U4Ch1L7 _ Simple Encryption: Caesar Cipher & Random Substitution Cipher *(35pts.)*
Purpose: Students will understand the early forms of encryption and how they work.
Vocabulary:

- Encryption: *a process of encoding messages to keep them secret, so only "authorized" parties can read it.*
- Decryption: *a process that reverses encryption, taking a secret message and reproducing the original plain text.*
- Cipher: *The generic term for a technique (or algorithm) that performs encryption.*
- Caesar Cipher: *a technique for encryption that shifts the alphabet by some number of characters.*
- Cracking Encryption: *When you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to "crack" the encryption.*
- Random Substitution Cipher: M*atch every letter of the alphabet to a random different letter of the alphabet.*

Activity: Caesar Cipher.
In Roman times Julius Caesar encrypted messages to his soldiers and generals by using a simple alphabetic shift - every character was encrypted by substituting it with a character that was some fixed number of letters away in the alphabet.
Hint:

1. *Write out the alphabet on a piece of paper.*
2. *Start with the shortest word and crack it first. That letter shift will apply to all the other words.*
3. *Each time you decrypt a letter, now apply it to all matching letters in the other words.*
4. *Next, decrypt the letters that are near the ones you have already cracked.*

With pencil and paper, how long does it take you to Decrypt the following message: *(Partners!) (5pts.)*

serr cvmmn va gur pnsrgrevn

How long does it take you?
How difficult was it to crack?
How many letter shift was it?

Lets try another one... *(Partners!) (5pts.)*

QIVVC GLVMWXQEW

How long does it take you?
How difficult was it to crack?
How many letter shift was it?

Visit: Code Studio.org_U4Ch1L7_ Simple Encryption
Go to Puzzle #2 - **"Crack a Caesar Cipher"** and read the explanation.
Decrypt the messages from the pulldown menu. Time yourself. Enter your own message!

Journal:
On average, how much faster could you crack the code when you used a computer?

Part 2: Cracking a Random Substitution Cipher

What if instead of shifting the whole alphabet, we mapped every letter of the alphabet to a random different letter of the alphabet? This is called a random substitution cipher. Now, instead of the secret message being encoded with a simple alphabetic shift seen with the Caesar Cipher, you'll face messages encoded with random substitution.

Go to Puzzle #4 - "Crack a Random Substitution Cipher" and Read the Explanation!

For 5 Minutes, Just Play!!!!

The only way you will figure it out is to just poke around!

Harrington Hints:

1. **Understanding How To Encrypt a Message:**

Create a very short message by selecting "WriteYourOwn": and enter "dog." Click on the "Random Substitution" tab. Then select - "Sort Substitution / Random / Assign." You will notice that the word "dog" was encrypted in the screen to the left.

Notice on the "Letter Frequency Screen" there should only be 3 large golden bars, one for "D", one for "G" and one for "O". The corresponding letter in blue beneath "D" "O" "G" are the randomly encrypted letters.

Note: The frequency (or height) of the encrypted (blue) letter does NOT represent the frequency in this secret message (or else they would be the same height as the gold bars), but represents the frequency upon which that letter appears on average in the English language.

Now you select a word and encrypt it. *(3pts.)* What was the word you created? What was its encrypted form?

2a. **Hints that will help you Decrypt a Message:**

Write and encrypt the following message: "I like pizza." Then sort the original."By%". Now analyze the gold bar letter frequency and notice that the letters that repeat obviously appear more frequently ("i"&"z"). Think about sentence structure and begin dragging the encrypted "Blue" letter under the gold "i" and other "Blue" letters under the gold "z". Switch some more. Can you now guess the letter/word/sentence. Be patient...it is a puzzle.

Now you select a short sentence and encrypt it. *(5pts.)* What was the sentence you created? What was its encrypted form? Pretend you do not know the sentence. Are you able to decrypt it?

2b. **Tricks that will help you Decrypt a Message:**

Open "Encrypted Sample #3". Always start by cracking small words that are fairly common in most sentences, "I", "We", "Is", "The", etc. Think about how sentences are usually structured. Do you see any patterns. Remember, this is a puzzle...Be Patient! Work Out Loud As A Class!

Answer to "Encrypted Sample #3" -Do Not look at the answer until a few minutes before the end of class!

Were you able to Crack any of the "Encrypted Samples"? *(10pts.)* Whether you did or did not succeed, what protocol or process did you decide to follow? Explain.

Journal: Define…, *(5pts.)* Explain in no more than 1 sentence how a Caesar Cipher Works: Explain in no more than 1 sentence how a Random Substitution Cipher Works: