Block Ciphers

Welcome back. In this video, we're going to take a look at a block cipher. In a block cipher, we take a block of data and encrypt that or decrypt that before moving on to the next block. This is in contrast to a stream cipher, where we take each bit per bit or each byte per byte. In terms of block size, typically, we're looking at 128 to 156 and so on and so forth. So we're taking a set of bits, working on that before moving on. There are a number of different operations which can be completed within a block cipher.

A very basic example is shown here. What we do in this block cipher is take our block of data, split it into half, switch the order of those two halves, and then perform an XOR operation. I'd like you to take a minute, pause the video, and apply this operation to the example shown. Another element to consider when looking at block ciphers is the length of the message. What happens when the length of the message is shorter than a multiple of the key length? In the example that we've just seen, the length of the message happened to be a multiple of the key length, but that's very unlikely to be the case in real-world applications. So what do we do? We look at a primitive, which is a fundamental operation defined within cryptography, which is referred to as padding. Padding is the process of expanding the length of a message to ensure that it's a multiple of the key. There are a range of different standards which can be used to achieve this.

A simple example standard based on the cryptographic message syntax is shown here. In this example, what we're doing is we're figuring out effectively what the remainder is upon division by the key size. So if we have, for example, a key size of 12 and a message of length 8, then we've got 4 bytes left over. So we need to pad that up by another 4 bytes. So what we do there is we replicate that number in bytes for four different bytes. This isn't necessarily the best example in terms of real-world use. So if you are applying this in modern use, you'd want to make sure what the context is within your workplace to identify an appropriate padding algorithm. In saying that, it is a nice, easy example to give you a flavour for what that could be.

That's it for this video, where we've looked at a basic block cipher to get used to the idea of how they might work. I hope you've enjoyed the video, and I'll see you next time.