AN EXPLORATION OF CODES AND CRYPTOGRAPHY

A ONE-HOUR PRESENTATION TO A GRADE 3 GIFTED CLASS AT MUTCHMOR
PUBLIC SCHOOL, OTTAWA

Dr. Monica Nevins, University of Ottawa

1. INTRODUCTION

The teacher, Rhonda Birenbaum, approached me after my Holiday Science Lecture for the Faculty of Science, to ask if I’d be interested in speaking about codes to her Grade 3 gifted class. Of course I was, and we discussed what might be appropriate in the course of a few phone calls and emails over the next weeks. The class was exploring the codes used in the Underground Railroad, as part of a project for Black History Month. My visit was one hour long.

2. THE DISCUSSION

Mathematics is about finding patterns and solving puzzles, and there is new mathematics being discovered every day. One prime example of this is in cryptography, which has evolved drastically in the past half-century, with the advent of computers and, of course, the internet.

2.1. Caesar cipher. How far back might we go to find people using cryptography? Julius Caesar went off and conquered most of Europe for the Roman Empire around 50 BCE. The logistics of this massive movement of troops is overwhelming. He needed to tell Rome where he’d been and who he had conquered, he needed to communicate with his troops spread over a large geographic area, and he needed to request supplies and new troops from Rome. How did he communicate over long distances? He used messenger, who could easily be intercepted; and if his enemies discovered where he would go next, they could perhaps defeat him.

Julius Caesar used and invented several secret codes to help keep his messages indecipherable except to his trusted allies. One of these codes is now called the Caesar cipher and it works as follows. Each letter of the alphabet is replaced by the letter three ahead. We can make a “key” to help us encode and decode more quickly: write the alphabet on one line (the “real letters”) and then write the shifted alphabet underneath (the “coded letters”). For example

ATTACK REIMS

becomes

DWWDFN UHLPV.

The latter message being complete nonsense, and no one expecting the use of cryptography at the time, this was quite a good system.

Date: February 20th, 2006.
To decode the gobbledegook back into a real message, you reverse the process, by finding the letter in the coded message on the bottom line and translating it into the letter on the top line. Try this for KXUUB WR URPH and PDWK LV IXQ.

This kind of cipher has limitations, the main one being that as soon as someone realizes you're just shifting the alphabet, they can fairly easily go through all 25 possible shifts until they discover the one you've used, and then they can read all your messages.

2.2. Substitution ciphers. One improvement to the Caesar cipher is the general substitution cipher. Now you replace each letter of the alphabet by some other letter, with no rules except that every letter has to show up in the encoded alphabet exactly once. We keep track of the substitution being used with the same kind of key as before: two rows of letters, one for the “real” alphabet, and one for the coded one.

Now we ask everyone to think of a secret word or two words, to encode it with their unique key, and to pass it to their neighbour. When the neighbour tries to decode it using their own key, it doesn’t work — the message is still a random mix of letters. But when the correct key is used, the message can be decoded.

How many such keys are there? In other words, if we wanted to make all the possible keys for substitution ciphers, how many would there be? The answer:

\[26! > 400 \text{ septillion}\]

which is quite huge; there isn’t enough paper on the earth to make that many keys. So if we wanted to “crack” your code, trying to find out which of these is your key wouldn’t be a reasonable approach.

One thing to note, however, is that when we encode longer messages using substitution ciphers, we start to give away lots of clues about our secret key. For example, a three-letter word might stand for “the” or the most common letter might be “e” — so in fact, it isn’t impossible to figure it out. But substitution codes are pretty secure for short messages.

2.3. Public key cryptography. Now in modern times, everyone who buys something over the internet is making use of cryptography. The reason: when we send information via email, that information is as accessible as Julius Caesar’s messages, since email can be intercepted and read without your knowing it. Thus to protect my credit card information, I need to encrypt it in some way.

The modern set-up is known as Alice, Bob and Eve. Alice wants to send some information to Bob, but anything she wants to send to Bob has to go through Eve, who can copy anything she likes (but won’t destroy the message). It is imperative that Eve NOT decipher the secret message, but that Bob does.

