

The Chapter Problem—Cryptography Answers

By the end of this chapter, students should be able to provide comprehensive, well-explained solutions to the problem. Students should also be able to <to come >.

Section 3.2

CP1. *The coding method described in the Chapter Problem is an example of a function. Why?*

Each letter is coded with a different number (the independent variable). Then the same calculations on each of these numbers produce a unique number for each coded letter (the dependent variable).

CP2. *What is the domain of this function? Why?*

The domain is the set of the 26 numbers that represent the 26 letters of the alphabet. In this case, the domain is the set of numbers from 1 to 26.

CP3. *What is the range of this function? Why?*

The range will be the set of coded numbers for the 26 letters. The range depends on the numbers selected for the code. There can only be 26 letters and 26 numbers. In this case, the range is the set of numbers between 1 and 26.

CP4. *What does it mean to “break the code”?*

To break a code means to discover the coding rules or patterns that will enable you to translate and then see the disguised message. In other words, to break the code means to find the inverse of the coding algorithm.

Section 3.4

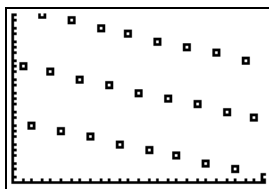
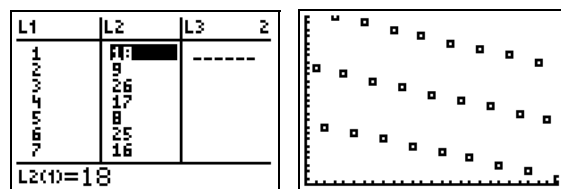
CP5. *Graph the coding function.*

Enter the numbers from 1 to 26 representing the letters of the alphabet in order from A to Z into L1. Code each letter and enter the result in L2

For example, take each number, multiply by 17. Then divide the product by 26, take the remainder, and add 1.

A = 1, then $1(17) = 17$. $17 = 0(26) + 17$. $17 + 1 = 18$, which equals R.

B = 2, then $2(17) = 34$. $34 = 1(26) + 8$. $8 + 1 = 9$, which equals I.



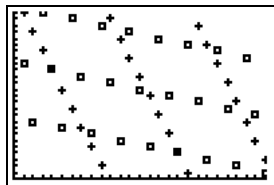
CP6. *How does this graph show that the relation is a function?*

A vertical line could be drawn anywhere on this graph, and this line would not intersect more than one point, which means that the relation is a function.

CP7. *Is the inverse relation a function? Why must the inverse relation be a function for any encryption method?*

Yes. The inverse for any encryption method must be a function so that the decoded message has only one meaning. A decoded message might have two meanings if some of the original letters had different values for each letter, and this would be unacceptable.

CP8. *Graph the inverse relation on the same axes in a different colour.*



CP9. *Use the graph of the inverse relation to decode the message.*

I LOVE MATH

CP10. *What features of this coding technique make it easy to decode?*

The domain and range are both small, so we could probably encode, or decode, this message by using a table rather than by calculating. Unfortunately, the smallness of the domain and range make the code easy to break. The code is also numeric, so once the “decoder” finds an equation and enters the equation into a computer, the computer could encode, or decode, messages very quickly.

Section 3.6

CP11. *What is the restriction on the domain of the coding function in the Chapter Problem on page 218? Why?*

The domain is $\{x \mid 1 \leq x \leq 26, x \in \mathbf{I}\}$ so that each letter of the alphabet can be assigned a unique number.

CP12. *What is the restriction on the range of the coding function? Why?*

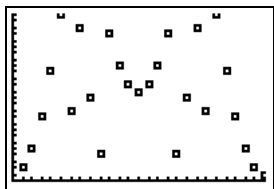
The range is $\{y \mid 1 \leq y \leq 26, y \in \mathbf{I}\}$. Adding 1 to the whole-number remainder, after dividing the product of the number and 17 by 26, will give a range of whole numbers.

CP13. *What was there about the coding function that guaranteed the range would work out appropriately?*

Dividing by 26 (mod 26) gives remainders from 0 to 25. By adding 1 to each remainder, we get values from 1 to 26, and these values correspond to the letters in the alphabet.

CP14. *A student suggested this code: instead of multiplying by 17, square the number, divide by 26, and add 1 to the remainder.*

(a) *Graph this function.*



(b) *Why would this code not work?*

A horizontal line can intersect at least two points on the graph, which indicates that the inverse relation will not provide a unique decoding.

(c) *What is necessary for any code to work?*

Both the encoding relation and the decoding relation must be functions.

Section 3.7

CP15. You could write the code in question CP14 in function notation as follows:

$$f(x) = \text{mod}(17x, 26) + 1, x \in \{1, 2, 3, \dots, 26\}$$

where $\text{mod}(a, b)$ is the remainder when a is divided by b . For example, $\text{mod}(17, 5) = 2$ because 17 divided by 5 is 3 with remainder 2.

- (a) Suppose that the equation is $y = 17x + 1$. What is the equation for the inverse function (the decoder)?

$$y = \frac{x \pm 1}{17}$$

- (b) The last operation is “add 1.” What do you know about $f^{-1}(x)$?

The first operation of $f^{-1}(x)$ will be “subtract 1.”

- (c) What is the purpose of taking the remainder after dividing by 26?

Taking the remainder after dividing by 26 produces numbers between 1 and 26 that we can code as letters.

- (d) Suppose you multiply a certain number by 17 and divide the result by 26. The remainder is 1. What is the number?

Because the result is 1, the product of 17 and the certain number must be 1 more than a multiple of 26. The number is 23, because $17(23) = 15(26) + 1$.

- (e) $f^{-1}(x)$ is very much like $f(x)$, but involves the number you found in (d). Determine $f^{-1}(x)$.

$$f^{-1}(x) = \text{mod}[23(x - 1), 26], \text{ where } 0 \text{ is equivalent to } 26, \text{ that is, the letter Z.}$$

- (f) Verify your answer for all possible values of x .

- (g) Use $f^{-1}(x)$ to decode the message in the Chapter Problem on page 218.

The decoded message is “I LOVE MATH.” Some students may find the message by encoding the letters of the alphabet and using a table to decode, rather than using the algebraic expressions for the function.