Cryptography Overview

Hi again. In this video, I'm going to be introducing the key components of a cipher. A cipher is effectively an algorithm which allows us to send a message across an insecure network in a secure fashion. It means that if anyone were to intercept that message, they would be unable to read the contents of that.

So if we start off by looking at the three key components, we have the plain text, the key, and the ciphertext. The plain text is the unencrypted message. This is a message that if anyone were to intercept that, they would be able to read it irrespective of whether they have access to the key or not. The key itself is the thing that allows us to apply the encryption. It's the secret information that allows us to encrypt and potentially decrypt that information as well. The bottom line here shows the ciphertext.

ciphertext is the result of applying encryption to the plain text using the key. So those are the three key components. As I say, the intention here is that if someone was to send a message over an insecure network, anyone intercepting that would not be able to read that message without the key. Three of the key names that you might hear in relation to cryptography include Alice, Bob, and Eve.

These are just traditional labels used to represent intended recipients, and the sender, as well as someone trying to intercept that message. So Alice is sending a message, Bob is receiving it or vice versa, and Eve is trying to intercept that message. The overall process when it comes to ciphers is that we take our plaintext and we can apply our encryption algorithm using the key and that results in our ciphertext.

And then we can perform the reverse, the decryption. We apply the decryption key to the ciphertext to get the plain text out. And as shown on screen here, some of the annotation that you might see in relation to this. The example that we have here, the key is basically a substitution where we're taking every letter in English alphabet and translating that into a little diagram or figure if you like. Now, when we're looking at ciphers, there's two general classifications that you might come across--

symmetric and asymmetric. The distinction here is down to the key that's being used for encryption and decryption.

Within symmetric cryptography, we've got the same key for encryption as we do for decryption. Within asymmetric cryptography, we have a different key. We'll come to more of the detail on these in a later video. But that's it for this video where I've introduced encryption, and decryption, and how that falls within cryptography.

We've looked at the key terminology--

plaintext, ciphertext, and keys. And we've looked at the distinction between symmetric and asymmetric cryptography. I hope you've enjoyed the video, and I'll see you next time.