TECH for Tomorrow

CLASSROOM ACTIVITY

Cryptography: Security Alert

Objectives

Students will be able to:

- Develop a cipher (or key), create their own encrypted message, and decrypt their peers' messages.
- Consider the limits of symmetric key encryption.
- Compare and contrast symmetric key encryption with asymmetric public key encryption.

Overarching Question

How is information securely transmitted online?

Activity Summary

As a continuation to the Crytobabel activity,* students will return to their roles as interns at a cryptology agency. Except this time, the Internet is down and it's up to the interns to explore how to securely exchange messages! Students will develop their own cipher and simulate an exchange of data using symmetric encryption. After considering the limits of this kind of encryption, students will watch a video that explains the concept of asymmetric encryption. The activity will culminate with a discussion that compares symmetric and asymmetric encryption in order to understand how information can be exchanged securely.

***Instructor Note:** This activity will work best following the Cryptobabel Activity. If your students could use a quick refresher before this second activity, the first section of The Internet: Encryption & Public Keys video (until 1 minute 43 seconds) should bring students back up to speed!

Grades

4–6

Timing

50–60 minutes

Materials

- Cipher Creation handout, enough for half the class
- Scissors, several pairs
- Device with the ability to project video
- The Internet: Encryption & Public Keys video (from 4 minutes 11 seconds—end)

TECH for Tomorrow

Activity Directions

Premise | 5 minutes

- Begin with an important announcement: Students will be returning to their cryptanalyst internships at the cryptology agency!
- Then write *Zhofrph edfn!* on the board. Share that the cipher key needed to decode this message is A–3, and encourage student pairs to decode this message by applying what they have already learned. After a few minutes have passed, make sure everyone was able to decode the message to: *Welcome back!*

  Tell students that while the agency is glad to have them back, they have been experiencing some technological difficulties and their Internet is down indefinitely. Therefore, the interns' first task is to explore how the office employees can send private and secure messages to each other and/or their clients.

Investigate | 30 minutes

- Divide students into pairs and distribute one Cipher Creation handout to each pair.
- Review the directions for Steps 1–3. Be sure students understand that their objective is to create a cipher that they will use to **respond** to the question: *Where can we meet privately?*
- Tell students that they will have about 15 minutes to create their cipher and write their message, and then encourage them to get to work!
- Once students have completed their handout, instruct each pair to cut out the message and cipher portion and make sure their names are on the back of both slips. Then ask students to form a large circle, with partners sitting next to each other.
- Explain that the class will now explore how encrypted information (i.e., their coded message) can be exchanged. Tell the class that everyone will be sending their message to the pair sitting *two* pairs clockwise away from them in the circle.
- Go on to explain that every pair is also a snoop! In other words, they're curious about messages that are not intended for them, and they will try to decrypt a message as it passes them by.
- Ask: What will the actual recipient of your message need in order to decrypt and understand what you wrote? [Answer: Cipher/Key].
- Instruct students to first pass their cipher/key once clockwise to the pair next to them. Give these "snoops" a minute to look at the cipher, and then instruct them to pass the cipher clockwise one more time. The pair next to the snoops is the intended recipient.
- Now that the intended recipient has the cipher, instruct pairs to pass their encrypted message clockwise to their intended recipient as well. Again, the message should first stop at the snoop pair next to them. Challenge the snoops to use their memory of the cipher they just saw to decrypt some or all of the message.

  Note: It may be helpful to distribute a piece of scrap paper, as the snoops won't want to leave evidence of their work on the original message!

TECH for Tomorrow

- After students have two minutes to work on the decryption, instruct them to pass their message clockwise one more time so it arrives as the intended recipient. Allow pairs a few minutes to decode their message using the cipher.
- Then instruct the recipients to compare their decoded message with the message that the snoops were able to decode in the time provided.

  Ask: Through a show of hands, how many snoops were able to decrypt at least part of the message? Which snoops were able to decrypt the entire message?

