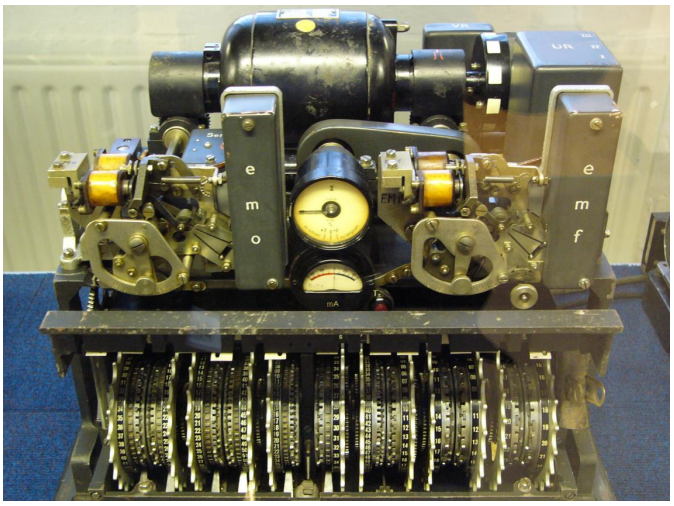
Lorenz cipher



The Lorenz SZ42 machine with its covers removed.

The **Lorenz SZ40**, **SZ42A** and **SZ42B** were German rotor stream cipher machines used by the German Army during World War II. They were developed by C. Lorenz AG in Berlin and the model name *SZ* was derived from *Schlüsselzusatz*, meaning *cipher attachment*. The instruments implemented a Vernam stream cipher.

British cryptographers, who referred to encrypted German teleprinter traffic as *Fish*, dubbed the machine and its traffic ***Tunny***.

The SZ machines were in-line attachments to standard Lorenz teleprinters. An experimental link using SZ40 machines was started in June 1941. The enhanced SZ42 machines were brought into substantial use from mid-1942 onwards for high-level communications between the German High Command in Berlin, and Army Commands throughout occupied Europe. The more advanced SZ42A came into routine use in February 1943 and the SZ42B in June 1944.

Wireless telegraphy (WT) rather than land-line circuits was used for this traffic.[1] These non-Morse (NoMo) messages were picked up by Britain's Y-stations at Knockholt and Denmark Hill and sent to Government Code and Cypher School at Bletchley Park (BP). Some were deciphered using hand methods before the process was partially automated, first with Robinson machines and then with the Colossus computers. The deciphered messages made an important contribution to *Ultra* military intelligence.

The Vernam cipher

Gilbert Vernam was an AT&T Bell Labs research engineer who, in 1917, invented a cipher system that used the Boolean "exclusive or" (XOR) function, symbolized by ⊕. This is represented by the following "truth table", where 1 represents "true" and 0 represents "false".

INPUT		OUTPUT
A	***B***	***A ⊕ B***
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Other names for this function are: Not equal (NEQ), modulo 2 addition (without 'carry') and modulo 2 subtraction (without 'borrow').

Vernam's cipher is a Symmetric-key algorithm, i.e. the same key is used both to encipher plaintext to produce the ciphertext and to decipher ciphertext to yield the original plaintext:

Plaintext ⊕ Key = Ciphertext

and:

