

Quantum cryptography

What is cryptography?

Cryptography is a method used to change a message that will be sent between two points.

The original message is transformed into a cipher that cannot be understood by anyone except the person sending the message. When the sender turns the message into a cipher this is called encrypting. The sender then sends the encrypted message to the person who needs to receive it. In order for the receiver to understand the message, they must decrypt it and transform it from a cipher into the original message to understand it.

To decrypt a message, the receiver must have the key: the set of rules that the sender used to turn the original message into a cipher. So, in order for a message to be safe and secure, the sender has to send two pieces of information: the cipher and the key. Passing a message safely relies on the idea that someone else cannot get access to the key used to create the cipher. With the key and the cipher anyone can decrypt the message, not just the intended receiver.

A popular term for encrypting is code-making, and a popular term for decrypting is code-breaking.

Cryptography is used frequently. For example, credit card numbers are encrypted when you buy something on the internet. Many government agencies rely on cryptography to get messages safely around the world.

Cryptography methods

Many historians say that code-making dates back to 1900 B.C. (almost 4000 years ago) in ancient Egypt where secret hieroglyphics were made. Since then there has always been a race between code-makers and code-breakers. Code-makers have always looked for ways to create an unbreakable code, and just as fast, code-breakers have looked for a way to work out the key and the message.

Modern methods of cryptography use mathematics and the speed of computers. Most keys are built on complicated mathematical problems that cannot easily be solved by code-breakers and their computers. However, the fact remains that if the wrong party did get the key, and spent enough time working out the mathematical problem, they could decrypt a secret message.

What is quantum cryptography?

Quantum cryptography is a new way of coding messages. It was developed because of one of the major problems with code-making. Let's say the receiver had successfully taken the key and the cipher and understood the secret message. Everything seems fine, but the problem was that neither the sender nor the receiver could tell if anyone else had also received the cipher and key and read the message as well!

However, in quantum cryptography the key is not made of words, numbers or even complicated mathematical problems. It is instead made of light. A key made of light uses one of the basic properties of light: that when it is detected it is disrupted and changed. In other words, if someone had used the key to read the cipher the receiver of the message would know before he tried to use it again. It would be like opening someone's mail and trying to tape it shut again before putting it back in the post box – the receiver would know that someone else had already read the message!

What does all this have to do with Einstein?

In 1905 Einstein proposed the theory that light could act as both a wave and a particle. The particles of light would turn one direction or another, called polarization. If one direction is “0” and the other direction is “1” a stream of light particles produces a list of 1’s and 0’s. These numbers are used to create the key for the message. Einstein later showed in 1935 that measuring the light again would give a different list of 1’s and 0’s and both the sender and receiver would know that the message had been read.

Where can I find out more?

<http://www.qubit.org/library/intros/crypt.html>