Bringing cutting edge science into the classroom

**Quantum Key Distribution**

The idea of encoding messages to keep them secret began thousands of years ago. Julius Caesar encoded private communications by shifting the letters in the alphabet, and over time increasingly complicated methods have been invented to help keep messages secure. During the Second World War electromechanical computers were created to help humans to crack the Enigma codes.

Since then, as computers have developed and increased in speed, more secure codes have been created. However, all cryptography methods are only secure whilst the keys that they use to encode the messages are kept secret.

Over the last 30 years scientists have begun to exploit the unintuitive quantum properties of light, Heisenberg’s Uncertainty Principle and entanglement, to ensure keys can be shared that are guaranteed to be secure.

This package of materials briefly explores a history of cryptography in order to explain the value behind a truly secure method of sharing a cryptographic key. Quantum Key Distribution (QKD) methods are then explained, before students are given a task to research how QKD systems may be used in practice.

Materials produced by Alan Denton.

With thanks to Professor Tim Spiller, Director of the EPSRC Quantum Communications Hub.

Supported and funded by

National Science Learning Network  
Research Councils UK (RCUK)

**Using the materials**

As well as talking about the theory and uses of Quantum Key Distribution (QKD), students using this package will develop cooperation in a group, put a research bid together, respond to Q&As and think about the value and application of scientific developments. Linear polarisation is explained in the context of QKD.

**Quantum Key Distribution – intro.pptx**

The introduction PowerPoint describes what Quantum Key Distribution is, and how it can fundamentally improve upon standard cryptography.

To understand this students must first understand

* what cryptography is
* the importance of a key
* the uncrackable nature of a one-time pad.

It then discusses the science behind QKD, without really describing the uses. The notes section contains detailed descriptions to support the PowerPoint for the teachers, and links to other places with more information in. These slides are intended for teachers that understand QKD, to support them in lessons. Teachers that are not sure about QKD are recommended to read about it before teaching it (see below for readings).

**History of Cryptography.mp4**

**Transcript from History of Cryptography Video.docx**

The video can be used by itself during the **QKD – intro** slideshow. However, if preferred, teachers may use the transcript to read 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

**Cipher examples.docx**

This contains four worksheets explaining and testing an understanding of four different types of cipher. It also contains answer-sheets to all of the problems. They are generally of increasing difficulty.

It is recommended that a mixed-ability group of four have a look at the problems together, for about 15 minutes, at the appropriate point during the **QKD - intro** slides. The main focus of this activity is to demonstrate that all codes have keys to encode/decode them, and that keeping the keys secure is important.

**Research competition – stimulus sheets.docx**

These are instructions and stimulus sheets to run an activity where groups research a use of QKD, and bid for funding. It takes about an hour for the research activity, and about another hour as the bids are presented to a research council (in a similar fashion to Dragons’ Den).

**Quantum Key Distribution - research competition.pptx**

This is a very short presentation that can be used to explain to students how the research activity will work.

**Other material**

**Quantum Key Distribution – recommended reading**

There are a lot of descriptions online about how QKD works, and they generally explain it using Heisenberg’s Uncertainty Principle and the linear polarisation of light.

<http://qcvictoria.com/QCV-Technology/QKD>

However, in reality there are other ways that Quantum Key Distribution can be used in practice. You can use other properties of light (such as the circular polarisation of light or phase difference) in an analogous fashion to the linear polarisation. It is also possible to use entanglement. To fully understand entanglement requires some detailed understanding, so many teachers will not mention it unless students ask about it. A nice introduction of how entanglement could be used is here.

[http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/ - hup](http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#hup)

There is a thoughtful analysis about the uses of QKD in chapter 9 of Sheila Coburne’s report, Quantum Key Distribution Protocols and Applications, from Royal Holloway, University of London.

<https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf>

More codes

If students are interested in looking at codes in more detail, there are many excellent resources that can take this further.

Simon Singh’s, *The Code Book,* is an excellent read and contains many fascinating stories about the battle between code-setters and code-breakers over history. It also contains a description of QKD.

The Khan Academy has produced an excellent suite of exercises and videos that go from ancient codes right through to modern computer codes, such as RSA.

<https://www.khanacademy.org/computing/computer-science/cryptography>

*Vigenère**cipher solver*

<http://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx>

*Transposition solver*

<http://tholman.com/other/transposition/>

*Caesar cipher solver*

<http://www.xarg.org/tools/caesar-cipher/>

*Enigma simulator*

<http://enigma.louisedade.co.uk/enigma.html>

Research and Intellectual Property

In the research competition equal weight is initially given to the deployment uses of QKD, despite the fact that some are much closer to reality than others (and some are already being used).

Intellectual Property is also not mentioned, which could alter the direction that researchers take.

It is also possible that students could assume that research councils fund all research, but companies and governments are also very interested in research into QKD. The following companies have a QKD offering.

<http://www.idquantique.com>

<http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/>

<http://www.magiqtech.com/Products.html>