Substitution Ciphers

Welcome back. In this video, we'll examine two different techniques as they relate to cryptography, substitutions and permutations. We'll look at these through the lens of traditional cryptography. We'll look at some traditional ciphers and show how these demonstrate these techniques. The reason that we're doing that is because it's often easier to wrap our heads around that looking at letters compared to thinking about it with ones and zeros. But as we progress into more modern cryptography, we'll start to see how this can be applied to ones and zeros.

To start off with, I'm going to introduce you to the Caesar cipher. You may already have heard of this cipher. It's a very simple cipher and one of the earliest known examples of a cipher. It's related to Julius Caesar, who used this for his communications. It's obviously not at all secure in modern day use, but it is an excellent example of how substitution can be used. In the Caesar cipher, each letter is shifted three down the alphabet and that is the corresponding ciphertext.

So for example, if we start at A and move three possessions, we end up with D as our ciphertext ouput there. Now, as we get near the end of the alphabet, we have to start and cycle around to the beginning of the alphabet. This is shown in this slide here where you can see as we get towards X, if we move three along, we come back to the letter A as the output. On the screen now, you should be able to see an example of this being applied to our plaintext "life finds a way" and the resulting ciphertext is shown there.

So as you can see, substitution is simply a case of taking a letter or component within your plain text and substituting it with a different value. In this instance, we're mapping letters to letters. But it could also relate to ones and zeros or bytes or even a longer set of bits. But we don't need to use just the one cipher alphabet. We can actually expand that and use a range of different possible cipher alphabets. The Vigenre cipher is a really good example of this.

It makes use of the Caesar cipher except with the whole range of possible shifted values. So it starts off with a shift of 0, shift of 1, and goes further down until you get to the maximum shift of 25. Traditionally, this is done using a Vigenre cipher grid, as you can see on the screen here. We have rows and columns. And then, we have all the cipher alphabets shown on the screen with the range of shifts. So you can see where it starts to shift. If we look at the very top line underneath the header and the side column, we can see that that's a shift of zero and then a shift of one. So A maps to B, B to C, and so on and so forth.

Within the Vigenre cipher, we pick a key which doesn't have any repeated letters. And we then place that key above every letter within our plaintext. Repeat that key as needed over the plaintext. And we then use that to evaluate which alphabet we should be using in order to encrypt. So an example that

we've got here, I've taken the key word of Alice. And in our plaintext, I've got the word hello. From there, what I need to do is I'm taking the keyword value above the first letter.

So that's A. So I need to use the first row in our cipher alphabet square. And then, the actual letter I want to encrypt is H. So I go to the column H and I find where those two intersect, and that happens to be H. From there, I take the second letter in the keyword, so that's L. And I take the second letter in our plaintext that I want to encrypt. So again, L is giving me the row within that square that I want to use. And the plaintext E is giving me the column.

And where those two intersect is P. So I'd like you to take a minute to see if you can apply that to the rest of the words there. Another way of looking at the Vigenre cipher is to translate every letter and into a position number. So A would be 0 through to 25. We can then translate any letter, whether that's in our plain text or whether that's in the key. And then, perform the addition for those. And the resulting value, obviously, it needs to be calculated mod 25. But the resulting output can then be translated back from a number into the corresponding letter.

So that's a slightly easier way if you ever want to implement this in code, for example. But often, that visual representation of the Vigenre square can be helpful in wrapping your head around what's happening. Moving on now to the technique of permutation. Permutation is probably exactly what you think it is. It's basically moving components around. One example of this is the Rail-fence cipher. So in the Rail-fence cipher, what we do is we take every second letter and move it down to the line beneath that one. So if we look at hello world here, on the top line, we end up with H, L, O, O, L. And then, the second line we've got E, L, W, R, D. The idea then is that you put the second line after the first line.

So effectively, you end up with an anagram at the bottom there. Now, as I say, in modern cryptography, we're looking at using ones and zeros. So we'll come back to this. But you'll be able to see how this can be applied to ones and zeros where the ones and zeros are permuted in a specific fashion. So that's us for this video. We've looked at two different techniques which can be used within ciphers. We've looked at substitution where we're replacing a character or element within the planetext with the corresponding character in the ciphertext. And we've looked at permutation, which is effectively transposing numbers and muddling things around a little bit in a specific way. Obviously, because we need to reverse that.

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

REF UK TOP 20 RESEARCH-INTENSIVE UNIVERSITY
THE UK UNIVERSITY OF THE YEAR WINNER
THE UK ENTREPRENEURIAL UNIVERSITY OF THE YEAR WINNER

The place of useful learning
The University of Strathclyde is a charitable body, registered in Scotland, number SC015263