Middle School Scholars' Newsletter

Lent Term 2020

Code Breaking at Bletchley Park

Introduction

"A gifted and distinguished boy, whose future career we shall watch with much interest." This was the parting remark of Alan Turing's Headmaster in his last school report. Little could he have known what Turing would go on to achieve alongside the other talented codebreakers of World War II at Bletchley Park. Our trip with the third year academic scholars this term explored the central role this site near Milton Keynes played in winning a war.

CONTENTS

A Short History of Bletchley Park

by Alex Mapplebeck

The first mention of Bletchley Park in records is in the Domesday Book, where it is part of the Manor of Eaton. In 1711, the mansion was built there by Browne Willis, but in 1793, the mansion was pulled down by Thomas Harrison. It came to be known as Bletchley Park when the estate was purchased by Samuel Lipscomb Seckham in 1877. In 1883, the pre-existing farmhouse was expanded into the house that it is today, incorporating many different architectural styles in what some people called a "maudlin and monstrous pile". In 1938, the estate was purchased by Sir Hugh Sinclair for the MI6 for £6000 (roughly £386000 today).

The key advantage of Bletchley Park for the Secret Service was its geographical centrality, being near to the "Varsity Line" (a railway route that linked Oxford and Cambridge). This would play a pivotal role in the hiring of employees for cracking the codes for the war effort. In addition to this, Bletchley Park was located near Watling Street, which linked London to the North-West and to nearby intercept stations. During the war, Bletchley Park had many cover names, which included "B.P.", "Station X" and the "Government Communications Headquarters".

Alastair Denniston was the operational head of the GCHQ from 1919 to 1942, starting off his work with other cryptanalysts in Room 40 of the Admiralty and then moving to Bletchley Park. As more and more recruits were inducted into the ranks of cryptanalysts through solving puzzles such as a cryptic crossword, one of which was arranged by the Daily Telegraph as a competition, after which promising contestants were approached for "a particular type of work that contributed to the war effort". Most of the people who worked at Bletchley Park were from a linguistic or mathematical background or were chess champions. These skills were vital to the deciphering and translation of the coded messages of the Germans and Japanese.

A common misconception is that many people think that the cipher employed by the Germans, Enigma, was broken here. When, in fact, it was broken by Polish mathematicians in 1939. Their efforts were recognised and today there is a bilingual monument that commemorates their efforts. However, a different cipher was broken exclusively at Bletchley Park, Lorenz. This cipher was broken

using multiple tactics, which included the use of the Colossus computer, the first computer in many aspects. The colossus was developed in 1943 and it included simple logic circuits that enabled it to work out the arrangement of the cipher wheels within the Lorenz machine in a far shorter amount of time than if a person was doing it purely through brute force.

At the time of the Second World War, Bletchley Park was home to the mansion and codebreaking huts that each had a different purpose such as translating the messages or working out the configuration of the cipher wheels. Hut 8 is one of the most notable huts, since it was where the codes, having found the cipher key, were processed and put back into plaintext. Hut 8 was originally led by Alan Turing, who was then replaced by Hugh Alexander in November 1942. Most of the messages read by Hut 8 in quantity were Luftwaffe messages, however, they did manage to read a few “Dolphin” code messages that were employed by the German navy.

A long and complex process was used to get the messages from “Y” intercept stations to be able to be read by cryptanalysts. Firstly, the intercepted message was written down on paper and handed to a volunteer rider who would ride to Bletchley Park on a motorcycle (using a different route each time). They would then hand the message to someone who would run the cipher through a “Bombe” machine to find the cipher key quickly. These would then be decrypted in Hut 4 or Hut 8 and then they were translated and ferried off to London to be given to a military leader or someone else.

There is only one known case of espionage that occured at Bletchley Park. In 1942, there was a Soviet spy called John Cairncross. He somehow managed to smuggle messages out by concealing them in his trouser leg and then he gave them to a NKVD agent in London. The only known use of these messages in war was when he supplied the Soviet Union with Germany’s plans which led to their defeat at the Battle of Kursk.

After the Second World War, GCHQ was moved to Eastcote in North-West London, and the site seemed as though it was going to be demolished to make way for a housing estate in the 1990’s. However, a trust was set up to protect the site and eventually, the Bletchley Park Museum was founded.

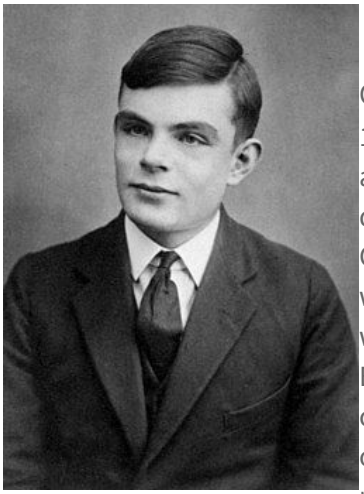
Alan Turing: A Profile by Sam Ramsey

Alan Mathison Turing was born on 23 June 1912 at 2 Warrington Crescent, London W9. His parents, Julius Mathison Turing (father) and Ethel Sara Stoney (mother), led fairly uneventful lives although his father was in the army, but their child would go on to live one of the greatest, most prolific and, sadly, shortest lives the codebreaking world has ever seen.

Turing, even at an extremely young age, showed signs of his genius that he would later prominently display. Being fairly well-off, he attended Hazelhurst Preparatory School, before later studying at Sherborne School in Dorset. His first day of term happened to coincide with the 1926 General Strike in Britain, but Turing was so adamant on attending that he rode his bicycle unaccompanied 60 miles (he was only 13 at the time) from Southampton to Sherborne. Ironically, despite his obvious talent for maths and science, one of the teachers wrote to his parents telling them that their son needs to, 'aim at becoming educated.'

In 1931, when Turing was 19, he went up to King's College, Cambridge, to read Mathematics and, unsurprisingly, was awarded First Class Honours. In 1935, at the age of only 22, Turing was elected a fellow of the Kings for his dissertation in which he proved the central limit theorem. However, it later turned out that this theorem had already been proved in 1922 by Finnish mathematician Jarl Lindeberg.

