BLETCHLEY PARK

British Cryptanalysis during World War II

Christian Lendl

BLETCHLEY PARK

British Cryptanalysis during World War II

Christian Lendl

Please scan this QR-code with your mobile device or visit *www.bletchleypark.at* to get the eBook and audiobook version of this book.

First Edition, December 2012

Printed in Austria
ISBN 978-3-200-02924-8

Nothing should be as favorably regarded as intelligence.
Nothing should be as generously rewarded as intelligence.
Nothing should be as confidential as the work of intelligence.

Sun Tzu

TABLE OF CONTENTS

INTRODUCTION

The breaking of the Enigma code was a state secret in the UK for nearly 30 years after the end of the Second World War. After the ban was lifted and the first publications came out – like the most famous book „The Ultra Secret“ by Frederick Winterbotham – history books had to be rewritten. Breaking the codes of the German Wehrmacht, Luftwaffe and Kriegsmarine was not „the icing on the cake“, but essential for the Allied forces to gain the upper hand in the course of the war. It was the first time in history that cryptanalysis had such a big impact on warfare. As the encryption of messages was dramatically improved with the development of the rotor cipher machines as the Enigma, also the code breakers had to develop new methods to decipher encrypted text. Statistical methods, probability functions and finally the first programmable computers were used during the war. Especially those computers not only had a direct impact on the war, but also laid the foundation for the development of the computer and most modern electronic communication and entertainment devices. But it was not only the great minds and technological developments, which made the code breaking possible. First of all there was a big portion of luck, represented by the codebooks or Enigma machines that the Allies found or captured. Secondly there was the laziness of the German Enigma operators. Their lazy operating habits and errors helped the code breakers a lot – most deciphering methods were even based on those mistakes. If the Enigma was used properly, it would have been much harder (some say impossible) to break. Finally, this is not just the story of the people at Bletchley Park. Of course, they played the most important role in the code breaking endeavour. But also the other players are not only worth mentioning, in fact their work was essential spadework for the Ultra project, which would not have been that successful without the prior achievements of the Polish code breakers of Buiro Szyfrów.

This book gives an overview of the cryptanalytic work of both the Buiro Szyfrów in Poland and the Ultra project in Bletchley Park, provides mechanical and mathematical details of the Enigma machine and summarizes Ultra‘s influence on the Second World War. Furthermore the Lorenz cipher machine – the second important German cipher machine – and its code breaking with the Colossus computer are explained in detail.

CRYPTANALYSIS BEFORE WORLD WAR II

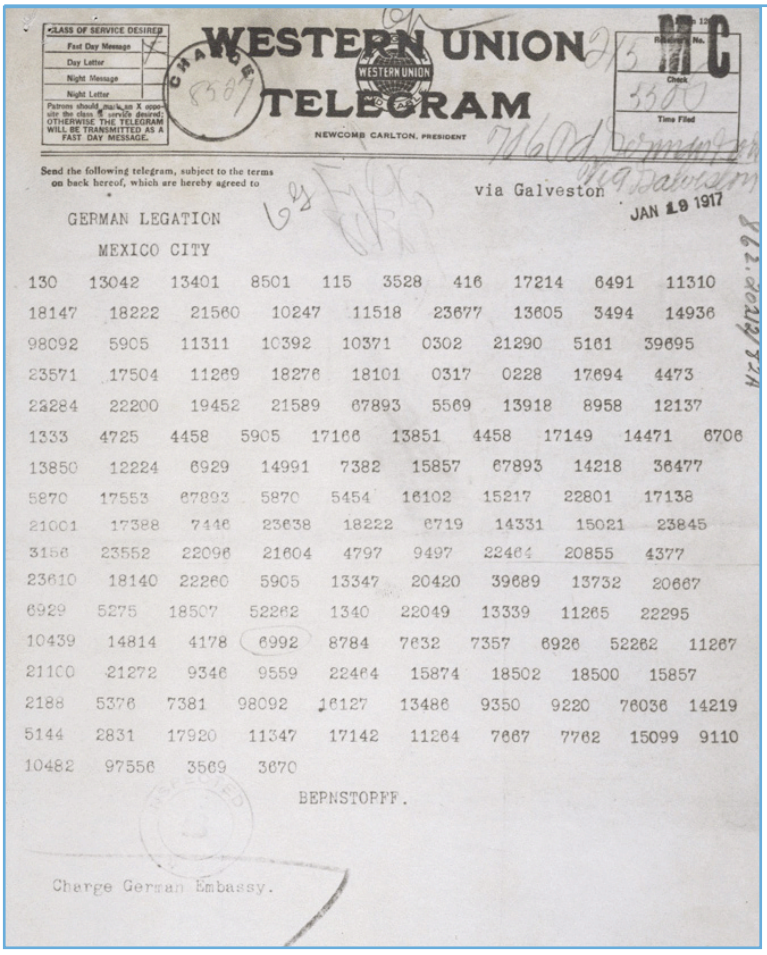
Cryptography (and therefore cryptanalysis) was not invented with the development of the Enigma machine – it had been used for the last 2,000 years. It would go beyond the scope of this book to tell the complete story of cryptography and cryptanalysis. For interested readers Simon Singh's book „The Code Book: The Secret History of Codes and Code-breaking" is a great source to get an overview of the evolution of cryptography. To illustrate the big advantage of rotor cipher machines (like the Enigma), the British cryptanalytic work in the First World War – before the invention of those machines – is briefly summarized in this chapter.

Cryptography based on codes

With the invention of wireless radio at the end of the 19th century, new chances evolved for military communication. Every ship within the fleet could be directed in real-time. As military radio communication uses strong shortwave transmissions, the radio waves are bounced between the ground and the upper atmosphere of the earth[1]. Therefore signals can be received over extremely long distances. But the greatest strength of radio is also its greatest weakness: the radio signals are also received by the enemy, therefore the messages have to be encrypted.

In the First World War cryptography was mainly based on codes. Both the sender and the receiver of a message had to have the same codebook to encrypt and decrypt the message. Every word in plaintext[2] had to be enciphered with the corresponding code of the codebook. If that word was used repeatedly, most of the time the same code was used (only the most frequently used words had multiple codes). Therefore, the only thing that was necessary to break the ciphertext[3] was the codebook.

The British Naval Intelligence – commonly called Room 40 after their location in the Admiralty building – did exactly that: From 1914 onwards they analyzed the wireless telegraph messages of the German Navy with various codebooks that they had captured from a German submarine or were handed over by the Russians, who captured them from the German cruiser Magdeburg[4]. Room 40 consisted mostly of „linguists, classical scholars and puzzle addicts"[5].



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8367

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

MC

Check 3380

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

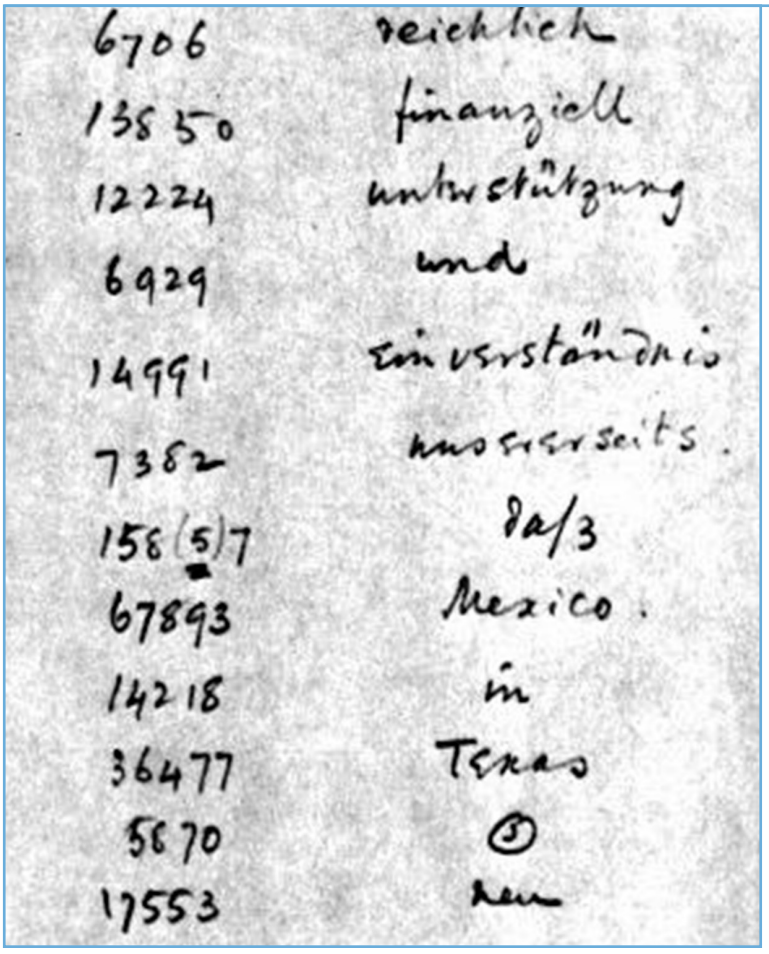
Charge German Embassy.

