
Connections

The Chapter Problem

This *Chapter Problem* uses an environment familiar to students to develop and motivate the concept of functions and their inverses. The security of transactions on the Internet is of growing concern, and the public is becoming more and more aware of the issue. The public is less aware that the security of e-business is based on the concept of creating really hard math problems ... in the hope that no-one can solve them. “Hackers” who solve these problems (break the codes) are discovering the inverse of the original code, allowing them to decipher any message!

To begin with, students might break the given code by listing completely the alphabet, the output value, and coded letter. The message can be decoded by working backward. By graphing the relationship, students can understand why any encryption scheme must be a function. By graphing the inverse, students can also understand why the inverse must be a function (one-to-one). Later in the chapter, students develop a formula for $f^{-1}(x)$, so they do not need to list all elements of the domain to decode. At this point, there are tremendous opportunities for enrichment with matrices, jamming codes, and so on.

To make codes more complicated, you can disguise the domain by grouping letters together. By grouping every four letters together, the number of elements in the domain becomes 26^4 . This makes it harder to put all possible elements of the domain through the encoder to create a list for decoding purposes. The problem is open-ended, because no encryption system is perfect. The mathematics becomes more complicated, but students have access to the basic ideas.

Many Canadian universities offer courses in encryption. Companies like Certicom invest heavily in research and development of increasingly sophisticated codes in hopes that they can stay ahead of those who try to break the codes. A. J. Menzies is part of a team that has developed elliptic path encryption techniques—a new “really hard math problem”!

Challenge 1

This challenge is reasonably easy. Students can tabulate the frequencies of the letters in a paragraph and compare them with the frequencies of letters in the coded message. After matching by frequency, students may have to make some changes to decode the sentence. Others might decode the message by focussing only on the frequency and location of vowels, and then use the context of other words to decode the entire message.

Challenge 2

This challenge is very open-ended. Error-correcting codes are prevalent in communication technology, and a great deal of mathematics has been developed to support them. The simplest possible error-correcting code is a repetition of the word three times. Sending HIIHI and receiving HIPIHI would leave us quite certain that the original message was HI. However, if it was fairly likely that there could have been two errors, we would be less certain of the original message (could it be PIPIPI?). The problem with such codes is that to send a two-letter word, we had to send six letters, and we could only be certain to correct one error. The open-ended problem for mathematicians is to design codes that can correct as many errors as is ever likely to happen without having to send a huge message.

Web Challenge

You will find support for this internet activity at the teachers’ Web site: www.math.nelson.com.

All three Challenges can be used as rich learning tasks or for formative/summative assessment purposes. Refer to the front matter of this Teacher Resource for more detailed instructions.