Lesson 2.2: Keeping Information Safe- Part 1

Objectives

In this lesson, students will:
- ❖ Learn the fundamentals of encryption and decryption
- ❖ Be introduced to Caesar Cipher
- ❖ Experience and practice encrypting a decrypting messages using Caesar Cipher

Agenda

1. Encryption and Decryption	20 mins	
2. Caesar Cipher	10 mins	
3. Student Activity: What Is the Secret Word?	10 mins	
4. Wrap Up and Reflections	10 mins	

Preparation

- ❏ Watch the video listed under resources to help you become familiar with the material.

Resources & Links

- ❏ Caesar Cipher video: https://tinyurl.com/nwmks7m

1. Encryption & Decryption

Engage students in an interactive discussion and instruction:

When sending a private message to a friend or when you type your password, do you want someone else to see it?   Probably not. You want it to be secret.

Encryption is used to keep data secret.   Encryption scrambles a message using a secret code so that only the person it is intended for can read it. The secret code, which is a sequence of steps to scramble the message, is called a **cipher**.

If you are using computing devices such as a smartphone or a computer online, you are using encryption all the time. Many text messages or payments made online are encrypted.
Why do you think that is important? Without encryption, all the data going over your wifi could be read by someone who could use it for unintended purposes, like buying something with someone else's credit card number – so encryption is critical to make computer systems safe and usable.

Since encryption scrambles a message so others can't read it, the recipient has to figure out what the message says. To do that, they use a **key** to unlock the secret code and convert the scrambled message back to its original text. Unscrambling the message is called *decryption*.

The secret code and the *key* have to be agreed upon by the sender and receiver so that the receiver can read the message. The image below can help explain the concept of encryption and decryption.

Encryption and Decryption
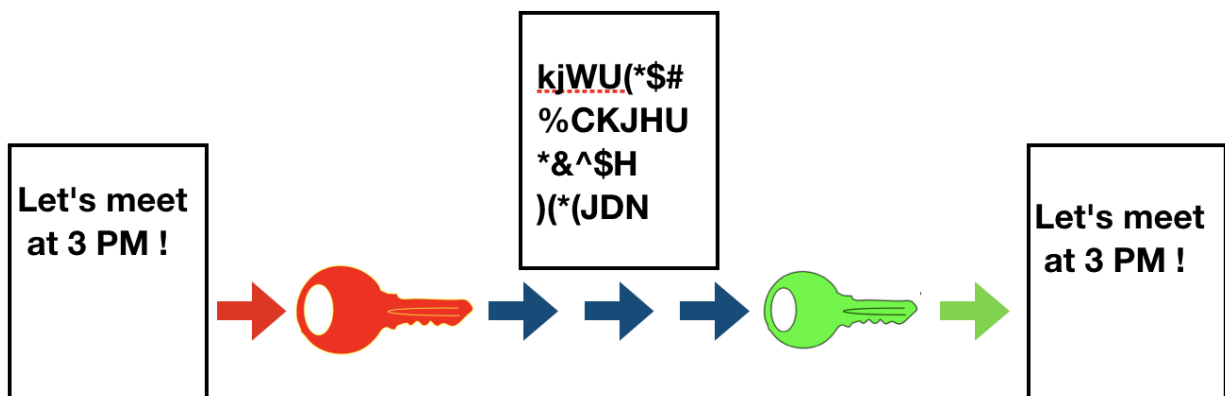
Student Activity:

Students share ideas with an elbow partner and try to come up with ways to send secret messages and be able to decrypt them using a secret code.

2. Caesar Cipher

Encryption has been used for many, many years. In fact, over 2000 years ago a great military leader called Julius Caesar invented a substitution cipher to encrypt secret battle messages to his generals. His cipher is called **Caesar Cipher.**

Today we are going to learn Caesar Cipher to write our own secret messages. Even though Caesar Cipher is not safe enough for the internet as it is fairly easy to crack, the technique is similar to other more difficult ciphers to crack.

Here is an encrypted phrase using Caesar Cipher:

UQ DWUVGF

Can anyone guess what it might say? It's not that easy, it just looks like gobbledygook.
Here is what is says: SO BUSTED

Now how did SO BUSTED become UQ DWUVGF ?!

There is a pattern in how letters from the original message correspond to letters in the encrypted one. If we look at the alphabet,
- the letter S became the letter U
- the letter O became the letter Q
- the letter B became the letter D   and so on.

What can we observe from this?

Each letter in the original message became the letter that was 2 places after it in the alphabet. So our secret code or cipher is to shift every letter by 2 letters of the alphabet. In this example we also say the key is 2 which is how far the letter is shifted.

What if we reach the end of the alphabet and there are no more letters within our key range? Let's look at an example of how that works by encrypting the word WAY with a key value of 4.

The first letter **W** becomes **A** as shown below. We simply loop back to the beginning of the alphabet:

Next the letter **A** becomes **E** and the letter **Y** becomes **C**, looping back to the beginning as we did with the letter W.

So **WAY** becomes **AEC** when encrypted with a key of 4.

Decryption

How do we **decrypt** a message? Meaning how do we take an encrypted message and convert it back to the original readable message.

We take each letter in the encrypted message and instead of counting forward, we count backwards. Let's take our example of the word **WAY** with a key value of 4.

Example: We want to decrypt the secret word AEC.
We take A, move back 4 positions and we get W. See below:
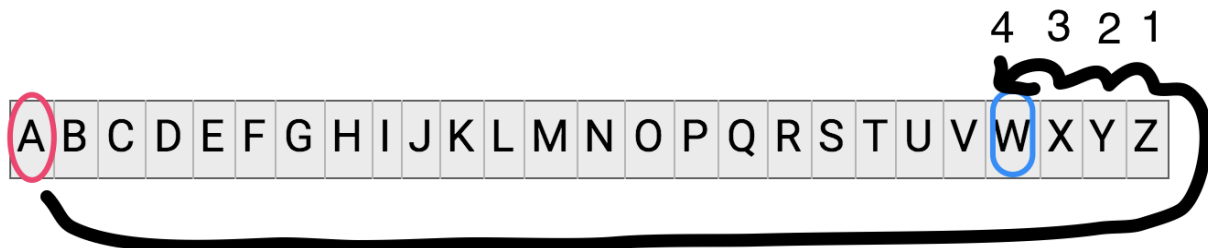
Then we take E, move back 4 positions and we get A.
Finally we take C, move back 4 positions and we get Y, looping back to the end of the alphabet.

3. Student Activity: What Is the Secret Word ?

For this activity display the alphabet in appendix A or write it on the board beforehand.

Students pair up.   The first student, student A, comes up with a 3 letter word and encrypts it using a chosen shift value.   Student A hands their partner the encrypted word and tells them what the shift value is. Student B decrypts the word.   Students then reverse roles.

This can be repeated a second time if time allows or each student can encrypt their words for their partner to decrypt at the same time.

3. Wrap Up and Reflections

Reflection Points
- What did you like about today's activity?   - What does it mean to encrypt a message?   - What is Caesar Cipher?   How does it work?   - What are reasons for wanting to encrypt a message?

Appendix A

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

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

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

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