The Decryption of the Zimmerman telegram was the first famous use of cryptanalysis, which had a major impact on diplomacy, world politics and the course of the war.

On 16 January 1917, the German foreign minister Arthur Zimmermann sent an encrypted telegram to the German ambassador in Washington, who then retransmitted it to the German ambassador in Mexico. It included a message to the President of Mexico. The German Empire wanted Mexico to attack the USA from the South and reclaim Arizona, New Mexico and Texas, so that the USA would not have the resources to send troops to Europe. If the Mexican president would have followed this plan, Germany promised to provide military and financial support. Furthermore, it stated that Germany would instigate unrestricted U-boat warfare on 1 February, 1917.[6]

At the beginning of the First World War (to be exact: on the very first day of the war), a British ship had secretly cut off the German transatlantic cables near the German coast. Therefore all transatlantic communication had to be done via radio transmission or via cables of other nations. In the case of the Zimmermann telegram an American and a Swedish cable were used – both touched British ground, so the message could be intercepted and was handed over to the cryptanalysts of Room 40. Within just one day, the cryptanalysts of Room 40 recovered the outline of the telegram, which was enciphered with a code only used for high-level diplomatic communications[7]. They used previous analysis from similar encrypted telegrams and soon discovered that this telegram was of utmost importance and would likely change America's position – either because of the unrestricted U-boat warfare or the possible attack from the South[8].

The British Naval Intelligence did not pass the decrypted telegram on to the Americans immediately. Any American response before 1 February would have revealed that the German method of encryption had been broken. As America stayed neutral after 1 February, the commander of the British Naval Intelligence decided to exploit the telegram. In order to not reveal the real source, they conceived a ploy including a British agent in Mexico, who stole the final version[9]. Finally, the telegram was made public. America entered the war on 2 April and


6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 ein verständnis
7382 unsererseits.
158(5)7 da/3
67893 Mexico.
14218 in
36477 Texas
5870 ⑤
17553 neu

Germany came to the conclusion that „various indications suggest that the treachery was committed in Mexico“[10].

The cryptanalytic work in the First World War had proven to be extremely important for the course of the war. But just as important as the code breaking itself was the careful use of the decoded intelligence not to reveal the decryption and therefore blow one‘s cover – this would be remembered about 20 years later.

THE ENIGMA

The development of the rotor cipher machines started a new era in the world of cryptography. Mathematically these machines are based on substitution with multiple alphabets (also called polyalphabetic cipher). The very basic principle is the same as for the Viginère-cipher, which had at that time already been broken. So the designers of the cipher machines had to think of new ways to increase the number of possible encryptions and therefore enhance the security of the code.

There were various rotor cipher machines; the Enigma was only the most widely known one. The development started during or shortly after the First World War. Numerous designers worked independently on the invention of different models at the same time, therefore there was no single inventor. Other machines were e.g. the German Lorenz SZ 40 and SZ 42, the British TypeX or the American SIGABA.

Technical details of the Enigma

Enigma is the ancient Greek word for puzzle[11]. The German engineer Arthur Scherbius invented it shortly after the end of the First World War as a battery-operated electrical version of a mechanical cipher disc. It basically consists of three major parts, which are connected with electric wires: the keyboard for inputting letters, the scrambler unit for encrypting the letters and the lamp board for displaying the enciphered letters[12]. When the user presses a button, an electric pulse is sent through the scrambler and the corresponding encrypted letter is illuminated on the lamp board. The keyboard has 26 keys ordered in the pattern of a standard German typewriter. It does not include keys for numerals, umlauts, punctuation or blanks[13].

The scrambler consists of three rotors (Walze in German), each of them with 26 contacts on both sides representing the alphabet. All rotors have different inner cross-connections[14]. They act similar to a mileage indicator in a car. Every time after a key is pressed, the first rotor moves one position. The second rotor only moves one position when the first rotor finishes a full turn (26 position changes, also known as the turnover position), the third rotor moves one position when the second rotor completes a full turn. The three rotors offer 26 x 26 x 26 = 17,576 different rotor positions. The entry wheel (Eintrittswalze in German) connects the keyboard with the rotors, but does not move or alter any electrical signal[15]. One more part in the scrambler unit is the reflector (Umkehrwalze in German)[16]. It sends the signal back through

3 The Enigma (outer lids open)

the three rotors (but on a different way) to the lamp board. It functions as a mirror so that encryption and decryption can be done with the same machine – mathematically, the cipher is self-inverse[17]. To decrypt a ciphertext, the same rotor-settings have to be set that were used for encryption. The electrical inter-connection works in both ways, so input A will be output B and input B will be output A (with the same settings)[18]. These settings are defined as the key. The rotors themselves can be taken out of the Enigma, interchanged and inserted in any position, which increases the number of initial settings (for three rotors) by a factor of 6. Furthermore, from 1938 on the military version had five available rotors to choose three from – this further enhanced the security[19].

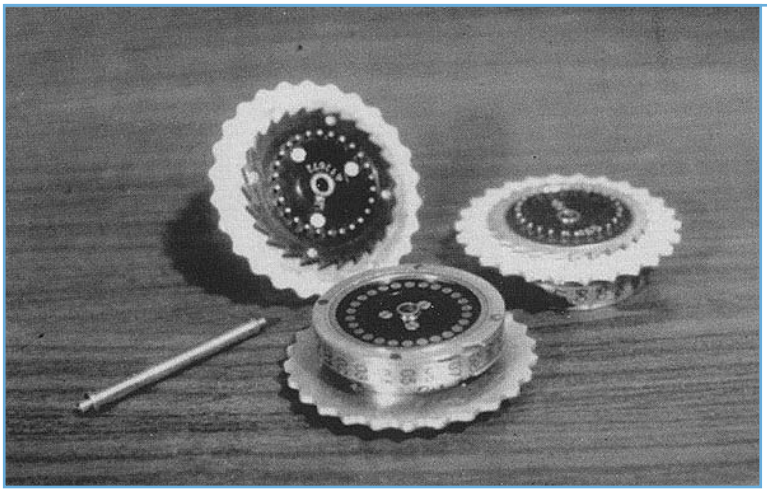
To further increase the number of possible encryptions, Scherbius added another part: the plug board, also called steckerboard (Steckerbrett in German). The user could insert up to six cables or steckers (this number changes later), which swapped letters. So if e.g. the letters A and B were swapped (also called steckered), A was encrypted like B would have been without swapping (and vice versa). One more security feature is the ring. Each rotor features a ring that has the 26 letters printed on it. It can be rotated relatively to the rotor. This does not have any influence in the actual encryption, but enhances the security of the whole machine as it changes the turnover-position of the rotor.

