Machines Invented for WW II Code Breaking

Beryl Plimmer
Department of Information Systems
Manukau Institute of Technology
Auckland, New Zealand
Bplimmer@manukau.ac.nz

Abstract

In 1944 a computer was commissioned at Bletchley Park in England. This computer was designed specifically to find the settings used by German cipher machines to encrypt messages, which it did very effectively. Before "Colossus" the Polish and British military had developed mechanical machines to aid with cryptography. All of this work was top secret and only with the recent release of documents has the true significance of these machines and the people who created them been appreciated.

Introduction

Security on the net and encryption of information is a real issue of the nineties. Claims of codes that can not be broken abound, many of which are later disproved. A look back at the history of machine cipher codes is a fascinating journey through European espionage, traveling through the fields of linguistics, cryptology, mathematics and engineering. Cryptography is the encrypting of messages. The flip side cryptology, the breaking of codes, is a complex process requiring message interception, decryption, and translation before the contents of the message can be assessed and distributed. The successes of the World War II Allied code breakers, some claim, shortened the war by up to two years. The Polish military contributed significantly to this work by breaking the Enigma code and developing two machines to assist the finding of keys. They shared their work with their British and French counterparts shortly before the outbreak of war. The British then went on to refine the Polish machines and develop the groundbreaking Colossus computer, a secret that remained hidden for fifty years.

The Germans used Enigma machines to encrypt military messages from 1926. The Poles broke this code in 1932. As the Germans became more sophisticated with their use of the Enigma machine, the Poles developed a mechanical device called a "Cyclometer" to do some of the more repetitive calculations. As the Germans changed the Enigma again, a more flexible device was needed. The Poles response was another machine, the "Bomba." The British refined the Polish Bomba and develop a series of valve [vacuum tube] -based devices. The prototype "Robinson," named after Heath Robinson a cartoonist renowned for drawings of fanciful machines, was followed by Colossus I and II. Little information was released on these machines until the 1970's and then much of it was sketchy. Papers released by the USA government in 1996 have revealed the true significance of these wartime machines.

The German Enigma and the Poles

The encryption or coding of messages is probably as old as written language itself. The introduction of radio transmission and machine generated ciphers brought about quantum changes in the art and science of secret messages. A broadcast message was easy to intercept and therefore encryption became more important. As early as 1918 the Germans were considering the use of cipher machines [Kozaczuk, 1984]. This experimentation was briefly interrupted by their defeat in World War I. In 1926 the German army and navy began using the Enigma cipher machines. These were a variation on the commercial Enigma machine, which had been available for some time.

The military Enigma had a twenty-six-character typewriter keyboard, which was connected through a plug board to three drums. Each of these drums had the characters arranged around the drum. Each drum had rotors, which moved the drum in a regular pattern. Next there was a reversing drum. Each character was transposed from the keyboard, through the plug board, through each of the three drums, the reversing drum and back through the three drums. The beauty of the Enigma was that there was no correspondence between the frequency of a letter in the cipher to the frequency of a letter in the original message. The transposition method also meant that to decipher the message the receiver had only to set their machine to same settings as the sender's and type in the coded message for plain text to emerge. If matching drums were used (as they were by the German military) 263 combinations were possible. The order of the drums could be altered thus giving six times this number of combinations a total of 105,456 different combinations. The machine therefore had three different types of variables that made up the key: the order of the drums, the plug board setting, and the initial start position of each drum. The Germans reasoned that even if an adversary got hold of a machine, not knowing the key would mean they would be unable to decipher messages. They were mistaken. [Rejewski, 1984a, p. 250]

A remarkable group of Polish cryptologists worked on the Enigma code from 1932. Marian Rejewski was the first assigned to the task of breaking the Enigma he was then joined by Jerzy Rozycki and Henryk Zygalski. All three were mathematicians and fluent in Polish and German. In earlier times knowledge of the encryptor's language was the most essential skill. With the advent of machine encryption,

Reviewed Papers

mathematics assumed more importance. The subterranean world of European espionage provided the team with some vital clues. They received a commercial Enigma machine, which although different from the military version it was based on the same principles. The French at one stage provided the keys settings for two months. The Poles used the commercial machine as a model to construct their own Enigma. They also developed techniques for deciphering the daily keys and message keys. The Poles manufactured a number of Enigmas and from 1933-1935 daily broke the German codes. When the code was found, a small team set about deciphering the messages using their Enigmas and then translating the German military messages [Rejewski, 1984b].

