condemnation of those responsible for German security, who then had to admit in their own report that, "the German fleet command, whose radio messages were intercepted and deciphered by the English, played so to speak with open cards against the British command."

- The German military held an enquiry into how to avoid repeating the cryptographic fiascos of the First World War, and concluded that the Enigma machine offered the best solution. By 1925 Scherbius began mass-producing Enigmas, which went into military service the following year, and were subsequently used by the government and by state-run organizations such as the railways. These Enigmas were distinct from the few machines that Scherbius had previously sold to the business community, because the scramblers had different internal wirings. Owners of a commercial Enigma machine did not therefore have a complete knowledge of the government and military versions.

Over the next two decades, the German military would buy over 30,000 Enigma machines. Scherbius's invention provided the German military with the most secure system of cryptography in the world, and at the outbreak of the Second World War their communications were protected by an unparalleled level of encryption. At times, it seemed that the Enigma machine would play a vital role in ensuring Nazi victory, but instead it was ultimately part of Hitler's downfall. Scherbius did not live long enough to see the successes and failures of his cipher system. In 1929, while driving a team of horses, he lost control of his carriage and crashed into a wall, dying on May 13 from internal injuries.

4 Cracking the Enigma

In the years that followed the First World War, the British cryptanalysts in Room 40 continued to monitor German communications. In 1926 they began to intercept messages which baffled them completely. Enigma had arrived, and as the number of Enigma machines increased, Room 40's ability to gather intelligence diminished rapidly. The Americans and the French also tried to tackle the Enigma cipher, but their attempts were equally dismal, and they soon gave up hope of breaking it. Germany now had the most secure communications in the world.

The speed with which the Allied cryptanalysts abandoned hope of breaking Enigma was in sharp contrast to their perseverance just a decade earlier in the First World War. Confronted with the prospect of defeat, the Allied cryptanalysts had worked night and day to penetrate German ciphers. It would appear that fear was the main driving force, and that adversity is one of the foundations of successful codebreaking. Similarly, it was fear and adversity that galvanized French cryptanalysis at the end of the nineteenth century, faced with the increasing might of Germany. However, in the wake of the First World War the Allies no longer feared anybody. Germany had been crippled by defeat, the Allies were in a dominant position, and as a result they seemed to lose their cryptanalytic zeal. Allied cryptanalysts dwindled in number and deteriorated in quality.

One nation, however, could not afford to relax. After the First World War, Poland reestablished itself as an independent state, but it was concerned about threats to its newfound sovereignty. To the east lay Russia, a nation ambitious to spread its communism, and to the west lay Germany, desperate to regain territory ceded to Poland after the war. Sandwiched between these two enemies, the Poles were desperate for intelligence information, and they formed a new cipher bureau, the Biuro
Szyfrów. If necessity is the mother of invention, then perhaps adversity is the mother of cryptanalysis. The success of the Biuro Szyfrów is exemplified by their success during the Russo-Polish War of 1919–20. In August 1920 alone, when the Soviet armies were at the gates of Warsaw, the Biuro deciphered 400 enemy messages. Their monitoring of German communications had been equally effective, until 1926, when they too encountered the Enigma messages.

In charge of deciphering German messages was Captain Maksymilian Ciezki, a committed patriot who had grown up in the town of Szamotuty, a center of Polish nationalism. Ciezki had access to a commercial version of the Enigma machine, which revealed all the principles of Scherbius’s invention. Unfortunately, the commercial version was distinctly different from the military one in terms of the wirings inside each scrambler. Without knowing the wirings of the military machine, Ciezki had no chance of deciphering messages being sent by the German army. He became so despondent that at one point he even employed a clairvoyant in a frantic attempt to conjure some sense from the enciphered intercepts. Not surprisingly, the clairvoyant failed to make the breakthrough the Biuro Szyfrów needed. Instead, it was left to a disaffected German, Hans-Thilo Schmidt, to make the first step toward breaking the Enigma cipher.

Hans-Thilo Schmidt was born in 1888 in Berlin, the second son of a distinguished professor and his aristocratic wife. Schmidt embarked on a career in the German Army and fought in the First World War, but he was not considered worthy enough to remain in the army after the drastic cuts implemented as part of the Treaty of Versailles. He then tried to make his name as a businessman, but his soap factory was forced to close because of the postwar depression and hyperinflation, leaving him and his family destitute.

The humiliation of Schmidt’s failures was compounded by the success of his elder brother, Rudolph, who had also fought in the war, and who was retained in the army afterward. During the 1920s Rudolph rose through the ranks and was eventually promoted to chief of staff of the Signal Corps. He was responsible for ensuring secure communications, and in fact it was Rudolph who officially sanctioned the army’s use of the Enigma cipher.

After his business collapsed, Hans-Thilo was forced to ask his brother for help, and Rudolph arranged a job for him in Berlin at the Chiffrierverwaltung, the office responsible for administrating Germany’s encrypted communications. This was Enigma’s command center, a top-secret establishment dealing with highly sensitive information. When Hans-Thilo moved to his new job, he left his family behind in Bavaria, where the cost of living was affordable. He was living alone in expensive Berlin, impoverished and isolated, envious of his perfect brother and resentful toward a nation which had rejected him. The result was inevitable. By selling secret Enigma information to foreign powers, Hans-Thilo Schmidt could earn money and gain revenge, damaging his country’s security and undermining his brother’s organization.

On November 8, 1931, Schmidt arrived at the Grand Hotel in Verviers, Belgium, for a liaison with a French secret agent codenamed Rex. In exchange for 10,000 marks (equivalent to $30,000 in today’s money), Schmidt allowed Rex to photograph two documents: “Gebrauchsanweisung für die Chiffriermaschine Enigma” and “Schlüsselanleitung für die Chiffriermaschine Enigma.” These documents were essentially
instructions for using the Enigma machine, and although there was no explicit description of the wirings inside each scrambler, they contained the information needed to deduce those wirings.

Thanks to Schmidt's treachery, it was now possible for the Allies to create an accurate replica of the German military Enigma machine. However, this was not enough to enable them to decipher messages encrypted by Enigma. The strength of the cipher depends not on keeping the machine secret, but on keeping the initial setting of the machine (the key) secret. If a cryptanalyst wants to decipher an intercepted message, then, in addition to having a replica of the Enigma machine, he still has to find which of the millions of billions of possible keys was used to encipher it. A German memorandum put it thus: "It is assumed in judging the security of the cryptosystem that the enemy has at his disposition the machine."

The French Secret Service was clearly up to scratch, having found an informant in Schmidt, and having obtained the documents that suggested the wirings of the military Enigma machine. In comparison, French cryptanalysts were inadequate, and seemed unwilling and unable to exploit this newly acquired information. In the wake of the First World War they suffered from overconfidence and lack of motivation. The Bureau du Chiffre did not even bother trying to build a replica of the military Enigma machine, because they were convinced that achieving the next stage, finding the key required to decipher a particular Enigma message, was impossible.

