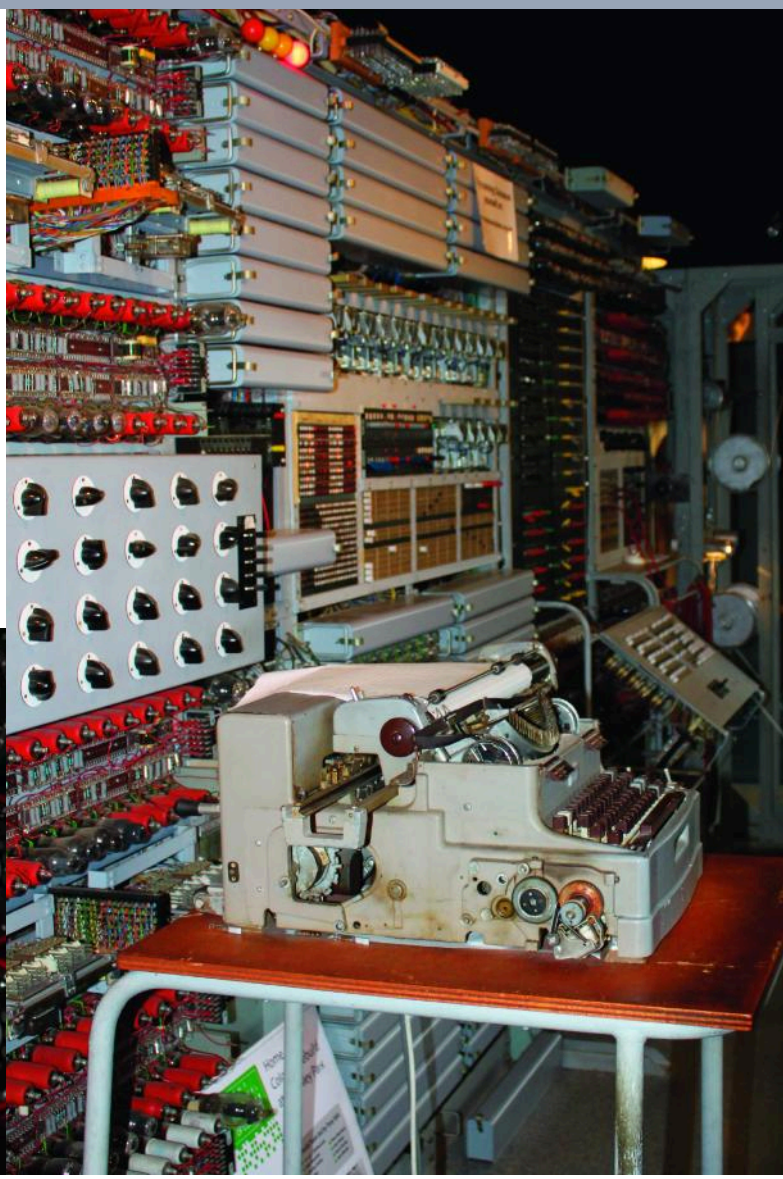
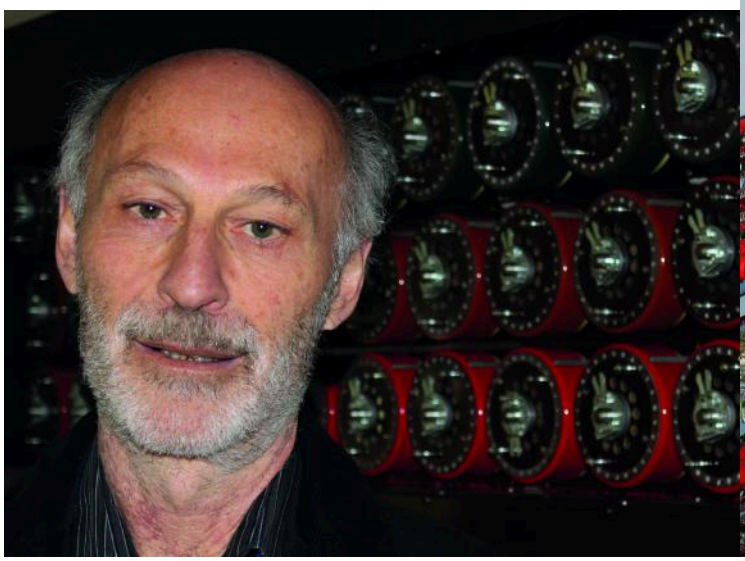
CRACKING CODE



Seventy five years ago, Bletchley Park began work on deciphering German military messages. The story was shrouded in secrecy for nearly three decades after the end of the Second World War and, even then, it filtered out slowly and reluctantly as some secrets still had currency.

