Building Cryptosystems

By Dan Sturtevant

Hi, my name is Dan Sturdevant. I'm at the Massachusetts Institute of Technology. Today we're going to be talking about cryptography. Cryptography is a method of creating and sending secret messages in such a way that only the intended recipient can understand them. Now this is important for a lot of reasons. It's used in military applications, but today more and more it's used in both communications and in banking and lots of other places. Now what we're going to be doing in the class is we're going to be creating three different devices. The first one is the Caesar cipher. The second on is one that's a little bit more sophisticated, and the third one is a machine that was actually invented by Thomas Jefferson who was the third President of the United States. He used his device to actually send messages from France to people in the United States so that they couldn't be intercepted by European governments. Now the device that we're going to be creating as the Jefferson cipher actually has the same architecture as was used in enigma machines by Germans during WW II.

So you need to have a few materials ready to begin. Each student should have three cups and should have few pieces of paper. I would like it if you could all just make sure that you have what you need now. Also you need to split into pairs. Each pair of students should have a team number and each student within that pair should have a color. It could be red or blue. So go ahead now, split up in pairs, choose your color and your team number. Get your materials ready and I'll see you soon. Thanks!

Hi! Welcome back! I hope you all have your devices or you have all your materials ready to create the devices. Now we're going to figure out how to turn them into cryptography devices so that we can proceed with encryption and decryption. So the first thing you should have is you should have a work sheet with seven columns in it. Two of those columns should be blank and five of them should have your alphabet in order down them. Now the first thing that we're going to do is we're going to cut out one of the strips. Now this strip is going to be used to create a

random sequence of letters. So what I want you to do is take this strip and cut out each letter individually and place it in a cup. So I'm cutting out the letter A and I'm cutting out the letter B and C and so on. Now I have a cup full of random letters and what I'm going to do is I'm going to use this cup to generate a random sequence for the two blank columns here.

So I'm going to draw my first letter which happens to be an H. And my second letter which is an R. And I'm going to write them in. So H and H. Then I'm going to write R and R. I'll take a third letter, it's a V. I'll write V and I write V. Ultimately what you're trying to do is you're trying to generate a random sequence of letters down those columns. Now notice that you have six columns left. Each person in your pair will have three of these strips, so I want you to cut them all out. Now ultimately what you're creating is you're creating three cups per person. What I want you to do is take the strip and tape it around the rim of the cup so that it's good and tight. Then what I want you to do is take the other strips which are… you have one more strip which is the letters in sequence, and one more which is random. And what you should end up with is these three cups which can rotate against each other.

The last thing I need you to do is to write your team number and your individual color on the bottom of each cup. So let's say I'm in team four. I'm going to write the number four on the bottom of my cups and I'm going to write the color red on the bottom of the cup. Now my partner is going to be blue and my partner is going to write the number four, but he might write the color blue on the bottom of the cup. So that's what you need to do. Why don't you go do that now and then we'll talk when you're done. Thanks!

Hi, welcome back! Now the fun part begins. We're going to start by creating and sending our first message using the Caesar's method. This method was used by Caesar to send message to the battlefield. So what I want you to do first is to start with the cups that have the alphabet in sequence. Next what I want you to do is get together with your partner and choose a key that you're both going to use. The key in this instance is a single letter. So I'm going to choose the letter F for my key.

The second thing to do is to choose a message to send to your partner. Now make sure the message is nice right now because other teams are going to try to crack it later in a different module. I'm going to choose the message hello. Now both of these things are inputs to the cipher

machine to create the secret message. What I'm going to do first is I'm going to take the left hand column and find the first character in the alphabet and I'm going to line that up with the key, which is the letter F. What I'm going to do then is I'm going to find the first letter in my message in my left hand column and look at my right hand column to see what letter to write down as the encrypted version of the message. So in this instance it's the letter M for H. I'm going to find E which is J. I'm going to find the letter L which is Q. Another Q for L and I'm going to find O which is the letter T.