During this period the Germans did not make any changes to the Enigma, altering the drum positions only quarterly. This gave Rejewski, Rozycki and Zygalski time to refine their methods. From February 1936 the drums were moved monthly and then from October of the same year they were moved daily. At the same time the number of plug pairs was increase from original six to seven or eight. Germany had by now expanded its military and the number of codes that had to be broken daily had consequently increased. By using the characteristic of configurations that occurred infrequently the Polish team devised a machine to determine the drum settings. This machine they named a "Cyclometer". This machine consisted of two drums, and a set of twenty-six bulbs and switches for each letter, and cards (similar to Hollerith cards) to record matches. It took more than a year for this work to be completed, but when it was, the daily key could be obtained in ten to twenty minutes. Unfortunately, at about the time the Cyclometer was completed the Germans changed the reversing drum and the task had to be redone.

In September 1938 the Germans changed the procedure for giving message keys. The techniques that the Poles had by now perfected were ineffective. They worked on a number of ideas, one of which resulted in the construction of a machine that consisted of a set of drums which over a period of about two hours could work through the 263 permutations possible with one arrangement of the three drums, the "Bomba". The Poles built six of these machines to allow all possible combinations to be explored. They also started to make a series of punch sheets that showed all possible combinations of the codes.

In December 1938 the Germans introduced two new drums, there were then five drums, any three of which would be used at one time. In January 1939 they increased the number of plug pairs to ten. The Polish team was still able to read some of the German messages, but its success rate was greatly reduced from the 75% they had achieved a year earlier.

In July 1939 representatives of British and French intelligence were invited to a meeting in Warsaw. Up until this time the Poles not disclosed their discoveries to no one. At this meeting the Poles shared their knowledge with the French and British and gave each an Enigma machine. Either then or sometime later they also gave the British the plans for the Bomba. At this point it seems that the French and British had not cracked the Enigma code, nor had they an Enigma or any deciphering devices such as the Polish Cyclometer or Bomba. Rejewski states "from our guests we learnt nothing" [Rejewski, 1984b, p.269].

Shortly after this the Germans invaded Poland. The cipher bureau fled a team of about fifteen people and re-established itself in Paris. In 1940 they were forced to flee again, this time to Algeria, later to return to the unoccupied zone of France. They continued to work but changes to the German systems and lack of resources limited their effectiveness. Rozycki died in 1942 when a boat he was a passenger on was sunk. Later that year the Germans invaded the unoccupied zone. The cipher bureau was again disbanded travelling together, Rejewski and Zygalski made their way to Spain. Eventually, they found their way to Britain where they worked on solving German ciphers until the end of the war, though not on the Enigma. They were not involved with Bletchley Park, the centre for British code breaking.

It should be noted that the above is the Polish version of the Enigma decoding based on the book "Enigma: How the German machine cipher was broken, and how it was read by the Allies in World War Two" by Kozaczuk [Kozaczuk, 1984]. There are other versions of this story, and they vary widely. Which is true? It is possible that there are elements of truth in many of the different accounts and some of the discrepancies are most certainly as a result of the secrecy that has surrounded this code breaking.

Bletchley Park

Bletchley Park was the World War II centre for the British Government Code and Cipher School (GC & CS), a section of the British Intelligence Service. It was a large establishment. By 1945 there were 9000 people working at Bletchley Park. The work that was carried out there was perhaps the best kept secret of WW II. Such was the secrecy within the establishment that people did not know what the people in the room next to them were doing [Stripp, 1989]. The whole operation was compartmentalised with few (if any) people having complete knowledge of what was going on. The 'need to know' principle was rigorously applied; people were only told what they really needed to know. Stripp muses that sometimes the lack of sharing of information may have slowed the work.

There was a flurry of publications in the 1970's about the work at Bletchley Park. There are inconsistencies and contradictions, many of which could be attributed to the limited knowledge that each individual held. Even in 1970 much of the information was still classified and it was when the Americans released some WW II documents in 1996 that a fuller picture emerged.

When the British returned from Warsaw in 1939 armed with the knowledge the Polish team had shared with them, they began again on the Enigma cipher. Alan Turing with contributions from Gordon Welchman [Hodges, 1996] generalised the Polish Bomba, making it a more flexible and powerful device. This machine is generally referred to as the Turing Bombe. Different branches of the German military

had been using different coding techniques on the Enigma for some time. The Germans continued to complicate the encrypting process, hence making the decryption more difficult. Each new advance by the Germans had to be countered with either enhancements to the Bombe or refinement of its use. The British also made their own versions of the Enigma to convert the ciphers once the keys had been deduced.

A large number of Bombes were made and positioned at Bletchley Park and a number of other sites. They were operated by Wrens (Women's Royal Naval Service). Diana Payne [Payne, 1993] describes the machines as being about 8 feet tall and seven feet wide. The front showed a row of drums, each of which had the letters of the alphabet painted on it. The back was a tangle of plugs on rows of letters and numbers. The Wrens were given a 'menu', which was drawing of how to plug up the machine. When in operation the drums rotated making a lot of noise. When the key was deciphered the machine stopped and the Wrens read off the setting which were then used to decrypt the messages.