Mathematically, the Enigma offers a variety of about 10,000,000,000,000,000 different keys[20]. Although this is just a theoretical number (certain keys can be eliminated when analyzing the operational instructions), nevertheless it shows the complexity and sophistication of this rotor cipher machine and explains, why the Germans thought of it to be unbreakable.

Operating the Enigma

The operation of the cipher machine involved three people[21]: the originator, the cipher clerk and the radio operator. The originator would prepare the message on a standard form with letter groups, the cipher clerk would encipher it letter by letter (numbers had to be written out in full, spaces were replaces with the letter X) with the Enigma machine using the daily keys of the code book and his own conceived message keys and then hand it over to the radio operator who would transmit it via Morse code.

4 Lamp board and keyboard



5 Three rotors

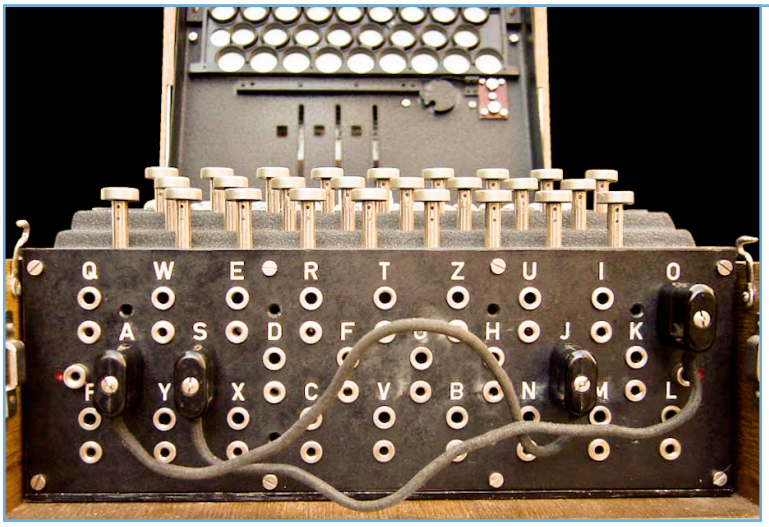
Every Enigma operator had a codebook that included daily keys for a certain period (e.g. one month). These daily keys consisted of the following settings[22]:

- Wheel order (Walzenlage in German)
  The selection and arrangement of the rotors (e.g. II-I-IV)
- Ring setting (Ringstellung in German)
  The setting of the alphabet-rings relatively to the rotors (e.g. DIX)
- Plug board connections (Steckerverbindungen in German)
  The list of the steckered letters (e.g. DI-SU-KL)

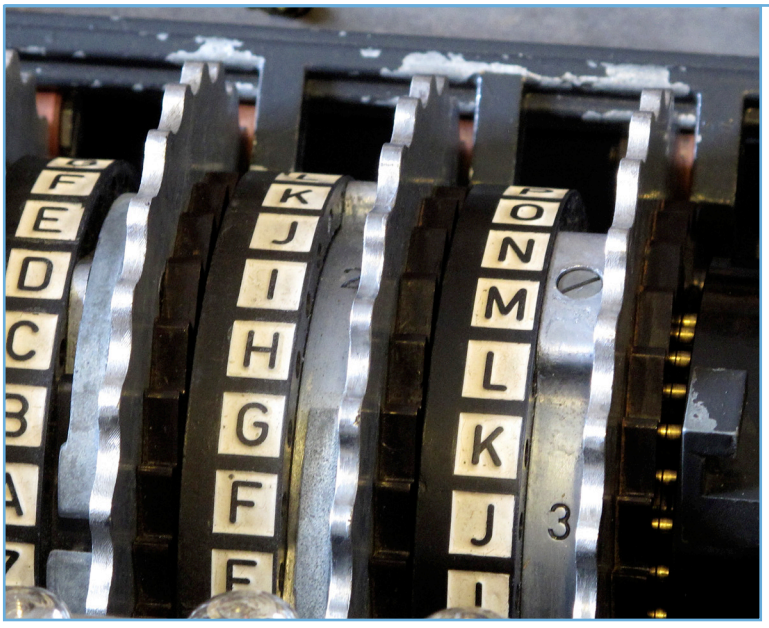
Different divisions of the German armed forces had their own codebooks. As the enemy could have deciphered the messages easily with a stolen codebook, another key – the message key – was added. Even when the daily key was known, the message could not be decrypted without the message key. The operator had to turn the rotors to a randomly chosen position, the indicator-setting. He then keyed his own randomly chosen message setting twice. The result was the indicator. Finally he set the rotors to his message setting and enciphered the clear text of the message letter by letter[23]. For any particular setting, the rotor position would be repeated after 16,900 (26 x 25 x 26) keys pressed, therefore the Germans set a limit of 250 characters for each message to avoid recurrence[24] (which would have helped the enemy a lot for decryption).

Some parts of the German armed forces had adapted versions of the Enigma machine. For example, the Naval Enigma had eight rotors to choose from and an adjustable reflector (Umkehrwalze)[25]. The Abwehr[26] Enigma was significantly different from the „normal“ version. The reflector also moved and had its own turnover-position and the rotors had multiple positions for turnovers (instead of just one). Also, this machine did not have a steckerboard[27].

German Enigma operators made several mistakes, which were of utmost importance for the British analysts in Bletchley Park (and also the Buiro Szyfrów in Poland). Most of their decryption methods were based on them. Some of the mistakes happened because of the carelessness of the operators, others had their background in the



6 Steckerboard



7 Alphabet rings

design of the whole Enigma communication system. Following is a list of all helpful Enigma peculiarities, each of them summarized briefly. The cryptanalytic methods that used them are described in the next chapters.

One of the most helpful operational procedures was the twice done sending of the message key at the beginning of each message[28]. As repetition is a cryptanalysts best friend (because it creates patterns, which can be statistically analyzed), this habit was extremely helpful. Standardized messages at certain points of time were also helpful. For example, every day at 6 a.m. the weather report was sent. It always started with the same words. German military communication involved a lot of standardized phrases, which were included regularly in messages – e.g. `KEINE BESONDEREN EREIGNISSE` (German for „no special occurrences“)[29]. These phrases were called cribs.

The Herivel Tip[30] (named after its founder John Herivel) was another example for the laziness of the German operators. After inserting the rotors into the Enigma and adjusting the ring setting, the operator had to turn the three rotors to a random setting for the message key. Often they would leave the initial setting (= ring setting) or just turn the rotors very few positions, so that the message key was very similar to the ring setting.

```
Q  W  E  R  T  Z  U  I  O
  A  S  D  F  G  H  J  K
P  Y  X  C  V  B  N  M  L
```

The figure above shows the keyboard layout of the Enigma. Sometimes, the German operators chose adjacent keys for their message key, e.g. `QWE`, `EDC` or `TGB`. This often happened for multi-part messages. These slovenly manners were called sillies[31] (or cillies[32]). Reg Parker, a member of Hut 6, discovered that sometimes the daily keys of a previous month were repeated at the beginning of a following month. This finding was called Parkerismus[33].

8

General Heinz Guderian using an Enigma machine

For long-range communication, the Germans often used message relays, where a message was re-sent from a wireless station that was located somewhere between the sender and the designated receiver. The message was deciphered and then enciphered again – but with a different key[34]. This was a bad cryptographic mistake. The steckerboard was one of the major security features of the Enigma. One operating rule forbade the operators to swap neighboring letters – e.g. `S` could be steckered with any letter except `R` and `T`. This should avoid obvious choices, but reduced the number of possible keys dramatically[35].

