Cryptography and Cyber Security: Instructor Notes

Cryptography and Cyber Security is one of iD's newest courses. Being new, it has a host of problems; I want to attempt to identify and solve as many of these issues as I can.

The Problem

In a nutshell, Cryptography is too broad a class. The student game plan covers C++, Python, and an introduction to binary through the Commodore 64. In every other programming class I've taught at iD, it takes several days of focus on one language to achieve acceptable comprehension for most students. The modules that are present now glaze over important topics such that students are "finished" with all of the curriculum early in the week, but they haven't *comprehended* any of the information.

Another issue is the complexity of the *topic* of cryptography. Without extensive background in math and computer science, students won't be able to program very many cryptographic algorithms. Outside of shift ciphers, bitwise XOR, or other simple encryption, algorithms will be too difficult for students to understand, much less implement in a programming course.

The lack of comprehension paired with the difficulty of cryptography make for a course that fails to teach use of cryptography in programming. The course must change in order to deliver on the promise iD makes to students and parents.

Solutions

After teaching the class, I have a few ideas to improve it for the rest of the summer:

- *Teach one language.* I would say pick either C++ or Python, but the student transcript says we focus on C++, so you should teach that.
- *Spend most of your time teaching programming.* I'd say the first two days (Monday and Tuesday) should be used to teach C++. Students should be able to use for loops. In order to implement any level of cryptography, they need to understand the language up to looping.
- *Spend time to teach actual cryptography*. If it were me, I would spend a lot of unplugged time on Wednesday teaching crypto topics. You could cover binary,

symmetric/asymmetric encryption, and give a couple of example algorithms. They need to understand enough to implement some amount of cryptography in their final projects.
- *Use Libraries*. Cool final projects might include implementation of actual cryptographic algorithms through libraries. This way, they are using and (sort of) understanding actual industry cryptography with programming they can actually understand. You could potentially even teach programming with the goal of eventually implementing cryptographic libraries, so all the projects at the end look really impressive.
- *Cut out the Commodore 64.* Honestly, I think it's a bad way to teach binary. It isn't even that useful at the level these students are at.

In summary, there isn't enough time to teach the breadth of topics that the term "Cryptography and Cyber Security" encapsulates. Focus on one language, and teach a manageable amount of cryptography such that they can use it in their final projects. I wish you luck with the course!

P.S: I've written some example code for the course. If you want to use it, you can find it at github.com/Capprin/tech-crypto