Stream Ciphers

Welcome back. In this video, I'm going to briefly introduce a stream cipher. A stream cipher effectively works with a stream of data. This could be a stream of bits or a stream of bytes. The most simple example that I give is to work with the bitwise operations. So for example, an exclusive OR operation. In this example, we would take each bit of the plaintext, in turn, perform an exclusive OR operation with the corresponding key bit. So let's take a look at an example.

As you can see on the screen here, this reflects the exclusive OR bitwise operation. We have the stream of data plaintext, and we also have the key. Now, the key is obviously going to be varying in terms of its length. And we would repeat that key where appropriate underneath the corresponding plaintext. We then perform an exclusive OR operation bit by bit. You can see some of that has been completed here. But why don't you take a minute and complete that for the rest of the plaintext. That's a very quick rundown of how a stream cipher works.

We'll be able to compare this to the likes of a block cipher, which works on a block of data, such as a set of bytes. For decryption in this particular example, we would repeat the same process. Effectively, we need to exclusive OR the ciphertext with the key which is repeated once more, and the resulting output would be the plaintext. If you're not sure about that, why not give it a go and check that you come out with the same values. So that's a quick summary of a stream cipher.

I hope you've enjoyed the video, and I'll see you next time.