Middle School Scholars' Newsletter

Spring Term 2022

Bletchley Park Special

Introduction

Two years ago, a few days before the first lockdown, Dr Burnand and I took the 3rd Year Academic Scholars to Bletchley Park. On the minibus home we received an email stating that all trips from then on would be cancelled, with Covid cases increasing. How the world has changed since then. What is still striking though, upon revisiting Bletchley Park, is the remarkable work carried out there during World War 2, and how it remains such an inspirational symbol of defiance, resilience and ingenuity at a time of national and global crisis. I think you'll agree these sentiments are well reflected in the following articles from our current 3rd Year Academic Scholars.

CONTENTS

Bletchley Park Trip Overview by William Walters

On the 21st of March, the 3rd year academic scholars embarked on an inspiring and enlightening excursion to Bletchley Park, the home to the Government Code and Cypher School (GC&CS) who were instrumental as part of the effort made by numerous civilians during the second world war. Centred around mathematicians, European linguists and classists, those who worked in Bletchley Park were responsible for the deciphering of codes sent to and from the axis powers: Germany, Austria-Hungary and Italy. Not only was Bletchley Park a major asset to the Allied Powers, but also saw the building of Colossus, the world's first programmable electronic computer constructed in the latter half of the second world war. Overall, this visit promised to be informative, engaging and motivating.

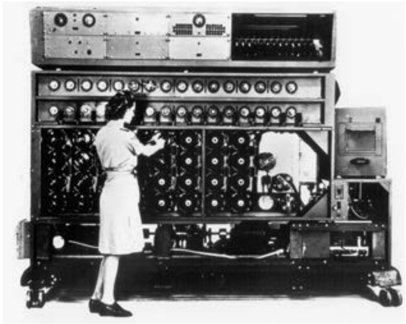
As mentioned previously, Bletchley Park was where the GC&CS were based during the course of the conflict from 1939-1945. Those who were present at the school were part of a small community of cryptanalysts heavily involved in code breaking, as to provide the Allied forces with the best possible chance of anticipating what the Axis powers would proceed with next. Some of the codebreakers at Bletchley Park include Alan Turing, who developed the first modern computer whilst here, and Bill Tutte, a mathematician responsible, with others, for the decoding of the Lorenz cipher system. This cipher system was used to carry Adolf Hitler's messages to German army officers; by enciphering this machine, the British along with their allies could anticipate where and when the German army would be at any time. This was achieved down to the Colossus computer, a culmination of smaller computers with the aim to decipher Axis powers', in particular German, messages about military tactics. Imperative breakthroughs in Bletchley Park also include the breaking of Enigma, a machine used to scramble German military messages into obscure cipher text, by using the Bombe Machine. Developed by Alan Turing and Gordon Welchman, this mechanism was developed to accelerate the process of breaking the Enigma code, so that the messages that were deciphered were valuable and current.

The contents of our day at Bletchley Park included guided tours, visiting the huts inhabited by those involved in codebreaking and deciphering differing codes. During the first part of our visit, we visited the museums at Bletchley Park and the mansion situated there. The former included information about the people working at this site, the recruitment process by the Government Code and Cypher School and artefacts such as a headset and Dispatch Rider, or more colloquially called the Don Rs. These motorcycles were responsible for collecting intercepted radio traffic and delivering vital information to Bletchley Park. During the afternoon, the entire group were involved in a guided tour of the stableyard and blocks at this location. The stableyard was the predominant place where Dispatch Riders and other vehicles would be parked and was where the first breakthroughs by Alan Turing and Dilly Knox into the ever-changing Enigma were made. Meanwhile, the blocks were the home of innumerable machines were placed, carrying out rapid analysis of enemy codes and cipher systems. Finally, the academic scholars were tasked with different codebreaking conundrums, all of which involved Morse Code and deciphering of letters to create important military communications. This experience emphasised how skilful those who worked at Bletchley Park were, and the extreme levels of pressure they were under during their time of codebreaking in this secret location.

Overall, the excursion to Bletchley Park was an enlightening one for all involved, illuminating crucial aspects of the war effort not situated on the battlefront. As COVID continues to diminish, hopefully trips like this one can be planned in the future more frequently. I would like to thank Dr Burnand, Mr Jamison as well as all the other staff members for making this outing possible.

What Did Bletchley Park Achieve During WW2? by Charlie Martin

Bletchley Park was a British government cryptological establishment in operation during World War II. Where Alan Turing and other agents of the Ultra intelligence project decoded the enemy's secret messages, most notably those that had been encrypted with the German Enigma and Tunny cypher machines.



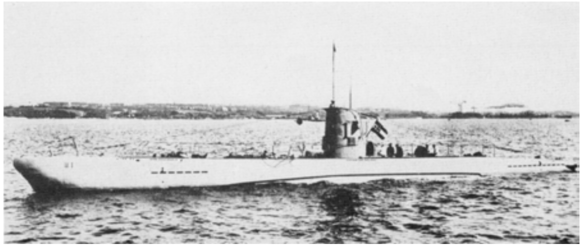
Bletchley Park was purchased by the Head of MI6, Admiral Hugh Sinclair in 1938. Later that year, at the time of the Munich crisis, several MI6 officers, and members of GC&CS (the Government Code & Cypher School), arrived from London and took up occupation. They referred to themselves as 'Captain Ridley's shooting party'. In September, the Germans made an important change to the procedure they used with their Enigma machines and in December they increased the number of rotors that can be used with the machine to five. As a result, the Polish were no longer able to read the cyphered messages.

In 1939 the main Japanese Fleet cypher (JN 25) was partially broken by GC&CS cryptographer John Tiltman. However, the main preoccupation at GC&CS was the German Enigma cyphers. In late July, the Polish Government disclosed to representatives from GC&CS and French Intelligence all the information they had about the Enigma machine. They also provided the details of the methods for breaking the cyphers that they had been using up until the end of the previous year. They made a gift to each of the two visiting parties of a Polish-made replica of the German military Enigma machine. GC&CS as a part of MI6 returned to Bletchley Park, Alan Turing and Gordon Welchman arrived on 4th September and reported to the senior cryptographer Dillwyn Knox. Initially, they were located in the 'Cottage' in the Stable Yard, a short distance from the mansion. Developing further a method for breaking Enigma cyphers, bequeathed by the Polish, John Jeffreys, with a small team of assistants, worked in the 'Cottage' to produce a vast number of sheets of card each with about 1,000 perforations made in predetermined positions. The original method had been invented by the Polish mathematician Henryk Zygalski (see picture), but for reasons of security the cards were referred to as 'Jeffreys sheets.' This task was completed by the end of December.

In early January 1940, Alan Turing took a duplicate set of the perforated sheets across to France to give to the Polish who, having escaped from their own county, were now working at the French Cypher Bureau. Later in the month, the perforated sheets were used to make the first successful break at BP a wartime Enigma cypher. On 29th January John Herivel arrived at Bletchley Park having been recruited by Gordon Welchman. He thought of a new procedure to speed up the decryption of Enigma messages. It was based upon the assumption that some of the German operators may be using a 'shortcut' when setting up their machines each day, which could be exploited. His idea was tried out but initially produced no useful results. In March, the first version of the Bombe arrived at Bletchley Park. This machine was intended to provide an alternative way of breaking Enigma messages independently of the weakness in the German procedures currently being exploited by the perforated sheet technique. However, the performance of the machine proved to be disappointing and it was of only limited operational value. In April, the German armed trawler Polares was captured and provided some valuable information about how the German Navy was using its Enigma machines. This enabled a small number of German Naval Enigma messages to be read; the first to be broken since the beginning of the War. On the 1st May, the German Army and Air Force changed their Enigma operational system, and consequently, it was no longer possible to break Enigma messages by means of the perforated sheets. Bletchley Park had no other regular procedure to carry out the work and this was a cause for great concern. On the 10th May, the Germans launched their offensive against France. The number of Enigma signals rose dramatically and the German operators were kept remarkably busy.

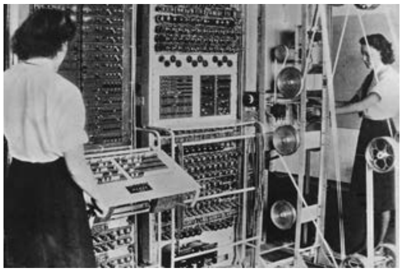
Providentially some of them now began to make the mistake that John Herivel had earlier predicted might occur. His procedure, known as the 'Herivel Tip' was now invaluable, and together with additional clues arising from other lapses in German security, allowed the codebreakers in Hut 6 to resume the breaking of Enigma messages. On the 8th August, an updated version of the Bombe was delivered. It had additional circuits incorporated in it, known as the 'diagonal board' that had been devised by Gordon Welchman. This new machine (named the 'spider' bombe) was a huge improvement on the original version. From the end of August, the spider bombes provided the principal means for breaking Enigma cyphers for the rest of the war. The problem of producing these machines in sufficient numbers falls on the shoulders of Harold ('Doc') Keen the chief engineer at the British Tabulating Machine Company. It was realised that for some time that the breaking of German Naval Enigma cyphers was not possible until copies of the codebooks used in conjunction with the Enigma machines were captured. In September, a Royal Navy Intelligence Officer (Ian Fleming, the post-war author of the James Bond Books), put forward a plan for a dramatic operation to capture a German rescue boat operating in the Channel. This plan was later abandoned as it was impractical.

