Tales from the Encrypt

Encryption and Keys

Teresa Lansford, Aaron Coffey, Bradly Cusack, Dewey Hulsey, Andy Marang, Laura Young
Published by *K20 Center*

Grade Level	7th Grade	**Time Frame**	90 min
Subject	Computer Science	**Duration**	2 class periods
Course	Computer Science		

Essential Question

Why does electronic information need to be protected when being transmitted on the internet? How do we encrypt data?

Summary

Students learn about data encryption, why it is needed, and how it works by engaging in a range of group activities exploring cyber security. First, they attempt to pass along an unsecured message and learn how difficult it is to do so without some sort of plan. Then, they participate in a Jigsaw activity and read about real life security breaches. After learning about how breaches have happened, they explore different encryption methods and discuss their uses in Chat Stations. Finally, they create their own methods of encryption, test them, and reflect on the process in an Exit Ticket.

Snapshot

Engage Students are placed into groups of three and tasked with trying to share a message between two of them without the third finding out. They will later connect this experience to a need for encryption.

Explore Students engage in a Jigsaw of articles with real world examples of cyber security breaches and share what they have learned to identify common areas of need and solutions to the breach.

Explain Next, students dig deeper into types of encryption uses as solutions for ensuring the safety of data by watching a video from Code.org and visiting Chat Stations that share information on types of encryptions.

Extend Students create their own encrypted messages and test them.

Evaluate Finally, students reflect on the overall experience, what they have learned, what their thoughts of creating their own encrypted messages are, and what makes encryption successful.

Standards

Oklahoma Academic Standards for Computer Science (Seventh Grade)

7.NI.C.1: Explain how to protect electronic information, both physical (e.g. hard drive) and digital, identify cybersecurity concerns and options to address issues with the Internet and the systems it uses.
7.NI.C.2: Identify and explain two or more methods of encryption used to ensure and secure the transmission of information.

Attachments

- Chat Stations Reflections—Tales From the Encrypt - Spanish.docx
- Chat Stations Reflections—Tales From the Encrypt - Spanish.pdf
- Chat Stations Reflections—Tales From the Encrypt.docx
- Chat Stations Reflections—Tales From the Encrypt.pdf
- Cyber Security Tales—Tales From the Encrypt - Spanish.docx
- Cyber Security Tales—Tales From the Encrypt - Spanish.pdf
- Cyber Security Tales—Tales From the Encrypt.docx
- Cyber Security Tales—Tales From the Encrypt.pdf
- Encryption Chat Stations—Tales From the Encrypt - Spanish.docx
- Encryption Chat Stations—Tales From the Encrypt - Spanish.pdf
- Encryption Chat Stations—Tales From the Encrypt.docx
- Encryption Chat Stations—Tales From the Encrypt.pdf
- Exit Ticket—Tales From the Encrypt - Spanish.docx
- Exit Ticket—Tales From the Encrypt - Spanish.pdf
- Exit Ticket—Tales From the Encrypt.docx
- Exit Ticket—Tales From the Encrypt.pdf
- Lessons Slides—Tales from the Encrypt.pptx

Materials

- Lesson Slides (attached)
- Cyber Security Tales (attached; minimum 1 per group)
- Encryption Chat Stations (attached; 1 per class)
- Chat Station Reflection (attached; optional; 1 per student)
- Encryption Exit Ticket (attached; 1 per student)
- Paper
- Pens/pencils

10 minutes

Engage

Use the attached **Lesson Slides** to introduce the lesson. Share **slides 3-4** to review the essential question and lesson objectives as needed. Create groups of three. Move to **slide 5** and introduce the following scenario:

Friend A and B are trying to pick the perfect present for Friend C. Friend A needs to share an idea with Friend B without Friend C knowing what they are talking about. Friend A will have a pencil, paper, and can speak. However, anything written or spoken needs to be shared with Friend C because Friend C does not like to be left out. Ask Friend A to find a way to successfully share their idea with Friend B without revealing to Friend C what is being shared.

Have each group member select whether they will be Friend A, Friend B, or Friend C. Give them some time to attempt to share their message. As needed, remind them they cannot share any messages that Friend C cannot hear or see, which includes making a plan for how to share any information.

Have groups share their thoughts about how successful they were. If they were able to share their present idea successfully, what strategy did they use to make that work? Ask if they have any ideas for how they could have made sure their message got across without Friend C finding out.

