Unit 4 Lesson 7: Simple Encryption

CSTA K-12 Computer Science Standards (2017)	**Computer Science Principles**
NI - Networks & the Internet ● 2-NI-06 - Apply multiple methods of encryption to model the secure transmission of information. ● 3A-NI-07 - Compare various security measures, considering tradeoffs between the usability and security of a computer system. ● 3B-NI-04 - Compare ways software developers protect devices and information from unauthorized access.	1.2 - Computing enables people to use creative development processes to create computational artifacts for creative expression or to solve a problem. 3.3 - There are trade offs when representing information as digital data. 6.3 - Cybersecurity is an important concern for the Internet and the systems built on it. 7.3 - Computing has a global affect -- both beneficial and harmful -- on people and society
Objectives: Students will be able to: ● Explain why encryption is an important need for everyday life on the Internet. ● Crack a message encrypted with a Caesar cipher using a Caesar Cipher Widget ● Crack a message encrypted with random substitution using Frequency Analysis ● Explain the weaknesses and security flaws of substitution ciphers	

Aim: How does encryption play a role in how data is transferred on the internet?
VotD: Caesar Cipher, Cipher, Decryption, Encryption, Random Substitution Cipher

1. **Do Now (5 min)**: Students will start with a think-pair-share based on the following prompt: *"In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?"*
    a. Ask them to brainstorm as many areas as they can where they or other people rely on secrecy. Try to touch on as many different people and contexts as possible!
    b. Potential areas to discuss: Social interactions (e.g., a surprise birthday party); A play in a sports game, your hand in a card game; Personal identification information, PIN numbers, etc.; Business and government negotiations; Military activity
2. **Introduction (2 min)**: Secrecy is a critical part of our lives, in ways big and small. As our lives increasingly are conducted on the Internet, we want to be sure we can maintain the privacy of our information and control who has access to privileged information.Digital commerce, business, government operations, and even social networks all rely on our ability to keep information from falling into the wrong hands.
    a. Recall: As we saw with our activities on the Internet Simulator the internet is NOT secure. We need a way to send secret messages...

3. **Mini-Lesson** (8 min): What is Encryption?
    a. We will briefly discuss encryption and look at an example of encryption.
    b. This message was encrypted using a Caesar Cipher (an "alphabetic shift"). Let's see how long it takes you to decode this message (remember it's just a shifting of the alphabet): `serr cvmmn va gur pnsrgrevn`
    c. Students will have about 5 minutes to work on this.
        i. ANSWER: "free pizza in the cafeteria" - the A-Z alphabet is shifted 13 characters.
        ii. Hints for students: Find a small word and try alphabetic shifts until it's clear that it's an English word; Remember the letters aren't randomly substituted - the alphabet is just shifted.
    d. What if the message was longer? What if you had a tool to help you?
4. **Activity:** Cracking the Code
    a. In this set of activities students will use two different versions of a simple widget in Code Studio to "crack" a messages encoded with substitution ciphers, including an alphabetic shift and random substitution. This will be a discovery based approach, so there will be no explanation beforehand!
    b. Part 1: Caesar Cipher
        i. In pairs/partners, students will select a message encrypted with a caesar cipher and use the provided widget to "crack" it. They will have 5 minutes to get into the tool and crack at least **two** messages
    c. Part 2: Random Substitution Cipher
        i. What if instead of shifting the whole alphabet, we mapped every letter of the alphabet to a random different letter of the alphabet?
        ii. Students will explore for 5-10 minutes to discover what the tool is showing them and allowing them to do. After some exploration time, regroup to clarify what the tool is and how it works
        iii. Give students about 15-20 minutes to crack one of the messages.
            1. If they finish before time, there are more to try.
5. **Summary**
    a. **Students will answer the following question in their notes:** Why encryption is an important need for everyday life on the Internet?
    b. Time permitting, students will complete the assessment questions on Code.org. If they don't finish, they will continue for HW.

Name:_____

Unit 4, Lesson 7: Simple Encryption

By the end of today's lesson, you should be able to:
- Explain why encryption is an important need for everyday life on the Internet.
- Use the Caesar Cipher Widget to crack an encrypted message
- Use frequency analysis to crack a message encrypted with random substitution
- Explain the weaknesses and security flaws of substitution ciphers

Do Now- See board!

STOP HERE!

Task 1: Decode this message!

Tips:

- Find a small word and try alphabetic shifts until it's clear that it's an English word
- Remember the letters aren't randomly substituted - the alphabet is just shifted.
- Once you have found the amount of shift the rest comes easily.

serr cvmmn va gur pnsrgrevn

Use the Alphabet here to count your shifts!