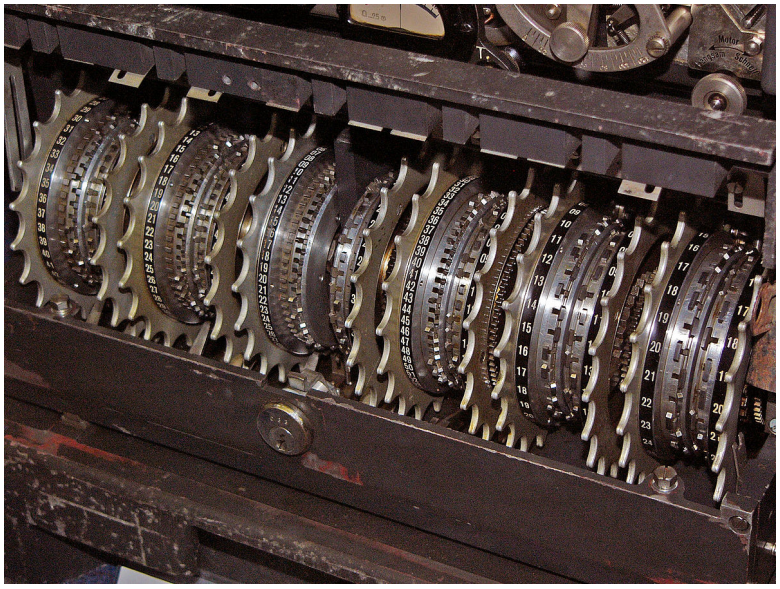
Ciphertext ⊕ Key = Plaintext

This produces the essential reciprocity that allows the same machine with the same settings to be used for both enciphering and deciphering.

Vernam's idea was to use conventional telegraphy practice with a paper tape of the plaintext combined with a paper tape of the key. Each key tape would have been unique (a one-time tape), but generating and distributing such tapes presented considerable practical difficulties. In the 1920s four men in different countries invented rotor cipher machines to produce a key stream to act instead of a tape. The 1940 Lorenz SZ40/42 was one of these.[2]

Structure

The logical functioning of the Tunny system was worked out well before the Bletchley Park cryptanalysts saw one of the machines—which only happened in 1945, shortly before the allied victory in Europe.



The Lorenz SZ machines had 12 wheels each with a different number of cams (or "pins").

The SZ machine served as an in-line attachment to a standard Lorenz teleprinter. It had a metal base 19 in (48 cm) × 15.5 in (39 cm) and was 17 in (43 cm) high. The teleprinter characters consisted of five data bits, encoded in the International Telegraphy Alphabet No. 2 (ITA2). The enciphering machine generated a pseudorandom character-by-character key that was XOR-ed with the input characters to form the output characters.

Each of the five bits (or "impulses") of the key for each character was generated by the relevant wheels in two parts of the machine. The Bletchley Park analysts called these the χ ("*chi*") wheels, and the ψ ("*psi*") wheels. Each wheel had a series of cams (or "pins") around them. These cams could be set in a raised (active) or lowered (inactive) position. In the raised position they generated a '1', in the lowered position they generated a '0'.

The *chi* wheels all moved on one position for each character. The *psi* wheels also all moved together, but not after each character. Their movement was controlled by the two μ ("*mu*") or "motor" wheels.[3] The SZ40 μ61 wheel moved one position with each character, but the μ37 wheel moved on only when the cam on the μ61 wheel was in the active position. If the cam on the μ37 wheel was in the active position, all five *psi* wheels then moved. The SZ42A and SZ42B models had additional complexity to this mechanism, known at Bletchley Park as *Limitations*.[4]

The key stream generated by the SZ machines thus had a *chi* component and a *psi* component that were combined together with the XOR function. Symbolically, the key that was combined with the plaintext for enciphering—or with the ciphertext for deciphering—can be represented as follows.

$$\text{Key} = \textit{Chi}\text{-Key} \oplus \textit{Psi}\text{-Key}$$

The number of cams on each wheel equalled the number of impulses needed to cause them to complete a full rotation. It should be noted that these numbers are all co-prime with each other, giving the longest possible time before the pattern repeated. With a total of 501 cams this equals 2^{501} which is approximately 10^{151}, an astronomically large number. However, if the five impulses are considered independently, the numbers are much more manageable. The product of the rotation period of any pair of *chi* wheels gives numbers between 41×31=1271 and 26×23=598.

Operation

Each "Tunny" link had four SZ machines with a transmitting and a receiving teleprinter at each end. For enciphering and deciphering to work, the transmitting and receiving machines had to be set up identically. There were two components to this; setting the patterns of cams on the wheels and rotating the wheels for the start of enciphering a message. The cam settings were changed less frequently before the Summer of 1944. The *psi* wheel cams were initially only changed quarterly, but later monthly, the *chi* wheels were changed monthly but the motor wheel patterns were changed daily. From 1 August 1944, all wheel patterns were changed daily.[5]

Initially the wheel settings for a message were sent to the receiving end by means of a 12-letter indicator sent un-enciphered, the letters being associated with wheel positions in a book. In October 1942 this was changed to the use of a book of single-use settings in what was known as the QEP book. The last two digits of the QEP book entry were sent for the receiving operator to look up in his copy of the QEP book and set his machine's wheels. Each book contained one hundred or more combinations. Once all the combinations in a QEP book had been used it was replaced by a new one. The message settings should never have been re-used, but on occasion they were, providing a "depth", which could be utilised by a cryptanalyst.

