Conventional Cryptography, 21 Feb 2002, 6pm
Modern Cryptography, 28 Feb 2002, 6pm

Harold Thimbleby
Gresham Professor of Geometry

Conventional secret codes, such as the World War II Enigma code, rely on keeping keys secret to remain secure. Anyone who knows the keys can decode messages. The person you are sending a secret coded message to has to know beforehand how to decode it. If you want to send the person secrets, you hardly want to send them the key (which anyone can read) and risk it being intercepted by the enemy! In a situation like the second World War, you can start off with the assumption that your army is on your side, so you can send trusted soldiers around with the secret keys hidden on them.

One of the important things codes can be used for is for exchanging money securely. For example, cash machines routinely encode all the signals on their wires, so that criminals can’t easily intercept or dig up the cables and get access to your transactions and (for instance) later pretend to know your PIN numbers and steal from your account. Much like the army, the bank controls both ends: the bank installed the cash machine, laid the wires, and runs the bank at the other end, so they have no problem getting the same secret keys in the cash machine and at their head office.

But today, we have the internet, and we want to send secret messages to people who we have never met before. There is no obvious way to share keys with them before we want to send the secret messages that need the keys. For instance, we might want to buy stuff from companies we’ve never visited. We need secret codes to do this securely, yet we can’t get the secret keys to the people we want to work with. They might be on the other side of the world. We can’t even be sure the people we send keys to are in fact the right people to get them, or that the keys aren’t intercepted and copied en route by people we don’t want to see them.

In the 1970s a new scheme called public key cryptography was invented, which — paradoxically — allows the keys to be public knowledge and yet for communication to remain secret! If the keys are public knowledge, then the people you want to can decode secret messages. How you stop other people doing so is tricky, but possible.

The techniques are based in mathematical ideas, and the normal explanations of how they work are very hard to follow. Fortunately it is possible to explain all the principles in very clear terms, and indeed to get people in the audience to send secret messages around the room using a simple public key system. Once the basic idea is seen to work, some of the further magic becomes a lot more plausible: the same techniques can be used to create reliable signatures that cannot be forged, to allow money to change hands without revealing who people are, to stop people denying they’ve sent messages which they did (but now wish they hadn’t) … and so on.

The lecture will be suitable for sixth formers. It’s great fun to send secret messages around a lecture theatre. The lecture ends on a more serious note about the politics of cryptography in modern society: whether it is used for secure commerce, humanitarian causes or for illegal activities, and what governments are doing to regulate it.

Further reading
http://www.cosc.canterbury.ac.nz/tim/crypto/newcrypto2.pdf
http://www.gresham.ac.uk