Now what you should do is you should trade worksheets with your partner. You should send them your encrypted version of the message but not the original. Now because your partner has the same key as you, the letter F again, and they have the secret which is MJQQT, what they can do is they can take their cipher machine and they decrypt it. So again what they're going to do is they're going to find the letter A and line it up with the key, which is the letter F. And then they're going to decrypt the message by looking in the right hand column for the letter M and looking to the left hand column to see what the original letter was, which was the letter H. And so on. So you should be able to get the world HELLO out just by having the key and the secret message. So why don't you go ahead and do that now and come back and tell me how it goes?

Welcome back. I hope sending your first message went well. Unfortunately the cipher you used, Caesar's method, was not a very good one. The reason for that is that there were only 26 possible keys in the English language anyway. In your language it's just whatever number of characters you happen to be using in the device you just created. The problem with that is that someone could intercept your message and only have to try out 26 possible keys before they would get it.

So what I want you to do is I want you to trade your encrypted message with a team that doesn't have your key. What they're going to do is they're going to try to figure out how to get the message out without it. You're going to receive a message from another team and you're going to try to figure out how to do the same.

Now you could do this the hard way by trying out 26 possible keys but there are other easy ways of getting the message out more quickly. One of them is to look for statistical patterns in the particular language you're using. The reason for this is for example in the English

language there are two letters, A and I that make up single letter words. If you saw a message that had only a single letter in one of the words, you could easily test those first two letters first and then you would only have to try out two keys instead of all 26. There are lots of other patterns you can use in different languages to try to get messages out more quickly. So what I want you to do is I want you to try to go and crack each other's code. We're going to have a competition to see who can do this most quickly. So good luck! See you soon.

Welcome back and congratulations to the winner! Hopefully that lesson taught you two important things. The first is how to crack message using statistical or language based or even brute force techniques. The second and more important message is that it's important to use strong crypto systems so that other people can't crack your messages. The reason the last system was so weak is because it only had 26 possible keys. That's because there were 26 possible letters in the English language.

The next system that we're going to try has 26 factorial possible keys. The reason for that is this. When you generated your random strip of letters, first you drew from 26 possible letters. The second time you drew there were 25 letters left in the cup and so you had 25 possible letters. The third time, you had 24 and so on and so on until the strip was completely filled in down to one. This number is equal to 26 factorial.

Now we're going to use our random strip to use cryptography again in a much stronger way. So what we're going to do now is instead of having the two columns having the alphabet in sequence, we're going to have the alphabet in sequence in the first column and the randomized alphabet in the second column. Now again I'm going to demonstrate using the message Hello. Now the key is still the letter F because I have to line up with the letter F, but it's also stronger because I have 26 factorial possible combinations of letters in this column. Now I've got a different cipher machine. It's no longer a Caesar cipher, but I can go through the same process. I'll find H. This time it's Z. I'll find E, it's Y. I find L, which is U. L is U again. And finally I'll find O which is R. Now we're going to trade messages. My partner has the same random strip around the right hand cup as I do. I've handed them the secret and they already know that the key is F. So my partner will like up F with A as before, and then will decrypt the message by looking

in the right hand column and then looking for the letter in the left hand column. So again I look for the letter Z in the right hand column which turns into the letter H. And I look for Y which turns out to be E and so on. Until I get the word Hello out. So why don't you go ahead and do this. Try it again with the left hand column being the alphabetically ordered column and the right hand column being the random one that's 26 factorial strong. Bye!