As was normal telegraphy practice, messages of any length were keyed into a teleprinter with a paper tape perforator. The typical sequence of operations would be that the sending operator would punch up the message, make contact with the receiving operator, use the *EIN / AUS* switch on the SZ machine to connect it into the circuit, and then run the tape through the reader. At the receiving end, the operator would similarly connect his SZ machine into the circuit and the output would be printed up on a continuous sticky tape. Because this was the practice, the plaintext did not contain the characters for "carriage return", "line feed" or the null (blank tape, 00000) character.

Cryptanalysis

British cryptographers at Bletchley Park had deduced the operation of the machine by January 1942 without ever having seen a Lorenz machine, a feat made possible by a mistake made by a German operator.

Interception

Tunny traffic was known by Y Station operators used to listening to Morse code transmission as "new music". Its interception was originally concentrated at the Foreign Office Y Station operated by the Metropolitan Police at Denmark Hill in Camberwell, London. But due to lack of resources at this time (~1941), it was given a low priority. A new Y Station, Knockholt in Kent, was later constructed specifically to intercept Tunny traffic so that the messages could be efficiently recorded and sent to Bletchley Park.[6] The head of Y station, Harold Kenworthy, moved to head up Knockholt. He was later promoted to head the Foreign Office Research and Development Establishment (F.O.R.D.E).

Code breaking

On 30 August 1941, a message of some 4,000 characters was transmitted from Athens to Vienna. However, the message was not received correctly at the other end, so (after the recipient sent an unencoded request for retransmission, which let the codebreakers know what was happening) the message was retransmitted with the same key settings (HQIBPEXEZMUG); a forbidden practice. Moreover, the second time the operator made a number of small alterations to the message, such as using abbreviations, making the second message somewhat shorter. From these two related ciphertexts, known to cryptanalysts as a depth, the veteran cryptanalyst Brigadier John Tiltman in the Research Section teased out the two plaintexts and hence the keystream. Then, after three months of the Research Section failing to diagnose the machine from the almost 4,000 characters of key, the task was handed to mathematician Bill Tutte. He applied a technique that he had been taught in his cryptographic training, of writing out the key by hand and looking for repetitions. Tutte did this with the original teleprinter 5-bit Baudot codes, which led

him to his initial breakthrough of recognising a 41 character repetition. Over the following two months up to January 1942, Tutte and colleagues worked out the complete logical structure of the cipher machine. This remarkable piece of reverse engineering was later described as "one of the greatest intellectual feats of World War II".

After this cracking of Tunny, a special team of code breakers was set up under Ralph Tester, most initially transferred from Alan Turing's Hut 8. The team became known as the Testery. It performed the bulk of the subsequent work in breaking Tunny messages, but was aided by machines in the complementary section under Max Newman known as the Newmanry.

Decryption machines: world's first programmable computer

Several complex machines were built by the British to aid the attack on Tunny. The first was the British Tunny.[7] This machine was designed by Bletchley Park, based on the reverse engineering work done by Tiltman's team in the Testery, to emulate the Lorenz Cipher Machine. When the pin wheel settings were found by the Testery, the Tunny machine was set up and run so that the messages could be printed.

A family of machines known as "Robinsons" were built for the Newmanry. These used two paper tapes, along with logic circuitry, to find the settings of the *chi* pin wheels of the Lorenz machine. The Robinsons had major problems keeping the two paper tapes synchronized and were relatively slow, reading only 2000 characters per second.

