Feistel Structures

Welcome back. In this video, I'm going to be introducing Feistel ciphers, more specifically, the Feistel network structure. What we can see here on the screen is referred to as a Feistel structure. This is a format which can be used within block ciphers and kind of gives you a blueprint for how a block cipher might operate. The structure is as shown here. We start off with a plaintext block, and we split this into two halves.

Now, in this example, I'm working on the basis that these two halves are even, but we can have uneven halves. There are Feistel ciphers which do work with that. But for ease, we will focus only where these two can split evenly. So, we take that plaintext block, we split it into a left half and a right half. Now, the right half stays as is. The left half, on the other hand, is XOR'd with the result of a function being applied to the right half using a key, which is derived from the main key. Now, the idea with Feistel structure is that a number of rounds are completed.

Obviously this number of rounds can be as long as you like. The longer it is, the more complication you're starting to introduce and the harder it's going to be to try and reverse that process without access to the key. So, within each of these rounds, we have what's referred to as a round key. So, this is a variant, which is derived from the main key for that round specifically. So, the right half, you apply a function--

now, the function itself depends on which block cipher you're really using, and that round key is used there.

So, we execute that function with that round key, XOR the result of that with the left half, and that is the output on the left-hand side. Now, before we go into the next round, we flip the order of those. And then we complete the next round with the next round key, and so on and so forth, until we get to the end. Now, just at the end, we do that final flip, and the result there is our ciphertext block. Then, we move on to our next block and complete the same thing again.

So, as I say, the function itself varies depending on the actual block cipher that you're using. So, for example, Twofish or DES, they have functions defined specifically for those, and they use the Feistel structure that we see here. So you might be wondering, what about decryption? Well decryption, what's really cool about this, we can effectively perform the same thing again, reverse the order of the keys that we're using. So, at the start, rather than using the round one key, we'll use the round n key. So, that's the final round key. Now, the reason that this works irrespective of what your function is is down to the XOR operation.

With XOR, you can XOR the encrypted stream with the same key stream and get the plaintext back no matter what that function is. So I think that's a really cool part of the Feistel structure. But that's it for this video where I've

introduced the Feistel structure, and we can see how that can be used to implement a block cipher. I hope you've enjoyed the video, and I'll see you next time.