

Discussion 2:

Inverse Functions and Cryptography

In this module, you learned that an **inverse function** undoes the operations done by a function. This concept can be used in basic cryptography—the practice of writing and deciphering codes. For example, imagine a basic code where each letter of the alphabet is numbered from 1 to 26. $A = 1$, $B = 2$, $C = 3$, and so on up to $Z = 26$. Secret messages can now be coded as sequences of numbers paired with punctuation. The message “HELLO, WORLD!” would be encoded as:

8 5 12 12 15, 23 15 18 12 4!

Obviously, this code would not be very hard to decipher as is. To improve upon the code, we choose a function. Let $f(x) = 2x + 1$ as an example. Substituting each of the numbers in the above message into this function, we now get the following encoded message.

17 11 25 25 31, 47 31 37 25 9!

This code is now a little bit trickier to decipher. The person receiving the secret message needs to be provided with the function used to encode the message. They can then use the inverse function to decipher it. In this case, the inverse function is

$$f^{-1}(x) = \frac{x-1}{2}.$$

Substituting each of the numbers in the new message into the inverse function gives the original message

8 5 12 12 15, 23 15 18 12 4!

which can then be decoded back into letters so it can be read.

HELLO, WORLD!

You are now ready to write your own code!

1. Come up with a function that you can use to code secret messages. Get into groups or pairs as instructed by your teacher, and write them a message using numbers for letters. Then, encode your message using the function you came up with.
2. Give the encoded message to your partner. Also give them the function you used to encode the message. Your partner should do the same for you.
3. Find the inverse of your partner's function.
4. Substitute each of the numbers in your partner's message into the inverse function, and decode the message.
5. Read/send the decoded message back to your partner. Did you get it correct? If not, work with your partner to figure out what went wrong.
6. Is there anything you could do to improve upon your code? What could be done to make it harder for a stranger or easier for your partner to decode? Discuss this with your partner and share with the class.