In 1936, Turing published one of his most important scientific papers entitled, 'On Computable Numbers, with an Application to the Entscheidungsproblem,' which proved that his "universal computing machine" (Turing machine) would be capable of performing any conceivable mathematical computation if it were representable as an algorithm. Two years later, Dr Alan Turing completed his Ph. D. thesis on the Systems of Logic Based on Ordinals.

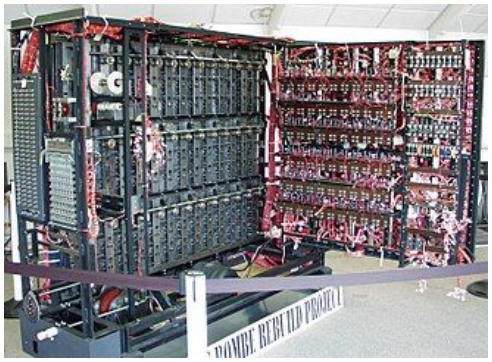


On 4 September 1939, one day after Britain declared war on Germany, Turing who was already working for the British codebreaking organisation, reported to Bletchley Park where he would spend the next 6 years and save countless lives because of his work. The Allies' main codebreaking problem was in translating the German messages which had been enciphered using the infamous, complex Enigma machine. Remarkably soon

after arriving, Turing had specified a new electromechanical machine called the Bombe to decipher the rotors which had been used on the Enigma Machine that day and ultimately break the code … for 24 hours. The Bombe, after an enhancement suggested by Gordon Welchman, became one of the key machines used in breaking Enigma.

In December 1939, Turing solved the key naval indicator system, which was significantly more complex than other indicator systems. On the very same night, Turing gave birth to the idea of Banburismus, a sequential technique to help break the naval Enigma. Turing said that he went to work on the German naval Enigma, "because no one else was doing anything about it and I could have it to myself."

The Bombe, which Turing designed, detected when a contradiction had occurred and therefore ruled out that setting of which it was testing. This contradiction would happen when an enciphered letter was turned back into the same normal letter which couldn't happen on the Enigma machine - its fatal flaw. The first Bombe named Victory was installed in Hut 8 in Bletchley Park on 18 March 1940. By the end of the war, more than 200 Bombes were in operation.



[Pictured: Fully working replica of The Bombe at Bletchley Park]

In 1941, Turing finally broke the Naval Enigma for the first time, decisively contributing to the Allies' victory in the U-boat war.

In July 1942, Turing joined the attack on the German Lorenz Machine - the machine that Adolf Hitler himself used to personally send his messages. He devised a system called, 'Turingismus,' or, 'Turingery,' which was the first systematic method for breaking Lorenz and the precursor of Colossus, the world's first programmable digital electronic computer. After this, he crossed the Atlantic to liaise with US codebreakers and Bombe engineers.

In 1945, he joined the National Physical Laboratory (NPL) at Teddington where he worked on and designed the ACE (Automatic Computing Engine). That same year, Dr Alan Turing was awarded an OBE for his wartime services, although 99.9% of people didn't know what he had been doing during the last 6 years.

After World War II, Turing went on to give an abundance of lectures on computer design in London. In 1947, he gave the earliest known lecture to mention Computer Intelligence, therefore founding the field now known as Artificial Intelligence (AI). Only a year later, Turing hypothesised and described simple neuron-like computing machines, hence anticipating the field known as connectionism. In 1948, he left the NPL to join the Manchester Computing Machine Laboratory. Here, he was pioneering the work in the field now known as 'programme verification.

In 1950, he published one of his most thought-provoking papers entitled 'Computing machinery and intelligence.' This paper was the birthplace of what is now known as the

Turing Test. The Turing test is a test to see if a computer can trick a person into believing that the computer is a person too. Alan Turing thought that if a human could not tell the difference between another human and the computer, then that computer must be as intelligent as a human. This year, he also wrote the Programmer's Handbook for Manchester Electronic Computer.

To go along with being a Fellow of the Kings, in 1951 Turing was elected Fellow of the Royal Society of London. The preceding year, he published one of his final papers: 'The Chemical Basis of Morphogenesis,' which anticipated the field known as artificial life.

In 1952, Turing started a relationship with Arnold Murray, a 19-year-old unemployed man. On 23 January 1952, Turing's house was burgled, and whilst talking to the police, he acknowledged his relationship with Murray. At his trial (homosexuality was a crime in England at the time), Turing pleaded guilty and both men were charged with gross indecency. Over 60 years later, he was granted a posthumous royal pardon for this conviction.

On 8th of June 1954, when he was only 41, Turing's housekeeper found him dead in his bedroom with a half-eaten apple lying beside his body. The cause of death was established as cyanide poisoning and the court ruled it as a suspected suicide however this is constantly disputed. The day before, Dr Alan Turing, O.B.E, one of the greatest codebreakers and scientists that the world had ever seen, had breathed his last breath.

Bletchley Park's Role in World War II by Harry Martin

In May 1938 the head of the Secret Intelligence Service, Admiral Sir Hugh Sinclair, bought the Bletchley Park mansion and the 58 acres of land for £6,000 (£386,000 today) to be used by the GC&CS and SIS in the occurrence of war. He was forced to purchase the land with his own money as the Government said they did not have the budget to do so, clearly overlooking how crucial the operations that would transpire in Bletchley Park would be. The work completed at the site was arguably the difference that resulted in the victory of the Allies in World War II.

Sinclair had been inspecting the grounds under the cover that he was part of 'Captain Ridley's shooting party'. The geographical advantages that the base posed were vital in his decision to purchase the estate. The house neighbours Bletchley railway station, which had trains links to Oxford and Cambridge University. These prodigious universities were expected to supply many of the code-breakers; they employed mathematicians, classicists and computer scientists. Equally the West Coast railway line that connects all of

England's predominant cities London, Birmingham, Manchester, Liverpool was easily accessible. The A5, the main road linking London to the north-west, was convenient. In addition some pivotal communication links were available at the telegraph and telephone repeater station in Fenny Stratford.

Early work began in the Mansion and its outbuildings, with a population of around 150 staff. As more and more people arrived to join the codebreaking operations, the various sections began to move into large prefabricated wooden huts. For security reasons, the various sections were known only by their hut numbers and the workers were forced to sign a document that pledged their secrecy. The first operational break into Enigma (the code the axis forces used to communicate together) came around the 23 January 1940, when the team working under Dilly Knox, with the mathematicians John Jeffreys, Peter Twinn and Alan Turing, unravelled the German Army administrative key that became known at Bletchley Park as 'The Green'. Encouraged by this success, the Codebreakers managed to crack the key used by the German air force (Luftwaffe). In addition to other German codes, Italian and later Japanese systems were also broken.