Maybe the biggest German failure was that they did not monitor their operating procedures. As Gordon Welchman, then one of the leading British cryptanalysts, noted in his book, they could have discovered most of the mentioned errors, which would have stopped the British code breaking efforts immediately[36]. There were even some helpful peculiarities based on the construction of the Enigma machine itself. The wiring of the entry wheel was on of them. It connects the keyboard with the rotors and does not alter the letters (`A` => `A`, `B` => `B`, etc.), although it could use any combination (e.g. `A` => `L`, `B` => `X`, etc.). As mentioned before, the message key (e.g. `WDO`) was always sent twice at the beginning of each message (e.g. `WDOWDO`). This meant that the first and fourth letter in ciphertext were equal in plaintext (same goes for second/fifth and third/sixth letter). For some settings, those letters were also equal in ciphertext (e.g. `STUSVD`):

Letter	1.	2.	3.	4.	5.	6.
Cleartext	**W**	D	O	**W**	D	O
Ciphertext	**S**	T	U	**S**	V	D

These occurrences were called females. Another very interesting entity of the Enigma was that no letter could be enciphered with itself[37]. This was essential to find those so-called cribs.

PRELIMINARY WORK

As the Enigma was developed right after the First World War and began to be deployed by the various parts of the German armed forces and government departments during the 1920s[38], the other European nations and especially their intelligence services took note of this new cipher machine long before the outbreak of the Second World War. One of those nations was Poland. With the rise of the Nazi regime they realized the growing danger of their aggressive neighbor in the West (along with Russia in the East) and got interested in intercepting foreign military communications. They were very successful in deciphering Russian messages in the Russian-Polish war 1920-21[39]. Also a lot of German messages were decrypted, but that stopped in 1926 when the Enigma came into play.

Help from Germany

Hans-Thilo Schmidt was an employee of the Chiffrierstelle, the German office for cryptographic communications. He was almost destitute and disappointed by the German state – his military career had not been successful, neither was an attempt to build up a soap factory – and envious of his brother, who was chief of staff of the Signal Corps and therefore responsible for the sanction of the Enigma in the German army. Schmidt made plans to sell secret Enigma documents to foreign countries to get both revenge and money. In 1931, he allowed a French spy in Brussels to photograph Enigma instruction manuals for 10,000 marks.[40] The French cryptographic bureau was not able to use this information properly, but passed it on to the Polish intelligence service[41]. With the secret documents the Poles would be able to build an adequate replica of the Enigma machine, but not to decipher any messages – therefore the key was necessary.

Buiro Szyfrów

Buiro Szyfrów, the Polish cipher bureau, acquired a commercial version of the Enigma (slightly different to the military version) at the beginning of the 1930s[42]. As the cryptanalysts had to deal with a mechanical cipher, more and more mathematicians were recruited instead of linguists, who were in charge of cryptanalysis until then. Most of the new analysts were recruited from the university of Poznán – not because it was the best university, but because of its close distance to the German border. The city was German until 1918; therefore the people spoke German fluently[43].

One of the most talented mathematicians was Marian Rejewski. He focused on the message key (e.g. WDO), which was repeated twice at the beginning of each message (WDOWDO). As the key was sent at the very beginning of the enciphered part of each message (RJGGAQ), it had to be directly related to the daily keys. The first and fourth letter in ciphertext were equal in plaintext (the same goes for second/fifth and third/sixth letters), so there was a relationship between those letters.

Letter	1.	2.	3.	4.	5.	6.
Message 1	**R**	J	G	**G**	A	Q
Message 2	**B**	R	A	**X**	L	V
Message 3	**M**	D	K	**S**	I	Y
Message 4	**W**	F	C	**P**	U	H

If Rejewski received enough messages during one day, he could complete a full alphabet of relationships[44].

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CXLUMWVDKEZOSRAYFGHJTQPINB
```

By analyzing these letters in terms of patterns, he found out that there were chains of letters.