Solve | 15–25 minutes

- Bring the class back together and lead them in a discussion:
  - Ask: Was this type of data transmission (i.e., the way you sent your message) more secure or less secure than if you had written the note normally in plain text? Why?
  - Ask: What prevented this data transmission from being entirely secure? In other words: Why were some snoops able to decrypt your messages?
  - Explain: The fact that the same cipher was used to encrypt and decrypt your message made your data transmission less secure. This type of encryption is called symmetric encryption, because the cipher is the same on both sides (like a *symmetric* design).

    When both the sender and the recipient need to know the same cipher or key, it's easier for others to get ahold of it too. Even if you hadn't been sitting in a circle, it may have been possible for someone else to overhear your cipher, find it on a slip of paper that you accidentally dropped, etc.

    Just like the snoops could figure out your message when it was passed in person, hackers are able to decrypt these kinds of messages when your digital data is passed over the Internet. Symmetric encryption is therefore not ideal for keeping data safe!
  - Ask: Can you think of anything we could do to help make the messages we exchange in the office *more* secure?
- Tell students that they are about to watch a video (or continue the video, if you showed it at the beginning as a refresher) featuring someone who works for the Department of Defense and focuses on keeping private information safe. As they watch the video, instruct students to think about the similarities and differences between this kind of key and the symmetric key/cipher that they just developed.
- Show The Internet: Encryption & Public Keys video from 4 minutes 11 seconds until the end.
- Conclude with a discussion that compares and contrasts symmetric encryption with public key (or asymmetric) encryption.
  - Ask:
    - How are these two types of encryption similar? How are they different?
    - Why is asymmetric encryption more secure than symmetric encryption?
    - How could the office employees set up an asymmetric encryption method with each other or with their clients?

TECH for Tomorrow

- Ensure students understand that symmetric encryption can't ensure security. For this reason, information transmitted online uses public key (or asymmetric) encryption. This type of encryption is the most secure method because every recipient has a key that is completely private and doesn't need to be shared. Because the key is not the same for both the sender and the receiver, it is much more difficult for a snoop/hacker to figure out the key and interfere!

Standards

Common Core Mathematics

- CCSS.MATH.PRACTICE.MP1 Make sense of problems and persevere in solving them.
- CCSS.MATH.PRACTICE.MP7 Look for and make use of structure.

Standards for Technological Literacy (ITEAA) Standards

- Standard 17: Students will develop an understanding of and be able to select and use information and communication technologies. In order to select, use, and understand information and communication technologies, students should learn that:
  - F. Communication technology is the transfer of messages among people and/or machines over distances through the use of technology.
  - G. Letters, characters, icons, and signs are symbols that represent ideas, quantities, elements, and operations
  - J. The design of a message is influenced by such factors as the intended audience, medium, purpose, and nature of the message.

English Language Arts Common Core

- Speaking and Listening
  - CCSS.ELA-LITERACY.CCRA.SL.1: Prepare for and participate effectively in a range of conversations and collaborations with diverse partners, building on others' ideas and expressing their own clearly and persuasively.

Cipher Creation Handout

Challenge: Can you create a cipher that helps you transmit information more securely?

STEP 1: Work with your partner to change each letter of the alphabet. You may create symbols, shift letters a certain number of spaces, or come up with something completely different. Be creative!

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

STEP 2: What would the person who receives your encrypted message need to know in order to decrypt it? This is your cipher or key. It may need to be a copy of what you created above for each letter of the alphabet *or* it could be a little simpler (such as A+4). Decide what someone would need to know to understand your message and write it in the "CIPHER" section below.

STEP 3: Respond to the question: "Where can we meet privately?" in cipher text in the MESSAGE section below. In other words: Use your cipher to write a response! Once you have written it, double-check that someone could decode it using the cipher.

Tip: It may be helpful to write your message using the regular alphabet first in the space below!

CIPHER:

MESSAGE:

Respond to: Where can we meet privately?