On 20 November 1940 the park received its first and only direct enemy damage, by three bombs that were intended for Bletchley railway station; Hut 4, shifted two feet off its foundation. Had this damage affected more of the huts or the mansion the codebreaking operations and significant documents would have been demolished.

Bletchley Park was able to read a substantial number of German and other axis powers' air force messages. These decryptions reduced the number of innocent citizen deaths, prevented the british from falling into enemy traps and the ability to understand future axis intelligence. The first Enigma messages to be successfully decrypted were from the German Luftwaffe. The breakthrough by Hut 6 of the cypher allowed Bletchley Park to predict the targets and routes of the Luftwaffe bombers, which ensured that a British fighter aircraft could ambush the fleet on their way to the targets, and that the authorities could anticipate and prepare for the raids, limiting the numbers of deaths and severity of damage. In March 1940 the first Bombe machine was invented by Alan Turing, this machine could decrypt code messages efficiently and it removed human error from the codebreaking process. In October 1941 after receiving a letter from some of the senior codebreakers denouncing the lack of resources and funding, Prime Minister Winston Churchill directed: 'Make sure they have all they want, extreme priority.' After this enquiry Bombe machines were being produced at an increasing rate to ease the great flow of potentially vital encrypted messages.

The second half of 1941 saw Hut 8, led by Alan Turing, make the breakthrough on the Enigma key used by the U-Boats attacking the trans-Atlantic convoys. From then on,

throughout the naval conflicts, they helped to track the U-Boat wolf packs, considerably reducing the German Navy's ability to sink the merchant navy ships bringing supplies to Britain from America. In the Mediterranean, the victory at the Battle of Matapan in March was a direct result of Bletchley Park's break into the Italian Naval Enigma system, this restricted the Italian Navy's operations for the rest of the war. Furthermore the faculty to read Japanese codes led to the routine sinking of enemy ships.

Not only were the decryptions beneficial for defence they made critical contributions to the allied bombing offensive over Germany from 1943 onwards. Copious interceptions and analyses of communication between the German air defence network allowed Allied bomber routes and strategies to be updated, to give them a continuous advantage. False broadcasts were also made to confuse the enemy. Tuesday, 6 June 1944 The Codebreakers also made a vital contribution to D-Day. The ability to read Japanese diplomatic, naval and military ciphers provided British military commanders with full details of the German defences in Normandy. The breaking of the ciphers of the German SIS allowed the British to confuse Hitler over where the Allies were to land. The decision to divert troops away from the Normandy beaches to Calais undoubtedly helped secure the invasion's success. They interpreted teleprinter links from Berlin to the battle fronts which also gave details of German plans laid down by Hitler.

After the war, the Government Code & Cypher School became the Government Communications Headquarters. Bletchley Park Trust was set up in 1991 by a group of people who recognised the site's importance and refused the plans to destroy the monument. In 1994 its Chief Patron, the Duke of Kent, opened the site to the public, as a museum and a reminder of all the men and women who worked profusely to prevent the spread of Nazi influence and control.

Review: Bletchley Park Museum by Joseph Conway

On the 13th March, the scholars went to Bletchley Park to learn about the place which was a significant factor in the winning of the Second World War. On the day, we had a guided tour of the grounds, we watched a film about how Bletchley Park affected D-Day, we had a classroom session and, to conclude the day, a self guided tour of the museum. Despite this being far different from how the general public would visit the museum, I believe that this variety of activities gives me a greater insight to whether Bletchley Park is worth visiting.

The sight of Bletchley Park was at the crossing of two railway lines: one which went from Oxford to Cambrigde, and the other which went from London to Birmingham. This allowed for easy access from the capital of the country and for academics, from Oxford or Cambridge Universities, working at Bletchley Park.

In the morning we had our guided tour of the grounds. This was relatively informative, but was not so much as to overwhelm you, since the man talking to us asked questions and told us stories of children answering with weird statements, which relieved you and allowed you to absorb his many facts. The staff throughout the day were all engaging and knowledgeable. The information he was talking about was extremely interesting. For example, there were about 10,000 workers at Bletchley Park (code breakers, morse code translators, language translators, communicators etc.), 8,000 of those were women. This is arguably a contributing factor in furthering women's rights: women were now seen to be able to do a job as well or better than a man (a concept largely unthought of at the time), this was especially the case when the job was extremely difficult: to decode the enigma machine. Another example is that the grounds were originally made in 1877 along with the large mansion, until the owner at the time, Samuel Lipscomb Seckham, sold the grounds and the mansion to the government, for about two hundred thousand pounds (in today's money). These pieces of information were very interesting to me and kept me wanting to learn more about Bletchley Park.

The classroom session was also very engaging and as aforementioned the staff member was ready to answer any questions. There we

learnt about a few different types of cypher such as a Ceasar cypher, about how the enigma machine worked and about how many possible ways the enigma could be set up. This was quite intriguing since we were set many tasks to do in groups and this session was especially exciting since we were all allowed to press a key on an original enigma machine. For example, we spent most of the time working out how many configurations of the enigma machine were there. We had to take into account the plug board, the three rotors and their settings (which became 4 during the Second World War, and was chosen between 5 rotors), and all of that put together. This session was even more interesting, and engaging than the guided tour, and was overall the best part of the Bletchley Park trip, in my view.

In conclusion, I would highly recommend visiting Bletchley Park due to how engaging the park is and its history. But I would also recommend that you try to explore the whole of Bletchley Park not only one aspect as your experience would be far better this way.

The Women of Bletchley Park by Sammy Jarvis

Whilst war produces countless horrors we are determined not to repeat, it provides mankind with revelations advancing humanity far beyond what peace offers. New technologies, medicines, beliefs and rights rapidly develop expanding the next generation into a stronger and more unified society. For instance, prior to World War II, women were generally encouraged to stay at home, or work low-skilled, low-paid jobs such as receptionists or department store clerks. Once World War II began, however, millions of men departed to join the war and women were requisitioned into the civilian and military jobs they left behind. This service consequently inspired their fight for social change and equality. Bletchley Park is one example of women becoming part of the workforce, later supporting the feminist movement.