The most important machine was the Colossus of which ten were in use by the war's end. They were the world's first large-scale programmable electronic digital computers, the first becoming operational in December 1943. These were developed by senior engineer Tommy Flowers at the Post Office Research Station at Dollis Hill in London. Like the later ENIAC of 1946, Colossus did not have a stored program, and was programmed through plugboards and jumper cables. It was faster, more reliable and more capable than the Robinsons, so speeding up the process of finding the Lorenz *chi* pin wheel settings. Since Colossus generated the putative keys electronically, it only had to read one tape. It did so with an optical reader which, at 5000 characters per second, was driven much faster than the Robinsons' and meant that the tape travelled at almost 30 miles per hour (48 km/h). This, and the clocking of the electronics from the optically read paper tape sprocket holes, completely eliminated the Robinsons' synchronisation problems.

Testery executives and Tunny codebreakers

- Ralph Tester linguist and head of Testery
- Jerry Roberts shift-leader, linguist and senior codebreaker
- Peter Ericsson shift-leader, linguist and senior codebreaker
- Victor Masters shift-leader
- Denis Oswald linguist and senior codebreaker
- Peter Hilton codebreaker and mathematician
- Peter Benenson codebreaker
- Peter Edgerley codebreaker
- John Christie codebreaker
- John Thompson codebreaker
- Roy Jenkins codebreaker
- Tom Colvill general manager

By the end of the war, the Testery had grown to 9 cryptographers, 24 ATS girls (as the women serving that role were then called) with a total staff of 118, organised in 3 shifts working round the clock.

Notes

[1] of *German Tunny*
[2] of *German Tunny*
[3] of *German Tunny*
[4] of *German Tunny*
[5] of *German Tunny*
[6] in *Knockholt*
[7] Bletchley Park completes epic Tunny machine (http://www.theregister.co.uk/2011/05/26/bletchley_park_tunny_rebuild_project/) The Register, 26th May 2011 (http://www.theregister.co.uk/2011/05/26/), Accessed may 2011

References

- Churchhouse, Robert (2002), *Codes and Ciphers: Julius Caesar, the Enigma and the Internet*, Cambridge: Cambridge University Press, ISBN 978-0-521-00890-7
- Copeland, B. Jack, ed. (2006), *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford: Oxford University Press, ISBN 978-0-19-284055-4
- Copeland, Jack (2006), *The German Tunny Machine* in Copeland 2006, pp. 36–51
- Copeland, Jack (2006), *Machine against Machine* in Copeland 2006, pp. 64–77
- Davies, Donald W., *The Lorenz Cipher Machine SZ42*, (reprinted in *Selections from Cryptologia: History, People, and Technology*, Artech House, Norwood, 1998)
- Flowers, Thomas H. (2006), *Colossus* in Copeland 2006, pp. 91–100
- Good, Jack (1993), *Enigma and Fish* in Hinsley & Stripp 1993, pp. 149–166
- Good, Jack; Michie, Donald; Timms, Geoffrey (1945), *General Report on Tunny: With Emphasis on Statistical Methods* (http://www.alanturing.net/turing_archive/archive/index/tunnyreportindex.html), UK Public Record Office HW 25/4 and HW 25/5, retrieved 15 September 2010 That version is a facsimile copy, but there is a transcript of much of this document in '.pdf' format at: Sale, Tony (2001), *Part of the "General Report on Tunny", the Newmanry History, formatted by Tony Sale* (http://www.codesandciphers.org.uk/documents/newman/newman.pdf), retrieved 20 September 2010, and a web transcript of Part 1 at: Ellsbury, Graham, *General Report on Tunny With Emphasis on Statistical Methods* (http://www.ellsbury.com/tunny/tunny-001.htm), retrieved 3 November 2010
- Halton, Ken (1993), *The Tunny Machine* in Hinsley & Stripp 1993, pp. 167–174
- Hinsley, F.H.; Stripp, Alan, eds. (1993) [1992], *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Hinsley, F.H. (1993), *An introduction to Fish* in Hinsley & Stripp 1993, pp. 141–148
- Klein, Melville, *Securing Record Communication: The TSEC/KW-26* (http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/tsec_kw26.pdf), retrieved 17 September 2010
- Roberts, Jerry (2006), *Major Tester's Section* in Copeland 2006, pp. 249–259
- Roberts, Jerry (2009), *My Top-Secret Codebreaking During World War II: The Last British Survivor of Bletchley Park's Testery* (http://www.ucl.ac.uk/news/news-articles/0903/09031601) (iTunes U), University College London
- Tutte, W. T. (19 June 1998), *Fish and I* (http://www.usna.edu/Users/math/wdj/papers/cryptoday/tutte_fish.pdf), retrieved 7 April 2012 Transcript of a lecture given by Prof. Tutte at the University of Waterloo
- Entry for "Tunny" (http://www.alanturing.net/turing_archive/archive/b/B06/BO6-092.html) in the GC&CS *Cryptographic Dictionary*
- The Lorenz Cipher and how Bletchley Park broke it (http://www.codesandciphers.org.uk/lorenz/fish.htm) by Tony Sale

Further reading

- Stephen Budiansky, *Battle of Wits* (Free Press, New York, 2000). Contains a short but informative section (pages 312–315) describing the operation of Tunny, and how it was attacked.
- Paul Gannon, *Colossus: Bletchley Park's Greatest Secret* (Atlantic Books, 2006). Using recently declassified material and dealing exclusively with the efforts to break into Tunny. Clears up many previous misconceptions about Fish traffic, the Lorenz cipher machine and Colossus.
- F. H. Hinsley, Alan Stripp, *Codebreakers: The Inside Story of Bletchley Park* (Oxford University Press, 1993). Contains a lengthy section (pages 139–192) about Tunny, the British attack on it, and the British replicas of the Lorenz machine.
- Small, Albert W. (1944), *The Special Fish Report* (http://www.codesandciphers.org.uk/documents/small/smallix.HTM), retrieved 21 September 2010
- Michael Smith, *Station X: Decoding Nazi Secrets* (TV Books, New York, 2001). Contains a lengthy section (pages 183–202) about Tunny and the British attack on it.

External links

- Lorenz ciphers and the Colossus (http://www.codesandciphers.org.uk/lorenz/index.htm)
- Information on Lorenz (http://www.eclipse.net/~dhamer/lorenz.htm)
- Photographs and description of Tunny (http://www.jproc.ca/crypto/tunny.html)
- Simplified Lorenz Cipher Toolkit (http://www.cimt.plymouth.ac.uk/resources/codes/lorenz/default.htm)

Article Sources and Contributors

Lorenz cipher *Source*: http://en.wikipedia.org/w/index.php?oldid=594031093 *Contributors*: *Kat*, A. Carty, Adamlock, Agentbla, Ahoerstemeier, Angela, Angusmclellan, Beauguide, Bjmullan, BlaiseFEgan, CWesling, Centrx, Cnwilliams, Cojoco, CosineKitty, DabMachine, DagErlingSmørgrav, Dave w74, Davidgothberg, Davidhorman, Delphi234, Dennywuh, Dhugot, DocWatson42, Dodo19, Elminster Aumar, Fg2, Gabbe, GeneralPatton, Gerhard51, Hellbus, Hmains, Inkling, Jan D. Berends, Jgrahamc, Jnc, John.Oakley, JonEAhlquist, Jpbowen, Kbabej, Kbrose, LorenzoB, Lumos3, MagneticFlux, Math Champion, Matt Crypto, Michael Zimmermann, Nabokov, Nihil novi, Oliverlewis, Olivier, PBS, Pembers, ProhibitOnions, R'n'B, Rich Farmbrough, Sannse, Securiger, Signalhead, SimonArlott, Sommerfeld, Suisui, TedColes, The PIPE, Thincat, Todd Vierling, TubularWorld, Vaughan Pratt, WO2, Wafry, Wavelength, William Avery, Wizzard1406, Wonder88jerry, Ww, XJaM, Yintan, 83 anonymous edits

Image Sources, Licenses and Contributors

Image:Lorenz-SZ42-2.jpg *Source*: http://en.wikipedia.org/w/index.php?title=File:Lorenz-SZ42-2.jpg *License*: Public domain *Contributors*: Avron, Dbenbenn, Sissssou

Image:SZ42-6-wheels-lightened.jpg *Source*: http://en.wikipedia.org/w/index.php?title=File:SZ42-6-wheels-lightened.jpg *License*: Public Domain *Contributors*: Avron, Heierlon, Matt Crypto, TUBS, Verica Atrebatum

License