```
A => C => L => O => A
B => X => I => K => Z => B
D => U => T => J => E => M => S => H => D
F => W => P => Y => N => R => F => V => Q => F
```

These chains changed every day (both their length and the arrangement of the letters). Rejewski had a „profound insight“[45] and detected that the lengths of these chains were influenced only by the

scrambler unit – the rotors. The steckerboard connections swapped letters, but did not alter the length of the chains. This insight reduced the number of possible daily keys from 10,000,000,000,000,000 down to 105,456 – the product of rotor arrangement (6) and rotor orientation (17,576)[46]. Although this is also a relatively high number, it was „within the realm of human endeavor"[47]. Rejewski and his colleagues created a catalog for the chain lengths of all 105,456 rotor settings. They even built an electromechanical machine, which included three rotors (equal to those of the Enigma) to automatically deduce the chain lengths: the cyclo-meter[48]. It took them nearly a year to complete this catalog, which was a major step towards the finding of the daily keys. To find the daily rotor settings, the analysts collected enough intercepted messages to complete the letter chains. Then they compared the chain lengths with their catalogue to find the ring setting with the same lengths.

They could now decrypt the messages, but still had to find out the steckered letters. As the analysts were speaking German, they could guess them most of the time by analyzing the deciphered text by looking at „vaguely recognizable phrases"[49]. For example, the term `werretbetichr` should presumably be `wetterbericht` (German for weather report), which meant that the letters `R` and `T` were steckered.

In 1938, the Germans changed their way to transmit messages, which made the catalogue useless. Instead of building a new one, Marian Rejewski developed a mechanized solution to find the settings – the bomba kryptologiczna. As there were six possible scrambler arrangements to check, he had to run six bomby in a parallel way that were running through the 17,576 settings. They needed about two hours to find the daily key.[50]

Henryk Zygalski, one of Rejewski's colleagues, developed another method to find the daily key. He concentrated on the occurrence of females, which were independent from the steckerboard-settings[51]. This method involved perforated paper sheets (named after the founder: Zygalski-sheets) with 51 x 51 matrices (standing for the rotor positions) that had holes at the positions where the females occurred. About ten messages with females were necessary[52], then he could pile up the corresponding sheets. After each new sheet, the number of visible

apertures would decrease, finally showing the possible rotor settings that allowed these ten females[53]. These could then be tested on the Enigma replica.

Agent Asche, as Hans-Thilo Schmidt was called, continued to meet with French agents for seven years and delivered them a total of 38 codebooks, which included daily keys for the German Enigma operators. These codebooks were always passed on to the Polish cipher bureau by the French, but they were never used. The chief of Buiro Szyfrów, Major Gwido Langer, kept them secret from his analysts to have them practice their code breaking skills for the time when Agent Asche would not deliver codebooks anymore.

This time came in 1938, when the Germans increased the number of rotors from three to five and the number of steckered letters from six to ten. Rejewski's methods and the bomba were not successful anymore and Buiro Szyfrów did not have the resources to cope with the new challenge – both financially and personnel-wise[54]. A couple of weeks before the German attack on Poland in 1939, the Polish code breakers met with French intelligence officers and also British analysts from Bletchley Park to share with them all their knowledge and hand over to them their Enigma replica[55]. Marian Rejewski and his colleagues had to abandon their work and escape to France. Rejewski continued his escape from France to the UK and was transferred to a minor intelligence unit in Boxmoor (not working on Enigma ciphers) and did not play a major role in cryptanalysis anymore during the rest of the Second World War. There are only vague descriptions, why the brilliant Polish minds were not transferred to Bletchley Park. Rejewski did not notice the importance of his work as the basis for the British code breakers until the declassification of the Ultra documents and the publication of „The Ultra Secret" in 1974[56] – more than 30 years later.

Hey, you read more than half of this book,
I hope you liked it so far!

Please continue...

BLETCHLEY PARK

The operation around the decryption of the Enigma got its name „Ultra“ by Frederick Winterbotham (author of „The Ultra Secret“), then Group Captain[57] and chief of the Air Department of the Secret Intelligence Service and therefore responsible for the organization, distribution and security of the decrypted messages. He simply wanted to distinguish the Enigma intelligence from the other types.[58]

In 1938 a Polish worker employed in a German factory made notes of the cipher machines (later identified as military versions of the Enigma), which this factory was producing. He was sacked after a security check, sent back to Poland and once there, he contacted the Polish Secret Service. They got in touch with the British Intelligence to share their knowledge and later were successful in stealing one Enigma machine from that factory with British financial and logistical support. This machine was directly transferred to the British Government Code and Cypher School (GC&CS), which set up its headquarters in Bletchley Park in August 1939 (later followed by the SIS, the Secret Intelligence Service)[59]. This stolen Enigma was not the only machine, which the code breakers in Bletchley Park could make use of. In 1940, another machine together with operational keys was obtained from a shot down German aircraft in Norway. Later, more useful materials were captured from a German tank signals unit and in 1941 the Royal Navy captured a German submarine, complete with its Enigma and the chart of operation keys.[60]

The first employees of Bletchley Park were recruited by the existing employees of the GC&CS (and former Room 40) through their „old-boy network“[61], which meant their old Oxford and Cambridge colleagues. The focus was not anymore on linguists and classicists, but on mathematicians and scientists. They also recruited new members through a crossword puzzle in The Daily Telegraph (anonymously, of course). Anyone, who would be able to solve it in less than twelve minutes, should contact the newspaper. 25 readers replied, six of them made their way through interviews and tests and became code breakers[62]. Additionally, also chess grandmasters were invited, they were believed to be good cryptanalysts[63]. At the beginning, there were about 200 people working in Bletchley Park. This number increased to 7,000 during the war[64]. When cryptanalysts began working in Bletchley

9 Bletchley Park

10 Hut 4

Park in 1939, they already knew the Enigma operating procedures the Germans were using – thanks to their Polish colleagues[65].

As the main building in Bletchley Park did not have enough space for all employees of the GC&CS, they built several wooden huts for the individual teams. The teams kept the number of their huts as their team name even after being relocated to other facilities. The activities of the GC&CS were „highly compartmentalized“[66] because of security reasons, only very few people knew exactly what the different huts were working on. The analysts themselves did not know what their colleagues of the neighboring team were doing exactly. Each group was responsible for a specific task[67]. The following table shows selected huts:

Hut No.	Task
3	Intelligence (translation and analysis of decoded army and air force messages)
4	Intelligence (translation and analysis of decoded navy messages)
6	Decoding of the Enigma traffic of the German army and air force
8	Decoding of the Enigma traffic of the German navy
11	Building of the bombes

Normally, the workflow for getting a message would include the following stages[68]:

1. Interception of German messages at the Y-stations[69]