Throughout World War II, nearly 10,000 workers were stationed at Bletchley Park, of whom over 75% were women. However, very few of these women were cryptanalysts working at the same level as their male peers. Interestingly, at the start of the war, it was mainly upper-class, well-educated women who were offered jobs at Bletchley Park, as

after attending foreign finishing schools they could understand German, and were therefore recruited as linguists. Nevertheless, as more and more men were shipped off to war, women were introduced into the numerous listening stations, intercepting German radio communications, and as secretaries, filing calls into date order. After the first Bombe machine became operational in August of 1940, women then commenced to operate these huge Enigma readers, described as “great metal bookcases”. Although everyone at Bletchley Park made a huge contribution to the Allies’ cause, I will specifically focus on the role played by one of the rare female code breakers, Joan Clarke.

Joan, the youngest of four children, was educated at Dulwich High School, from where she moved to Newnham College, Cambridge in 1936 to study Mathematics. In 1939 she graduated, achieving a double first in Mathematics, however this was not fully recognised, as Cambridge did not admit women to “full membership of the body academic” until after the end of World War II. During Joan’s degree at Cambridge, Gordon Welchman, one of the first mathematicians transferred to Bletchley Park, supervised her in Geometry. Aware of her unique mathematical ability, he was responsible for recruiting Joan to join the ‘Government Code and Cypher School’ at Bletchley. Reports on her work there describe her as congenial but shy, gentle and kind, and always subordinate to the men in her life, qualities that allowed her to flourish among the male-dominated world of Bletchley Park.

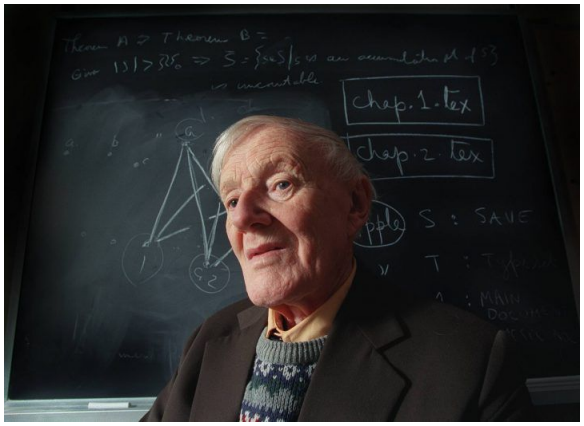
Once at Bletchley Park, Joan faced the overwhelming challenge of breaking the Enigma code, a task so daunting that Alistair Denniston, the first head of the operation, is recorded telling his fellow code breakers, “All German codes are unbreakable.” Nevertheless she quickly progressed within this field, gaining promotion after promotion until she found herself joining a small team that included Alan Turing. Joan instantly developed a close friendship with Turing, spending time with him both inside and outside work. In fact, they had actually met prior to working at Bletchley Park, as Turing knew her older brother. As the friendship thrived, Turing proposed and Joan accepted. However, a few days later Turing admitted in a letter to a devastated Joan that “he had homosexual tendencies,” and so the marriage was abandoned.

Joan proceeded to break two forms of the most complicated Enigma codes, used by high-ranking members of the German Army. Her endeavours were rewarded in 1947 when

she was appointed a Member of the British Empire, however due to the restraints of the Official Secrets Act, her work remained confidential into the late 1980s. Although her code-breaking achievements remain one of the greatest contributions to the war effort, Joan was originally paid just £2 a week, even though similarly qualified men received significantly more money. Additionally, she recalled only ever knowing one other female mathematical cryptanalyst. Following her death in Headington, near Oxford, in 1996, Joan was described in her insightful obituary as “one of the really good cryptanalysts of GCHQ who was liked and admired by colleagues throughout her long and dedicated career”.

It is disturbing to think that without World War II Joan’s substantial talents may never have been recognised. She, and all the other women stationed at Bletchley Park, not only made an immense contribution to the Allies’ effort but also advanced social change. Their momentous actions may have sped up the integration of women into the workforce, promoting the more acceptable society we are deeply grateful for today.

Bill Tutte: The Unsung Codebreaker by Archie Leishman



Without the work of Bill Tutte, the outcome of World War Two may have been very different, yet few people know about the genius codebreaker. Born in 1917 in Suffolk, Tutte’s humble background was no obstacle for his incredible mathematical ability and in 1935 he gained a scholarship to study Natural Sciences, specializing in chemistry, at Trinity College Cambridge. He graduated in 1938 with a first class honours degree. He continued to study physical chemistry until 1940 when his focus changed to maths, which would prove to have a profound effect on the future of his country.

Whilst studying maths he and three of his Cambridge friends became some of the first to solve the problem of ‘squaring the square’, and the first to solve it without a sub rectangle. Tutte was one of the brilliant mathematicians recruited to join the Government Code and Cypher School at Bletchley Park.

Alan Turing and his colleagues were already working on decoding the Enigma Machine. However there was evidence that the Nazis were sending secret messages using another

system. Initially Tutte worked on the Hagelin cypher, which was a rotor cypher machine being used by the Italian Navy. However as it was commercially available, the team at Bletchley already knew how the mechanics of the machine worked and so only needed to work out the settings in order to decipher the messages.

However, in summer 1941 Tutte was transferred to a project called 'Fish' so named due to intelligence revealing that the Germans called the wireless teleprinter systems "Sägefisch" meaning sawfish. Fish was the British codename for the German teleprinter cipher system. Until that point, most messages had been sent via Morse code however the Germans had invented the first non-Morse link which the British nicknamed Tunny meaning tuna. This system of non-Morse communication (Tunny messages) was subsequently used by the Germans for the Lorenz SZ machines and was significantly more complicated than Enigma.

Tutte played a pivotal role in the decoding of the Tunny enciphered code. Despite never having seen the machine, nor reading anything about it, he was able to work out the functioning of the machine. It took Tutte just 6 months during 1941 for him to break the code yet the first time he set eyes on one was when a machine was brought to Bletchley in 1945 shortly before Allied victory!

