Enigma machine: military messages kept secret with maths

Video transcript: clip from *Horizon: The Hunt for AI*, first broadcast on BBC Two on 3 Apr 2012

MARCUS DU SAUTOY:

The main problem that Turing had to wrestle with whilst he was here at Bletchley Park was this.

It's an Enigma machine and it's an incredibly clever piece of kit. It was used by the German military to scramble secret messages into code that nobody could understand.

Cracking this code was incredibly difficult for humans to do. In fact, the Germans believed that the Enigma code was uncrackable.

It was up to human minds to decipher the cryptic communication that was being picked up on the airwaves. This was an impossibly long task but we were on the brink of war and didn't have time to waste.

So, the Enigma machine consists of a keyboard which I'm going to type my message on to try and encode it.

So for example, if I press an 'R', then the wires in the machine go through and light up a letter at the top here. So in that case the 'R' was encoded by the letter 'N'.

But the incredible clever thing is, about the machine, that if I press 'R' again it doesn't get encoded by 'N' the next time. Because these rotors have kicked on one step and so the wires are connecting up the letters in a completely different way this time. So, now when I press 'R' it gets encoded by the letter 'F'.

Now, the operators had different ways that they could set up the machine so they could make a choice, for example, of which rotors they were using inside the machine.

So, there were five different rotors and they would choose three of them and then they could put them inside in different orders and then they would set each of the rotors on one of 26 different settings.

And then not only that, they had some plugs at the front here which would also scramble up all of the letters. So, the combined effect of this is that there are over 150 million million million different ways that the Enigma machine could be set up.

So Turing was being faced with having to find the one out of the 150 million million million ways that the operator had used on that particular day, so it really was human versus machine.