their guess, and put it into an envelope.
2. Brainstorm a strong password. Mentees should be able to remember their passwords that they generate. Encourage them to use special symbols, capital letters, and numbers. \*Note: Discourage them from using the passwords that they actually use on their personal or family devices.
3. Mentors will check to see how strong mentees’ passwords are using the following website:  
<https://www.security.org/how-secure-is-my-password/>
4. Once the password has been confirmed to be secure (ex. The screen should say “It would take a computer about 5 years or more to crack your password). Give each team of mentees a piece of paper.
5. Take the piece of paper and fold it in half hotdog style.
6. Tape one side of its folded form onto the front of the envelope.
7. Open the folded paper and on the inside (the shaded part in the picture), write the password you created. Have the letters evenly spaced out as much as possible near the edge.
8. Lightly vertical mark lines between each letter.



**Figure 1:** Passwords usually look like this! They are hidden because we want to keep our information private.



**Figure 2:** Mentees will make a paper model for their passwords where they can reveal each letter/number/symbol one at a time.

9. Close the piece of paper and mark vertical lines (about 1-2 cm depending on the size of the handwriting) on the outside (white part in Figure 2) near the edge so that it overlaps with the lines in step 8.
10. Cut along the lines created in step 9. The flaps created will help to cover the password, but allow mentees to reveal one letter at a time if desired (much like the action of typing in a password).
11. If time permits, have mentees decorate their password envelope by:
  - a. Adding dots or asterisks to each of the flaps
  - b. The word “password”
  - c. Adding their “username”

#### **Classroom Notes**

Make sure mentees are safe with sharp materials such as scissors. It is also good to encourage them when they are making their passwords and give them tips on how to make them stronger, if needed.

## Conclusion

Every team's guess is revealed within their groups. Teams that guess correctly will receive the treasure (candy!) and teams that guess incorrectly can be told to guess again. After finishing the scavenger hunt, regroup with the whole class. Talk about what methods they used to crack the case of the hidden treasure and introduce possible careers and applications that are related to what they learned. Reinforce the importance of secure communication and open it up to mentees to think about how they can protect their own information.

## References

- Virtual STEM for Kids: Codes and Ciphers, Nova Southeastern University.  
<https://nsufl.libguides.com/virtual-stem/codes-ciphers>
- Caesar Cipher Exploration, Brit Cruise, Khan Academy.  
<https://www.google.com/url?q=https://www.khanacademy.org/computing/computer-science/cryptography/crypt/pi/caesar-cipher-exploration&sa=D&source=docs&ust=1665965474391759&usg=AOvVaw1CDde9b01RF9fKFOsn7VI2>
- 6 Amazing Secret Codes Your Kids Will Really Enjoy, Rediscovered Families.  
[https://www.google.com/url?q=https://rediscoveredfamilies.com/secret-codes-for-kids/&sa=D&source=docs&ust=1665965739014105&usg=AOvVaw0Y-4sDKwedNlylfD\\_gO6n](https://www.google.com/url?q=https://rediscoveredfamilies.com/secret-codes-for-kids/&sa=D&source=docs&ust=1665965739014105&usg=AOvVaw0Y-4sDKwedNlylfD_gO6n)
- Two classroom activities for teaching students about password security, Samantha Garrett, Using Technology Better.  
<https://usingtechnologybetter.com/blog/two-classroom-activities-for-teaching-students-about-password-security/>
- History of Cryptology, Gustavus Simmons, Britannica.  
<https://www.britannica.com/topic/cryptology/History-of-cryptology>

## Summary Materials Table

Material	Amount per Site	Expected \$\$	Vendor (or online link)
Split Brass Paper Fasteners	1 per group (4 total)	0	Bechtel
Cipher Printouts	1 per group (4 total)	0	<a href="#">Printouts</a>
Crayons	3 per group (12 total)	\$2.50	<a href="#">Safeway</a>
Salt	1 tbsp per group (4 tbsp total)	\$2	<a href="#">Safeway</a>
Container for water + lids	1 per group (4 total)	0	Bechtel

Plastic spoons	1 per group (4 total)	0	Bechtel
Cotton swabs	3 per group (12 total)	0	Bechtel
Scissors	1 per group (4 total)	0	Bechtel
Envelope	1 per group (4 total)	0	Bechtel
Tape	1 roll	0	Bechtel
Copy paper	12	0	Bechtel