Welcome back! For a final exercise we're actually going to be constructing Thomas Jefferson's wheel cipher. Thomas Jefferson was the third President of the United States and also was an inventor. This is the device that he invented. You can actually see it over here in this picture. What it is is it's a sequence of plates that are numbered. The reason for the numbering is that the key that he used was actually the ordering of plates. So he and a friend would share a sequence of numbers that was the ordering and then they would dial the message into the machine and then get a secret by looking at a different row. Now you've created this system already. I would like all of the red people to go to one side of the classroom and all of the blue people to go to the other side of the classroom. Now notice that on each cup you've actually written your team number. The team number corresponds with the number in Jefferson's plates. Now as a class what you can do is you can choose a key that you share between you. Write it on a board and then encrypt messages for each other. What you need to do is you need to order the cups that you have in the same sequence and then you need to encrypt a message by putting all of the cups in the order and then rotating them so that you create the message that you want to send.

So now we're going to send a message to the other side of the classroom. I'm going to take my Jefferson wheel cipher and pick a key. The key is going to be the ordering of the cups. So I'm going to use cup three. Then I'm going to use the cup twelve. Then I'm going to use cup two. Then I'm going to use cup four. And finally I'm going to use cup 13. Now once I've placed all these cups in the proper order I'm going to pick a message. Once again I'm going to use the word Hello. In order to encrypt this message what I'm going to do is I'm going to find the word Hello by spinning these cups in the plated order. So first I find the letter H. Then I find the letter E, then L, L, O. Now, in order to create the encrypted message what I'm going to do is I'm going to pick randomly a different line on the cups. In this instance I'm going to pick F, N, H, T and D.

Now the red team on the other side of the classroom should have the same key. Again, the key is three, twelve, two, four, and thirteen. If the red team arranges their plates in the same order they should be able to get the message out. The reason for this is because if they have F,N,H,T,D, they should be able to find that sequence of letters and then search through the entire cup until they happen upon a message that's in the language that you speak. In my instance, Hello.

So as a classroom I want you to split up now and create messages for the other side of the class. Encrypt them, send them, and then decrypt from the other side.

So in closing you actually have a device now that's very powerful. The same architecture was actually used inside enigma machines during WW II by Germany. Now modern cryptography doesn't use letters. It actually uses bits inside computers, but the principles are all the same. You have all the basics that you need to get started. There are a lot of exercises you can do in computer programming or in mathematics to better understand the field, but in general you really understand all that you need to know to get started. So I hope you had a good time and I hope you're interested in this topic in the future. Thanks!

Hi! This module is about cryptography which is the field dedicated to understanding how to encrypt and decrypt messages. The idea is that you can encrypt a message and then send it to someone in public in such a way that only the intended receiver can understand it. This is a very interactive module. Students will be creating cipher machines out of cups and out of paper strips. So they'll be creating these devices and rotating them against each other to create secret messages, send them to other people in the classroom and then decrypt them. In one of the modules they'll actually be cracking each other's messages to see why it's important to have strong encryption and to learn about cracking techniques. And they're going to end up by creating a device that was invented by Thomas Jefferson a few hundred years ago to actually send messages from France to the United States when he knew that European countries were intercepting his messages. This basically introduces all the key concepts in cryptography. It doesn't involve too many materials but there are a few things that you need to be aware of The

first is that they need to be able to create this device, which is a cup with a strip around it. The strip contains every letter in the English alphabet. Now you can create this for any alphabet that you want. The key is that the strip has to fit around the cup perfectly and all the letters have to be evenly spaced. So the way that I did that is that I created a grid with all of my letters in a row and did in such a way that it was the same length as the circumference of the cup. The way that I did that was in the application Excel, I spaced the columns appropriately. Another way to do that is just with a ruler and knowing the number of letters in your alphabet and knowing how wide your particular cup has to be, you could measure it and make sure that it lines up right. But that's a very important thing to get right before the classroom experience. Now the materials that you need in the class are for each student or pair of students, a pair of scissors, some tape or some glue, and some of these strips of paper, some of which are going to be blank and some of which are going to have your alphabet. Each student is going to have to have I guess five that have the alphabet and two that are blank. So those are all the materials that you need, and I hope that you enjoy the module.

END OF MODULE