We enact this with teams of Alice and Bob (and Eve). Through discussion, we realize how difficult this problem is — even if we encode a message, Bob can’t decode it without the secret key. But there is no way to get the secret key to Bob without Eve getting it as well.

Let’s add something: each of Alice and Bob have a box with a lock and a key. Now Alice can put her message in the box and lock it, and send the locked box to Bob. Eve can’t read it; but neither can Bob. Now Alice can’t send her key to Bob (because we’re assuming Eve can make a perfect copy of anything she gets her hands on, and hence she would be able to unlock her copy of the box). But Bob has a lock, and he can put a second lock on the box. Then he sends the doubly-locked
box back to Alice, who removes her lock, and sends the box back to Bob, who can finally unlock it and read the message inside.

Now Bob can send a secret message back to Alice in exactly the same way.

OR: if Alice sends Bob her lock (unlocked), then Bob could lock the box with Alice’s lock, and send it to her, and thus the secret message is passed in fewer steps.

This latter solution is the prototype for public-key cryptography, which is what is used in internet security today. The idea is that each individual (e.g., a business on the internet) publishes a mathematical function which is the equivalent of an unlocked lock, making it available to absolutely everyone. Absolutely anyone can use it, but once it’s used ONLY the individual with the private key can unlock it.

3. Summary of the activity, and class involvement

The session was quite interactive, with students guessing at a number of answers to the questions posed in the early part, and then constructing codes more actively in the second part.

During the discussion of the Caesar cipher, I handed out pieces of cardboard with a picture of a key; inside the key was the alphabet, with a second row underneath with the shifted alphabet. Students used these keys to encipher and decipher the messages written on the board; the enciphering was done together, letter by letter, to get used to using the keys in the correct direction; the deciphering was done as a challenge for each group, with a candy prize when the message was deciphered.

Then each student got a blank key card, and was asked to make up their own substitution cipher. I pointed out that a good way to be sure not to lose any letters would be to fill in the alphabet randomly from A to Z in the empty boxes; those who didn’t tended to need a few more minutes to find their missing letters, but the teacher and her aide were also there to help. (They were also asked to name their keys, to make them easier to track.)

The students enciphered a secret word or two, and then passed it on to a neighbour; they very easily deduced that the decoding wouldn’t work without the proper key. Eventually all messages were properly decoded.

Once the Alice/Bob/Eve set-up was explained, the class split into three groups: about 10 for each of Alice and Bob, and 4 for Eve. (To do it again, I would simply play Eve myself; this group thought things through carefully and so Eve never had a chance to do any code cracking; that wasn’t fun for them.) I gave each of Alice and Bob a short codeword and a few minutes to think things over; I overheard them discussing the relative merits of paper airplanes and the like. They certainly saw the difficulties of establishing secure communications in an insecure environment.

When the locks and keys were handed out, Alice realized they should put their note in the box and lock it; they were unsure as to how to get their key to Bob (and in fact tried to send it over via Eve just a few minutes later). When Bob got the box, they tried their key and agreed that it didn’t work; someone suggested locking the box with their lock and shortly thereafter, someone realized, to great excitement, how it could work. When Alice got the box back, they spent some time trying to undo Bob’s lock, not realizing that they could just return the box. Oh well.

Now it was Bob’s turn to send the box back to Alice, with the secret message for Alice from Bob; it was at this point that someone from Alice realized that they
could simplify things by sending Bob an unlocked lock. (Although Eve, ever eager to foil secret communications, locked the lock along the way.)

3.1. **Conclusion.** The activity was great fun, with lots of teamwork and thinking things through. For an older group, it might be nice to present a more complex but more original (to them) cipher such as Vignère, as substitution ciphers are quite well-known.

The box used was a simple plastic “toolbox” and the locks were the smallest size padlocks. In fact, I had several different padlocks on hand, each part of a set where the same key opens several locks (a great model for public-key cryptography, although I didn’t get a chance to use it in this presentation).

For high school students, the math behind the RSA cryptosystem could be reasonably well presented (to interested students) in about an hour, by simply recalling early forms of cryptography and then devoting the bulk of the time to developing RSA.