2. Traffic analysis
3. Hunting for cribs
4. Bombe runs
5. Testing of the possible Enigma settings
6. Decoding of the German messages with adapted TypeX[70] machines
7. Translation and analyzing of the messages by the intelligence

11

Replica of a British bombe with open front door

Before the analysts started to look for cribs, they regularly tried the known cillies. This meant some extra work, but sometimes it paid off and saved hours of work. Another timesaver was the fact the Enigma operators were not allowed to use a certain scrambler setting for two days in a row. As soon as the code breakers got the daily keys, they could rule out a lot of settings for the next day, which roughly reduced their work by half[71].

Alan Turing & the British bombe

Alan Turing was one of the leading mathematicians in Cambridge. His thesis „On Computable Numbers" was most influential in the world of mathematics and was also to become very important later in the 20th century for the evolution of computer science – Turing is widely known as the father of computer science. In September 1939, he was invited to Bletchley Park to become a cryptanalyst.

Turing continued Rejewski's idea of the letter chains, but connected plaintext and ciphertext letters within a crib instead of the message key. He supposed that the Germans would stop to send the message key twice (what they actually did in 1940). He started planning a machine, which included three rotor sets, connected with an electrical circuit. The output of the first set was connected with the input of the second set and the output of the second set was connected with the input of the third set. The second set was one step ahead of the first one and the third set was two steps ahead. Turing's construction nullified the steckerboard settings and dramatically reduced the number of different settings to check[72]. A light bulb was illuminated when the electrical circuit was complete – which meant that the right setting was found. In most other cases all of the light bulbs were illuminated (= false settings)[73]. This machine would need five hours to find the right scrambler setting, if it changed the scrambler position every second. The GC&CS was able to finance the construction of this machine, which was named like the Polish machine some years before: bombe[74]. The first version was much slower than expected (needing a week to find a particular key), but after several improvements and 15 built bombes, they needed just one hour to find an Enigma key[75].

The bombe worked on the basis of the principle „reductio ad absurdum"[76], which meant that each particular assumption (= Enigma setting) had to be proved wrong before the bombe could move on. To

reduce the number of bombe runs, Alan Turing developed a statistical method to decrease the number of possible settings based on the probability of cribs. This method was called Banburismus[77] (later sequential analysis).

Daily hunt for cribs

The bombes were a big improvement, but the search for the daily keys continued to be an intense fight, which restarted every 24 hours. The hardest work was to find the cribs, which were used as a basis for the bombes. A tough nut to crack was the Naval Enigma of the Kriegsmarine. As already mentioned, it had more rotors to choose from and had an adjustable reflector. The operators were trained not to use those stereotypical messages (which were essential for cribs) and had a different system for selecting the daily keys. For the Allies, cracking these messages was essential to gain the upper hand in the war for the Atlantic Ocean. The German submarines were very successful in attacking the Allied convoys on their way from the USA to Europe. Knowing their positions would help the Allies in two ways: Firstly, they could reroute their convoys and secondly, they could attack the German submarines. One way to get the useful cribs was the so-called „gardening". British planes laid mines on particular locations in the hope that German ships would send out warnings including the coordinates for the minefield – in further consequence this would result in a crib[78].

Another method to obtain the daily keys was to steal German codebooks. As mentioned before, this was successful several times. One never realized operation even included the crash-landing of a stolen German airplane in the English Channel to steal the codebook of a German ship. Operation Ruthless[79] was planned by a member of the Naval Intelligence who became famous for his spy stories later: Ian Fleming, creator of James Bond.

The information obtained from either cracked messages or stolen codebooks had to be used very carefully to prevent disclosure of the source of information. For example, German ships were sunk after their codebooks were stolen (to make the Germans believe the codebook was also lost), spotter planes were sent out before an attack on a German U-boat (to mock a sighting by the plane), or fake messages containing U-boat sightings were sent out[80].

The Enigma messages of the parts of the German armed forces – Wehrmacht, Kriegsmarine, Luftwaffe, SS, etc. – differed not only in terms of how hard they were to decipher (depending on different Enigma settings and operational procedures), also the amount of traffic was different. Before the Allied invasion in Normandy in 1944, messages of the German army and air force were mainly transmitted via landline[81], which made interceptions impossible.

Although Alan Turing and his colleagues had access to all the Polish knowledge, they re-invented some of the methods that were already worked out by Marian Rejewski and his fellows. Gordon Welchman, one of the leading cryptanalysts besides Turing, concentrated on females and invented his own version of the perforated sheets (like Henryk Zygalski years before). But he went one step further by developing an electrical add-on to the bombe that Turing built before: the diagonal board[82]. It consisted of a 26 x 26 matrix of electrical terminals, diagonally connected so that e.g. `G` was connected to `L` and vice versa. It was directly attached to the bombe and enabled the use of any crib of three or four words[83], which reduced the possibility of turnovers and made the cryptanalyst's work much easier.

Until 1943, Britain did not share its knowledge about the breaking of the Enigma with its Allies. Of course, Ultra intelligence was passed on to American commands, as they were fighting along with British troops. The first American intelligence officers were invited to Bletchley Park in 1943[84]. Later, the US Navy and US Army built their own bombes, based on those developed in Britain.

THE LORENZ MACHINE & COLOSSUS

In addition to the Enigma – an offline[85] cipher machine, whose output was then transferred via Morse code – German cryptographers were also working on an online[86] cipher machine, which used the international five-unit teleprinter code[87]. The big advantage was that encryption and transmission as well as reception and decryption could be done simultaneously. Furthermore, the number of possible keys was much higher than for the Enigma.

The Lorenz SZ[88] 40 and its successor, the SZ 42 – cryptanalysts in Bletchley Park called it Tunny[89] – were the main machines used for this kind of communication in the Wehrmacht. They were mainly used for high-level military messages. A second machine, the Siemens and Halske T52 Geheimschreiber (called Sturgeon[90]), was used by the Luftwaffe.

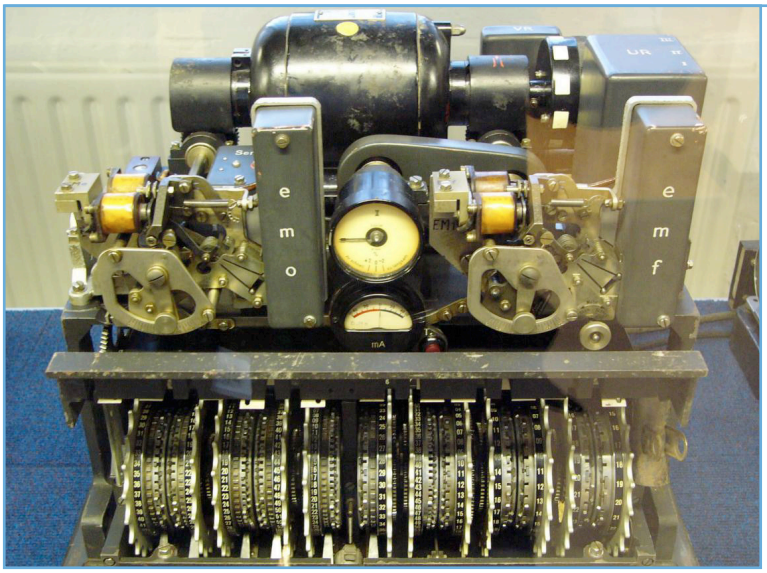
Morse code uses long (`dah`) and short (`dit`) electronic pulses as basic units, every letter needs between one to four basic units (e.g. E is `dit`, K is `dah-dit-dah`). In contrast, teleprinter code uses regular patterns of electronic pulses – pulse (`1`) or no-pulse (`0`) – as the basic units. A letter always consists of five basic units (e.g. Q is `00010`)[91].

Tunny

The Tunny machine consisted of 12 rotors, each with different numbers of positions, ranging from 23 to 61 (the three Enigma rotors all had 26 positions)[92]. In contrast to the Enigma, the plaintext was not enciphered through these rotors. For every letter of the plaintext, another letter was generated by the rotors (those letters were the key) and then merged with the plaintext to generate the ciphertext.