His breakthroughs in the understanding of the machine led to the bulk decryption of the Tunny enciphered messages of the German High Command. This ability to view the minds of the German High Command contributed greatly to the defeat of Germany, as it also allowed the British to view the precise movements of the enemy forces. . General Dwight D. Eisenhower, Supreme Allied Commander of Allied forces wrote in a Letter:

The intelligence which has emanated from you before and during the campaign has been of priceless value to me. It has simplified my task as a commander enormously. It has saved thousands of British and American lives and, in no small way, contributes to the speed with which the enemy was routed and eventually forced to surrender.

It was possibly the single biggest intellectual achievement at Bletchley during World War Two however before Tutte could make his breakthrough, John Tiltman, Bletchley Park's cryptanalyst, made his own, working out that a Vernam Cypher was being used after view two versions of the same message that were sent with identical keys. After no further breakthroughs, in terms of diagnosing the cipher machine, Tutte was handed this key. It was then that Tutte took over. Tutte followed his training where he had been taught the Kasiski technique, which involved writing out the key on squared paper only starting a new line on the set number of characters that was suspected of being the point of repetition of the key. He tried multiple repetitions through this method, and then he found a repetition

where he observed not column repetitions, but rather diagonal ones which enabled him to develop his theory and crack the code.

With this breakthrough Tutte and the other members of the Research Section worked out the complete structure of the Lorenz machine. Moreover by November 1942 Tutte had produced a way of discovering wheel starting points of the Lorenz machine which became known as the 'Statistical Method' which was necessary in order to decrypt one of the messages. Along with his colleagues, Tutte developed algorithms and a machine to decipher the encrypted messages at greater speed as out of date secret messages are worthless!

The first machine which soon took over the breaking the codes was nicknamed "Heath Robinson" by the Wrens who operated it, after the cartoonist William Heath Robinson who drew immensely complicated mechanical devices for simple tasks. The 'Heath Robinson' was then replaced by the Colossus, which was developed by Tommy Flowers and used algorithms written by Tutte and his colleagues. The Colossus was the first programmable, electronic, digital computer. You just wouldn't want to try carrying it in your backpack!

After the war, in late 1945, Tutte returned to his studies at Cambridge, as a graduate student in Maths. He went on to create a groundbreaking PhD thesis, An algebraic theory of graphs. Tutte completed his doctorate in Mathematics in 1948. He was invited to take a position in the University of Toronto. Then in 1962 he moved to the University of Waterloo where he stayed until he retired in 1985.

Tutte's love of decoding cyphers wasn't limited to helping the Allied Powers, he also used it to beat his great nephew at the children's game Mastermind!

A Very Short Introduction to Bletchley Park by Sam Corbett

Bletchley park was originally built in 1877, and lies fifty miles north-west of London, and was originally inhabited by the Leon family, whose father was a wealthy City of London financier. The family bought 300 acres of land between the London and North-Western Railway line that passed through places such as Oxford and Cambridge, where two prominent universities were based. He started to develop sixty of these acres into his country estate. At the heart of this estate he built a mansion in a mix of different architectural styles, some like it, others hate it. He was one of the main benefactors to Bletchley village, so he was much loved by most of the local people around this area and was awarded a baronetcy in 1911.

Following the deaths of Sir Hubert and Lady Leon, in 1937, the park fell into the hands of a property developer called Captain Hubert Flaulkner, who intended to demolish the mansion and sell the land as a housing estate. This never happened though because as the threat of war loomed in 1938 amd as Hitler invaded Austria and then Czechoslovakia the government decided that the Code and Cypher School (GC&CS) was in need of a safer location to stay so the school can continue intelligence throughout air attacks unhindered. Bletchley park was decided as a perfect location for it to relocate to as it was near a junction of major reads, rail and teleprinter connections to many major parts of the country. The estate was bought by the government and was commanded by Alastair Denniston. The area was given the cover name of Station X, this was due to it being the tenth of a large number of sites acquired by MI6 for its war time efforts.

After much preparation and a series of trial runs the first codebreakers arrived in August 1939. They told the surrounding locals that they were “Captain Ridley’s Shooting Party” to disguise their identity. They were the first installment in multiple groups that worked here and helped to shorten the war by an estimated 2 years.

In Germany at this time the Enigma machine was the backbone of the German military and intelligence communications. The Enigma machine was created in 1918 and was initially designed to facilitate secure banking communications, but achieved little success in this field, however the Germans, as they were

building up their military, noticed the potential that it has in the military field. At this point it was thought to be unbreakable, and this wasn't without reason. The Enigma machine was complex and those who didn't know the settings had a chance of 150 quadrillion to one of breaking it. However in 1932 the polish had broke Enigma, when the encoding machine was undergoing trials in the German military, they even managed to reconstruct one, at this time the cypher was only altered once a month though, so an extended solution was eligible, however when war started they started to change the settings once a day effectively locking the Polish out. However in 1939 two of these code breakers decided to pass their information that they had previously gathered to the English and the French. This is expected to have saved those at bletchley park anywhere between 6 months and 2 years of time before breaking enigma. Using the knowledge that they were given the codebreakers were able to exploit a chink in Enigma's armour. It had a fundamental flaw, a letter would never be encrypted as itself. Using this information they set up a listening network to listen to German communications, and spent the next few years attempting to decode the german communications. Finally Alan Turing developed an idea proposed by the Polish cryptanalysts. The result was the Bombe, an electro-mechanical machine that greatly reduced the odds, and therefore the time required to break the daily-changing Enigma keys.

After peace had been declared, the code breaking activity ceased. On the orders of Churchill every scrap of evidence was destroyed. As the second world war gave way to the Cold War, it was vital their former ally, the USSR, would learn nothing of Bletchley Park's achievements. Everyone who worked there departed, some went to work on other countries' cyphers and worked under a new name, "Government Communications Headquarters", or as most people know it GCHQ.

Post-war, Bletchley Park was made home to a variety of different organizations such as the General Post Office and the Civil Aviation Authority, the employees of which knew nothing of the great effort that went on during the war. In 1974 FW Winterbotham, who had worked in Bletchley park during the war published a book called, "The Ultra Secret". It is an account of the work and accomplishments of the codebreaking hub. The secret was slowly revealed over the next few years. In 1991, many of the organizations who had occupied Bletchley Park had left, and there were many people who wanted to demolish the site in favour of building a housing development and a supermarket. However in 1992, a young Milton Keynes Councillor, Sam Crooks had persuaded that the remainder of the park should be protected, and a few days later the Bletchley Park Trust was formed, and that brings us to where we are today, Bletchley park is still protected by Bletchley Park Trust, and you can go and visit it and see the history of it for yourself.

The Impact of Bletchley Park on Today's World by Toby Pinnington

At the end of the Second World War, General Dwight D. Eisenhower, the Supreme Allied Commander, wrote to those working at Bletchley Park. In part of his letter, he says: 'The intelligence which has emanated from you before and during the campaign has been of priceless value to me. It has simplified my task as commander enormously. It has saved thousands of British and American lives.' This summarises the obvious impact of Bletchley Park on how we live today: if it were not for their hard work then many more would have died. The Nazis may have even won the war. Whilst this is the clearest effect, there are many others we just don't realise; all of which stemmed from the groundbreaking work done at Bletchley Park.

One huge, yet unnoticed, impact of Bletchley Park is the work they did which paved the way for the modern computer. In 1940, Hut 8 had a machine called the BOMBE (pronounced 'bom') installed. It was designed by Alan Turing and Gordon Welchman, two highly respected codebreakers and mathematicians. The machine worked by finding the positions and settings of the Enigma using a 'crib'. A 'crib' is a word or phrase that would be frequently used by a German radio operator. One example is the phrase 'Das Wetter', which began every German weather report sent at 6.00AM. These settings were then used on the British version of the Enigma, Typex, to discover if the result was an actual German message. The BOMBE was vital to breaking early Second World War messages, and also because it paved the way for the Colossus.

By 1942, German High Command began using the Lorenz Cipher Machine. This was more complex than any other cipher previously used, and the codebreakers at Bletchley had never seen one before. After months of detailed study, Bill Tutte completed what is widely regarded as 'the greatest feat of reverse engineering in history'. This allowed the Allies to understand how the Lorenz worked without even owning one. They subsequently created the Colossus, which would find the settings of the Lorenz machine and then decipher the message. This was pivotal to breaking German High Command messages, many of which were signed by Hitler himself. Furthermore, it was of huge technological importance. This was the first machine to undertake operations using entirely vacuum tubes, the predecessor of the modern transistor. It was basically a large-scale modern computer. This was the first of its kind and it shows how the necessity for invention at Bletchley Park contributed greatly to our modern lives. Even after the War, those who worked there still contributed to computing developments. In the 1960's, Gordon Welchman wrote an article on a concept now called cloud computing. At the

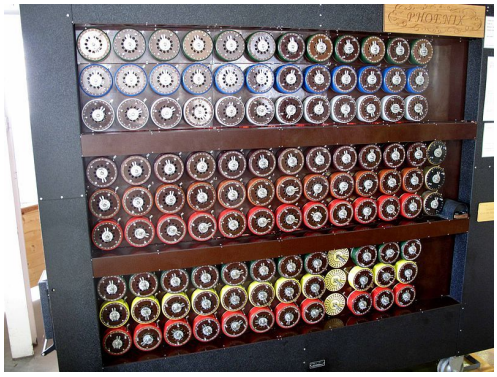
time it was important to the US military, who needed a central location to store their data. However, it is now used by all of us to store our documents and access them on any device. It just shows how important Bletchley Park, and all those who worked their, were to creating the modern technological world.

Another important contribution of Bletchley Park was towards our modern codebreaking centres. In 1919, Alastair Denniston founded the GCHQ (Government Communications Headquarters). This organisation presided over Bletchley Park, and is responsible today for signals intelligence and cyber-security. In 2017, they managed to foil seventeen terrorist attacks. This is a huge number of lives still being saved by what Bletchley Park pioneered in 1938. Many codebreaking techniques still important to modern security were created by Bletchley Park. The most important of these is the use of computers in decrypting and encrypting codes, in which the BOMBE and the Colossus were vastly important. It would be an understatement to say that Bletchley Park was an enormous development in cryptanalysis and codebreaking.

In summary, it is plain to see how Bletchley Park shaped the war effort. Through their hard work, the soldiers of D-Day knew everything about every Nazi fortress, and the Nazis were fed incorrect information about where the troops would land. They made just as great a contribution to the war effort as every other soldier. But this is only the surface of their contribution to our lives today. As shown above, they revolutionised modern, digital computing and the cyber-security we find so important today. They did so much more too, making advances in areas of mathematics and crypto-analysis. Bletchley Park is a testament to how the necessities of war have ended up making our lives better, even 100 years later.

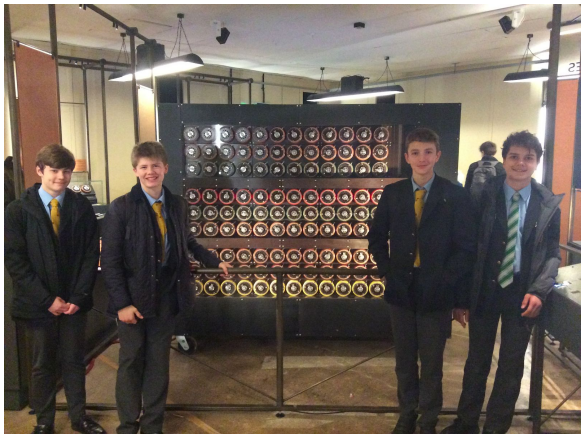
A Beginner's Guide to the Bombe

by Luca Zurek



What is a Bombe?

Essentially a Bombe is an electro-mechanical device or you could say computer, that was used to greatly narrow down the possibilities of what an enigma cipher could be. It was originally designed in 1939 by Alan Turing and was delivered to Bletchley Park in March 1940. The Bombe was based on the Polish Bomba which was designed to decode the old enigma codes used by businessmen in the early 1930s.