In March 1941 Bletchley Park broke the Italian Navy cyphers, using a technique known as ‘Rodding’, applied before the war by Knox. This enabled the British Fleet to achieve a dramatic victory over the Italian Fleet at the Battle of Cape Matapan. This was the first major success in the war that can be attributed to the codebreakers of Bletchley Park. In May, the capture of the German weather ship ‘Munchen’ and of the U-boat U110, provided sufficient information to enable codebreakers in Hut 8 to read German Naval signals within a few hours of their transmission, this had not been possible before. In June, the Germans established their first army communication link using a new cypher system based on a machine known as ‘Lorenz.’ It was much more advanced than Enigma and the breaking of these cyphers (given the security name ‘Fish’) presented Bletchley Park with some major challenges. In September Winston Churchill made an official visit to Bletchley Park to thank the codebreakers for their invaluable work. He called them his ‘geese that laid golden eggs and never cackled.’ Dilly Knox and his group, now known as ‘ISK’ (Intelligence Services Knox), begin the task of discovering the unknown design of the ‘Abwehr’ Enigma. This was a special machine used by the German Secret Service. By the end of the year, they had successfully completed it. (Later in the war this work contributed to the success of several clandestine operations intended to deceive the Germans about future Allied operations. In October 1941, a group of some of the most senior cryptographers wrote directly to Churchill, to complain about the limited resources they had available to deal with the huge growth in the work at Bletchley Park.



In January 1942, the German Nazy issued its new codebook to the U-boat fleet for use in conjunction with Enigma machines. Shortly after this they also began to use an updated version of the Enigma machine that incorporated an additional 4th rotor. Bletchley Park was not able to respond to the combined effect of these two changes and this new formidable cypher known as ‘Shark,’ was not broken for many months. In October, the current U-boat codebooks were captured from U-559, but at the cost of the lives of two British sailors. After the code books arrived at Bletchley Park, an intense effort was made to break the ‘Shark.’ After a brief time, the codebreakers were successful and were again able to read the U-boat signals. In November after Bletchley Park had some limited success in breaking the Lorenz cyphers using the slow hand methods. The mathematician Max Newman puts forward the revolutionary idea that some of the considerable work involved might be carried out very much faster by using special machines.

In June 1943, the first machine to be used to help break the ‘Fish’ cyphers arrived and it was given the name ‘Robinson’. However, the machines of this type were found to be very unreliable. As early as 1937, Alan Turing had developed a theory about the universal computing machine that could carry out calculations when it was fed information on a strip of paper. Under the aegis of Max Newman, a senior engineer from the Post Office Research Station (Tommy Flowers) built a new all-electronic machine to replace them. This was the start of Colossus and the birth of the computer age. In August, the codebreakers in Hut 8 reported that there were now enough bombes and message cribs to enable the U-boat cyphers to be broken with minor delay. This situation continued right up to the end of the War. By the end of the year there were about one hundred bombes of several types in operational use. (Almost all of these being located in ‘out stations.) It was recorded that up to the end of 1943 the bombes had been used to recover a total of 9,064 Enigma keys.



The completed sections of the first Colossus machine (see picture) had been delivered at the end of 1943. After assembling them, the initial tests prove to be an outstanding success. In order to be able to respond to certain changes that had been made to the Lorenz cypher machines by the Germans, a huge effort was made to produce a second and much faster Colossus machine. It was vital for this second machine to be ready before the D-Day landings. Flowers and his team had the machine running by the 1st June. On D-Day ,6th June, following the landings, up to 18,000 messages were being decyphered daily at Bletchley Park by 8,000 operatives.

By 1945 approximately 8,600 staff were working at Bletchley Park, with a further 1,500 at nearby locations. As the German threat diminished, increasing numbers of people were moved on to deal with Japanese codes and cyphers. They were given a short ‘crash’ course in Japanese at a ‘school’ that had been set up in Bedford, after which they were to be sent to Colombo, where most of the British work on Japanese codes occurred. The tenth Colossus machine was delivered to Bletchley Park. (Colossus number eleven was nearing completion when the War in Europe ended in May). By the end of the war the total number of operational bombes exceeded 200, while the total number of Enigma keys that had been recovered was over 20,000. The number of staff involved in operating these machines had grown to about 2,000 of which 1,676 were WRNS (The Women's Royal Naval Service). The end of the war on land brought about the surrender of the German Navy. On 8th May 1945, an Admiralty signal ordered all U-boats to surface, report their position and sail to designated British ports. 221 U-Boats chose to ‘scuttle themselves’ (sink their ship deliberately) instead and 150, including 18 of the newest models sailed under escort to British anchorages. Today Bletchley Park's work goes on at the Government Communication Headquarters (GCHQ) in Cheltenham.

The History, Function, and Cypher-Breaking of the Enigma Machine by Benedict Robinson

Introduction

In 1915, two Dutch naval officers developed a rotor-based cypher machine for the Dutch War Department, which is described in a paper by Karl de Leeuw, discovered in 2003. This provided the basis for the Enigma, in design and function. In 1918, the original design of the Enigma Machine was made by Arthur Scherbius, in order to protect communications in the banking industry. It was first launched commercially in 1923, but was adopted by government and military organisations as well. After that, it was used by the German navy, army and air force before and during the Second World War, along with the Italians and Japanese.

Design and Function

The Enigma, just like other rotor machines, was made up of mechanical systems, and electrical subsystems. It consisted of a set of rotating disks along a spindle, changing the letter from the original entered on the keyboard to a different letter, according to the combination of the wheels, which is changed each day, to try to ensure security. There was a keyboard for input, and also lamps, corresponding to each letter, which displayed the changed letter. On later models, as well as the models used in WW2, there was a plugboard (Steckerbrett) facing the user, which was used to complicate the cipher further, making it extremely difficult to solve, as there were 150 trillion different combinations which could be formed, between the plugboard and the rotors. The plugboard switched letters manually, before they were scrambled in the rotors on the spindles, and there were ten connections on the plugboard during WW2.

The combinations were provided manually to everyone using an Enigma machine every day, meaning that they could all decipher all of the other messages from the other machines, without their enemy even having the right letters to decode.

The rotor settings for month 649.

Operation

The Enigma machine was operated relatively easily, simply by pressing a key on the keyboard, and noting down which letter lit up on the lightboard. Even if you pressed the same key twice in a row, it would never come out as the same letter on the lightboard twice in a row, because the rotors moved every time that a new letter was pressed. Due to the fact that enigma machines do not transmit messages, the message which a cipher clerk had written down would be transmitted via radio to another radio operator on the receiving end of the message.

Cryptanalysis (code-breaking), the Bombe and The Colossus.

Before World War II, Polish cryptanalysts such as Marian Rejewski were attempting, and succeeding, to crack the cipher of earlier Enigma machines, but they hadn't consistently cracked the plugboard model of the machine until WW2.

Developed by Alan Turing in 1939, the Bombe (see picture) machine was an electro-mechanical machine, used to decipher the rotor order for each day of the Enigma machines. It was also used to determine the pair of letters on the plugboard (stecker partner). It examined all 17, 576 possible positions for the wheels, and effectively narrowed down all of the options to a point at which it was manageable for the codebreakers to try them themselves. On the Bombe itself, there were rotating drums, wired to each other and the rest of the machine identically to the Enigma itself, the only difference being that there were 104 contacts between each drum and the rest of the machine, because the input and output and output contacts for the left and right hand sides were separate. This meant that a set of scramblers could be connected in series with 26-way cables. A cryptanalyst would prepare a crib (piece of deciphered text, known to be in the message, such as the start of a weather report), for the Bombe, for comparison with the cipher text itself. The cryptanalyst would then compile a list (menu), of all of the connections of the panels on the back of the machine, and which letter's pair was sought. Due to the nature of the plugboard, no letter could be connected to more than one other letter, so, when there was a combination of two different letters seeming to be in a pair in the cipher text, the Bombe would move on, only stopping when there was a viable combination of letters, thereby finding the correct combination. However, sometimes there were false stops, when a letter which wasn't in the menu was detected as being in a pair. The cryptanalyst would eliminate such stops. When there was a true stop, the other plugboard connections and the rotor settings would be worked out, before the cipher was tested on a mimicked Enigma, the Typex machine. To avoid false stops, wasting Bombe time, Alan Turing made extensive probability analysis (without electronic help), to determine the maximum number of true stops on a wheel.

The hard-working nature and brilliance of the cryptanalysts at Bletchley Park, such as in this example, along with the incredible functionality of the Bombe machine and other technological inventions, allowed them to crack the code of the Enigma, most likely shortening the war, saving millions of lives.

Bletchley Park: What Life was Like Under the Radar by Lucas Ord

Introduction

Bletchley Park was an innovative, life saving and invisible institution in war time, saving possibly millions of lifes at the front. Some historians estimate that the war was shortened by two years, saving countless lives. But how was living and working at Bletchley, living lives officially you never lived?

The Start of Code Breaking in Bletchley

Due to the imminent threat of war, after 19 years based in London, 1939 was the year that the Government Code and Cipher School (GC&CS; see picture) moved to Bletchley Park. This was because Commander Alastair Denniston's (the leader of GC&CS) boss - Admiral Sir Hugh Sinclair, Chief of the SIS (Secret Intelligence Service) decided to move the main base for the GC&CS headquarters. So there is room to grow and it is in a remote and secure location. He decided on Bletchley, and discreetly bought it from Hubert Faulkner, using his own name to hide intentions. To stop the locals becoming suspicious of the work being done there, everyone is told that the government has bought Bletchley, for “air defence purposes”. In September 18th 1938, Hitler demanded territory in Czechoslovakia, war now seems inevitable causing GC&CS to send more people from London to Bletchley Park, preparing for the imminent conflict on the horizon. For three weeks roughly 70 staff work in the mansion in Bletchley. When locals started inquiring about what was happening, they were told that staff are here for the pheasant shooting season. Work started immediately: it was cramped and chaotic, causing little work to be done. Fortunately war was avoided after Hitler was permitted his seizure of land, however this acted as a test run, and better preparations were put into place for the not so far “next time”.