Many, especially those with an interest in technology, will recognise the name Alan Turing and associate him with the development of the first computer. However, such an association would earn a figurative rap on the knuckles from Bletchley historian Joel Greenberg. He acknowledged Turing's genius, but pointed out that he was not at Bletchley Park when Colossus, the first electronic programmable computer, was designed and built.

It has slowly emerged that Bletchley Park's success – and it was huge – was down to a collective effort. While Colossus was the crowning glory from a technology perspective – it only became operational in the last year of the war – it was far from the only achievement. In fact, Colossus was only invented to decrypt messages sent using the Lorenz encryption machine, used in the latter part of the war for high level strategic communications. All operational



communications during the entire conflict were made using Enigma machines and these were intercepted and decrypted successfully at Bletchley Park over the whole period.

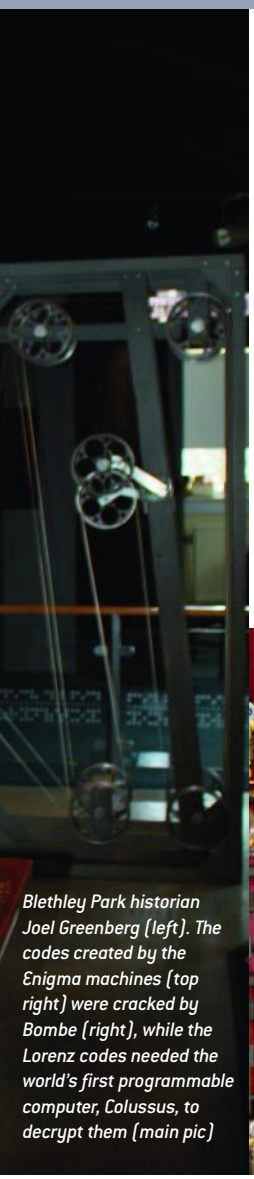
Enigma and Bombe

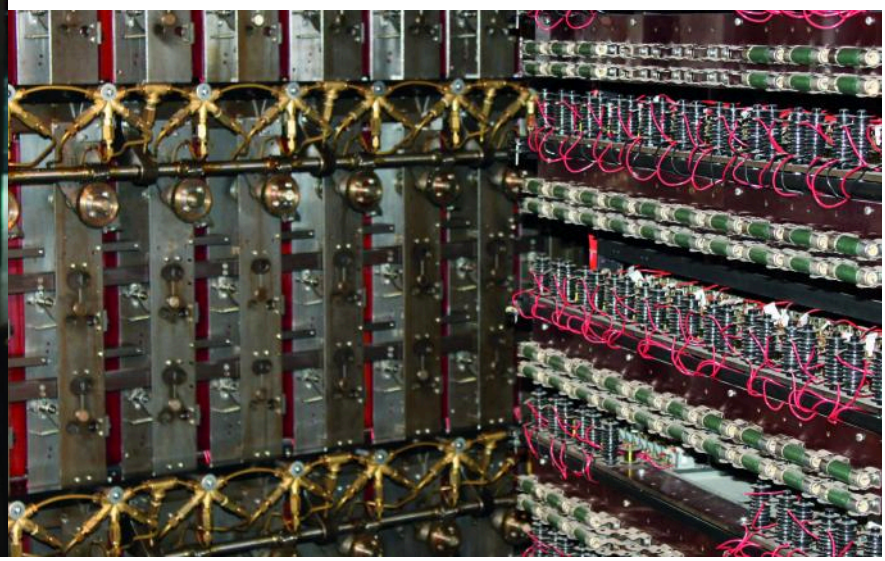
Enigma was a commercial solution that, in earlier forms, had been around since World War I. It was adapted during the 1920s and 30s to make it portable, before being adopted by the German military. The army developed the idea of Blitzkrieg [lightning war] and so needed fast, mobile communications. They decided to encrypt all operational communications. This was the age of machine encryption and Enigma was an electromechanical machine that performed alphabetic substitution, converting each character of a message with another as randomly as possible.

Greenberg explained: "Enigma was clumsy and unbelievably clunky. There was a keyboard with 26 keys – one for each letter of the alphabet – and a board with 26 circles of glass with a letter of alphabet embossed on it and a bulb behind. When you pressed a key, a bulb lit and that was the encryption letter of the key you pressed. But it was so clunky that maybe six people were involved in sending one 200 character message. One would input the message – he would go through it one character at a time. Every time a lamp lit, an

VISIT

A total secret for decades, Bletchley Park was the home of genius, intellectual courage and the modern computer. Tim Fryer went to visit.





