# Curriculum Map – An Interdisciplinary Approach to Cyber Security

**Author**

Ellen Tevik. High School Math Teacher. St. Mary’s Academy, Portland, OR. July 31st, 2016.

**Motivation**

In my experience, the main stumbling block to incorporating additional content into schools is time. While topics such as cyber security are essential, timely, and current, attempting to implement these “supplementary” topics often fails. Each discipline has its own content it must cover. The demands of standardized tests, school events, and other miscellaneous items reduce the time allotted to teach required content. Teachers are already overwhelmed with ever increasing demands on their time, and being asked to teach another topic that may not be in their content area is often too much. All these factors reduce teacher buy in, causing implementation to fail.

Including cyber security content outside of normal school hours as an elective activity can be more successful, but often fails to expose a widespread audience. Students predisposed to programming or security issues tend to attend these “extra workshops.” If the goal is to inform students about the potential in cyber security fields, many students will not attend due to their own preconceived notions of ability and interest, or they may honor other commitments. Underrepresented groups such as minorities and women are often in this second group of non attendees. An outside of school day format misses a significant core group of students that cyber security programs are trying to reach.

**A New Approach**

My idea is to increase exposure to more students by including cyber security content in several core courses. The intention is that a selection of teachers would take 5 or 10 minutes a couple of times a year to cover a portion of cyber security content. Doing this in several core classes across many disciplines will greatly increase the number of students exposed, and will highlight the interdisciplinary nature of cyber security.

Teachers could introduce the content through starters, review problems, discussion prompts, or time fillers. It could be done on days when regular content cannot be covered (such as retreat days that remove a certain grade level from classes, days before holidays, or testing days). Or the content could be given at the end of the year. It is fairly common to have small groups of students remaining in classes at this time of year. A coordinated effort could be made from several teachers of differing fields. They could do a mini cyber unit. It would be a great way to switch things up at the end of the year when students are pretty tired of the normal content. The intention is that teachers would be able to incorporate short topics in cyber security as they naturally occurred in the course of covering their own content.

Instead of asking a small group of teachers to learn and be responsible for covering the many facets of cyber security, this approach asks a larger group of teachers to learn and present a small portion of the content – a portion related to their field. This should increase teacher buy in and make implementation easier.. Hopefully by giving each discipline cyber security topics related to their specific field, teachers can substitute, not add to their own content.

The following is a very brief summary of how the facets of cyber security could be divided among the different disciplines. Further work will need to be done on the details of each, although I have tried to give ideas based on my experience at the cyber pdx camp.

**An Interdisciplinary Jigsaw**

* History courses would cover the history of ciphers. This could be covered very naturally in the flow of historical content. For example, covering substitution cyphers in a unit on Roman history and the Enigma code when dealing with WWII. Here is a logical place where students would practice using actual ciphers to encode messages. Perhaps give some review problems for assessments in cypher form.
* Religion/ethics courses could cover ethical issues of using ciphers and actions involved in breaking them. For schools without these subjects, this might fit well into civics, government, or political science courses. This would be a great place to also talk about personal responsibility issues related to the sharing of metadata.
* English could cover character analysis ideas as a way to break codes. This could be a logical place to discuss viginere codes as well. A knowledge of the complexity of words is key to creating good viginere codes. Here is a natural place for student to use and create their own codes.
* Foreign language might be able to cover Caesar cyphers in the context of using different alphabets.
* Math could talk about the combinatorics of cyphers. Students could learn to analyze the number of permutations for particular cyphers and use this to rate the strength and weakness of the different methods they learned about in history. This might be a natural place for students to use character analysis to design and break cyphers. Here is where you could also practice decoding messages.
* Music classes can talk about tonal ciphers. If available, students could use audio software such as audacity to garble and ungarble audio messages. This would be a natural place to cover morse code.
* Science could cover the possibility of DNA or chemical cyphers. Physics courses could also discuss quantum cryptography.
* Computer science courses could cover issues and content related to bar codes, RFID, QR codes, website encryption, etc. These courses could also cover machine driven cyphers.
* Journalism courses could talk about right to know versus national security. Recent events involving WikiLeaks have made this a relevant topic.
* Art classes might be able to talk about Steganography methods. This one is a bit of a stretch, but worth a shot. It might work better in a digital art course.

**My Hope**

I hopeq this resource gives people ideas about how they could implement cyber security content in their school or classrooms. I also hope readers will see how something as specific as cyber security ends up being amazingly interdisciplinary. With only my brief one week exposure to cyber security content, I was able to identify ten potential courses where content could naturally be introduced, practiced, or discussed. I hope that others will be able to expand the very preliminary ideas I put to paper, and make the content more relevant to their own courses.

To learn more and get OneNote, visit [www.onenote.com](http://go.microsoft.com/fwlink/?LinkID=523891).