Working conditions

In the early days of 1939 GC&CS started hiring people to create a better and more efficient team, expanding the size of the organisation by 4 times the original. Then this newly found and scouted team of only the best linguists, mathematicians and classicists alike were all called in on the 4th September 1939, the day after Britain declared war on Germany. However, even with a much more organised approach the mansion was too small to cope with such a large team causing more buildings to be constructed. A solution to this problem was already in the works, with four of the many famous huts already built and others starting to appear.

As many know today, no war is like the “game” described in Jessie Pope’s poem, ‘Who's for the Game?’ The same can be said in Bletchley. Work days were long with people working on 8-hour shifts, 8 am to 4 pm, 4 pm to midnight, and midnight to 8 am. With many going to work in the dark, working in the dark due to black out blinds, dark conditions or due to it being night, and then leaving in the dark. This was all due to the work being done there, and there was a lot to do. The workload never seemed to slow as the 3 rotor Enigma was capable of being set to approximately 159,000,000,000,000,000,000 possible combinations, and it changed each day.

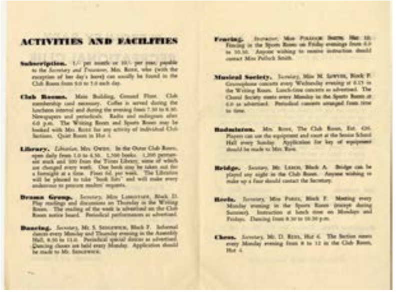
Jean Evans, Née Birtles, women’s Auxiliary Air Force, Bletchley Park 1942 - 1945 reported: “They were numbered, the signals, from 1X to 5X. And if a 5X came through, you just dropped everything and typed it out because it was top secret urgent. The others were sort of… not so important I suppose. But as i say, if you got a 5X you really had to get it out as quickly as possible”

A Lot of work needs a lot of people, and Bletchley was no different. At its height (early 1945), Bletchley Park employed close to 9000 people, up to three-quarters of whom were women. Work was close and somewhat chaotic, with even the expansion of the Huts not large enough, the people there had to make do. The huts were not in the best condition seen today at the open Bletchley Park. Many were dark and cramped, with the ones with windows often under blackout. Hut 11 and 11a were specifically built for the BOMBE machines, Hut 11a also became a training centre for the Women’s Royal Navy Service, who operated the machines. They recall the Huts being incredibly hot and very noisy. This room, due to this, was nicknamed the “hell-hole”. The tough conditions makes what was achieved at Bletchley more incredible.

Lastly, the secrecy is clearly the largest part of Bletchley Park. Nothing they did there was to leave the site, with death on their doorstep if it did. Perpetrators would face up to 7 years in jail for an accidental leak, or put to death for treason if the leak was found purposeful. Secrecy was at the centre of all life at Bletchley. Even now, some people, as we were told, are only now finding out that their husband or wife also worked at Bletchley Park.

Rozanne Colchester, Née Medhurst, foreign Office Civilian, Bletchley Park (1942-1945) reported: “We simply went through a pep-talk… Professor Boase told us it was the utmost secrecy, the work, and we were never to talk to each other about it, we must never go into each other’s huts, we must never ask anybody why they were doing what they were doing, etc, etc. And if we were caught really talking about it in the town or anywhere else, we were quite likely to be shot! So that was rather chastening news.”

Bletchley Park Recreational Club



ACTIVITIES AND FACILITIES

Subscription.

Club Rooms.

Library.

Drama Group.

Dancing.

Fencing.

Musical Society.

Badminton.

Bridge.

Reels.

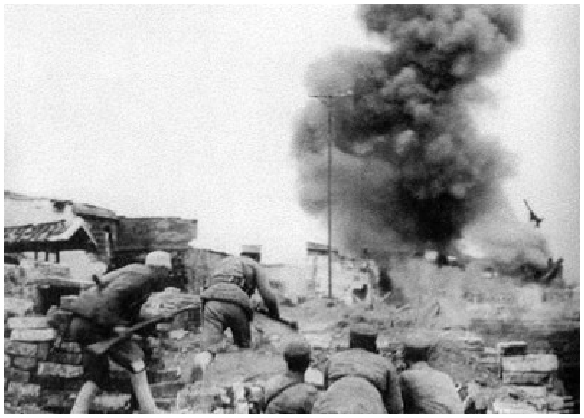
Chess.

Even with incredibly tough working hours the people working at Bletchley Park still found time to try to relax. The Bletchley Park Recreational Club was created in October 1940 under Captain Stanley Edgar, it was to “to provide, for all members of Bletchley Park, facilities for recreation and amusement which otherwise do not exist in Bletchley”. Shown here is the list of activities and facilities given to all people at Bletchley, advertising to get people to join the club. As seen here, however, people could play squash, tennis and table tennis. As well as this concerts would be held, often played by the music club, but occasionally by external sources.

Conclusion

In conclusion, conditions at Bletchley were hard, like everything in war. However, given the tough conditions the workers did what was thought to be impossible: to save potentially millions of lives on the front. Although the amount of work was massive, the people there had many activities to do and try, when time off was found. Except these breaks were often spent resting, for a long, dark day ahead.

Enigma: An Exploration by Benedict Donald



In the Second World War, German military leaders and commanders needed to send messages to each other and their troops. The easiest and fastest way to do this was to use radio, however enemy forces can easily tap into radio signals and intercept the information. This would have given the enemy an advantage because if they know where German troops would attack, they can fight back more easily. In order to combat the information being stolen, Germany needed to use a method of encrypting the messages, however, the encryption would need to be complex, as just a simple one would be easy for the enemy to decipher. If Germany managed to do this, then when the enemy got hold of the messages, they would make no sense since they were just a scramble of letters and no way to translate them.

Germany decided to use the Enigma Machine to encrypt their messages, a machine that looks like a typewriter that consists of several components, each which makes the code created much harder to decipher. It essentially works by typing in your message into the keyboard and watching letters on a lampboard light up. The people at each end of the communication line would need an Enigma Machine each, with the person sending out the messages typing the message into the machine and receiving gibberish, and the person at the other end typing in the gibberish and getting the original message. An Enigma Machine was typically used by two people, one person typing in the message and the other person noting down the encrypted message that was given to them by the lampboard. The radioed messages were usually sent round via morse code.

The Enigma Machine was first devised in 1918 by a German engineer called Arthur Scherbius. It was originally designed for commercial purposes until the military first used it in 1940 for communications in a battle vs France. It is one of the most complicated encryption machines ever, so complicated that there would be 158 000 000 000 000 000 000 (quintillion) possibilities that you could program the machine in, making it impossible to crack by hand, especially since German commanders were ordered to change the settings of the machine every day.

How does the machine work?

Enigma works by an electrical circuit - when you press a key on the keyboard, it sends an electrical current throughout the various components of the machine, scrambling up the letters, and into the lampboard, which makes one of the letters light up on the lampboard.

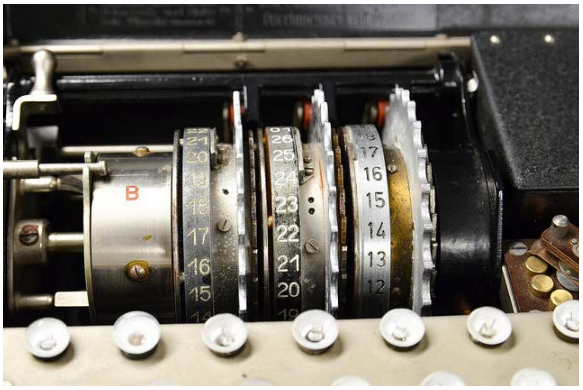
The circuit starts with a large battery, sitting in the right-rear corner of the machine. After that, it travels through wires into each of the 26 key switches. A key switch is made up of 3 layers of metal rectangular-shaped tabs, laying on top of each other, which are each separated by a layer of foam, at the rear end of the key switch. These layers of foam prevent the electrical current running between the metal layers. Each metal tab is connected to a different component of the machine through wires: The top tab to the light bulbs in the lampboard, the middle tab to the plugboard (a component which can swap two letters with each other), and the bottom tab to the battery. In the key switches' original position, it has the top tab touching the middle tab at the front end, meaning that the current coming from the battery would go into the bottom tab and the circuit would end. When you press a key, the middle tab is pushed down into the bottom tab, allowing the circuit to run through the middle tab and over to the plugboard.

The plugboard is on the front face of the machine, and it is simply a flat board with each letter of the alphabet on it, arranged like a keyboard, with two holes for each letter, one above the other. You can put in a set of two plugs with two pins each connected to each other by a cable. Without any plugs in the plugholes, the current comes into the plugboard from the key switches through the top plughole. Next, it goes through the shorting bar, a piece of metal connecting the top and bottom holes. Then it comes back out of the bottom hole and into the rest of the circuit. However, when you put a plug in the pin pushes the shorting bar back so it doesn't touch either the bottom or top plughole, instead the current goes through the cable in the plug and into the other letter that the plug is connected to, then out through the bottom hole and back into the rest of the circuit. The plugboard only came with 10 sets of plugs, meaning that 6 letters were not connected with any other at all times.

After the current exits the plugboard, it goes through the rotating wheels. The Enigma Machine comes with five of them but only three of them are used at once. Each wheel comes with the numbers one to twenty-six on the side, representing the letters (1 is A, 2 is B, etc.), and 26 contact points on either face for the circuit to run through. The current comes in through the right side and into the rightmost wheel through the contact point for whichever letter came out of the plugboard. However, all the wires are scrambled in the rotating wheels, so what comes in as a letter, would come out as any other letter. This happens in every wheel - if an "H" got turned into a "C", the "C" would change into something else again on the second wheel, then again on the third. After the third wheel, there is what is called a reflector - essentially a wheel but with only one side, where every letter paired up and wired to another letter, so if a "G" came into the reflector and was paired with "O", it would come out as an "O", or vice versa. After that the current goes back through all of the wheels again, changing each time, before it comes back out of the first as a completely different letter to what it was before.

