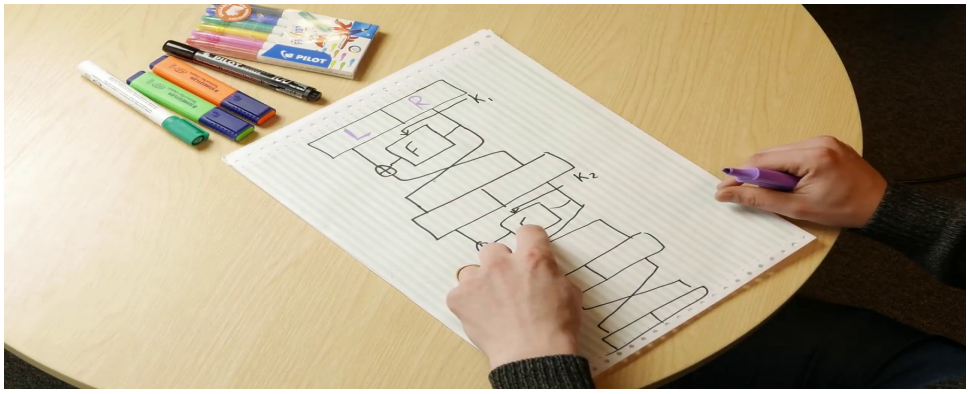
We're going to talk about Feistel networks. They're brilliant.Like the padding scheme used for digital signatures on certificates, Feistel cipher's are used for key schedules. It's a structure and then you put in some encryption rounds and a key and things like this and then it turns it into a cipher for you and it has some really neat properties.

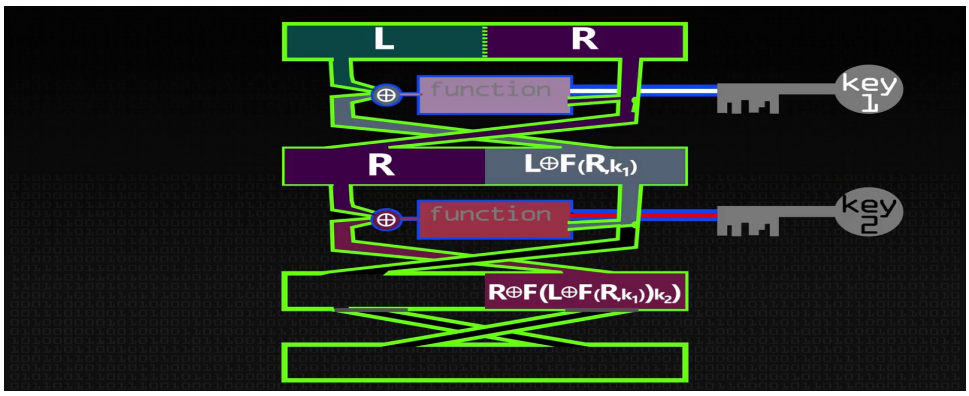
So you start with a block and we're gonna split that block into and then we're gonna take this as a right hand side. We're gonna take the right hand side down. We're gonna take it out here. And this is your next block.A lot on the right hand side. Do they have to be exactly half and? So in this case, yes, but in general no.So the next round is exactly the same we take whatever this new right is we bring it round.

And you can repeat this process as many times as you like for how many rounds and then at the very end after the last round you flip the output like this. Here it goes through. Here it goes through here and it goes for as many rounds as you want and you get some output. And even if this F is a one way hash function, that can't be reversed, that still decrypts it.I mean, I like bases bases, wildlife, faster ciphers, so we're just gonna do it. I mean, maybe you've seen it fast and I thought maybe you know this happens, right? But I think when the first time I learned about this, I thought that is that is awesome.

This is going to be key to like this.



This R comes through this F. The artist comes straight down. So let's do the next round. It's going to be X sword with this are so this output here is our X or F of this which is L.



Maybe it's a good thing that we didn't do 3 rounds or 4 rounds of this 'cause this could take me quite awhile by hand.F of. We're going to switch them around here. Feel free to animate it, Sean, thanks for that, right? So now we're going to see how we can decrypt this back to Eleanor and all we have to do is take this, put it in the top and we have to swap our subkeys around.So this could be a competition.I mean, they're not nearly wide enough for me to fit myself in.I think that's right, you know. And then we're going to see what happens.Reversible thing right? Yeah, right? That's the key to this whole thing.And it's going to be a combination of all of these, so this one times this one. Plus this one times this one plus this one times this one.