Teacher's Guide for Building Cryptosystems

Massachusetts Institute of Technology
Dan Sturtevant, dan.sturtevant@sloan.mit.edu

Goals:

This is a highly interactive introduction to the field of cryptography. Students will learn ways to create and send secret messages using three methods of increasing sophistication. The methods students will employ were actually used by Julius Caesar in ancient times and Thomas Jefferson (third president of the U.S.) in modern times to send sensitive messages. Students will also 'crack' the secret messages sent by others in the classroom. Cryptography can provide motivating examples for subjects including statistics, probability, computer science, and others. This class is designed for the junior high and high school level, but could probably work in classes with children as young as 11. Classroom discussion and assignments can be tailored to be age appropriate.

Pre Class Preparation:

Some materials are required. Watch the video to see how they will be used prior to getting them. These include:

- 3 small cups per person. These cups must have a lip that is visible when cups are stacked. Small Styrofoam cups are highly recommended for this purpose.
- One sheet of paper per pair (to be depicted later) that contains 7 columns of evenly spaced boxes for each character in your alphabet. These strips will be cut out and wrapped around the outside of the lip of the cups. Creating this sheet is the most complicated portion of pre-class preparation. Follow the instructions carefully. Other files on the Blossoms site may help you.
- Scissors
- Tape or glue. Tape may be preferable because mistakes can more easily be undone.

- 2-3 sheet of paper for writing messages, encrypting them, and doing scratch work to decrypt messages from others.
- Pencil, pen, marker: Must be able to write on paper and also make markings on the cups.

Part 1: This section introduces what we will be doing and then asks the students to make sure they have the necessary supplies. Make sure students are working in pairs. Each pair should have a team number assigned by you. Each person within that pair should have a designation such as 'red' or 'blue.' Each pair should have the supplies listed above.

Part 2: This section teaches the students how to use the materials to create the devices they will need throughout the course. It is very important to make sure that when they cups are being assembled that the strips are tight around the lip and are on fairly securely. It is *extremely* important that everyone in the classroom holds the cup using the same hand when taping the strips on. If everyone in the class stacks their cups, the alphabets you looked must all be right side up. If you do not make sure that all the cups in the class have the same orientation, then the last exercise will fail. This will be correctable if you use tape.

Part 3: This section demonstrates how to create and send a message using a cipher used by Julius Caesar. The video shows students how to use their cups to do this. Students should create messages and then decrypt the message created by their partner when this section of the video is done. These messages can contain multiple words, but they probably should not be too long. I created a worksheet that I use in the video that visually represents the encryption/decryption process. This worksheet is available to you if you would like to use it in class. Alternatively, students can simply do their work on blank paper.

Part 4: This section shows students how to crack messages sent by others. It introduces a competition for you to hold in the classroom. Students are asked to trade encrypted messages with other teams and then attempt to crack the messages sent by others.

There are a variety of other things you could do in this break. You can write a message on the board and have all of the students crack it alone, in pairs, or as a class. The fastest way for the class to crack the message is to have each student trying to use different keys in parallel. Parallelizing the process makes it much simpler.

You can also discuss features of your language that might make it easier to attack a message. This includes the placement and frequency of different letters and the patterns that exist that can help guide their intuition. Each language will be different. Cryptography experts use many statistical patterns in a language to guide their attacks.

Part 5: This section has the students encrypt another message using a slightly more sophisticated technique using random sequence strips that were generated in part 2. This should be relatively easy for the students.

A discussion you may want to have in the class is about the importance of random numbers in probability, statistics, and computer science. Many cryptography systems have been broken in the past because the process used to generate randomness was flawed in some way that attackers were able to explot.

Part 6: Students are asked to split into two large groups and send messages using a cryptosystem invented and used by Thomas Jefferson. Each device will have as many cups as there were teams in the classroom. The messages these teams send can be large. If the message exceeds the length of the column of cups, have the teams repeat the encryption process repeatedly until the entire message is encoded.

You may want to have multiple classes contribute to the same stack of cups so that you eventually have a very large device. In order to do this, assign team numbers that are a continuation of the numbers used in the previous class.

Part 7: This is a short conclusion.

After class assignments: This example can motivate probability, statistics, and computer science assignments. Students could be asked to figure out how many possible combinations are possible in Jefferson's device. They could be asked to write computer code that does encryption and decryption. Choose any assignments allow this lesson to dovetail with whatever topic you are working on in class.