Next, the current runs from the rotors back to the plugboard for a second time. Here it does the same thing it did before - if the letter that came out of the rotor was connected to another letter in the plugboard, they swap and if it wasn't, it stays the same. After that it goes back to the key switch for the new letter and into the middle tab. The middle tab is not being pressed down here, since it is a different letter to the one you pressed on the keyboard after all of the wire scrambling. This means that the middle tab is connected to the top tab which runs to the lampboard. This makes the lamp for the new letter light up, then the circuit runs through the lampboard and back into the battery to complete the circuit.

As well as the rotors scrambling the letters, they also move mechanically. When you press a key, the one on the right turns so that the top of the wheel turns to face further to the rear. It only moves by 1 number each time you press a key, but this adds to the complexity because it means that the setup is different every time you press a key. This is what makes the letter different each time, even if you press the same key twice. When the right wheel has moved 26 times this allows the centre wheel to turn once. When the centre wheel has moved 26 times, this allows the left wheel to move once.



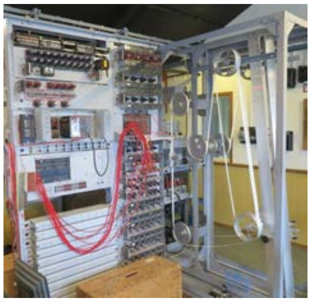
So that the messages could always be decrypted accurately, the German soldiers and commanders were issued a sheet of which letters to connect with which on the plugboard and how to arrange the rotating wheels for their starting position. This was because if they were in a different order, they wouldn't be able to decrypt the message so it would be useless for them. These sheets of starting instructions were given out monthly, but the preparations changed daily, so there would be a maximum of 31 days on each sheet.

The Enigma Machine is maybe the most complex encryption machine ever, because it has so many possibilities that you can arrange the settings in. It was first decrypted by a Polish Mathematician called Marian Rejewski in the 1930s, but the Germans changed the code slightly to make it harder for them. The more advanced code was decrypted by Alan Turing in 1942, which allowed the workers at Bletchley Park to find out the Germans war tactics. This helped the British greatly and saved countless lives.

The Creation of the First Large Scale Electronic Computer by Kit Rice

One of Bletchley Park's most well known achievements would have to be the creation of the first running large scale electronic computer, the Colossus. The Colossus was created to be able to run the necessary calculations to crack the Lorenz SZ40's chi wheels, the device used by the German Army High Command to protect and carry high level communications between German Army Headquarters in Berlin and the various Army Groups Field Marshals and Generals on all battlefronts. The chi wheels they deciphered could then be used by the code breakers to decipher the messages sent. There were two different types of code being received enigma in morse and 'fish' transmissions, as they were known, in electric teleprinter technology. The importance of deciphering these codes was apparent as various methods were created to decipher them by hand, one of these being Tutte's message. This was done by comparing two different pieces of paper with the code in teleprinter dots and crosses, counting for how many times they had dots and crosses in the same place. This method however was incredibly impractical due to involving calculations, that done by hand would take an incredibly long amount of time; Max Newman once said it would take hundreds of years for a long-ish sentence. Newman however saw the possibilities of this method and suggested speeding it up using a machine. This idea came from a device created by Wynn-Williams, who worked at Cambridge University, which was a high speed electronic counter used to count rapid subatomic particle emissions. Newman knew of the work and suggested its uses and, with Williams and the Post Office Research Station at Dollis Hill, created a suitable machine for the job at hand.

Construction of this ingenious machine began January 1943 and the first prototype reached Bletchley Park that same June. The device was mainly operated by the 'Wrens' (WRNS or Womens Royal Naval Service), and was soon nicknamed by them the Heath Robinson, after the cartoonist that drew fantastic machines. The Robinson (see picture) was a behemoth of a machine with a large steel frame resembling a bed, hence its nickname 'bedstead', which had two pieces of teleprinter paper wound round the ends. These tapes were moved by wheels and could move at 2000 words per second, but due to this speed they would often tear and rip causing severe damage to the machine itself that would also frequently break down. The patterns would be read and then electric pulses would be sent to the Robinsons logic unit, designed by Tommy Flowers, which would then use the counting system and display the results. Despite its initial success the device was far too impractical and further advancements were made to create a more effective machine than the current.



The prototype for the Colossus was delivered in the following January of 1944. It was soon clear how superior the device was when compared to the previous Heath Robinson, being able to operate at 5000 characters per second, later more improved versions even quintupling that to 25000 characters per second. As well as this only one tape was needed due to the Colossus providing the chi wheels electronically, making it more reliable and having less breakdowns. Furthermore, it was faster as well due to its use of electronic valves, superior to the electro-mechanical relays that the Robinson used, the only electronic part of the Robinson was its counting system. The output of messages doubled and continued to rise as the people working in the Newmanry and the Testery became more familiar with the device. These two parts of Bletchley park worked closely together to decipher the Lorenz, the Colossus at Newmanry deciphered the starting positions of the chie wheels, other devices then stripped away the letters that had been added by the Lorenz and sent the resulting de-chi to the codebreakers at Testery to finish of the decoding process by hand.

The arrival of the device was just on time as the Germans had recently added a device on the Lorenz that made deciphering them by hand impossible. However despite how amazing the Colossus was it was clear that more were needed to keep up with the rapid rate of Germany communications. The second Colossus parts arrived in May the same year and Tommy Flowers said that it would be operational by 1st June, however unlike what was said, in the early hours of the same day it was still suffering from problems, Bill Chandler was left alone to try and fix the problems and was successful in his endeavours, despite a radiator bursting, creating a pool of water around the computer. The problem was still not fixed the next day causing the Women operating it to have to wear heavy gumboots. This was just in time as the invasion of France was to begin on the 6th June, due to this the Germans had once again increased the security of their messages and increased the change of chi wheels from monthly to daily, a radical change. Colossus II was essential in keeping up with these messages. By the end of 1944 there were 6 Colossi active and when the Germans surrendered there were 9. Colossus has had a lasting impact not only on the war but also the world as we know it, the Newmanry was the first electronic computing facility and those like it would not be seen till the 1960's, two Colossi were also transferred to the University of Manchester, soon its successor Baby was created, the ancestor and inspiration for all modern all-purpose computers.

Alan Turing - A Short History by Tom Saunders

The men who defeated the Axis powers without ever setting foot on occupied territories, went into battle or handled a firearm. This man is Alan Turing, a Mathematician, Cryptanalyst and Computer Scientist. His work and the work of others around him at Bletchley Park to break the German cipher, Enigma, almost certainly saved Britain from Nazi Germany and won the Allies World War 2.

Education

Alan Turing was born on the 23rd March 1912 to a fairly wealthy family; his father worked in the Indian Civil Service. He showed his genius early and the headmistress at his prep School recognised this and recommended that he attended Sherborne School in Dorset (see picture). The first day of School coincided with the 1926 General strike and Turing, determined to attend, rode 60 miles on his bike unaccompanied. His time at Sherbourne was not the happiest time in his life and did not fit in. He enjoyed and thrived in Maths and the sciences, however he struggled with Classics, which was the main focus in Sherbourne and as such he was labelled as a subpar student. HIs headmaster wrote to his mother father saying 'If he is to stay at Public School, he must aim at being educated'. However, Turing found a friend in fellow pupil Christopher Morcom. Morcom was an inspiration for Turing and he is now known as Turing's 'first love' however their friendship was cut short by Morcom's death of Tuberculosis in February 1920 at the age of just 18. The death of his dearest friend inspired him to work even harder on the complex scientific and mathematical problems of which he had worked on with Christopher. Turing's relationship with the Morcom's did not end with the death of Christopher, but he frequently sent letters to Christopher's mother expressing his sorrow around the anniversary of his death and Christopher's birthday. After a troubled time at Sherbourne, he attended King's College, Cambridge (see picture) to study Mathematics of which he was awarded first class honours and was made a fellow of the University at the age of just 22 on the strength of his dissertation. In 1936,he published a paper which is known today as the foundation of Modern Computer Science and mentioned the idea of a Universal Computer which was capable of running any program. In that same year, he left the UK and went to Princeton University to obtain a PhD. In his course, he became more interested in Cryptanalysis and his dissertation introduced the concept of Ordinal logic and relative

computing. In 1938, he returned to the UK and on the 4th of September 1939, he walked through the gates of Betchley for the first time.

Wartime

The importance of Alan Turing's work at Bletchley Park cannot be overstated. His work for the GC&CS (Government Code and Cipher School) required Turing to sign the Official Secrets Act and his unconventional solution to solve Enigma and other German codes by using machines, saved countless military personnel. Turing took inspiration from the Polish 'bomba kryptologiczna' and together with Mathematician and Codebraker Gordon Welchman produced the Bombe Machine, which became one of the primary tools in the inventory to solve Enigma. The Bombe Machine searched through possible rotor settings and bearing in mind that it would take a human 1.8 billion years to search through every possible combination of Enigma, the Bombe proved vital in cracking Enigma. Enigma was finally cracked after Turing and his colleagues realised that they could significantly cut down the possible number of possible combinations entered into the Bombe machine by inputting certain letters that they knew would be in there, for example they realised everyday at 6 O'Clock the Nazi's would send a weather reoprt and as they realsied that 'Weather', 'Report' and 'Heil Hitler' would be in that message and so the Bombe machine cracked the rotor position each day. However, That was not the end as they had to keep the solving of Enigma secret otherwise the Germans would realise Enigma had been cracked and they would change the cipher. Turing became instrumental in Operation Ultra which was the cover up in solving Enigma and essentially deciding who lived and died but never to save too many and alerting the German Military that they had cracked Enigma. The extent of the trickery was immense and even high ranking Government officials were unaware that Enigma had been solved. The solving of Enigma was not Turing's only achievement at Bletchley and he created a way to solve the supposedly uncrackable Lorenz machine that was nicknamed Tunny. Turing's solution was called Turingery and his solution was a way of working out the settings of the rotors. Max Newman and Tommy Flowers, with indirect help from Turing, solved Lorenz by creating the world's first programmable digital computer called Colossus. Turing also helped the Americans to develop secure lines which enciphered speech electronically while speaking on the telephone.

Post War

The outstanding achievements of Bletchley Park were never recognised publicly in Alan Turing's lifetime but his work did not stop at the end of the War. In March 1946, Turing developed the Automatic Computing Engine which was the world's first computer which was capable of storing memory and able to run almost limitless applications. He became increasingly interested in the theory of life and whether Machines could think. However, throughout his life, Turing had homosexual tendencies and in 1952, he was prosecuted for gross indecency and he was offered a choice, imprisonment or hormonal treatemnet, or in effect Chemical Castration. Turing chose the hormonal treatment and he was injected with Oestrogen to 'feminise' the body. The treatment was extremely painful and in 1954, his security clearance was removed and his work became increasingly hindered by Police and their surveillance. On the 8th June 1954, Turing's housekeeper found him dead with a half eaten apple on his bedside table. The assumed reason was that he had killed himself, however there is sufficient evidence around the house that his death was an accident.

Alan Turing is a hugely important figure in modern history and his work at Bletchley Park certainly saved countless serviemen's lives. However, his work was never appreciated in his lifetime and only once the secrets at Bletchley Park have come out, have we truly been able to see how important he was. His persecution as a Homosexual warranted an official apology from the Prime Minister Gordon Brown in 2009 and the official pardon of everyone convicted under similiar 'gross indecney' laws and this pardon became known as the 'Turing Law'. His actions during the war was Immortalised by the film' The Imitation Game' (see picture) starring Benedict Cumberbatch as Alan Turing. A BBC programme found that Alan Turing was the most influential figure in the 20th Century and I am inclined to agree as he founded and laid foundations for Modern Computer Science and saved countless lives.

Methods of Encryption and Decryption used during WW2 by James Longworth

The work done at Bletchley Park during the second world war was essential for the D-Day landings and victory in Europe, as well as integral for Allied intelligence throughout the whole war. There, codebreakers such as Alan Turing, Gordon Welchman and Bill Tutte worked tirelessly to decrypt messages sent by the Nazi forces, in order to give vital intelligence to the allies. The Nazi forces used various methods of encryption, including the Lorenz, and most famously the Enigma Machine. The Enigma Machine was invented in 1919 by Hugo Koch, and was regarded by the Nazis as unbreakable. Every month, the Enigma operators would receive information with the settings for the Enigma Machine for each day that month. This information would tell them which rotors to use, the starting settings for the rotors, and the plugboard settings. The Enigma Machine had multiple stages of encryption: firstly, the plugboard had ten wires, each one connecting a certain pair of letters on a given day. This then swaps those two letters' occurrences in the text. The next setting is which rotors to use. The Enigma Machine had three rotor slots, and the information would tell the operator which rotors from a set of 5 to use for which slots. The final piece of information was the starting orientation of the rotors. Each time a letter is typed, the one or more of the rotors rotate, meaning that the next letter has a different encryption. For example, even if you typed ‘a a’, it could come out as ‘t i’. Once the message was encrypted, it was sent in morse code via radio, and at the other end another Enigma Machine with the same settings would be used to decrypt it. However, allied forces were able to listen in and note down the messages, before transporting them to Bletchley Park to attempt to break the Enigma code. This was a difficult job, as there were 158,962,555,217,826,360,000 possible combinations, and they had to break it in a single day, because the settings changed every 24 hours.

After the German army started using the Enigma Machine in the 1920s, the Polish Cipher Bureau aimed to break it due to the threat that they faced from Germany. One Polish codebreaker, Marian Rejewski, who joined the Bureau in 1932, was asked to work on cracking the enigma code. Rejewski worked out various methods of decrypting it, exploiting the fact that the first three letters of the code were the same as the second three, but as German forces upgraded their procedures his original methods became redundant. After his previous methods became useless, Rejewski created the ‘bomba kryptologiczna’. Each bomba contained six sets of enigma rotors, one set for each possible position of the six letter key. Six bomba machines were created, one for each of the possible rotor orders (at the time the enigma only had three rotors). However, in late 1938, the German forces introduced two more rotors, increasing the number of possible rotor orders from 6 to 60, and the Polish Cipher Bureau did not have the resources to create another 54 bomba machines.

The main method of decryption used by the codebreakers at Bletchley Park was ‘cribbing’ - searching for words/phrases that were expected to appear in the text, such as a weather report or ‘Heil Hitler’. One example of this was the ‘Eins Catalogue’ - a catalogue of all the 17576 ways that the German word ‘Eins’ (German for ‘one’) could be encoded. The codebreakers would then manually search through the encoded message for one of these occurrences, and if found, those could be the orientations for that day. Alan Turing and Gordon Welchman created the British Bombe, which used electrical circuits to decode the Enigma messages in as little as 20 minutes. The Bombe was essentially 36 Enigma Machines wired together, to work through more combinations at once. The Bombe 3 rows of drums, one row for each enigma rotor, which would rotate to try possible configurations. The Bombe would then guess a possible plugboard connection, and from there determine what the other letters on the plugboard must be. If a contradiction arose, then it ruled out that setting and moved to the next setting. When an arrangement without any contradictions arose, the machine would stop, let the operator note down the candidate solution, and could then be restarted to find further possible solutions. This allowed British codebreakers to read the Enigma code and decrypt Nazi messages, providing highly valuable information, and swaying the war in the allies favour.

Biography of Gordon Welchman by Isaac Conway

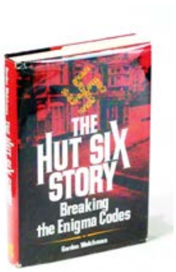
Gordon Welchman was born on the 15th June 1906 into a religious family. He was educated at Marlborough College School and then went on to study mathematics at Trinity College, Cambridge. He then became a research fellow at Sidney Sussex College, Cambridge in 1932. In September 1939 he became one of the first four recruits to Bletchley park. He worked alongside: Alan Turing, Hugh Alexander, and Stuart Milner-Barry.

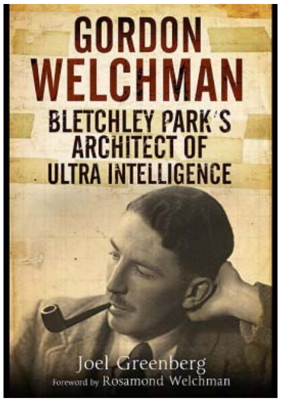
He was in the group of people that sent a letter to Winston Churchill asking for more funds in 1941. He spent his time at Bletchley park looking at German air force enigma signals. He was made head of Hut 6 doing this exact job, he can be seen on the right hand side of both of these images. He was part of the team that was trying to break the enigma code by using the mistakes made by German officers.

As part of this work he came up with something known as the “Diagonal Board”. This was part of Alan Turing’s Bombe that was made to counteract the enigma machine’s plugboard. The plugboard gave an extra level of encryption to the enigma machine whereby after inscription different letters were swapped. There were over 100 billion different ways of setting up this plugboard. The diagonal board section of the Bombe, which can be seen in the right image, allowed the plugboard settings to be found separately from the rest of the settings. This allowed the machine to go from taking days to find the complete settings of the enigma machine, to taking just hours. After this, in September 1943 he was made Head of Machines Coordination and Development, leaving hut 6.

In 1944 he was made Assistant Director of Machines and Mechanical Devices. This role entailed overseeing all of the uses of Bombes by the Allies. Making sure that all of the machines were working on different codes and making sure that all of the findings from them were efficiently and effectively distributed across the territories.

He was awarded an OBE in 1944 described as "Employed in a Department of the Foreign office". After the war he became director of research for John Lewis and Partners. In 1951 he started working for MIT. After this he worked at Remington Rand and then at Ferranti researching and manufacturing computers. He then worked at Mitre helping the US cybersecurity and defence ministries. The reason, perhaps, that he isn't remembered for his achievements as he should be today is that the goings on at Bletchley park had been declassified in the mid 1970s but much of the events that took place there were still a mystery to the general public. In 1982 he published a book called "Hut Six Story". The US defence ministry and GCHQ were against the publishing of the book. Welchman went against these wishes and the book was published. He was then stripped of his security clearance codes and was fired from Mitre. He died on 8th October 1985 in Newburyport, Massachusetts.





How did the Enigma Machine Work? by Samuel Price

The Enigma machine was used in the 2nd World War by the Germans to transmit information to each other secretly. It generated one of the cleverest and most complex codes invented; it was made so that only people who were told the numbers could read the message because the numbers changed every day. This made it fiendishly hard to break. But, in their headquarters at Bletchley Park, the British secret service didn't let that demoralise them. They figured out pretty quickly, in 1949, how the code worked, and used it to secure the Allies' victory. Despite the fact it was cracked so quickly by the British, even when told how, the way the code works is still confusing for people.

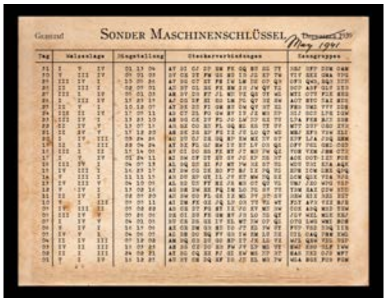
How and Why was the Enigma machine used?

