Cryptography Project for Year 12 students

Summer 2020

Dr. Julia Goedecke

This project will introduce you to some ideas in cryptography. You can extend it into a range of directions: pick one or two that interest you.

**Virtual Workshop**

Start your journey with this virtual workshop which introduces you to modular arithmetic (needed for many cryptography algorithms), an easy historical cryptosystem called the Caesar Cipher, and a more modern system called RSA. Make sure you do the optional routes, at least the ones in the middle column.

**Extend**

Here are some options for you to take this further. You should pick maybe one or two topics: they range from not very mathematical to more mathematical content. Of course you can take any of them further with your own internet searches if you wish.

- Research the **history of cryptography**, starting with Wikipedia for example. You can do your own internet searches and follow up any bit of the history you find most interesting.
- Explore some of the **Further Resources** from the virtual workshop. In particular, you can do a cipher challenge.
- Find out about the **Enigma machine** which the Germans used in World War 2, and the Allies cracked, working a lot from Bletchley Park. Here is a YouTube video on Enigma from numberphile. You can follow it up with more information for example from the Wikipedia article on the enigma machine. Maybe you’ve seen the film The Imitation Game, where Benedict Cumberbatch plays Alan Turing. If not, you might be interested in watching it.
- **Cracking code: Frequency Analysis**. The Caesar Cipher from the Virtual Workshop is an example of a Substitution Cipher: one letter from the alphabet is substituted for another. There is a way we can crack such codes using what is called Frequency Analysis. The website Frequency Analysis: Breaking the Code from Crypto Corner explains what this is and explores it on an example. See also an article on nrich: Cracking Codes. Once you’ve read this, you could get a friend or family member to send you a (long-ish) message encrypted by a substitution cipher such as the Caesar Cipher (they can use this website called cryptii for easy automatic encryption). Then you can try to crack it using frequency analysis. Or try this cipher challenge.
- An alternative to RSA: the **Diffie-Hellman Key Exchange**. This is a method to share data over an insecure channel to end up with a shared secret key (for example to use for a symmetric key encryption system). Start with these two videos from computerphile: metaphore explanation using colour mixing, and the maths behind Diffie-Hellman Key Exchange.
- Explore what it means to use **End-to-End Encryption** (like WhatsApp does) and what options or problems there are to stop criminals using such channels of communication. computerphile video on End-to-End Encryption.
- Explore how you can use public/private key pairs for **Digital Signatures**. YouTube video on digital signatures by Sunny Classrooms.