Blethley Park historian Joel Greenberg (left). The codes created by the Enigma machines (top right) were cracked by Bombe (right), while the Lorenz codes needed the world's first programmable computer, Colussus, to decrypt them (main pic)

assistant would write it down. A third person would send it in Morse code via wireless. At the other end, three guys did the reverse. It was an expensive way to send a short message, but it was easy to use and, by the end of the war, up to 100,000 machines being deployed."

The essential thing was the internal wiring. The machine was conceived as being reciprocal; if you had two machines set up the same way, you could use them to encrypt and decrypt. The machines had a daily setting known as the key. This determined how the three internal wheels were set up, along with a reflector wheel. Greenberg commented: "The military added a plug board, which essentially added ten pairs of letters, to the front and rewired the wheels – they thought it was unbreakable. There are 158 million million million variations in how the key could be set up.

"Fortunately, humans were involved in the process, which made it insecure. It is often said the people here broke this machine – we didn't break it. What we did was to exploit the mistakes the operators made, which is exactly how people hack into computers today. There was a huge range of mistakes, some of which you can hardly believe – a comedy of errors."

One of the main errors was the Germans not imagining that the British would set up an industrial scale code breaking operation – that is essentially what Bletchley Park was. Greenberg likens the early operation to the Skunk Works – Lockheed Martin's aircraft development team later in the war, where creativity flourished unhindered by corporate rules.

"In my opinion, Bletchley Park was the first of that kind," said Greenberg. "It put together some of the best minds in Britain and eventually bought over some Americans. In the early days, there were no rules. It was described as creative anarchy and Denniston allowed that to flourish – if it meant using a Ouija board, so be it; if you could break the key, nobody gave a damn how you did it."

Alastair Denniston was head of the Government's Code and Cypher School. He realised the code breaking model, which relied on classicists, was out of date and he followed the Polish example by trawling academic institutions for the most brilliant mathematicians – it was Polish mathematicians who first worked out how to decipher Enigma messages.

George Welchman, one of these so called 'Men of the Professor Type', joined Turing at Bletchley Park – the site had been bought in 1938 by MI6. Obviously unconvinced when Chamberlain returned from Munich declaring 'peace in our times', MI6 saw the need to set up a codebreaking facility away from central London. Welchman was instrumental in Bletchley's success.

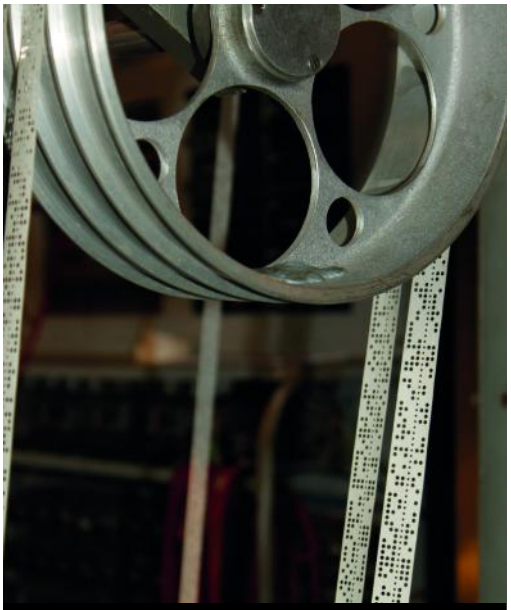
Turing came up with the idea for the Bombe, the machine designed to decrypt Enigma messages. Turing's initial version didn't work too well until Welchman's modification, known as the diagonal board, speeded the machine. Bombe machines were made by British Tabulating Machine Company in Letchworth and the 'brilliant young engineer' who built them was Harold Keen.

Greenberg commented: "The British machine exploited the weakness in Enigma's design; it couldn't encrypt a letter as itself. There was another weakness when they started using standard phrases. So if you could take a sequence of encrypted letters and marry them with other messages, this became known as a crib and that was the basis of the attack. From the crib,

they produced a menu – in effect how the Bombe machines were to be set up.

"The Bombe comprised 36 Enigma machines connected together to locate and eliminate wrong answers. That left a smaller number of possibilities that could be worked on manually. The Bombe found what mathematicians call 'reductio ad absurdum' and, in 20 minutes, the 158 million million million possibilities were reduced to a number small enough to be worked out in about two hours. Quite an amazing idea.