Each German general would have their own enigma machine to decode or code highly confidential information, to send with Morse code to the other generals. The reason for the code was, of course, to stop the British and other countries from intercepting the radio signal and nosing into their battle plans. The Germans knew that there were some pretty sophisticated code-crackers in the enemy's ranks, so they came up with something that would be virtually impossible to understand and solve. Not only did they make a machine that could change the message letter by letter, not only did the code change every time a letter was pressed, but there was also a sequence of 15 combinations of letters or numbers needed to use the machine. And these characters changed every day! Every German general was therefore given a sheet of the letters and numbers corresponding to each day called a Sonder-Maschinenschlüssel, and were told to keep it tucked up safe by their body at all times, lest the British get their hands on it. The British never did manage to get their hands on it, so they had to work out the code anew every day.

How did the Enigma machine look?

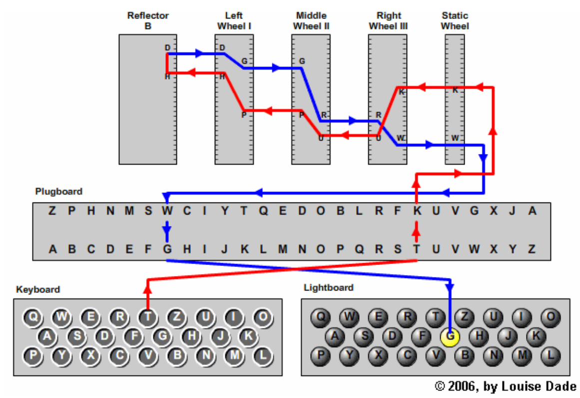
The enigma machine was structured like a typewriter, with a keyboard where any normal keyboard would normally be. This was used to input the letters that were going to be coded. There was a second keyboard above it called a lampboard, and this would show the output of the code. Under that was the plugboard where certain plugs had to be attached to one another. The only way of knowing which ones to connect was by using the Sonder-Maschinenschlüssel. At the top were three rotors, each of which had to be selected from a number of different rotors, and in certain orders and positions, also prepared using the special sheet.

How was the Sonder-Maschinenschlüssel used?



This is an example of the sheet the German generals were using. On the left is the date, so they could make sure they were on the right day. This was written from the bottom to the top so that the Germans could burn the bottom off every day, instead of having to burn off the beautiful title and subtitles at the top. On the next column, you had the number of rotors you had to use from left to right, for example on the 31st you had to use rotor number four, and then rotor number two, next to rotor number one. In total, there were ten rotors, so guessing was already not an option for the English. The next column told you which letter should be facing up on the rotor at the start of the sequence. You can see these letters at the side of the rotors on this diagram. On the diagram of the enigma machine, you can vaguely see a small square next to each cog, which is where the generals could line up the cog with the start letter according to the sheet. Finally, the combination of letters showed which plug to attach to which in the plug board. Once the person had done that all they had to do was type.

The Inner Workings of the Enigma Machine



All of the settings eventually result in a complex sequence of events which turns your original letter into a seemingly random letter. But after looking closely, the letter was not made as randomly as it looks. The letter goes from the keyboard to the plugboard, where it gets translated into the letter which the wire is connected to. This letter in turn gets taken to the right-most wheel, where the letter gets translated again into another letter, and this repeats itself until you get to the reflector, where the process happens again but reversed. Hopefully the diagram helps you understand, because it is very confusing. To add complexity, the setting of the rotors changed each time a key was used. The right rotor moved every time a key was pressed. The rotor next to it stepped forward once the first rotor had gone all the way around. The next rotor moved forward when the second one had turned all 26 positions. This meant that, even if you pressed the same letter twice in a row, you still got a different output for each. In order to crack a code that changed after every letter every day, the British needed to invent a similarly clever machine.

Alan Turing: A Life by Sam Wood

Alan Turing was born on June 23, 1912, in London. Alan Turing was to become one of the leading mathematicians who ended up breaking the enigma code and he was the inventor of one of the first computers. Despite these acts which undoubtedly saved thousands of lives, he died a criminal for gay having been convicted under Victorian laws as a homosexual and forced to endure chemical castration. Alan Turing was found dead in 1954 in his home and the verdict declared it a suicide.

Early Life

The son of a civil servant, Turing was educated mostly at Sherborne School. He entered the University of Cambridge to study maths in 1931. After graduating in 1934, he was elected to a fellowship at King's College in recognition of his research in probability theory. In 1936 Turing's paper "On Computable Numbers, with an Application to the Entscheidungsproblem'' was recommended for publication by the American mathematician Alonzo Church, who had himself just published a paper that reached the same conclusion as Turing's, although by a different method. Later that year Turing moved to Princeton University to study for a PHD in mathematical logic under Church's direction which he completed in 1938.

WW2

Having returned from the United States to his fellowship at King's College in the summer of 1938, Turing went on to join the Government Code and Cypher School, and, at the outbreak of war with Germany in September 1939, he moved to the organisation's wartime headquarters at Bletchley Park. A few weeks previously, the Polish government had given Britain and France details of the Polish successes against Enigma, the principal cipher machine used by the German military to encrypt radio communications. As early as 1932, a small team of Polish mathematician-cryptanalysts, led by Marian Rejewski, had succeeded in deducing the internal wiring of Enigma, and by 1938 Rejewski's team had devised a code-breaking machine they called the Bomb . The Bomba depended for its success on German operating procedures, and a change in those procedures in May 1940 rendered the Bomba useless. During the autumn of 1939 and the spring of 1940, Turing and others designed a related, but very different, code-breaking machine known as the Bombe. For the rest of the war, Bombes supplied the Allies with large quantities of military intelligence. By early 1942 the cryptanalysts at Bletchley Park were decoding about 39,000 intercepted messages each month, a figure that rose subsequently to more than 84,000 per month—two messages every minute, day and night. In 1942 Turing also devised the first systematic method for breaking messages encrypted by the sophisticated German cipher machine that the British called "Tunny." At the end of the war, Turing was made an Officer of the Most Excellent Order of the British Empire for his code-breaking work.

After War

After the war was won and over, Alan Turing was recruited by the National Physical Laboratory to create the first electronic computer. His design for the Automatic

Computing Engine was the first complete electronic stored-program all-purpose digital computer. Had Turing's ACE been built as he planned, it would have had vastly more memory than any of the other early computers, as well as being faster. However, his colleagues at NPL thought the engineering too difficult to attempt, and a much smaller machine was built, the Pilot Model ACE.

NPL lost the race to build the world's first working electronic stored-program digital computer. Discouraged by the delays at NPL, Turing took up the deputy directorship of the Computing Machine Laboratory in that year. His earlier theoretical concept of a universal Turing machine had been a fundamental influence on the Manchester computer project from the beginning. After Turing's arrival at Manchester, his main contributions to the computer's development were to design an input-output system — using Bletchley Park technology — and to design its programming system. He also wrote the first-ever programming manual, and his programming system was used in the Ferranti Mark I, the first marketable electronic digital computer.

Criminal Charges

In January 1952, Turing was 39 when he started a relationship with Arnold Murray, a 19-year-old man. Just before Christmas, Turing was walking along Manchester's Oxford Road when he met Murray just outside the Regal Cinema and invited him to lunch. On 23 January, Turing's house was burgled. Murray told Turing that he and the burglar were acquainted, and Turing reported the crime to the police. During the investigation, he acknowledged a sexual relationship with Murray. Homosexual acts were criminal offences in the United Kingdom at that time and both men were charged with "gross indecency". Since then, times have thankfully changed, and the film The Imitation Game (see below) goes a long way to telling the truth behind Turing's tumultuous life story and the injustices he faced.

... .- -- / .-- --- --- -.. (Sam Wood)

Joan Clarke: The Forgotten Lady of Bletchley Park by Dhruv Lakhani

Introduction

Joan Elisabeth Lowther Murray was an English cryptanalyst and numismatist best known for her work as a code-breaker at Bletchley Park during the Second World War. Although, she was not personally recognised in comparison to Alan Turing, she still went on to receive an MBE.

The Founding of a Star

Clarke attended Dulwich High School for Girls in south London and won a scholarship in 1936, to attend Newnham College, Cambridge, where she gained a double first degree in mathematics and was a Wrangler. She was denied a full degree, as Cambridge only awarded these to men until 1948.

Clarke's mathematical abilities were first discovered by Gordon Welchman, in an undergraduate Geometry class at Cambridge. Welchman was one of the top four mathematicians to be recruited in 1939 to supervise decoding operations at Bletchley Park. After noticing Clarke's mathematical abilities he recruited her to join him at Bletchley Park and be a part of the 'Government Code and Cypher School' (GCCS).

Bletchley Park

Joan Clarke became deputy head of Hut 8 but was prevented from growing any further due to her gender and was paid less than men. In Hut 8, she worked with the great Alan Turing and very quickly, they became very good friends. This was because both of them had similar interests such as chess and puzzles. Turing proposed to her in 1941 despite him being homosexual, she agreed. However, despite this, Alan Turing decided that the marriage could not go on and broke it off. Joan Clarke admitted she wasn't surprised and still remained friends with each other until Alan's death.

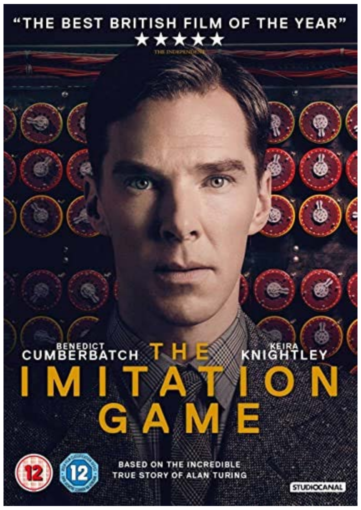
Because of the secrecy that still surrounds events at Bletchley Park, the full extent of Clarke's achievements remains unknown. Although she was appointed MBE in 1947 for her work during WW2, Clarke, who died in 1996, never sought the spotlight, and rarely contributed to accounts of the Enigma project.