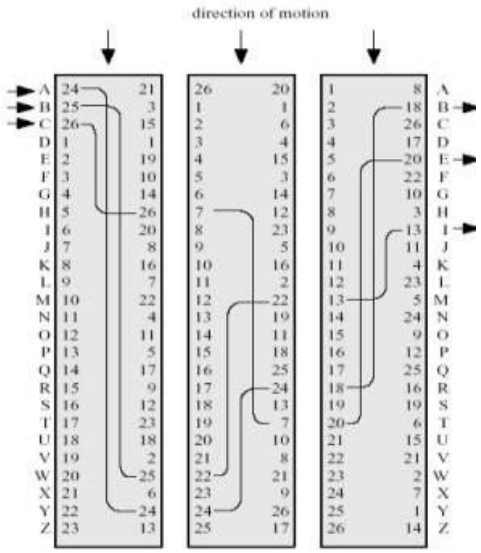
What is the Enigma Cipher?

Commonly called a code when it is really a cipher as it changes the letters from the input rather than substitute other words from the input. The enigma cipher was used by the germans during World War Two but it was really invented for wealthy businessmen who wanted to send private messages. It was later taken over by the German army and made much more complex. After the changes the enigma machine had an absurd amount of possible outcomes for every letter you type into it (103,325,660,891,587,134,000,000 to be precise).

How did the enigma machine create so many possible outcomes?

The enigma machine had three main ways of scrambling letters, the rotor combinations, the rotor settings and the plug board. There were five different rotors of which only three were ever in use (later models for german submarines used four of the rotors which complicated it even more but we will just talk about the three rotor model). The setting for which a rotor is at basically means what connection is for what letter. In the diagram(right), the first rotor setting is at 24 since 24 is the letter which 'a' is at. The connection between 24 and 26 is what the

rotor does, it scrambles the letter, and once it has done one operation the rotor rotates and then there are very different connections for ‘a’. This happens for all three rotors apart from the fact that the second and third rotor only rotate when the rotor to their left has made a full rotation. The plug board then scrambles the letters even more because it changes certain letters but not others. It works by placing up to ten wires between different plugs which represent letters. For example if ‘a’ is wired to ‘b’ then when you type an ‘a’ before it even goes into the rotors it gets converted into a ‘b’. This hugely complicates the whole system because there are roughly 150 trillion ways to wire up the plug board.

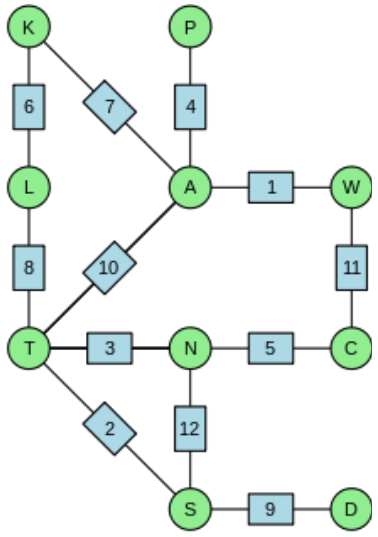


The Fatal flaw

There was one major flaw in the enigma machine that ultimately led to it being reliably deciphered. This was the fact that you couldn’t get the same letter out that you put in. This may sound like a good thing but it meant that if you predicted some words then you could greatly narrow down the possible outcomes. This is because if you knew what some words meant then if you tried deciphering it with a certain link though all the different stages of the enigma machine then it was unbelievably likely that you would come to a logical contradiction.

Basic Principles

The Bombe relied on the fact that you can’t get the same letter out of that which you typed in. The Bombe functions by looking for contradictions, the operator needs to put in an input which you have already deciphered, it then runs hundreds of thousands of possible outcomes and looks for contradictions. The Bombe will stop when it finds a crib(solution) that isn’t a contradiction, this doesn’t mean it is correct but it does mean that there is a decent chance of it being correct.



Cribs

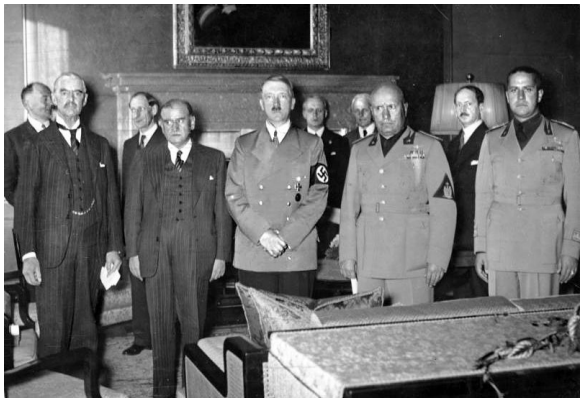
The Bombe worked on the fact that codebreakers were able to find words that they could decipher. A crib is a representation of these letters being deciphered, a crib can be

more and more complex depending on how much you were able to decipher, the more complex a crib is the better the chance of the bombe finding the right solution. A crib can be represented by a diagram, shown right, the letters are the letters that they have figured out and the numbers are the order in which they were figured out. The numbers are important because remember that the cipher changes with every letter. In the crib on the right there are three loops, 'KLAT', 'AWCNT' and 'TNS', these loops are very important because they greatly decrease the possible chances that the full crib can be. What the Bombe does is complete the crib without creating any logical contradictions, and this is when it stops.

The German Equivalent of Bletchley Park by Rupert Matthews

During WWII, every side was racing to discover what the others were going to do next. The British codebreakers were hugely successful, especially in Bletchley park. However, we never hear about what the Germans were doing.

In fact, the German codebreakers had some huge successes. Their aim was to intercept and decrypt the British naval cyphers. Yet just as they did not know about our spying, we did not know about theirs.



Germany had many places that worked on codebreaking. For example, there was one called Goering's Research Bureau. This was an organization set up by the Nazi party in 1933. It started out analysing the country's internal communications to stop dissent. But during the war, they grew. They started listening to the BBC and other broadcasters. At the start of the Second World War, this organization was able to decipher and break an entire system devised by the British and used by Neville Chamberlain to send messages to people.

As well as this, the German high command of the army, navy and airforce were all working on breaking cyphers. The army high command was extremely well manned. Over 12,000 people were working there, and in fact it was the main organization at work in Germany and was until 1945 at the end of the war.

The German naval high command had a much smaller group engaged in cypher analysis: just 1000 staff on the premise. The air force again had a large number of workers, in total it was over 13,000. After the war had ended, the British themselves commended this group of people for outstanding work in discovering the placement of the planes of both the British themselves and the Americans. This helped Germany immensely as they were able to pinpoint the Allied forces planes and destroy them.