As it happened, ten years earlier the French had signed an agreement of military cooperation with the Poles. The Poles had expressed an interest in anything connected with Enigma, so in accordance with their decade-old agreement the French simply handed the photographs of Schmidt's documents to their allies, and left the hopeless task of cracking Enigma to the Biuro Szyfrów. The Biuro realized that the documents were only a starting point, but unlike the French they had the fear of invasion to spur them on. The Poles convinced themselves that there must be a shortcut to finding the key to an Enigma-encrypted message, and that if they applied sufficient effort, ingenuity and wit, they could find that shortcut.

As well as revealing the internal wirings of the scramblers, Schmidt's documents also explained in detail the layout of the codebooks used by the Germans. Each month, Enigma operators received a new codebook which specified which key should be used for each day. For example, on the first day of the month, the codebook might specify the following day key:

1. Plugboard settings: A/L-P/R-T/D-B/W-K/F-O/Y.
2. Scrambler arrangement: 2-3-1.
3. Scrambler orientations: Q-C-W.

Together, the scrambler arrangement and orientations are known as the scrambler settings. To implement this particular day key, the Enigma operator would set up his Enigma machine as follows:

1. Plugboard settings: Swap the letters A and L by connecting them via a lead on the plugboard, and similarly swap P and R, then T and D, then B and W, then K and F, and then O and Y.
2. Scrambler arrangement: Place the 2nd scrambler in the 1st slot of the machine, the 3rd scrambler in the 2nd slot, and the 1st scrambler in the 3rd slot.
3. Scrambler orientations: Each scrambler has an alphabet engraved on its outer rim, which allows the operator to set it in a particular orientation. In this case, the operator would rotate the scrambler in slot 1 so that Q is facing upward, rotate the scrambler in slot 2 so that C is facing upward, and rotate the scrambler in slot 3 so that W is facing upward.

One way of encrypting messages would be for the sender to encrypt all the day's traffic according to the day key. This would mean that for a whole day at the start of each message all Enigma operators would set their machines according to the same day key. Then, each time a message needed to be sent, it would be first typed into the machine; the enciphered output would then be recorded, and handed to the radio operator for transmission. At the other end, the receiving radio operator would record the incoming message, hand it to the Enigma operator, who would type it into his machine, which would already be set to the same day key. The output would be the original message.

This process is reasonably secure, but it is weakened by the repeated use of a single day key to encrypt the hundreds of messages that might be sent each day. In general, it is true to say that if a single key is used to encipher
an enormous quantity of material, then it is easier for a cryptanalyst to deduce it. A large amount of identically encrypted material provides a cryptanalyst with a correspondingly larger chance of identifying the key. For example, harking back to simpler ciphers, it is much easier to break a monoalphabetic cipher with frequency analysis if there are several pages of encrypted material, as opposed to just a couple of sentences.

As an extra precaution, the Germans therefore took the clever step of using the day key settings to transmit a new message key for each message. The message keys would have the same plugboard settings and scrambler arrangement as the day key, but different scrambler orientations. Because the new scrambler orientation would not be in the codebook, the sender had to transmit it securely to the receiver according to the following process. First, the sender sets his machine according to the agreed day key, which includes a scrambler orientation, say QCW. Next, he randomly picks a new scrambler orientation for the message key, say PGH. He then enciphers PGH according to the day key. The message key is typed into the Enigma twice, just to provide a double-check for the receiver. For example, the sender might encipher the message key PGHPGH as KIVBJE. Note that the two PGH's are enciphered differently (the first as KIV, the second as BJE) because the Enigma scramblers are rotating after each letter, and changing the overall mode of encryption. The sender then changes his machine to the PGH setting and encrypts the main message according to this message key. At the receiver's end, the machine is initially set according to the day key, QCW. The first six letters of the incoming message, KIVBJE, are typed in and reveal PGHPGH. The receiver then knows to reset his scramblers to PGH, the message key, and can then decipher the main body of the message.

This is equivalent to the sender and receiver agreeing on a main cipher key. Then, instead of using this single main cipher key to encrypt every message, they use it merely to encrypt a new cipher key for each message, and then encrypt the actual message according to the new cipher key. Had the Germans not employed message keys, then everything—perhaps thousands of messages containing millions of letters—would have been sent using the same day key. However, if the day key is only used to transmit the message keys, then it encrypts only a limited amount of text. If there are 1,000 message keys sent in a day, then the day key encrypts only 6,000 letters. And because each message key is picked at random and is used to encipher only one message, then it encrypts a limited amount of text, perhaps just a few hundred characters.

At first sight the system seemed to be impregnable, but the Polish cryptanalysts were undaunted. They were prepared to explore every avenue in order to find a weakness in the Enigma machine and its use of day and message keys. Foremost in the battle against Enigma was a new breed of cryptanalyst. For centuries, it had been assumed that the best cryptanalysts were experts in the structure of language, but the arrival of Enigma prompted the Poles to alter their recruiting policy. Enigma was a mechanical cipher, and the Biuro Szyfrów reasoned that a more scientific mind might stand a better chance of breaking it. The Biuro organized a course on cryptography and invited twenty mathematicians, each of them sworn to an oath of secrecy. The mathematicians were all from the university at Poznán. Although not the most respected academic institution in Poland, it had the advantage of being located in the west of the country, in territory that had been part of Germany until 1918. These mathematicians were therefore fluent in German.

Three of the twenty demonstrated an aptitude for solving ciphers, and were recruited into the Biuro. The most gifted of them was Marian Rejewski, a timid, spectacled twenty-three-year-old who had previously studied statistics in order to pursue a career in insurance. Although a competent student at the university, it was within the Biuro Szyfrów that he was to find his true calling. He served his apprenticeship by breaking a series of traditional ciphers before moving on to the more forbidding challenge of Enigma. Working entirely alone, he concentrated all of his energies on the intricacies of Scherbius's machine. As a mathematician, he would try to analyze every aspect of the machine's operation, probing the effect of the scramblers and the plugboard cablings. However, as with all mathematics, his work required inspiration as well as logic. As another wartime mathematician put it, the creative codebreaker must "pereforce commune daily with dark spirits to accomplish his feats of mental ju-jitsu."

Rejewski's strategy for attacking Enigma focused on the fact that repetition is the enemy of security: repetition leads to patterns, and cryptanalysts thrive on patterns. The most obvious repetition in the Enigma encryption was the message key, which was enciphered twice at the
beginning of every message. If the operator chose the message key ULJ, then he would encrypt it twice so that ULJULJ might be enciphered as PEFNWZ, which he would then send at the start before the actual message. The Germans had demanded this repetition in order to avoid mistakes caused by radio interference or operator error. But they did not foresee that this would jeopardize the security of the machine.