But the esteem in which she was held by her colleagues, and the fact that "her equality with the men was never in question, even in those unenlightened days", as Michael Smith writes, are a tribute to her remarkable abilities.
Morten Tyldum, the director of The Imitation Game emphasises that Clarke succeeded as a female in cryptanalysis at a time "when intelligence wasn't really appreciated in women". There were a handful of other female codebreakers at Bletchley, notably Margaret Rock, Mavis Lever and Ruth Briggs, but as Kerry Howard - one of the few people to research

their roles in GCCS - explains, their contributions are hardly noted anywhere. "Up until now the main focus has been on the male professors who dominated the top level at Bletchley," she says. In order to find any information on the women involved, you have "to dig much deeper".

Film Review: The Imitation Game

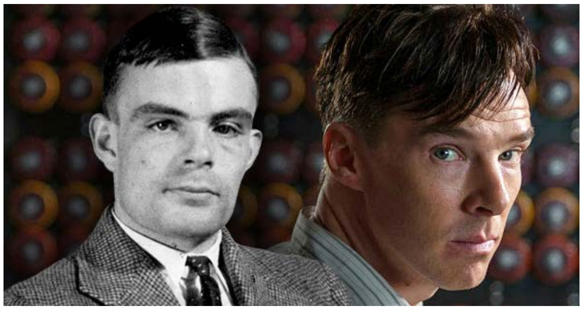
by George Crosthwaite



Following the Scholars' trip to Bletchley park on the 21st of March, the famous home of code breaking that solved the Enigma, I decided to watch the film The Imitation Game. The 2014 historical drama film directed by Morten Tyldum and written by Graham Moore was based on the 1983 biography Alan Turing: The Enigma by Andrew Hodges. With a star studded cast of Benedict Cumberbatch, Keira Knightly, Matthew Goode and Alan Leech, I expected a lot from this film, and it's safe to say it delivered on my expectations.

In terms of cinematography this film was excellent, shot on Kodak 35mm Film Stock, the feel of the film was moody and dark, possibly ahead of its time with its 'dark academia' type aesthetic in parts. This being said, the film is anything but a fad and is truly a timeless film with the cinematography equally ageless. The film perfectly balances scenes of intense stress and claustrophobia for the viewer inside the huts of Bletchley park with vivid and passionate scenes of Turing running through the fields near the park and flashbacks to Turing's school days in the green fields and majestic buildings of Sherborne School. Overall, the film manages to make computers and crosswords visually compelling which is of course, no small feat.

The plot of the film is interesting and manages to keep the viewer interested in what is otherwise a melancholy film through moments of success like when Alan secures funding from Churchill, breakthroughs such as when they work out the weather clue and, of course, when Alan's Machine 'Christopher' solves the Enigma machine. However, in order to keep the mood of the film melancholy these moments are juxtaposed with sad moments such as after they solve the Enigma the code-breaking team realise they cannot tell the British command intel they receive and have to watch as a civilian cruise ship is attacked by German U-boats.This is because they don't want to let the Germans know they have cracked the Enigma. Worsening the situation, this cruise ship happens to have one of the team member's brothers on the vessel. The film is not chronological and features various flashbacks and montages such as the aforementioned to Alan's school and also to British soldiers fighting in the war. The school flashbacks do help to understand Turing's psychology and his upbringing, giving context to his behaviour in the film. What's more, the montage scenes that flick to views of war help to bring the audience back to reality and why Turing's work was so important, allegedly shortening the war by two years. Aside from the Enigma work, Turing's sexuality is also a large part of this film's plot. The sub-plot of Turing's sexuality begins in his school days and his relationship with his friend Christopher Morcom, then his marriage with Joan Clarke. A short time after this he divorces Joan as he no longer needs her to help him solve the Enigma. In 1952 Turing is charged with gross misconduct and given sexuality conversion medication, finally in 1954 Alan could take it no more and allegedly commited suicide. Bringing an end to his fateful life as a homosexual person in the 20th century.



As with any historical film it is vital to consider the historical accuracy of the Imitation Game. I found this especially interesting after learning so much in my visit to Bletchely. The film is largely historically accurate with some interesting historical details such as the weather report clue being used very effectively in the film. However, there are some discrepancies in the film, firstly, most of the film is not filmed at Bletchley, the mansion is not the one in Bletchley but a mansion in Nettlebed, Oxfordshire. There are other examples where the film's directors took artistic liberties too, one example of this is in the film the cruise ship that could be saved by their code-breaking machine has one of the team member's brother on it however, in reality, this is simply not true.

In conclusion The Imitation Game is a moving celebration of Turing's life and gives a fairly accurate and compelling recount of Turing's work and the computing achievements at Bletchley.

CREATIVE WRITING

THE MESSAGE by Harry Owens

Berlin - 2nd February 1941, 5:00 pm

Admiral Karl Donitz, was pacing his room, up and down, up and down, over the plush carpet of his Berlin office. He walked over to his desk, laden with papers and documents, drowning in a sea of paperwork. His typewriter stood in pride of place, an island in the ocean of documents, its keys worn and polished by years of use. He picked up the letter and read it through once more, his face unreadable. This was the opportunity he was waiting for. This was his chance to strike. The letter was from Wilhelm Franz Canaris, Head of the Abwehr, the German Secret Service.

Dear Admiral,

My sources have received news of a large shipment of American arms from New York, to the UK. This shipment is the largest yet and it is vital that it does not arrive.

This convoy will be heavily protected by American warships for the majority of the journey, however 800km off the coast of Ireland, the American warships will depart, and the convoy will be escorted into port by a British patrol.

Due to bad weather this British patrol has been delayed and thus leaving the convoy unprotected, giving us a period of approximately 45 minutes to strike.

Should we eliminate this convoy? It will be hugely beneficial to the war effort, and I urge you to make the most of this opportunity.

Yours sincerely,

Franz Canaris.

Donitz carefully placed the message in the bin by his desk, where it would be collected and incinerated. Then he turned to the two men who were sitting at a small table across the room, flashing a rare smile. On the table sat a wooden box, secured by a lock. The first man carefully unlocked it, and lifted its worn lid, revealing the inner workings. Despite its humble exterior, this wooden box contained the most sophisticated and advanced cipher, the pinnacle of German engineering, the Enigma Machine. As Donditz carefully dictated his message, the first man typed it into the machine, the rotors whirring and clicking, scrambling the message. Meanwhile the second man recorded the encoded message, as the new letters were illuminated. Having finished the encryption, the second man turned his attention to a radio set that was positioned on the table, and proceeded to transmit the message using morse code, the soft bleeps echoing through the cavernous space.

Donitz's plan was simple: he would divert U-boat 23, already patrolling the North Atlantic, towards the path of the convoy, where it would lie in wait. When the convoy was unprotected, it would strike. The message had already been sent, and within 12 hours the arms shipment would be at the bottom of the Atlantic. It was perfect.

South Coast, British listening station - 2nd February 1941, 5:15 pm

DOT DOT DOT, DASH, DASH, DASH, DOT DOT….

For Elizabeth it was like falling into a trance, shutting out all other noises, everything. Concentrating only on the dots and dashes, coming so fast it just became a flurry of sound, crackling through the headset. Her pencil scribbling and scratching as she listened, an extension of her arm, decoding messages as they came through the radio waves. There were twelve of them, working all day decoding the radio traffic, dot after dot, dash after dash, message after message. Listening, pencils scratching, it was anxious work, losing concentration for less than a second could be disastrous, and any mistake would cost lives. Elizabeth had decoded hundreds of messages this week, thousands over the 3 months she had spent here, but this one was different, she could tell. She just knew. Finally the beeping stopped. Wiping sweat from her brow, she glanced down at the newly transcribed message, a chaotic jumble of letters. Her gaze lingered on it for a second, before she scribbled the date across the top, and placed it in the tray on her desk.

Half an hour later the very same message was on its way to Bletchley Park, carried by motorcycle, winding through country roads, the bike roaring as it ate up the miles.

James had only been a dispatch rider for a week and this was one of his first jobs, the Norton 16H's two cylinder engine roaring underneath him as he guided the bike along the coastal roads. The bike and its precious cargo raced through the countryside as the sun slipped further and further towards the horizon, its dying light barely illuminating the winding cliff top roads. The biting wind whipped over the cliffs, stinging his face, slicing through his leather gloves, numbing his fingers, as they grasped at the handlebars. With the wind came the smell of the sea, its salty tang stinging James' nostrils, searing his throat. As he raced along the winding road, hedge rows a blur as the bike swept forward, he gazed out to the ocean. The sun sank below the sea, and the darkness encroached. James continued through the night, rain lashing against his face, fighting to keep control of the bike, he knew every second he delayed would cost lives. Knowledge was power, and these messages would save lives, he was sure of that.

Atlantic ocean, U-Boat 23 - 2nd February 1941, 5:30 pm

Commander Wilhelm Franz, stood in the conning tower of U-boat 23. Within 12 hours he would be home. He would be able to escape this steel coffin, he would see his family again. For months his crew had been patrolling the North Atlantic, and now they were headed back to Hamburg. He listened to the U-boat, he had grown accustomed to its strange noises. The rumble of the engines, the soft gurgling of the pipes, and the creaking and groaning of the U-boat's skin. It was cramped, noisey, smelly, and thoroughly uncomfortable, and yet he had grown fond of her. She had protected them, kept them safe, hidden beneath the waves.

Wilhem’s thoughts were interrupted by a sudden metallic clang, which echoed around the conning tower, the sound amplified by the steel walls. He turned to see Gunter, the radio operator entering from the control room below. “A message from the Admiralty.” declared Gunter, handing Wilhelm a letter, before retreating down though the hatch, letting it clang shut behind him. Wilhelm read the letter carefully, before sighing loudly. The German admiralty had detected a US convoy, and he was ordered to change course. They would not be going home. He had to obey orders, U-23 changed course, slipping silently beneath the waves, towards its unsuspecting target.