20 minutes

Explore

Display **slide 6**. Explain to students that just like in the present challenge they just attempted, companies often find themselves needing to receive or share information that they do not want a third party to see, and just like some of their attempts, there are times those efforts fail. To learn more about the times big companies have failed and their attempts to fix those issues have been unsuccessful, they will Jigsaw 5 passages on “cyber fails.”

Break the class into five groups and hand out the **Cyber Security Tales** passages. If using multiple copies, each group member should have the same passage. Give groups time to read and determine what the issue was, the problem it caused, and what the company did to try to fix the problem. They can record their thoughts on the handout or on the back. Give students time to share out what they learned from their passage. Ask what these fails had in common and how the solutions were similar.

30 minutes

Explain

Teacher's Note

Post the **Encryption Chat Stations** around the room or at tables prior to class or as students are watching the Code.org video.

Now that students have explored the problems that can arise when there are security breaches, it is time to better understand how these breaches are addressed and prevented. Move to **slide 7** and show the Code.org video on encryption and public keys.

Embedded video

https://youtube.com/watch?v=ZghMPWGXexs

Next, display **slide 8**, and explain that students will now visit some Chat Stations in groups to learn more about the examples from the video as well as other methods for encryption. At each chat station, they will read what is on the Encryption Chat Stations handout and use their own paper or the **Chat Station Reflection** handout to record their thoughts. Give students 3-5 minutes at every station to read and record. You can give more time as needed.

Afterwards have them come back together as a class and share their thoughts. Ask them to share something new they have learned, which method they felt was the best, or which they felt was the most complicated and if they felt one would be easier to decipher than another.

Follow up questions could include:

- What kinds of data were exposed?
- Were there similarities between the data that was stolen?
- Who was behind the attempts at the theft? What was the outcome of the data breach?
- What kind of outcomes did the companies responsible for the data face?

25 minutes

Extend

Display **slide 9**. Explain that now students will work in groups of 3-4 to use what they have learned to design their own encryption method. Remind them of their original activity where they tried to share their present idea without Friend C finding out. Using what they have learned about encryption, is there a way to share their ideas securely? Give students time to both develop and test their encryption method. Groups can also share their messages with one another to see if their method can be cracked.

5 minutes

Evaluate

After students have had time to develop and test their encryption method, show **slide 10** and hand out the Encryption Exit Ticket. Have students share their thoughts on what they have learned about encryption, their thoughts on creating an encryption method, and what makes encryption successful.

Resources

- Capital One (2019). Information on the Capital One cyber incident. Capital One. https://www.capitalone.com/digital/facts2019/
- Capital One. (2022). Capital one data breach class action settlement. Capital One Data Breach - Home. https://www.capitalonesettlement.com/en
- Code.org. (2015). The internet: Encryption & public keys. [Video]. YouTube. https://www.youtube.com/watch?v=ZghMPWGXexs
- Federal Bureau of Investigation (2020). Chinese military hackers charged in Equifax breach. FBI News. https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020
- Federal Trade Commission (2019). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. Federal Trade Commission News and Events. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook
- Federal Trade Commission (2018). The Marriott data breach. Federal Trade Commision Consumer Alerts. https://consumer.ftc.gov/consumer-alerts/2018/12/marriott-data-breach#:~:text=December%204%2C%202018%20Marriott%20International,help%20guard%20against%20its%20misuse
- Federal Trade Commission (2022, December). Equifax Data Breach Settlement. Federal Trade Commission Refund Programs. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
- Fruhlinger, J. (2020, February 12). Equifax Data Breach FAQ: What happened, who was affected, what was the impact?. CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
- K20 Center. (n.d.). Bell ringers and exit tickets. Strategies. https://learn.k20center.ou.edu/strategy/125
- K20 Center. (n.d.). Chat stations. Strategies. https://learn.k20center.ou.edu/strategy/944
- K20 Center. (n.d.). Jigsaw. Strategies. https://learn.k20center.ou.edu/strategy/179
- Perlroth, N. (2017). All 3 billion Yahoo accounts were affected by 2013 attack. The New York Times. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html?unlocked_article_code=1.HE0.kxWE.f-QJEHuFLjoX&smid=url-share
- United States Attorney's Office Northern District of Georgia. (2019, June 27). Former Equifax employee sentenced for insider trading. Northern District of Georgia | United States Department of Justice. https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading