Bringing cutting edge science into the classroom

**Quantum Key Distribution**

**Video Transcripts**

Taken from History of Cryptography.mp4 video.

The video can be used by itself. However, if preferred, teachers may use the transcript over the top, or with the source Prezi. These alternatives will enable more discussion with the students, depending on time.

*Prezi URL*

http://prezi.com/sbm7faf9nz2n/?utm\_campaign=share&utm\_medium=copy&rc=ex0share

**Transcript**

Cryptography began thousands of years ago, and kings, queens, rich people and naughty people having affairs have relied on it ever since.

One of the earliest uses we know of was from 3500 years ago by a potter who wanted to keep his glaze recipe secret. The Kama Sutra, from around 400BC, recommended that lovers wanting to keep their messages secret might use cryptography.

The Romans loved a good code too. Spartans used a device called a scytale (skyt a lee) – which did a transposition of the letters – by wrapping around a stick with a polygon cross-section. In 404BC a bloodied messenger turned up at Lysander of Sparta‘s door – one of only five that had survived the journey from Persia. Lysander took the messenger’s belt and wrapped it around a scytale and discovered that Persia was about to attack. Lysander was able to prepare and eventually repel the attack. Julius Caesar was known to use a variety of ciphers, including a substitution cipher where each letter was replaced by others.

These substitution ciphers gave a high degree of security and were used for a long time. But in the 9th ninth-century scientist Al-Kindi was the first recorded person to write about the process of Frequency Analysis – that is that the most commonly coded letters are likely represent the most popular letters.

This led to the invention of systems that used multiple symbols to represent the same letter, to make them less susceptible to frequency analysis. In 1586 Mary, Queen of Scots, had secret plans to overthrow Queen Elizabeth. She wrote these plans down in a letter, albeit in an encrypted fashion. But, the messages were intercepted, and her fate depended on whether the messages would be decrypted or not. They were, she was found guilty of treason and eventually executed.

Better methods were needed, and were developed. One, the Vigenèrecipher (ve-sh-nere) was thought to be uncrackable for over three centuries.

The story of how Alan Turing and the allied forces cracked the German’s Enigma code during World War 2 is often told – and the team at Bletchley Park developed some of the world’s first programmable computers to help them in this task.

Encryption is now usually handled by computers. In 1975 the US Federal Register established the Data Encryption Standard (DES), an algorithm that computers for banks and financial organisations could use to share information.

All of these systems required a shared key, which must be protected at all costs.

In 1977 Ron Rivest, Adi Shamir and Len Adleman came up with a clever way of encoding messages using two different keys – one that is kept private and one that is made public. This forms the basis for all of our secure transactions online, and as long as we do not share our private key, we should be able to verify that the other party is who they say they are. It has not changed much in the last 40 years, except that as computers get faster, and our mathematical understanding increases, the length of keys needed to remain secure has increased.

In 1984 Charles Bennett and Gilles Brassard came up with the theoretical idea of quantum cryptography. And in 2004, as part of a technology demonstration in Vienna, the world’s first bank to bank transfer was completed using quantum cryptography. Quantum cryptography is fundamentally different from all other forms of cryptography – in that when properly implemented it is completely unbreakable. The physical laws of the universe prevent someone from snooping in on our messages. The challenges that remain are largely engineering ones – can we actually build the quantum networks that we need to keep us secure.

**Another interesting cipher**

If students are really fascinated by ciphers they may be interested in the $63,000,000 of gold that Thomas Beale buried in America in the 1820s, and left three cryptic messages to. Thousands of code-breakers have attempted it over the decades. To this day the treasure has not been found.

10-minute video about the Thomas Beale cipher:

http://www.thomasbealecipher.com

**Image copyright notices**

*Pottery image, Julius Caesar, Mary Queen of Scots, binary code* – public domain

*Kama Sutra and Enigma machine image.*

This file is licensed under the Creative Commons Attribution 2.0 Generic licence.

You are free:

* to share – to copy, distribute and transmit the work
* to remix – to adapt the work

Under the following conditions:

* attribution – you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

*Scytale and Al Kindi image*

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported licence.

You are free:

* to share – to copy, distribute and transmit the work
* to remix – to adapt the work

Under the following conditions:

* attribution – you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work)
* share alike – if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar licence to this one