Each day, Rejewski would find himself with a new batch of intercepted messages. They all began with the six letters of the repeated three-letter message key, all encrypted according to the same agreed day key. For example, he might receive four messages that began with the following encrypted message keys:

1st 2nd 3rd 4th 5th 6th
1st message L O K R G M
2nd message M V T X Z E
3rd message J K T M P E
4th message D V Y P Z X

In each case, the 1st and 4th letters are encryptions of the same letter, namely the first letter of the message key. Also, the 2nd and 5th letters are encryptions of the same letter, namely the second letter of the message key, and the 3rd and 6th letters are encryptions of the same letter, namely the third letter of the message key. For example, in the first message L and R are encryptions of the same letter, the first letter of the message key. The reason why this same letter is encrypted differently, first as L and then as R, is that between the two encryptions the first Enigma scrambler has moved on three steps, changing the overall mode of scrambling.

The fact that L and R are encryptions of the same letter allowed Rejewski to deduce some slight constraint on the initial setup of the machine. The initial scrambler setting, which is unknown, encrypted the first letter of the day key, which is also unknown, into L, and then another scrambler setting, three steps on from the initial setting, which is still unknown, encrypted the same letter of the day key, which is also still unknown, into R.

This constraint might seem vague, as it is full of unknowns, but at least it demonstrates that the letters L and R are intimately related by the initial setting of the Enigma machine, the day key. As each new message is intercepted, it is possible to identify other relationships between the 1st and 4th letters of the repeated message key. All these relationships are reflections of the initial setting of the Enigma machine. For example, the second message above tells us that M and X are related, the third tells us that J and M are related, and the fourth that D and P are related. Rejewski began to summarize these relationships by tabulating them. For the four messages we have so far, the table would reflect the relationships between (L,R), (M,X), (J,M) and (D,P):

1st letter A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
4th letter P M R X

If Rejewski had access to enough messages in a single day, then he would be able to complete the alphabet of relationships. The following table shows such a completed set of relationships:

1st letter A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Figure 42 Marian Rejewski.
Rejewski had no idea of the day key, and he had no idea which message keys were being chosen, but he did know that they resulted in this table of relationships. Had the day key been different, then the table of relationships would have been completely different. The next question was whether there existed any way of determining the day key by looking at the table of relationships. Rejewski began to look for patterns within the table, structures that might indicate the day key. Eventually, he began to study one particular type of pattern, which featured chains of letters. For example, in the table, A on the top row is linked to F on the bottom row, so next he would look up F on the top row. It turns out that F is linked to W, so he would look up W on the top row. And it turns out that W is linked to A, which is where we started. The chain has been completed.

With the remaining letters in the alphabet, Rejewski would generate more chains. He listed all the chains, and noted the number of links in each one:

\[
\begin{align*}
A &\rightarrow F \rightarrow W \rightarrow A & 3 \text{ links} \\
B &\rightarrow Q \rightarrow Z \rightarrow K \rightarrow V \rightarrow E \rightarrow L \rightarrow R \rightarrow I \rightarrow B & 9 \text{ links} \\
C &\rightarrow H \rightarrow S \rightarrow O \rightarrow Y \rightarrow D \rightarrow P \rightarrow C & 7 \text{ links} \\
J &\rightarrow M \rightarrow X \rightarrow S \rightarrow T \rightarrow N \rightarrow U \rightarrow J & 7 \text{ links}
\end{align*}
\]

So far, we have only considered the links between the 1st and 4th letters of the six-letter repeated key. In fact, Rejewski would repeat this whole exercise for the relationships between the 2nd and 5th letters, and the 3rd and 6th letters, identifying the chains in each case and the number of links in each chain.

Rejewski noticed that the chains changed each day. Sometimes there were lots of short chains, sometimes just a few long chains. And, of course, the letters within the chains changed. The characterisics of the chains were clearly a result of the day key setting—a complex consequence of the plugboard settings, the scrambler arrangement and the scrambler orientations. However, there remained the question of how Rejewski could determine the day key from these chains. Which of 10,000,000,000,000,000 possible day keys was related to a particular pattern of chains? The number of possibilities was simply too great.

It was at this point that Rejewski had a profound insight. Although the plugboard and scrambler settings both affect the details of the chains, their contributions can to some extent be disentangled. In particular, there is one aspect of the chains which is wholly dependent on the scrambler settings, and which has nothing to do with the plugboard settings: the numbers of links in the chains is purely a consequence of the scrambler settings. For instance, let us take the example above and pretend that the day key required the letters S and G to be swapped as part of the plugboard settings. If we change this element of the day key, by removing the cable that swaps S and G, and use it to swap, say, T and K instead, then the chains would change to the following:

\[
\begin{align*}
A &\rightarrow F \rightarrow W \rightarrow A & 3 \text{ links} \\
B &\rightarrow Q \rightarrow Z \rightarrow T \rightarrow V \rightarrow E \rightarrow L \rightarrow R \rightarrow I \rightarrow B & 9 \text{ links} \\
C &\rightarrow H \rightarrow S \rightarrow O \rightarrow Y \rightarrow D \rightarrow P \rightarrow C & 7 \text{ links} \\
J &\rightarrow M \rightarrow X \rightarrow G \rightarrow K \rightarrow N \rightarrow U \rightarrow J & 7 \text{ links}
\end{align*}
\]

Some of the letters in the chains have changed, but, crucially, the number of links in each chain remains constant. Rejewski had identified a facet of the chains that was solely a reflection of the scrambler settings.

The total number of scrambler settings is the number of scrambler arrangements (6) multiplied by the number of scrambler orientations (17,576) which comes to 105,456. So, instead of having to worry about which of the 10,000,000,000,000,000 day keys was associated with a particular set of chains, Rejewski could busy himself with a drastically simpler problem: which of the 105,456 scrambler settings was associated with the numbers of links within a set of chains? This number is still large, but it is roughly one hundred billion times smaller than the total number of possible day keys. In short, the task has become one hundred billion times easier, certainly within the realm of human endeavor.

Rejewski proceeded as follows. Thanks to Hans-Thilo Schmidt's espionage, he had access to replica Enigma machines. His team began the laborious chore of checking each of 105,456 scrambler settings, and cataloguing the chain lengths that were generated by each one. It took an entire year to complete the catalogue, but once the Biuro had accumulated the data, Rejewski could finally begin to unravel the Enigma cipher.

Each day, he would look at the encrypted message keys, the first six letters of all the intercepted messages, and use the information to build his table of relationships. This would allow him to trace the chains, and
establish the number of links in each chain. For example, analyzing the 1st and 4th letters might result in four chains with 3, 9, 7 and 7 links. Analyzing the 2nd and 5th letters might also result in four chains, with 2, 3, 9 and 12 links. Analyzing the 3rd and 6th letters might result in five chains with 5, 5, 5, 3 and 8 links. As yet, Rejewski still had no idea of the day key, but he knew that it resulted in 3 sets of chains with the following number of chains and links in each one:

4 chains from the 1st and 4th letters, with 3, 9, 7 and 7 links.
4 chains from the 2nd and 5th letters, with 2, 3, 9 and 12 links.
5 chains from the 3rd and 6th letters, with 5, 5, 5, 3 and 8 links.

Rejewski could now go to his catalogue, which contained every scrambler setting indexed according to the sort of chains it would generate. Having found the catalogue entry that contained the right number of chains with the appropriate number of links in each one, he immediately knew the scrambler settings for that particular day key. The chains were effectively fingerprints, the evidence that betrayed the initial scrambler arrangement and orientations. Rejewski was working just like a detective who might find a fingerprint at the scene of a crime, and then use a database to match it to a suspect.

Although he had identified the scrambler part of the day key, Rejewski still had to establish the plugboard settings. Although there are about a hundred billion possibilities for the plugboard settings, this was a relatively straightforward task. Rejewski would begin by setting the scramblers in his Enigma replica according to the newly established scrambler part of the day key. He would then remove all cables from the plugboard, so that the plugboard had no effect. Finally, he would take a piece of intercepted ciphertext and type it in to the Enigma machine. This would largely result in gibberish, because the plugboard cabling was unknown and missing. However, every so often vaguely recognizable phrases would appear, such as *alliveinberlin*—presumably, this should be "arrive in Berlin." If this assumption is correct, then it would imply that the letters R and L should be connected and swapped by a plugboard cable, while A, I, V, E, B and N should not. By analyzing other phrases it would be possible to identify the other five pairs of letters that had been swapped by the plugboard. Having established the plugboard settings, and having already discovered the scrambler settings, Rejewski had the complete day key, and could then decipher any message sent that day.

Rejewski had vastly simplified the task of finding the day key by divorcing the problem of finding the scrambler settings from the problem of finding the plugboard settings. On their own, both of these problems were solvable. Originally, we estimated that it would take more than the lifetime of the universe to check every possible Enigma key. However, Rejewski had spent only a year compiling his catalogue of chain lengths, and thereafter he could find the day key before the day was out. Once he had the day key, he possessed the same information as the intended receiver and so could decipher messages just as easily.

Following Rejewski's breakthrough, German communications became transparent. Poland was not at war with Germany, but there was a threat of invasion, and Polish relief at conquering Enigma was nevertheless immense. If they could find out what the German generals had in mind for them, there was a chance that they could defend themselves. The fate of the Polish nation had depended on Rejewski, and he did not disappoint his country. Rejewski's attack on Enigma is one of the truly great accomplishments of cryptanalysis. I have had to sum up his work in just a few pages, and so have omitted many of the technical details, and all of the dead ends. Enigma is a complicated cipher machine, and breaking it required immense intellectual force. My simplifications should not mislead you into underestimating Rejewski's extraordinary achievement.

The Polish success in breaking the Enigma cipher can be attributed to three factors: fear, mathematics and espionage. Without the fear of invasion, the Poles would have been discouraged by the apparent invulnerability of the Enigma cipher. Without mathematics, Rejewski would not have been able to analyze the chains. And without Schmidt, code-named "Asche," and his documents, the wirings of the scramblers would not have been known, and cryptanalysis could not even have begun. Rejewski did not hesitate to express the debt he owed Schmidt: "Asche's documents were welcomed like manna from heaven, and all doors were immediately opened."

The Poles successfully used Rejewski's technique for several years. When Hermann Göring visited Warsaw in 1934, he was totally unaware of the fact that his communications were being intercepted and deciphered.
As he and other German dignitaries laid a wreath at the Tomb of the Unknown Soldier next to the offices of the Biuro Szyfrów, Rejewski could stare down at them from his window, content in the knowledge that he could read their most secret communications.

Even when the Germans made a minor alteration to the way they transmitted messages, Rejewski fought back. His old catalogue of chain lengths was useless, but rather than rewriting the catalogue he devised a mechanized version of his cataloguing system, which could automatically search for the correct scrambler settings. Rejewski’s invention was an adaptation of the Enigma machine, able to rapidly check each of the 17,576 settings until it spotted a match. Because of the six possible scrambler arrangements, it was necessary to have six of Rejewski’s machines working in parallel, each one representing one of the possible arrangements. Together, they formed a unit that was about a meter high, capable of finding the day key in roughly two hours. The units were called bombs, a name that might reflect the ticking noise they made while checking scrambler settings. Alternatively, it is said that Rejewski got his inspiration for the machines while at a café eating a bombe, an ice cream shaped into a hemisphere. The bombs effectively mechanized the process of decipherment. It was a natural response to Enigma, which was a mechanization of encipherment.

For most of the 1930s, Rejewski and his colleagues worked tirelessly to uncover the Enigma keys. Month after month, the team would have to deal with the stresses and strains of cryptanalysis, continually having to fix mechanical failures in the bombs, continually having to deal with the never-ending supply of encrypted intercepts. Their lives became dominated by the pursuit of the day key, that vital piece of information that would reveal the meaning of the encrypted messages. However, unknown to the Polish codebreakers, much of their work was unnecessary. The chief of the Biuro, Major Gwido Langer, already had the Enigma day keys, but he kept them hidden, tucked away in his desk.

Langer, via the French, was still receiving information from Schmidt. The German spy’s nefarious activities did not end in 1931 with the delivery of the two documents on the operation of Enigma, but continued for another seven years. He met the French secret agent Rex on twenty occasions, often in secluded alpine chalets where privacy was guaranteed. At every meeting, Schmidt handed over one or more codebooks, each one containing a month’s worth of day keys. These were the codebooks that were distributed to all German Enigma operators, and they contained all the information that was needed to encipher and decipher messages. In total, he provided codebooks that contained 38 months’ worth of day keys. The keys would have saved Rejewski an enormous amount of time and effort, shortening the necessity for bombs and sparing manpower that could have been used in other sections of the Biuro. However, the remarkably astute Langer decided not to tell Rejewski that the keys existed. By depriving Rejewski of the keys, Langer believed he was preparing him for the inevitable time when the keys would no longer be available. He knew that if war broke out it would be impossible for Schmidt to continue to attend covert meetings, and Rejewski would then be forced to be self-sufficient. Langer thought that Rejewski should practice self-sufficiency in peacetime, as preparation for what lay ahead.

Rejewski’s skills eventually reached their limit in December 1938, when German cryptographers increased Enigma’s security. Enigma operators were all given two new scramblers, so that the scrambler arrangement might involve any three of the five available scramblers. Previously there were only three scramblers (labeled 1, 2 and 3) to choose from, and only six ways to arrange them, but now that there were two extra scramblers (labeled 4 and 5) to choose from, the number of arrangements rose to 60, as shown in Table 10. Rejewski’s first challenge was to work out the internal wirings of the two new scramblers. More worryingly, he also had to build ten times as many bombs, each representing a different scrambler arrangement. The sheer cost of building such a battery of bombs was fifteen times the Biuro’s entire annual equipment budget. The following month the situation worsened when the number of plugboard cables increased from six to ten. Instead of twelve letters being swapped before entering the scramblers, there were now twenty swapped letters. The number of possible keys increased to 159,000,000,000,000,000,000,000.

In 1938 Polish interceptions and decipherments had been at their peak, but by the beginning of 1939 the new scramblers and extra plugboard cables stymied the flow of intelligence. Rejewski, who had pushed forward the boundaries of cryptanalysis in previous years, was confounded. He had proved that Enigma was not an unbreakable cipher, but without the resources required to check every scrambler setting he could not find
the day key, and decipherment was impossible. Under such desperate circumstances Langer might have been tempted to hand over the keys that had been obtained by Schmidt, but the keys were no longer being delivered. Just before the introduction of the new scramblers, Schmidt had broken off contact with agent Rex. For seven years he had supplied keys which were superfluous because of Polish innovation. Now, just when the Poles needed the keys, they were no longer available.

The new invulnerability of Enigma was a devastating blow to Poland, because Enigma was not merely a means of communication, it was at the heart of Hitler's blitzkrieg strategy. The concept of blitzkrieg ("lightning war") involved rapid, intense, coordinated attack, which meant that large tank divisions would have to communicate with one another and with infantry and artillery. Furthermore, land forces would be backed up by air support from dive-bombing Stukas, which would rely on effective and secure communication between the front-line troops and the airfields. The ethos of blitzkrieg was "speed of attack through speed of communications." If the Poles could not break Enigma, they had no hope of stopping the German onslaught, which was clearly only a matter of months away. Germany already occupied the Sudetenland, and on April 27, 1939, it withdrew from its nonaggression treaty with Poland. Hitler's anti-Polish rhetoric became increasingly vitriolic. Langer was determined that if Poland was invaded, then its cryptanalytic breakthroughs, which had so far been kept secret from the Allies, should not be lost. If Poland could not benefit from Rejewski's work, then at least the Allies should have the

Table 10 Possible arrangements with five scramblers.

<table>
<thead>
<tr>
<th>Arrangements with three scramblers</th>
<th>Extra arrangements available with two extra scramblers</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>124 125 134 135 142 143 145 152 153</td>
</tr>
<tr>
<td>132</td>
<td>154 214 215 234 235 241 243 245 251</td>
</tr>
<tr>
<td>213</td>
<td>253 254 314 315 324 325 341 342 345</td>
</tr>
<tr>
<td>231</td>
<td>351 352 354 412 413 415 421 423 425</td>
</tr>
<tr>
<td>312</td>
<td>431 432 435 451 452 453 512 513 514</td>
</tr>
<tr>
<td>321</td>
<td>521 523 524 531 532 534 541 542 543</td>
</tr>
</tbody>
</table>

Figure 43 General Heinz Guderian's command post vehicle. An Enigma machine can be seen in use in the bottom left.
chance to try and build on it. Perhaps Britain and France, with their extra resources, could fully exploit the concept of the bombe.

On June 30, Major Langer telephoned his French and British counterparts, inviting them to Warsaw to discuss some urgent matters concerning Enigma. On July 24, senior French and British cryptanalysts arrived at the Biuro’s headquarters, not knowing quite what to expect. Langer ushered them into a room in which stood an object covered with a black cloth. He pulled away the cloth, dramatically revealing one of Rejewski’s bombs. The audience were astonished as they heard how Rejewski had been breaking Enigma for years. The Poles were a decade ahead of anybody else in the world. The French were particularly astonished, because the Polish work had been based on the results of French espionage. The French had handed the information from Schmidt to the Poles because they believed it to be of no value, but the Poles had proved them wrong.

As a final surprise, Langer offered the British and French two spare Enigma replicas and blueprints for the bombs, which were to be shipped in diplomatic bags to Paris. From there, on August 16, one of the Enigma machines was forwarded to London. It was smuggled across the Channel as part of the baggage of the playwright Sacha Guitry and his wife, the actress Yvonne Printemps, so as not to arouse the suspicion of German spies who would be monitoring the ports. Two weeks later, on September 1, Hitler invaded Poland and the war began.

**The Geese that Never Cackled**

For thirteen years the British and the French had assumed that the Enigma cipher was unbreakable, but now there was hope. The Polish revelations had demonstrated that the Enigma cipher was flawed, which boosted the morale of Allied cryptanalysts. Polish progress had ground to a halt on the introduction of the new scramblers and extra plugboard cables, but the fact remained that Enigma was no longer considered a perfect cipher.

The Polish breakthroughs also demonstrated to the Allies the value of employing mathematicians as codebreakers. In Britain, Room 40 had always been dominated by linguists and classicists, but now there was a concerted effort to balance the staff with mathematicians and scientists. They were recruited largely via the old-boy network, with those inside Room 40 contacting their former Oxford and Cambridge colleges. There was also an old-girl network which recruited women undergraduates from places such as Newnham College and Girton College, Cambridge.

The new recruits were not brought to Room 40 in London, but instead went to Bletchley Park, Buckinghamshire, the home of the Government Code and Cypher School (GC&CS), a newly formed codebreaking organization that was taking over from Room 40. Bletchley Park could house a much larger staff, which was important because a deluge of encrypted intercepts was expected as soon as the war started. During the First World War, Germany had transmitted two million words a month, but it was anticipated that the greater availability of radios in the Second World War could result in the transmission of two million words a day.

At the center of Bletchley Park was a large Victorian Tudor-Gothic mansion built by the nineteenth-century financier Sir Herbert Leon. The mansion, with its library, dining hall and ornate ballroom, provided the

---

**Figure 44** In August 1939, Britain’s senior codebreakers visited Bletchley Park to assess its suitability as the site for the new Government Code and Cypher School. To avoid arousing suspicion from locals, they claimed to be part of Captain Ridley’s shooting party.
central administration for the whole of the Bletchley operation. Commander Alastair Denniston, the director of GC&CS, had a ground-floor office overlooking the gardens, a view that was soon spoiled by the erection of numerous huts. These makeshift wooden buildings housed the various codebreaking activities. For example, Hut 6 specialized in attacking the German Army’s Enigma communications. Hut 6 passed its decrypts to Hut 3, where intelligence operatives translated the messages, and attempted to exploit the information. Hut 8 specialized in the naval Enigma, and they passed their decrypts to Hut 4 for translation and intelligence gathering. Initially, Bletchley Park had a staff of only two hundred, but within five years the mansion and the huts would house seven thousand men and women.

During the autumn of 1939, the scientists and mathematicians at Bletchley learned the intricacies of the Enigma cipher and rapidly mastered the Polish techniques. Bletchley had more staff and resources than the Polish Biuro Szyfrów, and were thus able to cope with the larger selection of scramblers and the fact that Enigma was now ten times harder to break. Every twenty-four hours the British codebreakers went through the same routine. At midnight, German Enigma operators would change to a new day key, at which point whatever breakthroughs Bletchley had achieved the previous day could no longer be used to decipher messages. The codebreakers now had to begin the task of trying to identify the new day key. It could take several hours, but as soon as they had discovered the Enigma settings for that day, the Bletchley staff could begin to decipher the German messages that had already accumulated, revealing information that was invaluable to the war effort.

