COLOSSUS

THE BRITISH COMPUTER THAT CRACKED THE NAZI CODE LAID THE FOUNDATIONS FOR TODAY'S MASS INTERNET SURVEILLANCE

During the Second World War, British intelligence gathered Nazi communications that were often encrypted. Those intercepted messages were broken on a British-built machine, the first electronically programmable machine called the Colossus.

STEP 1

INTERCEPTING THE MESSAGE

The Nazis used a device – the Lorenz Machine – that encrypted messages. British workers at Bletchley Park were tasked to decipher them. The Lorenz Machine transmitted messages using the International Teleprinter Code, in which each letter of the alphabet is represented by a series of five dots on paper tape.

STEP 2

THE COLOSSUS MACHINE

2.1 Input

The teleprint messages were put into the Colossus by spooling the tape through wheels. The length of tape fed into Colossus during the Second World War held around 63 million characters, enough to stretch from London to Southampton. Each teleprint character, made up of a unique series of dots, was fed into the machine by shining light through the teleprint holes. The light would hit a photocell that would register as a digital input – one or zero. This would allow the machine to read the message on the tape.

2.2 Programming

Colossus was the first machine to use electronic circuits for processing digital information. This is why it is considered the first "computer". "Thermionic valves" were used to switch the electronic signals on the circuits. The valves controlled the flow of electric current through the logic gates, just as a modern processor controls the electronic circuitry in a computer. Acting as electronic switches, they were many thousands of times faster than mechanical switches.

The valves were generally believed to be unreliable but Colossus creator Tommy Flowers said they would work as long as the machine was never turned off. Colossus ran 24 hours a day and used 2,500 thermionic valves with 7km of wiring.

2.3 Thyratron rings

Although Colossus could be "programmed" it didn't have "software" or memory. It was built to perform one function: to take encrypted messages and produce a statistical prediction for the wheel setting of the Lorenz Machine.

To work out which combination of Lorenz wheels could produce language from the ciphered text, part of the machine had to simulate the German encryption device. These were the Thyratron rings. Colossus had 501 Thyratrons made up of 12 rings to match the number of wheels on the Lorenz.

2.4 Typewriter

Colossus's output, the statistical "wheel setting", was printed on paper. A typewriter was connected by wire to the machine and would self-print the statistical calculations. An engineer took these predictions to set a similar wheel rotation with the encrypted message and convert the message from German into English.

STEP 3

DECRYPTION [Tunny machine]

Without having seen a Lorenz machine, the Brits worked out how it operated and built a machine that functioned in a similar way. Not knowing what the Germans called it, they named it Tunny. Before Colossus, Bletchley Park teams took 6-8 weeks to decipher a message. With Colossus's automated calculations this was reduced to 4-6 hours, allowing the allies to keep in step with the Nazi front line.

