Secure Messages

Topic Covered: Encryption

Purpose

To introduce students to the applications of number theory and the more opaque maths.

Goal

Give students exposure to the applications of concepts that might seem useless. Students ideally should be able to explain how encryption generally works, if not how the maths themselves work.

Level of background

Students in middle school or above are the best candidates, as they have experience not just with the number theory, but also with the technology that operates ”magically” on top of it.

1 Implementation

Resources Needed

1 lunchbox with the ability to be locked by TWO locks; **2-3** locks, **a small amount** of ”valuable substance” (may be candy, may be money, it doesn't matter as long as the students want it); **1** whiteboard and some markers

Time Needed

Can last anywhere from 30 to 60 minutes. Also easily combinable with any number of other modules.

Other Notes

This module is divided up into two parts. The first is an active demonstration of the basic idea of securing a message, and the second is an exploration of the concepts that make encryption possible.

2 Part 1: Motivating Question

You fill the lunchbox full of candy (or some other motivating substance). Ask the students how they would send it to a student at the other end of the class. What would they do to ensure that no one has access to the contents?

3 Part 1: Procedure

1. **Ask the Motivating question.** We begin with **(1)** lunchbox full of some motivating substance. This lunchbox is NOT LOCKED. After presenting the motivating question, have the class pass the lunchbox around until it gets to some designated person who is supposed to ”receive” the message (the RECEPTOR). Each student should have the opportunity to take either 1 piece of candy, or some measured amount of the motivating substance.

2. **Lock the box.** TALK about how this is not a secure way to pass a message. Solicit ideas about how to secure this. After you've gotten some discussion going, tell them that we're going to try locking the box. LOCK the box. Then, have the students PASS IT AROUND to the other designated receptor again. This time, no one should get candy because the box is locked.

3. **Lock the box a second time.** By the time the box gets to the designated receptor, the class may feel that this is an impudent demonstration. Depending on their response, you might have a discussion about the problem at hand. How does the receptor get the box back open? How do we do this without insecurely passing the message. After stewing for a while, the receptor PUTS HIS OWN LOCK on the box. There should be TWO locks on the lunch box at this point.

4. **Pass the lunchbox back to the receptor.** Now we have the class pass the lunchbox, now locked with TWO locks, back to the sender. The sender now UNLOCKS HIS LOCK. There is now ONE lock on the lunchbox.

5. **Pass the lunchbox once again back to the receptor.** At this point, there is ONE lock on the lunchbox. Since the receptor put this lock on the lunchbox, he can freely open it and get the candy.

4 Part 1: Drawing Conclusions/Discussion Questions

There are different schemes for transferring messages securely in this world. Talk about what we just did, and ask what constructs they have learned about can help them do this over, say the internet. How do you ”lock” a message? If they get stuck, ask whether perhaps they could make some sort of cipher. What ways can we make this really secure? Computers are powerful these days, they can calculate billions of things in a given second, so how do we protect against this.