Surprise is an invaluable weapon for a commander to have at his disposal. But if Bletchley could break into Enigma, German plans would become transparent and the British would be able to read the minds of the German High Command. If the British could pick up news of an imminent attack, they could send reinforcements or take evasive action. If they could decipher German discussions of their own weaknesses, the Allies would be able to focus their offensives. The Bletchley decipherments were of the utmost importance. For example, when Germany invaded Denmark and Norway in April 1940, Bletchley provided a detailed picture of German operations. Similarly, during the Battle of Britain, the cryptanalysts were able to give advance warning of bombing raids, including times and locations. They could also give continual updates on the state of the Luftwaffe, such as the number of planes that had been lost and the speed with which they were being replaced. Bletchley would send all this information to MI6 headquarters, who would forward it to the War Office, the Air Ministry and the Admiralty.

In between influencing the course of the war, the cryptanalysts occasionally found time to relax. According to Malcolm Muggeridge, who served in the secret service and visited Bletchley, rounders, a version of softball, was a favorite pastime:

Every day after luncheon when the weather was propitious the cipher crackers played rounders on the manor-house lawn, assuming the quasi-serious manner dons affect when engaged in activities likely to be regarded as frivolous or insignificant in comparison with their weightier studies. Thus they would dispute some point about the game with the same fervor as they might the question of free will or determinism, or whether the world began with a big bang or a process of continuing creation.

Figure 45 Bletchley’s codebreakers relax with a game of rounders.
Once they had mastered the Polish techniques, the Bletchley cryptanalysts began to invent their own shortcuts for finding the Enigma keys. For example, they cottoned on to the fact that the German Enigma operators would occasionally choose obvious message keys. For each message, the operator was supposed to select a different message key, three letters chosen at random. However, in the heat of battle, rather than refining their imaginations to pick a random key, the overworked operators would sometimes pick three consecutive letters from the Enigma keyboard (Figure 46), such as QWE or BNM. These predictable message keys became known as cillies. Another type of cilly was the repeated use of the same message key, perhaps the initials of the operator’s girlfriend—indeed, one such set of initials, C.I.L., may have been the origin of the term. Before cracking Enigma the hard way, it became routine for the cryptanalysts to try out the cillies, and their hunches would sometimes pay off.

Cillies were not weaknesses of the Enigma machine, rather they were weaknesses in the way the machine was being used. Human error at more senior levels also compromised the security of the Enigma cipher. Those responsible for compiling the codebooks had to decide which scramblers would be used each day, and in which positions. They tried to ensure that the scrambler settings were unpredictable by not allowing any scrambler to remain in the same position for two days in a row. So, if we label the scramblers 1, 2, 3, 4 and 5, then on the first day it would be possible to have the arrangement 134, and on the second day it would be possible to have 215, but not 214, because scrambler number 4 is not allowed to remain in the same position for two days in a row. This might seem a sensible strategy because the scramblers are constantly changing position, but enforcing such a rule actually makes life easier for the cryptanalyst. Excluding certain arrangements to avoid a scrambler remaining in the same position meant that the codebook compilers reduced by half the number of possible scrambler arrangements. The Bletchley cryptanalysts realized what was happening and made the most of it. Once they identified the scrambler arrangement for one day, they could immediately rule out half the scrambler arrangements for the next day. Hence, their workload was reduced by half.

Similarly, there was a rule that the plugboard settings could not include a swap between any letter and its neighbor, which meant that S could be swapped with any letter except R and T. The theory was that such obvious swappings should be deliberately avoided, but once again the implementation of a rule drastically reduced the number of possible keys.

This search for new cryptanalytic shortcuts was necessary because the Enigma machine continued to evolve during the course of the war. The cryptanalysts were continually forced to innovate, to redesign and refine the bombs, and to devise wholly new strategies. Part of the reason for their success was the bizarre combination of mathematicians, scientists, linguists, classicists, chess grandmasters and crossword addicts within each hut. An intractable problem would be passed around the hut until it reached someone who had the right mental tools to solve it, or reached someone who could at least partially solve it before passing it on again. Gordon Welchman, who was in charge of Hut 6, described his team as “a pack of hounds trying to pick up the scent.” There were many great cryptanalysts and many significant breakthroughs, and it would take several large volumes to describe the individual contributions in detail. However, if there is one figure who deserves to be singled out, it is Alan Turing, who identified Enigma’s greatest weakness and ruthlessly exploited it. Thanks to Turing, it became possible to crack the Enigma cipher under even the most difficult circumstances.

Alan Turing was conceived in the autumn of 1911 in Chatrapur, a town near Madras in southern India, where his father Julius Turing was a member of the Indian civil service. Julius and his wife Ethel were determined that their son should be born in Britain, and returned to London, where Alan was born on June 23, 1912. His father returned to India soon afterward and his mother followed just fifteen months later, leaving Alan in the care of nannies and friends until he was old enough to attend boarding school.
In 1926, at the age of fourteen, Turing became a pupil at Sherborne School, in Dorset. The start of his first term coincided with the General Strike, but Turing was determined to attend the first day, and he cycled 100 km unaccompanied from Southampton to Sherborne, a feat that was reported in the local newspaper. By the end of his first year at the school he had gained a reputation as a shy, awkward boy whose only skills were in the area of science. The aim of Sherborne was to turn boys into well-rounded men, fit to rule the Empire, but Turing did not share this ambition and had a generally unhappy schooling.

His only real friend at Sherborne was Christopher Morcom, who, like Turing, had an interest in science. Together they discussed the latest scientific news and conducted their own experiments. The relationship fired Turing’s intellectual curiosity, but, more importantly, it also had a profound emotional effect on him. Andrew Hodges, Turing’s biographer, wrote that “This was first love... It had that sense of surrender, and a heightened awareness, as of brilliant color bursting upon a black and white world.” Their friendship lasted four years, but Morcom seems to have been unaware of the depth of feeling Turing had for him. Then, during their final year at Sherborne, Turing lost forever the chance to tell him how he felt. On Thursday, February 13, 1930, Christopher Morcom suddenly died of tuberculosis.

Turing was devastated by the loss of the only person he would ever truly love. His way of coming to terms with Morcom’s death was to focus on his scientific studies in an attempt to fulfill his friend’s potential. Morcom, who appeared to be the more gifted of the two boys, had already won a scholarship to Cambridge University. Turing believed it was his duty also to win a place at Cambridge, and then to make the discoveries his friend would otherwise have made. He asked Christopher’s mother for a photograph, and when it arrived he wrote back to thank her: “He is on my table now, encouraging me to work hard.”

In 1931, Turing gained admission to King’s College, Cambridge. He arrived during a period of intense debate about the nature of mathematics and logic, and was surrounded by some of the leading voices, such as Bertrand Russell, Alfred North Whitehead and Ludwig Wittgenstein. At the center of the argument was the issue of undecidability, a controversial notion developed by the logician Kurt Gödel. It had always been assumed
that, in theory at least, all mathematical questions could be answered. However, Gödel demonstrated that there could exist a minority of questions which were beyond the reach of logical proof, so-called undecidable questions. Mathematicians were traumatized by the news that mathematics was not the all-powerful discipline they had always believed it to be. They attempted to salvage their subject by trying to find a way of identifying the awkward undecidable questions, so that they could put them safely to one side. It was this objective that eventually inspired Turing to write his most influential mathematical paper, “On Computable Numbers,” published in 1937. In Breaking the Code, Hugh Whitemore’s play about the life of Turing, a character asks Turing the meaning of his paper. He replies, “It’s about right and wrong. In general terms. It’s a technical paper in mathematical logic, but it’s also about the difficulty of telling right from wrong. People think—most people think—that in mathematics we always know what is right and what is wrong. Not so. Not any more.”