In 1940 the Germans introduced the Lorenz *Schlussel-zusatz* encryption machines. By 1941 these machines were used by the German army, and more importantly, German high command. These machines converted each character into a five-bit word of either dots or x's (a binary code) and then encrypted this code, before transmission. The encryption was via a series of wheels; each bit was passed through two wheels, which either changed or left unaltered the dot or x. The wheels had varying numbers of teeth and each tooth could be set on or off [Fox, 1997]. The first set of five wheels, that the British named K wheels, advanced one position for each character. The second set of five wheels, S wheels, advanced less frequently dependent on the setting of two other wheels, known as M1 and M2.

In August 1941 a German radio operator made a mistake. He transmitted a message a second time with the same wheel settings and start positions, abbreviating the first word on the second transmission. This allowed John Tiltman, a cryptologist to decipher the messages. Bill Tutte, a mathematician at Bletchley Park was then able to deduce the design of the 'Tunny' machine, as Bletchley named it.

The expression for encryption was described as $Z = P + K + S$. The encrypted message, Z, equaled the Plain message plus the first set of wheel settings, K, plus the second wheel setting, S. However because of the vast number of combinations, it took code-breakers up to two months to find the right settings for a message and thus decode it. An automated solution was required.

Max Newman, a mathematician, has been credited with the conceptual design of the resulting machines. Binary mathematics means that $Z + K = S + P$. The mathematicians found that repeated letters occurred more often than was statistically expected. If the maximum number of repeats were found, the K wheel start position could be deduced. This was to be the job of the machine. Donald Michie and Jack Good then showed how Colossus could be reprogrammed to work out the setting of each K wheel. The S wheels did not rotate with each letter but more infrequently depending on the setting of two auxiliary wheels M1 and M2. As about one-third of a message was readable with the K settings, the S and M settings were deduced by more conventional means.

T.H. Flowers at the Post Office Research Station at Dollis Hill was commission to design and make the machine. The prototype was called 'Heath Robinson'. It proved successful and Colossus Mark I was commissioned in January 1944. Colossus Mark II followed in June 1944. The encrypted message was read by the machine from paper tape. A message could require up to 13 metres of tape and was read at a rate of 5,000 characters a minute. The design of this reader was the work of Dr Arnold Lynch at Dollis Hill, and in keeping with the segregation of knowledge, he was given the specifications that the machine had to meet but was never told the purpose of the tape reader.

Colossus II had 2500 valves, some of which emulated the teeth of the wheels on the Lorenz machine and could be turned on and off by way of plug boards. The machine used exclusive OR's to compare the message against the settings of the thyratron valves and used special valves called pentodes to add the bits together. Colossus then counted the number of matches. The machine had to systematically work through all the possible combinations of K wheel settings. To enable the processing to progress at speed, the machine was arranged so that it could work on the two bit streams in parallel. Yes a parallel processor in 1944!

The Post Office Research Station was also given the job of constructing some Tunny machines. The German machines were mechanical, the British version electrical. The wheels of the Lorenz machine were simulated by electrical switches that could be set by telephone plugs. When the settings of the wheels had been found by Colossus, the Tunny machine could be set up to decrypt a message. Gill Hayward who was involved in the construction of the Tunny machines explains that although a mechanical model would have been easier to construct, this suggestion was turned down, as it would mean that too many people would have to know about it. He "privately cherished the idea of building a Tunny with Meccano." The parts, that were all from standard telephone exchanges of the time, had to be ordered in such a way that despatch would have no idea as to what use they were being put. He conceded that the resulting electrical Tunny was a versatile machine that could be adapted when the Germans made enhancements [Hayward, 1993].

Between June 1944 and the end of the war, 10 - 12 (accounts vary) Colossus machines were built and commissioned. Wrens in shifts operated them so the machines worked twenty-four hours a day. Catherine Caughey [Caughey, 1996] was one of the first group of Wrens to trained on the Colossus. She describes how a group of 15 of them arrived at Bletchley Park on 1st February 1944 and spent two weeks with Max Newman teaching them a new set of mathematics. They were then set to work on Colossus I. She describes how the German messages were intercepted in Kent and transmitted by phone to teleprinters. The start signal at the beginning of each tape

gave the cipher setting and was used to program Colossus. The tape would often break and require repair and Colossus would often break down. She reports that Colossus II was more reliable in both respects.