```
1 + 1 = 0
0 + 0 = 0
1 + 0 = 1
0 + 1 = 1
```

The above shown rules for adding basic units were used for both enciphering and deciphering: If a letter was added to another letter a second time, the original letter was the result[93] (see next page).



12

Lorenz SZ42, called Tunny

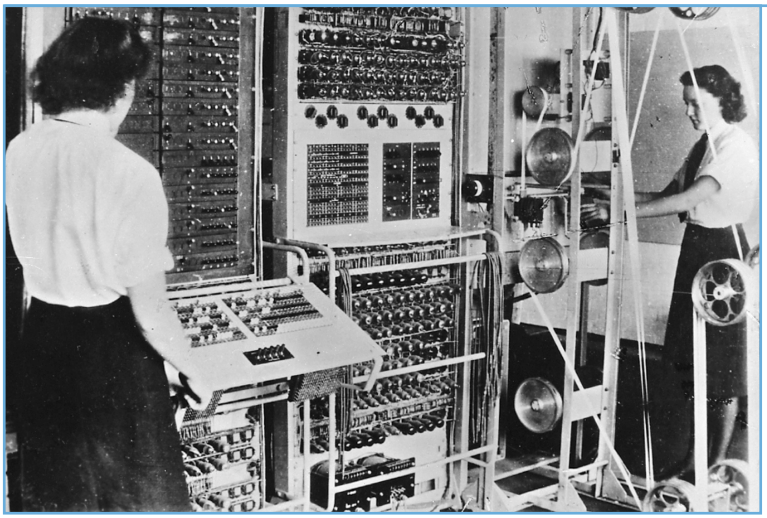
Q	+	B	=	Z
0	+	1	=	1
0	+	0	=	0
0	+	0	=	0
1	+	1	=	0
0	+	1	=	1

Z	+	B	=	Q
1	+	1	=	0
0	+	0	=	0
0	+	0	=	0
0	+	1	=	1
1	+	1	=	0

Tunny was called Schlüsselzusatz (German for cipher attachment) and, as the name suggests, was attached to a teleprinter. Messages were entered via a keyboard or automatically read from a tape, then enciphered and transmitted. Before 1942 (in the experimental phase of the Tunny machine), the rotor settings (also called indicator setting) were sent as cleartext before the enciphered message. Then the German army started the regular use and therefore introduced a codebook (the so-called QEP book), which included those settings. Only the three-digit number of the chosen setting was transmitted as cleartext[94].

Fish

Cryptanalytic efforts in Bletchley Park concentrated mainly on Tunny[95] (its intelligence was called Fish[96]), because the whole process of interception (transmission of the messages occurred at high speed, therefore interception was difficult) and code breaking (the analysts had to work extremely accurately, which made mechanization necessary) was much more complex than it was for Enigma messages. Otherwise it would have been necessary to shift resources from the Enigma decryption to this project and that would have resulted in a decrease of deciphered Enigma messages immediately[97]. The Tunny network grew steadily from 1942. It was used for communications between headquarters in Berlin and the commanders of army groups and also of armies. The number of monthly messages was lower than for the Enigma, but the significance of their content (e.g. strategic plans of German armies) was exceptional[98]. In August 1941, a message containing about 4,000 characters was sent from Athens to Vienna twice (it was repeated because of transmission problems). The messages had minor differences (due to mistakes of the sending operator), but had the same key. This occurrence was called „in depth“ by the cryptanalysts[99] and was „a gift from heaven“[100] for Bletchley Park. The British code breaker John Tiltman succeeded in decrypting the message and his colleague



13

Colossus

Bill Tutte managed to lay bare the functional details of the machine within the next six months – without ever seeing it[101]. The code breakers in Bletchley Park were looking for messages with similar rotor settings and successfully deciphered nearly all Fish messages until October 1942, when the Germans stopped sending the indicator setting and introduced the QEP book[102]. Tutte developed a mathematical method where the wheel settings were compared to a string of intercepted ciphertext until the one setting with the best statistical fit was found. This method was successful, but it was so sophisticated and time-consuming that a mechanized solution was needed to keep up with the increasing amount of Fish messages[103] – a job for Max Newman.

The first prototype (named Heath Robinson) was built from January to June 1943[104]. It was fed with two teleprinter tapes (one included the intercepted Fish message, the other the rotor settings). The individual characters of the two tapes were automatically read and merged position-by-position, electronic counters then showed the scores[105]. The machine worked, but was not fast enough and was prone to errors. As it was mainly built on slow relays, the synchronization of the two tapes also limited the speed. A new machine (named Colossus) was designed – this time fully electronic with about 1,600 electronic valves and only one tape input (for the Fish message). The rotor settings were generated electronically, the machine operated at 5,000 characters per second (later models processed up to 25,000 characters per second with 2,400 valves)[106]. It was delivered to Bletchley Park in January 1944 and was successful from the very beginning. Immediately, more Colossi were ordered. A method was designed so that Colossus could also be used to discover the wheel patterns – this resulted in the enhanced Colossus II. By the end of 1944, seven Colossi were in operation[107]. Fish intelligence was of utmost importance for the Allied invasion. In France, the Wehrmacht mainly used landlines for their Enigma communications, which made interception impossible. But there was a Tunny link between Berlin and the Commander-in-Chief in the West, Generalfeldmarschall[108] Gerd von Rundstedt. The deciphered Fish messages unveiled plans for countering the Allied invasion as well as information about the state and disposition of German divisions[109]. The Allies were also fully informed about the Soviet advances on the Eastern front – thanks to Fish intelligence[110].

IMPACT ON WORLD WAR II

Although Enigma messages were decrypted regularly from the beginning of 1940 onwards, they were not practically used during the first year because communications skills, security procedures and expertise were not on an equivalent level yet[111].

There were numerous occasions during the Second World War, when Ultra information played a decisive role. To name all of them would go beyond the scope of this book, so following are a few selected examples to illustrate Bletchley Park's importance. One of the first Ultra contributions, which were used for military operations, was during the Battle of Cape Matapan, where the Allied Mediterranean fleet defeated the Italian fleet thanks to the timely receipt of German and Italian messages[112]. The sinking of German supply ships on their way to North Africa due to Ultra intelligence was essential for Operation Crusader – between 20 % and 50 % of the sailed German ships were sunk before or during the offensive. It helped to force Generalfeldmarschall Erwin Rommel back to El Agheila in 1941. When the cryptanalytic factory in Bletchley Park was running on full power, it deciphered the German messages within an amazing short period of time. During the battle of El Alamein, Field Marshal Bernard Montgomery had Hitler's message to Rommel on his desk even before Rommel himself received it[113] – this was also due to a delay on Rommel's side, but nevertheless unbelievably fast.

In the Atlantic, Ultra intelligence was used to route convoys away from the areas where German submarines were patrolling. The average sinking per month rapidly declined from 282,000 tons in June 1942 to 62,000 tons in November, resulting in a (calculated) total of 1,500,000 tons (about 350 ships) that were saved[114]. Another major use – maybe the most important during the war – of Ultra intelligence happened during the preparations of Operation Overlord, the Allied cross-channel invasion of France. Bletchley Park revealed the exact positions of nearly all the German divisions in Western France and uncovered the German preparations against an Allied landing[115].

AFTER WORLD WAR II

As mentioned in the introduction, the Ultra project was a state secret until the spring of 1974[116]. Directly after the end of the war, most of the equipment and all blueprints were destroyed. Most of the code breakers returned to their civilian lives and were not allowed to talk about their work (until 1974)[117]. Sir John Slessor, a former Air Field Marshal of the Royal Air Force and former Chief of Air Staff[118], mentioned in the foreword of Frederick Winterbotham's book that he tried to lift the ban several times before 1974, but was never successful[119].

Britain captured thousands of German Enigma machines and distributed them amongst its former colonies. Of course, they were not told that the Enigma code had been broken. This ensured that British cryptanalysts could decipher their secret communication for years after the end of the Second World War[120].

During the almost 40 years since the release of the Ultra documents, the story of the Enigma and Bletchley Park has gained much popularity. There were numerous books, multiple documentaries and even blockbuster movies[121]. Sir Jeremy Isaacs, producer of the famous and groundbreaking British documentary series „The World at War" (aired in Great Britain 1973–74) said in an interview that he would have included the British code breakers in the series, but in a separate episode, if it had been unclassified at the time of the production[122].

Bletchley Park currently serves as a museum for the Ultra project[123], where some of the old Huts are restored to their original state and a special part of the exhibition is dedicated to the Enigma machine. In 2007, a replica of the Colossus programmable computer was finished and successfully deciphered the first message since the end of the Second World War[124].

Enigma machines have become valuable collectors' pieces. Models in good condition achieve prices up to $250,000 at open auctions[125]. There were several cipher machines, which used the principle of the Enigma machine, but with the rise of programmable computers cryptography was more and more shifted from electro-mechanical machines to computers. The programmable computers used in Bletchley Park were the first of their kind. As nearly all of the machines and their construction plans were destroyed directly after the war, they did not have a big direct impact on the evolution of

the computer. But many of their designers and engineers continued working in this field and therefore used their knowledge for further research.

Cryptanalysis and the use of deciphered intelligence got more and more important during the middle of the 20th century – especially during the Cold War. Not only the military and diplomatic use heavily increased, but also the field of industrial espionage evolved. Also with the rise of electronic telecommunications, the cryptographic and cryptanalytic methods made an immense advancement.

Congratulations,
you‘re done!

FOOTNOTES

[1] Welchman, Gordon: The Hut Six Story. Breaking the ENIGMA CODES. Kidderminster, 1997. p. 55