In his attempt to identify undecidable questions, Turing’s paper described an imaginary machine that was designed to perform a particular mathematical operation, or algorithm. In other words, the machine would be capable of running through a fixed, prescribed series of steps which would, for example, multiply two numbers. Turing envisaged that the numbers to be multiplied could be fed into the machine via a paper tape, rather like the punched tape that is used to feed a tune into a Pianola. The answer to the multiplication would be output via another tape. Turing imagined a whole series of these so-called Turing machines, each specially designed to tackle a particular task, such as dividing, squaring or factoring. Then Turing took a more radical step.

He imagined a machine whose internal workings could be altered so that it could perform all the functions of all conceivable Turing machines. The alterations would be made by inserting carefully selected tapes, which transformed the single flexible machine into a dividing machine, a multiplying machine, or any other type of machine. Turing called this hypothetical device a universal Turing machine because it would be capable of answering any question that could logically be answered. Unfortunately, it turned out that it is not always logically possible to answer a question about the undecidability of another question, and so even the universal Turing machine was unable to identify every undecidable question.

Mathematicians who read Turing’s paper were disappointed that Gödel’s monster had not been subdued but, as a consolation prize, Turing had given them the blueprint for the modern programmable computer. Turing knew of Babbage’s work, and the universal Turing machine can be seen as a reincarnation of Difference Engine No. 2. In fact, Turing had gone much further, and provided computing with a solid theoretical basis, imbuing the computer with a hitherto unimaginable potential. It was still the 1930s though, and the technology did not exist to turn the universal Turing machine into a reality. However, Turing was not at all dismayed that his theories were ahead of what was technically feasible. He merely wanted recognition from within the mathematical community, who indeed applauded his paper as one of the most important breakthroughs of the century. He was still only twenty-six.

This was a particularly happy and successful period for Turing. During the 1930s he rose through the ranks to become a fellow of King’s College, home of the world’s intellectual elite. He led the life of an archetypal Cambridge don, mixing pure mathematics with more trivial activities. In 1938 he made a point of seeing the film Snow White and the Seven Dwarfs, containing the memorable scene in which the Wicked Witch dunks an apple in poison. Afterward his colleagues heard Turing continually repeating the macabre chant, “Dip the apple in the brew. Let the sleeping death seep through.”

Turing cherished his years at Cambridge. In addition to his academic success, he found himself in a tolerant and supportive environment. Homosexuality was largely accepted within the university, which meant that he was free to engage in a series of relationships without having to worry about who might find out, and what others might say. Although he had no serious long-term relationships, he seemed to be content with his life. Then, in 1939, Turing’s academic career was brought to an abrupt halt. The Government Code and Cypher School invited him to become a cryptanalyst at Bletchley, and on September 4, 1939, the day after Neville Chamberlain declared war on Germany, Turing moved from the opulence of the Cambridge quadrangle to the Crown Inn at Shenley Brook End.

Each day he cycled 5 km from Shenley Brook End to Bletchley Park, where he spent part of his time in the huts contributing to the routine codebreaking effort, and part of his time in the Bletchley think tank,
formerly Sir Herbert Leon’s apple, pear and plum store. The think tank was where the cryptanalysts brainstormed their way through new problems, or anticipated how to tackle problems that might arise in the future. Turing focused on what would happen if the German military changed their system of exchanging message keys. Bletchley’s early successes relied on Rejewski’s work, which exploited the fact that Enigma operators encrypted each message key twice (for example, if the message key was YGB, the operator would encipher YGBYGB). This repetition was supposed to ensure that the receiver did not make a mistake, but it created a chink in the security of Enigma. British cryptanalysts guessed it would not be long before the Germans noticed that the repeated key was compromising the Enigma cipher, at which point the Enigma operators would be told to abandon the repetition, thus confounding Bletchley’s current codebreaking techniques. It was Turing’s job to find an alternative way to attack Enigma, one that did not rely on a repeated message key.

As the weeks passed, Turing realized that Bletchley was accumulating a vast library of decrypted messages, and he noticed that many of them conformed to a rigid structure. By studying old decrypted messages, he believed he could sometimes predict part of the contents of an undeciphered message, based on when it was sent and its source. For example, experience showed that the Germans sent a regular enciphered weather report shortly after 6 A.M. each day. So, an encrypted message intercepted at 6:05 A.M. would be almost certain to contain wetter, the German word for “weather.” The rigorous protocol used by any military organization meant that such messages were highly regimented in style, so Turing could even be confident about the location of wetter within the encrypted message. For example, experience might tell him that the first six letters of a particular ciphertext corresponded to the plaintext letters wetter. When a piece of plaintext can be associated with a piece of ciphertext, this combination is known as a crib.

Turing was sure that he could exploit the cribs to crack Enigma. If he had a ciphertext and he knew that a specific section of it, say ETJWPX, represented wetter, then the challenge was to identify the settings of the Enigma machine that would transform wetter into ETJWPX. The straightforward, but impractical, way to do this would be for the cryptanalyst to take an Enigma machine, type in wetter and see if the correct ciphertext emerged. If not, then the cryptanalyst would change the settings of the machine, by swapping plugboard cables, and swapping or reorienting scramblers, and then type in wetter again. If the correct ciphertext did not emerge, the cryptanalyst would change the settings again, and again, and again, until he found the right one. The only problem with this trial and error approach was the fact that there were 159,000,000,000,000,000,000 possible settings to check, so finding the one that transformed wetter into ETJWPX was a seemingly impossible task.

To simplify the problem, Turing attempted to follow Rejewski’s strategy of disentangling the settings. He wanted to divorce the problem of finding the scrambler settings (finding which scrambler is in which slot, and what their respective orientations are) from the problem of finding the plugboard cabling. For example, if he could find something in the crib that had nothing to do with the plugboard cabling, then he could feasibly check each of the remaining 1,054,560 possible scrambler combinations (60 arrangements × 17,576 orientations). Having found the correct scrambler settings, he could then deduce the plugboard cabling.

Eventually, his mind settled on a particular type of crib which contained internal loops, similar to the chains exploited by Rejewski. Rejewski’s chains linked letters within the repeated message key. However, Turing’s loops had nothing to do with the message key, as he was working on the assumption that soon the Germans would stop sending repeated message keys. Instead, Turing’s loops connected plaintext and ciphertext letters within a crib. For example, the crib shown in Figure 48 contains a loop.

