Components of modern block ciphers

Welcome back. In this video, we're going to introduce three of the key components of a modern block symmetric cipher. We'll look at substitution boxes, permutation boxes, and also key schedules. And we'll examine some examples as we move through the video. To start off with, we have the substitution or S-box. This mechanism is well-examined in the field of cryptography. It effectively allows us to take a block of data and replace that with a different block of data. This can be implemented in a number of different ways.

One of the common ways of doing this is through a lookup table where we are given a particular position and take the value at that position to replace the original value. Let's turn our attention now to an example of an S-box. This example has been taken from the Data Encryption Standard. This was defined in the '70s by the National Institute of Standards and Technology. However, it is not suitable for modern use, but does provide a practical example that's easy for us to see how it can work. Let's have a look at an implementation of an S-box.

This is a fairly straightforward example. But it demonstrates how they can be implemented. We will take an input, as we have shown at the top here. We have six bits. And what we do is we take the middle four bits, and use this to determine the column. We've got an example here, which shows 0100, which is this value here. We then take the first bit and the last bit of the outer bits, and use that to determine the rule. In this case, we have 11. We then find the intersection of that column and that rule to determine our output. And so as a result, we can see that our input of 101001 becomes 0100. This particular example is from the Data Encryption Standard, which is no longer deemed secure for modern use, but it does provide a straightforward example.

Having looked at S-boxes, let's now turn our attention to P-boxes, or permutation boxes. Again, this is using a similar mechanism to what we've seen in traditional cryptography as applied to modern cryptography. So that is looking at ones and zeros. Permutation box can do a few different things. So bits can be rearranged, repeated, and possibly discarded, but not changed. So it could be said that this is a subclass of an S-box. But that relationship doesn't go the other way around.

So an S-box cannot be a P-box. But a P-box could be classified as an S-box. Effectively what we're looking at as we are rearranging values, or expanding them out, or reducing them, but not changing the values themselves. A straight P-box just transposes the digits, the ones and zeros. And we'll see an example of that in a moment. In contrast, our compression P-box discards some of the bits. And we also have an expansion P-box that basically takes particular elements within a block and repeats the values. At this point, let's turn our attention now to an example of a straight P-box to see what this can look like. Let's turn our attention now to an example of a permutation box. We're going to look at a straight permutation box.

A straight permutation box effectively simply reorders the components within the input to result in the output. This is in comparison to a compression P-box, where it is going to discard elements of the input, or an expansion P-box, where it can repeat elements of the input in order to determine the output. In this example, we'll take the first bit and the last bit, and reposition those so that they are swapping. So we'll take bit 1, swap it with bit 6, and vise versa. We'll take bit 2, 3, 4, and 5, and keep those static.

This then provides the output at the bottom of our permutation box, where we can see that these have been reordered appropriately. Bit 1 and 6 swap places. And 2, 3, 4, and 5 remained static. We've now examined an example of an S-box and a P-box. These mechanisms provide two important properties of a secure cipher. This is as identified by Claude Shannon, who wrote a mathematical theory of cryptography in 1945. These two aspects are confusion and diffusion.

And modern cryptography attempts to achieve both of these for a secure cipher. With confusion, each bit of the ciphertext is dependent on multiple parts of the key. Effectively, we are obscuring the relationship between the key and the cipher. A substitution box helps us to achieve this property. Diffusion, in contrast, means that if one bit of the plain text is changed, then that should impact many parts, in fact, at least half of the ciphertext bits. And this is where the permutation block comes in.

So it's the combination of these two aspects which help us define a secure cipher. The final element that we need to consider is the key schedule. In modern symmetric block ciphers, we often repeat a series of steps multiple times. These are referred to as rounds. Within each round a subkey is used. This can also be referred to a round key. Sub keys, or round keys, are keys which are derived from the original key, adding further complexity to the cipher.

In order to determine what the round keys are, we have to define an algorithm called a key schedule. This algorithm allows us to take a key which is normally at least 128 bits in length and use it to generate these round keys. Doing this achieves a similar goal to the Vigenere cipher, which had multiple cipher alphabets. In this instance, we're generating multiple keys from the original, so as to help hide the relationship between the plaintext and the ciphertext even further. In the past, key schedules have been based primarily on relatively straightforward permutations and substitutions.

However, in more recent cryptography, we're looking at more complex ways of generating a key schedule. However, we won't go into that in particular depth here. It's just important to recognise that a single key can be used to generate round keys. That's it for this video. We've covered S-boxes, P-boxes, and key schedules. I hope you've enjoyed the video. And I look forward to discussing some modern cryptography which uses these elements. See you next time.