At the end of the war Churchill feared the new enemy, the Russians, would learn the Allies' code breaking secrets. He ordered the destruction of all but two of the Colossus machines. Those last two machines were dismantled in the 1960's. All the work that had gone on at Bletchley Park was classified. Little emerged until the 1970's. Most of the information on Colossus was still classified until 1996 when the Americans released documents on the Bombe and the Colossus. Tony Sale, an expert on early computers and now the Museum Director of Bletchley Park, received permission to rebuilt Colossus I in 1993. He went on to reconstruct the design of Colossus II from a few photographs, some drawings which engineers had kept (illegally), and interviews with some of the people who had worked on Colossus [Sale, 1995]. On June 6th 1996, the 52nd anniversary of D-day, the reconstruction was complete and Colossus went into operation. Present, among others, were Tommy Flowers and Bill Tutte.

Conclusion

The accomplishments of these pioneers of computing were outstanding. The Polish team were the first to crack the Enigma code and appreciate that machine encryption would benefit from machine assisted decryption. Their work in developing a copy of the Enigma machine and the Cyclometer and Bomba provided the foundation for the later British work. Amazingly, the Polish accomplishments were by a team of three, with about another dozen doing much of the routine work. In contrast, the British had thousands working on code breaking. They had many of their best mathematicians, statisticians, engineers and cryptologists working together at Bletchley Park. The refinement of the Polish Bomba by Turing proved the worth of machines to assist in code breaking. Newman's work on the possibility of mechanising the code breaking for the Lorenz machine set the scene for the development of the first electronic machines. The resulting Colossus computers were a remarkable achievement. They worked for 24 hours a day from the time they were installed until the end of the war providing the calculation power required to decode the German messages. They were extremely specialised and very effective. Sale [Fox, 1997] simulated the Colossus on a Pentium; the Colossus was twice as fast. The construction of the Tunny machines as electrical devices, rather than mechanical, also indicates a change in emphasis.

Some of the people who worked at Bletchley park went on to make further contributions to the development of computers. Often the source of their knowledge could not be identified as it came from their 'secret time' at Bletchley Park. Many were pleased to leave this world where they could share nothing of their daily work with friends and family. This concealment did not end with the end of the war. Caughey's [Caughey, 1996] husband never knew of her war work when he passed away before any of the work at Bletchley was declassified.

What can we learn from this part of our history as more and more information is transmitted electronically and encrypted? I for one, will never believe a code to be unbreakable. Clearly some codes require a great deal of effort to break, but if it's worth the effort, someone will do it. It is also clear that both the Poles and British made break throughs when they 'acquired material' or the Germans made a mistake. But to 'err is human' and who could set up a system which is absolutely foolproof? The ingenuity and persistence of these code breakers is something we can look back on and marvel at.

One question remains in my mind: much of the literature stresses that the Germans were confident that their codes could not be broken. If this was indeed the situation, why then did they continue to enhance the Enigma and the Lorenz machines? This continued development of their cipher machines implies to me that they had some idea that the Allies were breaking at least some of the codes.

References

1. Caughey, C.M. (1996). World Wander: Kenya to Bletchley Park to New Zealand. Auckland: Catherine M. Caughey.
2. Fox, B., Webb, J., (1997). Colossal Adventures. New Scientist, v154(n2081), 38-43.
3. Hayward, G. (1993). OperationTunny. In A. Stripp, Hinsley, F.H. (Ed.), Codebreakers: The Inside Story of Bletchley Park (pp. 167-191). Oxford: Oxfor University Press.
4. Hodges, A. (1996). Alan Turing --- a short biography, Part 4 --- The Second World War: <http://www.wadham.ox.ac.uk/~ahodges/Enigma.html>.
5. Kozaczuk, W. (1984). Enigma: How the German machine cipher was broken, and how it was read by the Allies in World War Two (Kasperek, C., Trans.). (English Translation ed.): University Publications of America, INC.
6. Payne, D. (1993). The Bombes. In A. Stripp, Hinsley, F.H. (Ed.), Codebreakers: The Inside Story of Bletchley Park (pp. 132-137). Oxford: Oxfor University Press.
7. Rejewski, M. (1984a). How the Polish Mathematicians Broke Enigma. In W. Kozaczuk (Ed.), Enigma: How the German machine cipher was broken, and how it was read by the Allies in World War Two (pp. Appendix D p. 246-270): University Publications of America, INC.
8. Rejewski, M. (1984b). The Mathematical Solution of the Enigma Cipher. In W. Kozaczuk (Ed.), Enigma: How the German machine cipher was broken, and how it was read by the Allies in World War Two (pp. Appendix E p. 272-290): University Publications of America, INC.
9. Sale, T. (1995). The Colossus of Bletchley Park. IEE Review, 41(March), 55-59.
10. Stripp, A. (1989). Codebreaker in the Far East. London: Frank Cass & Co. Ltd.