[2] Plaintext (also called cleartext) stands for the original not enciphered (clear) text of the sender and the final deciphered message of the receiver.

[3] Ciphertext stands for the encrypted text, which is transferred from the sender to the receiver

[4] Beesly, Patrick: Room 40. British Naval Intelligence 1914-18. London, 1982. p. 5-6

[5] Singh, Simon: The Code Book. The Secret History of Codes and Code-Breaking. London, 1999. p. 111

[6] ibid. p. 108-110

[7] Singh, Simon: The Code Book. p. 108-110

[8] Beesly, Patrick: Room 40. p. 206-208

[9] ibid. p. 112-114

[10] ibid. p. 115

[11] Winterbotham, Frederick: The Ultra Secret. The Inside Story of Operation Ultra, Bletchley Park and Enigma. London, 1974. p. 13

[12] Singh, Simon: The Code Book. p. 127-128

[13] Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 83

[14] Welchman, Gordon: The Hut Six Story. p. 42

[15] Hinsley, Francis Harry; Stripp, Alan: Code Breakers. p. 84

[16] Singh, Simon: The Code Book. p. 136

[17] Hodges, Andrew: Alan Turing. The Enigma. London, 1983. p. 168

[18] Welchman, Gordon: The Hut Six Story. p. 43

[19] ibid. p. 40

[20] Singh, Simon: The Code Book. p. 136

[21] Welchman, Gordon: The Hut Six Story. p. 47

[22] Stripp, Alan: The Enigma Machine. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 86-87

[23] ibid. p. 87

[24] ibid. p. 86

[25] Singh, Simon: The Code Book. p. 182

[26] The Abwehr (German for defense) was the secret intelligence service of the German Armed Forces High Command.

[27] Twinn, Peter: The Abwehr Enigma. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 124-125

[28] Singh, Simon: The Code Book. p. 148

[29] Milner-Barry, Stuart: Hut 6: Early Days. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 93

[30] Welchman, Gordon: The Hut Six Story. p. 98-99

[31] ibid. p. 99-101

[32] Singh, Simon: The Code Book. p. 162

[33] Welchman, Gordon: The Hut Six Story. p. 131

[34] ibid. p. 167

[35] Singh, Simon: The Code Book. p. 165

[36] Welchman, Gordon: The Hut Six Story. p. 167

[37] Milner-Barry, Stuart: Hut 6: Early Days. p. 93

[38] Stripp, Alan: The Enigma machine. p. 83

[39] Singh, Simon: The Code Book. p. 144

[40] ibid. p. 144-146

[41] Hodges, Andrew: Alan Turing. p. 170

[42] Welchman, Gordon: The Hut Six Story. p. 40

[43] Singh, Simon: The Code Book. p. 149

[44] Hodges, Andrew: Alan Turing. p. 172

[45] Singh, Simon: The Code Book. p. 152

[46] ibid. p. 153

[47] ibid. p. 153

[48] Hodges, Andrew: Alan Turing. p. 172 and Welchman, Gordon: The Hut Six Story. p. 212

[49] Singh, Simon: The Code Book. p. 154

[50] ibid. p. 156

[51] Hodges, Andrew: Alan Turing. p. 174

[52] ibid. p. 174

[53] Welchman, Gordon: The Hut Six Story. p. 215

[54] Singh, Simon: The Code Book. p. 158-159

[55] Milner-Barry, Stuart: Hut 6: The Early Days. p. 93

[56] Singh, Simon: The Code Book. p. 188-189

[57] Group Captain is the highest military rank below the general officer ranks

in the Royal Air Force (equivalent to the rank Colonel in the Royal Army).

[58] Winterbotham, Frederick: The Ultra Secret. p. 24

[59] ibid. p. 10-11

[60] ibid. p. 28

[61] Singh, Simon: The Code Book. p. 160-161

[62] ibid. p. 181

[63] ibid. p. 165

[64] ibid. p. 162

[65] Welchman, Gordon: The Hut Six Story. p. 46

[66] ibid. p. 58

[67] ibid. p. 58, 139, 90 and Dakin, Alec: The Z Watch in Hut 4, Part I. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 50-51

[68] Sale, Tony: Information flow from German ciphers to Intelligence to Allied commanders. URL: http://www.codesandciphers.org.uk/virtualbp/infoflow/infoflowie.htm (Checked on August 1, 2012)

[69] The Y-stations were responsible for intercepting German wireless radio communication.

[70] The TypeX was a British rotor cipher machine that was adapted so that it had the same inner wirings as the Enigma and could decode Enigma messages.

[71] Singh, Simon: The Code Book. p. 165

[72] ibid. p. 173

[73] Welchman, Gordon: The Hut Six Story. p. 239

[74] Singh, Simon: The Code Book. p. 174

[75] ibid. p. 177

[76] Welchman, Gordon: The Hut Six Story. p. 239

[77] Hodges, Andrew: Alan Turing. p. 196-197

[78] Singh, Simon: The Code Book. p. 183

[79] ibid. p. 183

[80] ibid. p. 184-185

[81] Hinsley, Francis Harry: An Introduction to Fish. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 145

[82] Hodges, Andrew: Alan Turing. p. 182

[83] ibid. p. 183

[84] Taylor, Telford: Anglo-American signals intelligence co-operation. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 70f

[85] An offline cipher machine only enciphers a message, but is independent from the transmission.

[86] An online cipher machine is able to encipher and also transmit a message.

[87] Hinsley, Francis Harry: An Introduction to Fish. p. 141

[88] SZ stands for Schlüsselzusatz, German for cipher attachment

[89] Smith, Michael: Bletchley Park Goes to War. In: Copeland, B. Jack: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford, 2006. p. 35

[90] Good, Jack: Enigma and Fish. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 149

[91] Copeland, B. Jack: The German Tunny Machine. In: Copeland, B. Jack: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford, 2006. p. 37

[92] ibid. p. 40

[93] ibid. p. 43

[94] ibid. p. 45

[95] Hinsley, Francis Harry: An Introduction to Fish. p. 141

[96] Good, Jack: Enigma and Fish. p. 149

[97] Hinsley, Francis Harry: An Introduction to Fish. p. 142

[98] ibid. p. 144

[99] Budiansky, Stephen: Colossus, Codebreaking and the Digital Age. In: Copeland, B. Jack: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford, 2006. p. 58

[100] ibid. p. 56

[101] Copeland, B. Jack: The German Tunny Machine. p. 50

[102] Budiansky, Stephen: Colossus, Codebreaking and the Digital Age. p. 58

[103] ibid. p. 59

[104] Copeland, Jack: Machine Against Machine. In: Copeland, B. Jack: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford, 2006. p. 65

[105] ibid. p. 69

[106] ibid. p. 74

[107] ibid. p. 77

[108] Generalfeldmarschall was the highest military rank in rank in the army of the Third Reich (only exceeded by Reichsmarschall Hermann Göring after 1940), equivalent to the rank Field Marshal in the British Army.

[109] Hinsley, Francis Harry: An Introduction to Fish. p. 146

[110] ibid. p. 147

[111] Hinsley, Francis Harry: Introduction. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 2

[112] ibid. p. 3

[113] Payne, Diana: The bombes. In: Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993. p. 135

[114] Hinsley, Francis Harry: Introduction. p. 6

[115] ibid. p. 9-11

[116] Winterbotham, Frederick: The Ultra Secret. p. xiv

[117] Singh, Simon: The Code Book. p. 188

[118] Air Field Marshal of the Royal Air Force is the highest military rank in the Royal Air Force while Chief of Air Staff is the most senior post.

[119] Winterbotham, Frederick: The Ultra Secret. p. xiv

[120] Singh, Simon: The Code Book. p. 187

[121] Enigma (2001) featuring actors Kate Winslet and Dougray Scott (Source: Internet Movie Database: Enigma)

[122] Isaacs, Jeremy: The World At War. Making the Series. A 30th Anniversary Feature-Length Retrospective (DVD). 2010.

[123] Bletchley Park Ltd.: Bletchley Park. National Codes Centre. URL: http://www.bletchleypark.org.uk

[124] BBC News: Colossus loses code-cracking race. (November 16, 2007) URL: http://news.bbc.co.uk/2/hi/technology/7098005.stm

[125] Perera, Tom: Enigma Cipher Machines For Sale. URL: http://w1tp.com/4sale/

BIBLIOGRAPHY

BBC News: Colossus loses code-cracking race. (November 16, 2007) URL: http://news.bbc.co.uk/2/hi/technology/7098005.stm (Checked on July 23, 2012).

Beesly, Patrick: Room 40. British Naval Intelligence 1914-18. London, 1982.

Bletchley Park Ltd.: Bletchley Park. National Codes Centre. URL: http://www.bletchleypark.org.uk (Checked on July 23, 2012).

Copeland, B. Jack: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford, 2006.

Hinsley, Francis Harry; Stripp, Alan: Code Breakers. The Inside Story of Bletchley Park. Oxford, 1993.

Hodges, Andrew: Alan Turing. The Enigma. London, 1983 (Vintage Edition, 1992).

Internet Movie Database: Enigma (2001). URL: http://www.imdb.com/title/tt0157583 (Checked on July 22, 2012).

Isaacs, Jeremy: The World At War. Making the Series. A 30th Anniversary Feature-Length Retrospective (DVD). 2010.

Perera, Tom: Enigma Cipher Machines For Sale. (January 12, 2012) URL: http://w1tp.com/4sale (Checked on July 23, 2012).

Sale, Tony: Information flow from German ciphers to Intelligence to Allied commanders. URL: http://www.codesandciphers.org.uk/virtualbp/infoflow/infoflowie.htm (Checked on August 1, 2012).

Singh, Simon: The Code Book. The Secret History of Codes and Code-Breaking. London, 1999.

Welchman, Gordon: The Hut Six Story. Breaking the ENIGMA CODES. Kidderminster, 1997 (Sixth impression with minor corrections, 2011).

Winterbotham, Frederick: The Ultra Secret. The Inside Story of Operation Ultra, Bletchley Park and Enigma. London, 1974.

IMPRINT

The following list shows the copyright owners and licenses of all images used in this publication:

1. U.S. National Archives (License: Public Domain)
2. Eloquence (License: Public Domain)
3. Shutterstock / markrhiggins
4. Bundesarchiv, Bild 183-2007-0705-502 (License: CC-BY-SA)
5. National Security Agency (License: Public Domain)
6. Bob Lord (License: CC-BY-SA)
7. TedColes (License: Public Domain)
8. Bundesarchiv, Bild 101I-769-0229-10A / Borchert, Erich (Eric) (License: CC-BY-SA)
9. Draco2008 (License: CC-BY)
10. Chris Nyborg (License: CC-BY-SA)
11. Tom Yates (License: CC-BY-SA)
12. Matt Crypto (License: Public Domain)
13. The National Archives (License: Public Domain)

The content of this book was initially published as a seminar paper for the course „Britain and Global Warfare 1914-1918, 1939-1945“, lectured by Dr. Finbarr McLoughlin at the University of Vienna in 2012. Content, design and layout by Christian Lendl.

About the author

Christian Lendl is a photographer and multimedia engineer in Vienna, Austria. He holds a Master of Science degree in Media Computer Science from the Vienna University of Technology, where he currently works on his PhD. Besides, he studies History at the University of Vienna.

For more information, please visit *www.lendl.pro.*

Vienna, 2012

ISBN 978-3-200-02924-8