"By 1943, there was virtually no limit to how many messages they could decrypt once they had worked out the daily setting."



The information input to Colossus was in the form of ticker tape, which had more of a limiting effect on the speed of the machine than did the pioneering electronics

Lorenz and Colossus

Although Bletchley's success is put down to the cryptography, there were less glamorous elements that were just as important in terms of making the information meaningful. Welchman, who had a rare aptitude for organisation, recognised the value of 'traffic analysis' – building a picture of German military movements by analysing from where messages were sent and when. This dovetailed with the 'Index', a vast manual database on the German military and its personnel. Thus, decrypted messages had genuine context and were far more useful.

Welchman's appreciation of this led to his suggestion the process could be made more efficient by turning it into an industrialised production line. This was adopted and huts were filled with people decrypting and dealing with messages. By the end of the war, around 10,000 people worked at Bletchley on a round the clock shift pattern.

However, cryptography was still at Bletchley's core and, in 1941, they started intercepting messages transmitted in a binary system which could not be deciphered. These were the first messages from the Lorenz machine – implemented by Hitler to provide more secure strategic communications.

Again, operator error proved the undoing of Lorenz – and that error only happened once. Two operators – one in Vienna, the other in Athens – were testing the system and one asked the other to repeat a 4000 character message, which he did without changing the machine settings and by abbreviating some of the longer words to save to time. The two messages were given to John Tiltman, who Greenberg describes as 'possibly the greatest codebreaker of his generation'. He worked out the original German text and, consequently, the key to the Lorenz machine.

Greenberg continued: "They had this stream of characters, but still couldn't make head nor tail of it. All they knew was that it was produced by some machine. Eventually, out of desperation, it was handed to a 24 year old mathematician called Bill Tutte. In six weeks, Tutte performed what some commentators refer to as the greatest feat of mental mathematics in the last 100 years – he worked out the logical design of the Lorenz machine. The algorithm is genius; one of the most brilliant things achieved during the war."

Despite this, the daily key was still being worked out by hand and taking too long. As traffic increased, it was decided machines were needed. Max Newman, one of Turing's professors at Cambridge and another Bletchley pioneer, built a machine called Robinson, which had limited success.

Newman, at Turing's suggestion, approached Tommy Flowers – an engineer working at the Post Office research facility in Dollis Hill, London. Flowers believed he could make a machine and was given the go ahead in 1943. He was probably the foremost expert in the use of valve technology at the time. He wanted to use valves, rather than switches, because a valve can have two states. However, he was proposing to use thousands of valves (2500 in the Mark II machine) in an era when valves were considered to be very unreliable. Flowers proved the unreliability was caused by turning them on and off repeatedly – they rarely failed when left permanently on. Using valves, Flowers developed the world's first semi programmable computer – Colossus – a feat not made public until 1974.

The machine's basis was that, by adding characters in messages together, there was statistically a greater chance of getting a dot (the binary equivalent of 1) if the settings of the Lorenz machine had been identified. correctly. Colossus therefore ran through all possible settings to see which yielded the highest proportion of dots. It could generally do this in 20 minutes, with the details of the code finalised by hand in less than two hours. The input to Colossus was ticker tape with rows of dots. At a time when holes in such tapes were counted using pins at a rate of maybe four per second, Flowers' team invented the optical reader. The tape ran at about 30mph and read 5000 character/s. It could run at twice this speed, but the tape kept breaking.

Greenberg added: "They invented a clock using a sprocket hole for the pulse – they invented everything. The main thing was using valves to replicate the Lorenz settings; the algorithms were all statistically based. They had plugs, so they could tweak the algorithms, and there would be a cryptoanalyst at the machine, along with the operators. From then onwards, they decrypted most messages. The most famous made it clear that Hitler believed the main invasion would be at Calais, and not Normandy. The decrypted message in the National Archive shows the German's entire order of battle for the defence of France – where their airplanes were, how many were operational. It was a huge document and the British knew all this. It is just phenomenal."

Bletchley's legacy

Despite its technological significance and its contribution to the war effort, Bletchley Park's nature meant it received no attention after the end of the war. Flowers went back to the Post Office and played no further part in the development of the computer industry. Those with academic credibility took their knowledge of valves and binary computing – to the US, in Welchman's case, and Manchester for Turing and Newman – and continued to play a role in the development of modern computing.

"This was the birthplace of the digital age," Greenberg concluded. "And Welchman was one of the guys who nurtured it through its infancy in the US; Turing and Newman were the equivalent in this country."