Encryption - GCSE Computer Science video Top 5 facts about Encryption

NARRATOR: Are you worried that your secret messages will become public?

Here are the top five facts you need to know about encryption.

One: it's a way of concealing a message so it can be sent secretly.

Encryption is a process of disguising a message or some data so that it cannot be easily understood, especially to prevent unauthorised access. A message for all to see is called plaintext. But once encrypted, it's known as ciphertext.

Two: encryption is secure when used correctly.

(TRUMPET)

A cryptosystem is the method you use to encrypt and decrypt messages. A Dutchman called Auguste Kerckhoffs came up with this principal - a cryptosystem should be secure, even if everything about the system is public knowledge, which means every detail about your cryptosystem can be public and it will still remain secret. Every detail, except for one important thing.

Three: you need a key.

The key tells you how the message has been jumbled up or encrypted. Get the key, unlock the message.

Four: Julius Caesar used encryption.

(BEEP)

One of the oldest and simplest forms of encrypted writing is called the Caesar cipher. It's very simple and works by realigning or shifting the alphabet. Each letter is replaced with one further up or down the alphabet.

For example, shifting the alphabet two letters forward would mean that A becomes C, B becomes D, C becomes E and so on. The key to unlock the code is whatever number of letters the alphabet has been shifted. The key in this case would simply be forward or plus two. You can see that the letter Y becomes A and Z becomes B.

The letters at the end of the alphabet have been shifted round to overlap letters at the start of the alphabet. This is known as a wrap around. As there are 26 letters in the alphabet, it means that this type of encryption is very easy to solve. You would only need to try a maximum of 25 combinations before you crack it.

Five: asymmetric is more sophisticated than symmetric.

Symmetric encryption, like the Caesar cipher, uses just one key to hide and read a message. It assumes both parties already share a secret key. The problem is that if that key becomes public then all messages can be unlocked.

A more sophisticated form of encryption is called asymmetric encryption.

To do it, you need a pair of keys: one public and one private. The two keys are uniquely paired from the time they are created. You share your public key with the world at large. Then anyone who wants to send you a message uses that public key to encrypt it.

And here’s the trick, only your private key can unlock a message that has been encrypted using your public key. So, as long as you keep your private key a secret then nobody else can read a message that has been encrypted just for you. Most websites use this form of encryption.

Emails, photos, videos, documents, calls, texts, voice messages, instant messages, status updates, cryptocurrency and credit card numbers are all encrypted.

Cryptography works, but only if you keep your secret key secret.