Cryptography Lesson #7: Code Breaking with Linear Ciphers Name _____

1. As we've seen with Caesar and Multiplication Ciphers, we can use encrypted messages to determine the key. This also works with Linear Ciphers but the process is more complicated. Let's try a couple of simple examples
    a. A LINEAR CIPHER (mod 29) was used so that A B C was encrypted as C H M.
        i. How does knowing what A is coded as help determine the ADDITION part of the cipher?

        ii. Now that you know the cipher is $C(x) = \# \cdot x + 2$, how can you determine the MULTIPLICATION part of the linear cipher?

        iii. What is the encrypting rule? What is the decrypting rule?

        $C(x) = \quad \cdot x +$ $\qquad$ $D(x) = \quad \cdot (x - \quad)$

    b. A LINEAR CIPHER (mod 29) was used so that A C E was encrypted as D N X. Use a similar process as above to determine the encrypting rule? What is the decrypting rule? Show or explain your process.

        $C(x) = \quad \cdot x +$ $\qquad$ $D(x) = \quad \cdot (x - \quad)$

2. But what if you don't know what A is encrypted as?
    a. A LINEAR CIPHER (mod 29) was used so that B E D was encrypted as J K A. Notice the E and D are CONSECUTIVE letters in the alphabet.
        i. How far apart (counting forwards) are the encrypted letters A and K? In other words, what is the slope of the scatter plot for this cipher?

        ii. How does this help you determine the MULTIPLICATION part of the linear cipher?

        iii. Now that you know that the cipher is $C(x) = 10 \cdot x + \#$, how can you determine the ADDITIVE part of the linear cipher?

        iv. What is the encrypting rule? What is the decrypting rule?

        $C(x) = \quad \cdot x +$ $\qquad$ $D(x) = \quad \cdot (x - \quad)$

This work was developed by Project Think and reflects our original thinking and design. We're happy to talk about how it might serve your context — please reach out to info@project-think.org before sharing or adapting it.

b. A LINEAR CIPHER (mod 29) was used so that SUN was encrypted as JAR.
   i. Notice now that you don't have consecutive letters in the alphabet. How far apart are the plain text letters S and U?

   ii. How far apart are their encrypted letters J and A?

   iii. Given that S and U are 2 letters apart and the encrypted letters are 20 letters apart, what is the slope of the scatter plot for this cipher and what does that tell you about your linear cipher?

   iv. What is the coding rule? What is the decoding rule?

$C(x) =$ $\cdot x +$ $D(x) =$ $\cdot (x -$ $)$

3. Code Breaking is what happens when you only know the encrypted message and have to figure out the cipher used to encrypt/decrypt the message. You can use the skills we have developed in this lesson but first have to use logic and knowledge to identify possible plaintext letters to work with.
   a. Simple Sentence: W RLAC L !JCLN (Notice the one-letter words)
   C(x)= D(x)=

   PLAINTEXT MESSAGE:

   Explain your thinking:

   b. President Name: CWBWLZ DCWOW (what could W be?)
   C(x)= D(x)=

   PLAINTEXT MESSAGE:

   Explain your thinking:

   c. Oregon Landmark: VYEIR AYYW
   C(x)= D(x)=

   PLAINTEXT MESSAGE:

   Explain your thinking:

This work was developed by Project Think and reflects our original thinking and design. We're happy to talk about how it might serve your context — please reach out to info@project-think.org before sharing or adapting it.

This work was developed by Project Think and reflects our original thinking and design. We're happy to talk about how it might serve your context — please reach out to info@project-think.org before sharing or adapting it.