GRAPHIC:
Will McQuhae

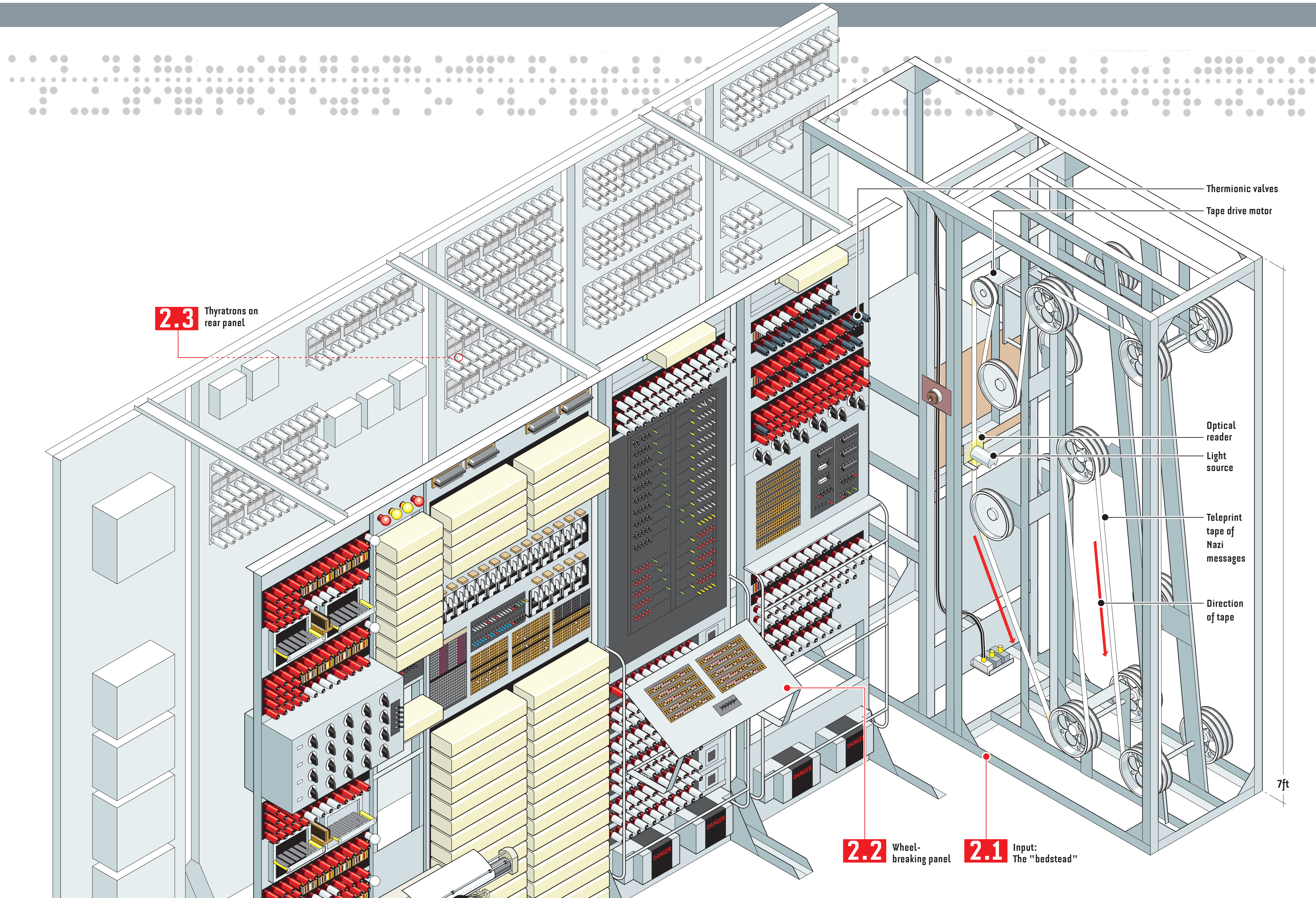
DATA COMPILED BY:
The Times Data Team: Stefano Ceccon, Nicola Hughes and Megan Lucero