But before the war started the Germans had the upper hand. The B-Dienst (B service) was a section of the Navy that was started in 1918 at the end of the First World War. The British mirror image of this was called the Y-service, due to the way that the letter Y sounds like the start of the word 'wireless'. The B services main breakthrough was the cracking of a type of the British Naval cypher No.1, which was being used to communicate about a British and French mission to Norway. This allowed the mission to be defeated and Germany was able to make Norway surrender within the same year.

Unfortunately for the Germans, Britain then changed the way they enciphered messages, meaning that Germany no longer had a window into British missions. This eventually led to the downfall of the B service.

Germany's downfall for the most part during WW2 was in not having a group of people entirely dedicated to cracking the cyphers of their enemies, like the British Bletchley Park was doing. This gave us, the Allied countries, an advantage over the Germans, for we could listen to what they were saying, but they couldn't even fathom what we spoke about after we changed codes. This meant we were able to make D-Day happen, with misdirection and false information, and so win the war.

Covering Up Bletchley Park: Operation Boniface by Philip Kimber

Since August 1940, with the introduction of the Bombe, Bletchley Park had access to huge amounts of information pertaining to Axis plans and communications, that would, as is claimed, shorten the war by two to three years and ensure an allied success. This sudden access to so much valuable knowledge, however, would present a significant challenge in avoiding alluding to the groundbreaking development in the intelligence field.

This newfound ability to decode Axis communications had an uncertain and risky future, given that if the Axis had made at any point significant changes to the Enigma design and protocol, Allied comprehension of these messages would require massive redevelopment of technology at Bletchley Park. Indeed, in 1942, when German Marine units were ordered to add a fourth rotor to their machines, such a challenge was presented and for months Allied intelligence relied on naval raids of keys and passwords to decode Marine transmissions. And whilst the 1942 change was found not to have been motivated by security fears, it was still evidently vital that Bletchley Park's work remain well covered-up.

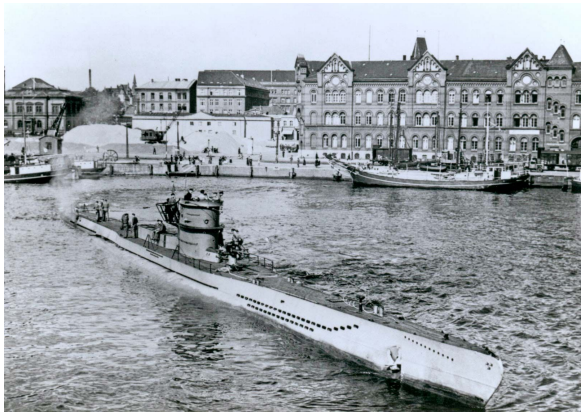
Whilst the Bletchley Park site's location and security were of utmost concern (and there was only ever one spy found to have defied this rigorous assurance), it was undeniably difficult to make use of the fruits of its labour and keep them hidden at the same time: the information they were able to decode was vital to the war effort, but mismanagement of its use could have been disastrous.

Therefore, Bletchley Park, and more crucially its information, needed a cover story. In general, all of the Park's work was claimed to have been collected by a spy called Boniface in Germany who controlled a large set of agents.

What is surprising about Boniface and his agents, however, is the fact that he did not exist to fool the Nazi High Command. Instead, their purpose was mostly to explain the information to the other Allied Forces, most importantly, the Americans. In November 1942, Alan Turing was sent over to the United States to speak to their Secret Service about the war effort, and his ultimate message, revealed by future James Bond writer Ian Fleming's diaries, was that British Intelligence was having similar events in trying to break German communication. Bletchley's work was attributed to the spy.

Much of the information in contention, given to the Americans, was the intelligence that allowed naval vessels to intercept or avoid German U-Boats. Particularly targeted were supply ships from the US to help British people survive avoiding starvation; the interception of

these being an aim to starve Britain into surrender. The cracking of the Enigma played an important role in the so-called Battle of the Atlantic.



Naval Enigma was, after 1942, modified to contain 4 rotors instead of 3, which made Bletchley Park's work in the so-called Battle of the Atlantic, much harder, and it was reported that no-one in British Intelligence bar Frank Birch and Alan Turing thought that it could ever be cracked. However, crucially, this change was not thought to have been underpinned by concern that codes had been cracked, but instead a desire for difference and revision in naval communication. Generally, the Nazis would believe rather long-winded arguments in favour of the prospect that the Enigma could have been broken, and this allowed relatively poor spotter raids to fool them into the belief that U-Boat captures were entirely coincidental.

Perhaps too much of British explanation of the unwillingness to change the Enigma has the implication that all of Hitler's High Command were completely mentally inept. There are reports of Hitler being warned of possible breach of the Enigma's security, and the Nazis came close to discovering various spies that were important in uncovering protocol information for Bletchley Park. But none of this culminated in complete realisation of the full extent of British Intelligence, and no big changes to the communications' design or protocol were ever made, which could be argued by some to have been a huge Achilles' heel of the Nazi control over Europe.

This aversion to the reality of the level of intelligence among the allies, which arguably should have been obvious to the Axis Powers, is perhaps representative of a wider issue in the figureheads of the Nazi state, particularly Hitler himself - and one that may be relevant in leaders in modern society. The strong unwillingness to believe any theory that was reflective of any elements of his forces' inferiority was an obvious bias to egocentrism. This effect can be described as egocentric bias, and can be a contributor to the false consensus effect, which confirms people to their belief that their own decisions are correct, ignoring a large amount of necessary judgement.

This effect is of course something that has been studied, and is perhaps of particular relevance today. We see lots of examples of this effect in history: for example, the Chernobyl control team believed that the fault was much more minor than it actually was, for a while, despite being told otherwise, as they put too much faith in their engineering, believing that Soviet RBMK design of reactor could not meltdown in such a way. The general concept of ego-centrism and overconfidence ultimately resulting in huge disadvantage to oneself (the Chernobyl disaster cover-up having been said to have contributed to the fall of the Soviet Union in publicising the need for transparency), is pertinent today given the

increasing tyranny of some of our world leaders.

This issue was brought to you by the Third Year Academic Scholars:

(Pictured here at the Polish Memorial at Bletchley Park)