Bletchley Park - 3rd February 1941, 12:15 am

Commander Denniston was in his office reading the message a final time. He placed the fateful piece of paper, alongside the rest of the clutter that inhabited his mahogany desk. One of the code breakers had brought him the message about 5 minutes ago. He had been standing by the bay windows gazing out over the night, when he had heard the knock on his door. It was a young man named George Williams, his face flushed with excitement. He had just decoded a message from the German Admiralty to a U-boat patrolling the Atlantic. He had worked tirelessly, all evening, decoding and deciphering this message, and just as George was about to give up he had found a breakthrough, with renewed determination he had grappled with the message, breaking it apart, letter by letter, word by word. What he had deciphered had astonished him, and he had rushed to the mansion, to deliver the message to commander Denniston himself.

Denniston glanced over the message again before picking up the phone by his desk. “Get me the Admiral.”

An hour later two U-boat hunting Corvettes, HMS Avenger and HMS Arrowhead, set sail for the North Atlantic.

The Work of Bletchley - A Haiku Sequence by Ewan Ellson

With 1918,

There came a new encryption,

The Deutsch enigma.

Hidden from the world,

Enciphered clues to the Reich,

A key locked away.

The Poles and the Brits,

An alliance formed from hate,

Changed the fate of war.

Every lock has flaws,

Every people owns a fault,

All exploitable.

The crew of Bletchely,

Pole Marian Rejewski,

All working as one.

Breaking the cipher,

Since 1941 it

Had been fully done.

The Bombe and people,

Managed, in conjunction to

Cut the endless struggle.

Sonnet - Early Bletchley

A call, from the paper, for the crossword

Clues that were deciphered. An invite to

The future home of what was never heard.

Seventy in a house but still too few.

The first crisis thought to be averted,

Yet the nazi leader brought the crew back.

The land of the Czechs did not stop his stead,

Not “peace for our time”, but the turn of track.

Now ten-thousand strong with bombe and tunny,

The unarmed force behind the greatest war,

It fought and fought, day on day, ‘till decree

That their efforts had won, and nevermore

Should the place be mentioned, or the work of

Ten-thousand ever sent beyond the ears of legend.

Limerick - Alan Turing/Computing

There was a young man named Turing,

Who had trouble solutions procuring,

For all in the scene,

A computing machine,

Which he solved in conclusion, securing.

Villanelle - Effects of Enigma

There were great powers in the West,

From them fine inventions arose,

To them all wars would attest.

One such machine reached high a crest,

The greatest war it halted from close,

There were great powers in the West.

It had many options and the west it would test,

Many people it would help dispose,

To them all wars would attest.

Enigma twas called and was held at the chest,

Of the greatest of all the opposed

There were great powers in the West.

Of the enemy plenty would manifest,

Each one a new task to dispose,

To them all wars would attest.

The code and trial, one colossal test,

An enemy to thwart and expose,

There were great powers in the West,

To them all wars would attest.

Villanelle - Necessity is the mother of invention

From death new life will always arise,

Necessity's the mother of invention,

There is no ultimate demise:

Death and destruction under the guise

That there will be suspension,

From death new life will always arise.

From ashes the ph’enix will rise,

That is without contention,

There is no ultimate demise.

Objects whose uses you oft exercise,

Were formed from this horrible dimension.

From death new life will always arise.

Penicillin and flu, freed by the wise,

Brought forth a new ascension,

There is no ultimate demise.

Though the horror is now realised,

As need is the mother of invention,

From death new life will always arise,

There is no ultimate demise.

BONUS FEATURE

How has the Bodleian Library evolved throughout its history? by Torsten Ayerst

The Bodleian Library, the non-lending, reference library of the University of Oxford, is one of the oldest in Europe, and the second largest in Britain. Today, it holds over 13 million printed items, and it has a copy of all the books and printed items published in Great Britain since 1610.

However, in the 700-year history of this impressive library, it has not always been so remarkable. The first library for Oxford University was housed in a room above the Old Congregation House, began around 1320, and was situated above the north side of University Church of St Mary the Virgin. This not particularly large or architecturally interesting room was funded by the Bishop of Worcester at the time, Thomas de Cobham, however it was still unfinished when he died in 1327. It held a small collection of chained books, and this collection slowly grew over the lifetime of the library. However, since it was not very big, a donation from Duke Humfrey of Gloucester (King Henry V's younger brother) of over 281 manuscripts in the years 1435-37 presented the opportunity for the library to move to a new building, as the original building would have become too overcrowded with this donation. In 1444, the University decided to build the new library over the then fairly recently built Divinity School, but due to a major shortage of funds, its construction only started in 1478 and was opened to the public 10 years later. It is still known as "Duke Humfrey's library".

Nevertheless, the new library did not last in its original form for long and, in fact, only for just over 60 years. During the reign of the Protestant King Edward VI (son of Henry VIII), he passed a law to purge all Roman Catholic-related manuscripts, and so in 1550, all the library's books were removed, and some were burnt. Unfortunately, the University was not wealthy enough to rebuild its collection, so in 1556, the room was taken over by the Faculty of Medicine – the shelves were dismantled, and its desks were sold.

About 50 years later, the old library was restored by an English scholar, diplomat, and collector of medieval manuscripts, Sir Thomas Bodley. In 1598, the University accepted his offer to refit and restore it. Around 2,500 books were housed in the new library, some donated directly by Bodley himself, a new librarian was hired, and finally the "Bodleian" Library opened on the 8th of November 1602, named after its generous donor who made it possible. Bodley's contribution to the library continued, and in 1610 he made an arrangement with the Stationers' Company of London – so that a copy of every book published in England and registered at Stationers' Hall would be deposited at the Bodleian Library. This agreement meant that the library would be forever expanding, so to make sure that there was enough space, between 1610 and 1612, Bodley planned and financed its first extension – "Arts End".

Bodley died in 1613, but the last additions to his buildings came after his death, with the construction of the Schools Quadrangle (fully completed in 1624) and another extension to Duke Humfrey's library in 1634-7 – Selden End – named after the lawyer who donated 8,000 books to be housed there.

These collections attracted scholars from all over the world, although as a non-lending library, no books could be taken out by anyone – not even by, most famously, King Charles I in 1645. Even so, the library did not receive many daily visitors - in 1831 there was averagely 3 or 4 readers in the library per day, and as there was no heating until 1845, the library had to limit its opening hours, so it wasn't too cold (in the winter, the library was only open from 10am to 3pm).

Since its collection continued to grow, by 1849 there were around 220,000 books in the library's possession – and the library kept on expanding to accommodate all of these. By 1859, the whole of the Schools Quadrangle was owned by the library, and in 1860, the Radcliffe Library (renamed to the Radcliffe Camera) was also taken over by the Bodleian to create more space for storing their books. By the end of the 1800s, the Bodleian's collection was growing by 30,000 books per year, so to provide extra space, an underground book storage area was dug beneath Radcliffe Square in the years 1909–12, which at the time was the largest store of this kind. Then in 1914, the Bodleian Library reached the milestone of 1 million items.

Though by the late 1920s, with both readers and books increasing, the library needed even more space, so in 1931 the decision was made to build a new library mainly just to house the books, and in 1937, the New Bodleian Library, designed by architect Sir Giles Gilbert Scott, began construction. The library, which was opened in 1946, contained a tunnel that linked it with the old library, and featured a pneumatic pipe system, mechanical book conveyor, and pedestrian walkway, so the library's readers could access any book in the collection without it needing to be brought outside. It also included reading rooms, and an 11-storey bookstack beneath the building. Also, from 1960 to 1963, Duke Humfrey's library was majorly restored, followed afterwards by the restoration of the Schools Quadrangle from 1964 to 1968.

With the beginning of the digital age, the library evolved with the improving technology at the time. From the start of the 1990s, the library began to digitize some of its items, and in 2002, an electronic stack request system was introduced to allow for readers across the Bodleian's different libraries to easily receive the books that they wanted. The old systems, like the pneumatic pipe and book conveyor, continued to be used for a while but were both shut down in the late 2000s.

The library was constantly running out of space for its ever-expanding collection, and in the 2000s had to start storing its books in salt mines in Cheshire – so, to solve their storage crisis, the library decided to build a warehouse for their books. On the 7th of November 2010, a new book storage facility was opened in the outskirts of Swindon for the Bodleian to store their millions of books. The £26 million warehouse encompassed 13 acres of land and had 153 miles of shelving – Students could order a book from the storage warehouse by 10am, and a truck drove it to one of the Oxford libraries by 3pm. The library could also scan books from the warehouse directly over to the desktop of one of their users.

In July 2011, a new area of the library was opened to link the Old Bodleian library and the Radcliffe Camera library. Previously the underground book storage, the "Gladstone Link" had shelf space for an additional 270,000 items, and it acts also as an informal study space.

Back in 2006, the decision had been taken to completely renovate the New Bodleian library, with the idea to make it more of a public building than it had originally been designed to be. The New Bodleian closed on the 29th of July 2011 and was reopened to the public, after years of renovations, on the 21st of March 2015, now renamed to the "Weston Library".

This new library, while it maintained the original façade from the 20th century library, provided improved storage, and better facilities for its readers – including a lecture theatre, three reading rooms and even a tearoom. Also, in November 2015, the library's total collection surpassed 12 million, only around 100 years after reaching the 1 million items milestone. In the same year, the "Digital Bodleian" was launched to bring together digitized content from the library, and it rapidly became a vital resource for research. It has now digitized around 17,000 items and this number is constantly growing.

Overall, in its 700-year history, the Bodleian Library has evolved massively - from being housed in a single small room, to occupying five buildings. It started out with less than 100 books, and now it adds over 1,000 books to its collection every single day. It will be interesting to see how the library expands and evolves in the future.