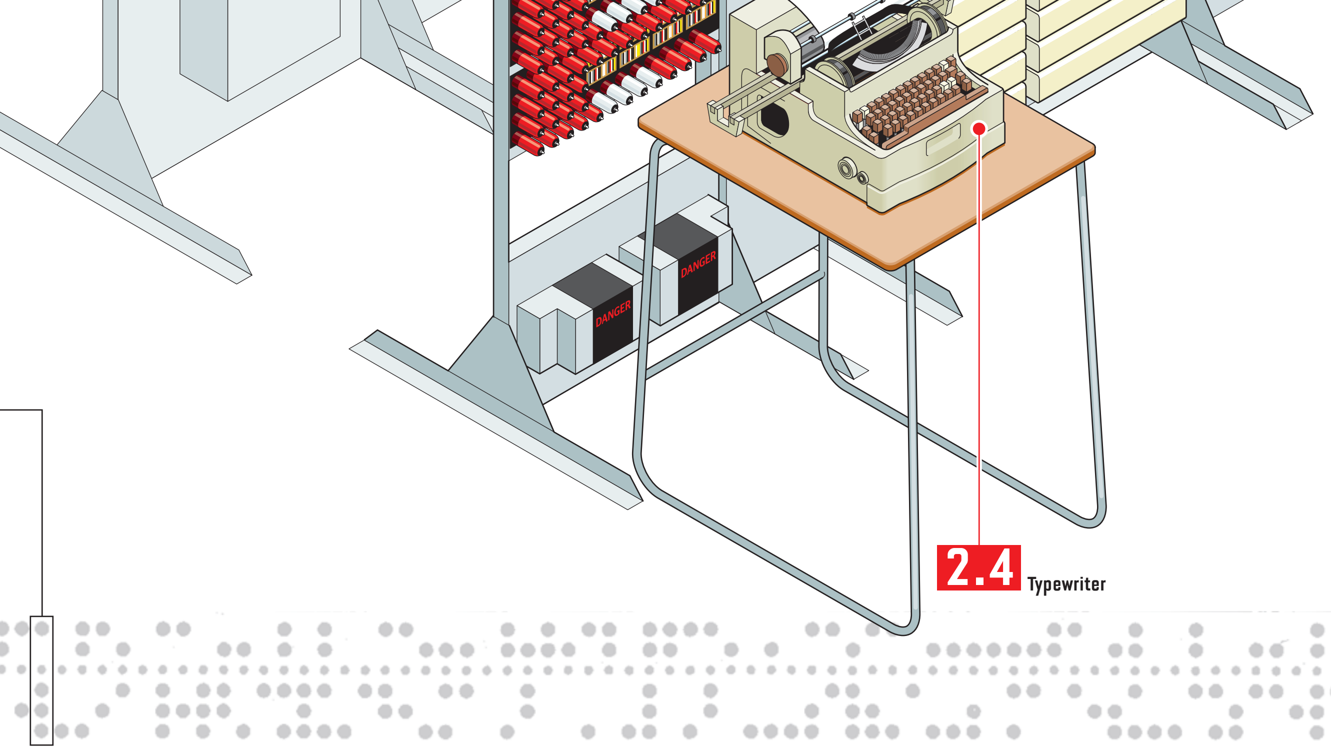
ONLINE INTERACTIVE
TRY BREAKING THE CODE YOURSELF
WWW.THETIMES.CO.UK/COLOSSUS

PAPER TAPE

Scan of original message. Colossus read intercepted Nazi messages using the International Teleprinter code. This series of five dots represents one letter in the message

The rebuild of Colossus can be seen at The National Museum of Computing at Bletchley Park





COLOSSUS FACTS...

- Power = 8kW
- Weight = 1 tonne
- 2,500 thermionic valves
- 501 thyratrons
- 10,000 resistors
- 7km of wires
- Broke code using mathematical algorithms
- First electronically programmable machine. The data processed used logic gates (the same schematics used in modern computing)
- Around 100 logic gates
- No memory
- Scanned 5,000 characters per second
- Decrypted 63 million characters

... AND HOW IT COMPARES WITH AN iPHONE 5S

- 83,680 stacked iPhones take up the same space as Colossus
- 8,929 iPhones weigh the same as Colossus
- The camera on an iPhone captures the same quality image as 500,000 Colossus machines
- All Nazi communications intercepted at Bletchley could fit 53 times into the 16GB iPhone
- A thermionic valve does a similar job as a transistor. There are 100,000 times more transistors in an iPhone 5 than thermionic valves in Colossus
- Photo of thermionic valve and original box taken using an iPhone 5S

••••• 4G
19:44
Number shown on this slip is the new designation of the
Supplies should be taken on charge, and demanded,
Pattern Number in future.
S.N.S.O. Haslemere, December, 1943.
MBER
ITT
6A/157D
Made in England
EF37A

BEHIND THE STORY FROM BLETCHLEY PARK TO THE NSA

Ben Macintyre

This is the story of two very different machines: one the size of a double bed set upright and weighing about a ton, and the other so tiny it fits in your breast pocket. One is called Colossus, and in 1943 there was only one in existence. The other is a mobile telephone, a mini-computer, and today there are more than seven billion of them.

The first machine was the ancestor of the second and it was created to eavesdrop electronically. Seventy years later, descendants of Colossus are at the centre of an eavesdropping controversy, amid claims that governments are routinely listening into global communications.

What began as a machine to uncover national secrets became a machine responsible for what is arguably the greatest invasion of privacy in history.

Building on the work of Polish cryptologists, scientists at Bletchley Park, the wartime code and cipher centre, first used the "bombe" designed by Alan Turing to identify the daily settings of the German Enigma encryption machine, enabling cryptologists to read messages that the Germans believed to be unbreakable.

By 1944, the engineer Tommy Flowers and his team had developed Colossus, the world's first programmable digital computer. Telegraphic messages between German High Command and army commands throughout Europe were encrypted using an electromagnetic cipher machine known as the Lorenz.

This encrypted German teleprinter traffic was codenamed "Fish" and the intercepted messages codenamed "Tunny". The Colossus used thermionic valves to perform calculations that could extract the meaning of the "Tunny" traffic. A Colossus Mark II, four times the speed of the first, came into service just a few days before D-Day, and by the end of the war, ten were in operation.

Historians say the intelligence produced by Bletchley Park may have shortened the war by as much as four years.

The intelligence gathered by the code-breakers was the most closely guarded secret of the war. Even though 20,000 people knew of the work, the truth did not emerge until the 1970s. Most of the Colossus machinery was broken up after the war to preserve secrecy, but the science discovered at Bletchley evolved at fantastic speed.

The work of Turing, Flowers and the other Bletchley Park scientists now touches every aspect of life. Every time you check your e-mail or send a photo, you are employing the latter-day fruit of ideas developed at Bletchley Park.

Today, GCHQ, the descendant of Bletchley Park, and the US National Security Agency (NSA), stand accused of amassing vast quantities of personal data from intercepted phone calls and e-mails.

The science behind Colossus was used to carry out secret surveillance of an enemy. Today, as the technology pioneered in wartime has exploded in scale, different enemies are under surveillance, and so are we.