---

Figure 48 One of Turing’s cribs, showing a loop.
Remember, cribs are only guesses, but if we assume that this crib is correct, we can link the letters \( w \rightarrow E,\ e \rightarrow T,\ t \rightarrow W \) as part of a loop. Although we know none of the Enigma machine settings, we can label the first setting, whatever it is, \( S \). In this first setting we know that \( w \) is encrypted as \( E \). After this encryption, the first scrambler clicks around one place to setting \( S+1 \), and the letter \( e \) is enciphered as \( T \). The scrambler clicks forward another place and encrypts a letter that is not part of the loop, so we ignore this encryption. The scrambler clicks forward one more place and, once again, we reach a letter that is part of the loop. In setting \( S+3 \), we know that the letter \( t \) is enciphered as \( W \). In summary, we know that

- In setting \( S \), Enigma encrypts \( w \) as \( E \).
- In setting \( S+1 \), Enigma encrypts \( e \) as \( T \).
- In setting \( S+3 \), Enigma encrypts \( t \) as \( W \).

So far the loop seems like nothing more than a curious pattern, but Turing rigorously followed the implications of the relationships within the loop, and saw that they provided him with the drastic shortcut he needed in order to break Enigma. Instead of working with just one Enigma machine to test every setting, Turing began to imagine three separate machines, each dealing with the encipherment of one element of the loop. The first machine would try to encipher \( w \) into \( E \), the second would try to encipher \( e \) into \( T \), and the third \( t \) into \( W \). The three machines would all have identical settings, except that the second would have its scrambler orientations moved forward one place with respect to the first, a setting labeled \( S+1 \), and the third would have its scrambler orientations moved forward three places with respect to the first, a setting labeled \( S+3 \). Turing then pictured a frenzied cryptanalyst, continually changing plugboard cables, swapping scrambler arrangements and changing their orientations in order to achieve the correct encryptions. Whatever cables were changed in the first machine would also be changed in the other two. Whatever scrambler arrangements were changed in the first machine would also be changed in the other two. And, crucially, whatever scrambler orientation was set in the first machine, the second would have the same orientation but stepped forward one place, and the third would have the same orientation but stepped forward three places.

Turing does not seem to have achieved much. The cryptanalyst still has to check all \( 159,000,000,000,000,000,000 \) possible settings, and, to make matters worse, he now has to do it simultaneously on all three machines instead of just one. However, the next stage of Turing's idea transforms the challenge, and vastly simplifies it. He imagined connecting the three machines by running electrical wires between the inputs and the outputs of each machine, as shown in Figure 49. In effect, the loop in the crib is paralleled by the loop of the electrical circuit. Turing pictured the machines changing their plugboard and scrambler settings, as described above, but only when all the settings are correct for all three machines would the circuit be completed, allowing a current to flow through all three machines. If Turing incorporated a lightbulb within the circuit, then the current would illuminate it, signaling that the correct settings had been found. At this point, the three machines still have to check up to \( 159,000,000,000,000,000,000 \) possible settings in order to illuminate the bulb. However, everything done so far has merely been preparation for Turing's final logical leap, which would make the task over a hundred million million times easier in one fell swoop.

Turing had constructed his electrical circuit in such a way as to nullify the effect of the plugboard, thereby allowing him to ignore the billions of plugboard settings. Figure 49 shows that the first Enigma has the electric current entering the scramblers and emerging at some unknown letter, which we shall call \( L_1 \). The current then flows through the plugboard, which transforms \( L_1 \) into \( E \). This letter \( E \) is connected via a wire to the letter \( e \) in the second Enigma, and as the current flows through the second plugboard it is transformed back to \( L_1 \). In other words, the two plugboards cancel each other out. Similarly, the current emerging from the scramblers in the second Enigma enters the plugboard at \( L_2 \) before being transformed into \( T \). This letter \( T \) is connected via a wire to the letter \( t \) in the third Enigma, and as the current flows through the third plugboard it is transformed back to \( L_2 \). In short, the plugboards cancel themselves out throughout the whole circuit, so Turing could ignore them completely.

Turing needed only to connect the output of the first set of scramblers, \( L_1 \), directly to the input of the second set of scramblers, also \( L_1 \), and so on. Unfortunately, he did not know the value of the letter \( L_1 \), so he had to connect all 26 outputs of the first set of scramblers to all 26 corresponding inputs in the second set of scramblers, and so on. In effect, there were now
26 electrical loops, and each one would have a lightbulb to signal the completion of an electrical circuit. The three sets of scramblers could then simply check each of the 17,576 orientations, with the second set of scramblers always one step ahead of the first set, and the third set of scramblers two steps ahead of the second set. Eventually, when the correct scrambler orientations had been found, one of the circuits would be completed and the bulb would be illuminated. If the scramblers changed orientation every second, it would take just five hours to check all the orientations.

Only two problems remained. First, it could be that the three machines are running with the wrong scrambler arrangement, because the Enigma machine operates with any three of the five available scramblers, placed in any order, giving sixty possible arrangements. Hence, if all 17,576 orientations have been checked, and the lamp has not been illuminated, it is then necessary to try another of the sixty scrambler arrangements, and to keep on trying other arrangements until the circuit is completed. Alternatively, the cryptanalyst could have sixty sets of three Enigmas running in parallel.

The second problem involved finding the plugboard cabling, once the scrambler arrangement and orientations had been established. This is relatively simple. Using an Enigma machine with the correct scrambler arrangement and orientations, the cryptanalyst types in the ciphertext and looks at the emerging plaintext. If the result is *tewwer* rather than *wetter*, then it is clear that plugboard cables should be inserted so as to swap *w* and *t*. Typing in other bits of ciphertext would reveal other plugboard cabling.

The combination of crib, loops and electrically connected machines resulted in a remarkable piece of cryptanalysis, and only Turing, with his unique background in mathematical machines, could ever have come up with it. His musings on the imaginary Turing machines were intended to answer esoteric questions about mathematical undecidability, but this purely academic research had put him in the right frame of mind for designing a practical machine capable of solving very real problems.

Bletchley was able to find £100,000 to turn Turing's idea into working devices, which were dubbed *bombes* because their mechanical approach bore a passing resemblance to Rejewski's *bombe*. Each of Turing's *bombes* was to consist of twelve sets of electrically linked Enigma scramblers, and would thus be able to cope with much longer loops of letters. The complete unit

---

**Figure 49** The loop in the crib can be paralleled by an electrical loop. Three Enigma machines are set up in identical ways, except that the second one has its first scrambler moved forward one place (setting $S + 1$), and the third has its scrambler moved forward two further places (setting $S + 3$). The output of each Enigma is then connected to the input of the next one. The three sets of scramblers then click around in unison until the circuit is complete and the light illuminates. At this point the correct setting has been found. In the diagram above, the circuit is complete, corresponding to the correct setting.
would be about two meters tall, two meters long and a meter wide. Turing finalized the design at the beginning of 1940, and the job of construction was given to the British Tabulating Machinery factory at Letchworth.

While waiting for the bombes to be delivered, Turing continued his day-to-day work at Bletchley. News of his breakthrough soon spread among the other senior cryptanalysts, who recognized that he was a singularly gifted codebreaker. According to Peter Hilton, a fellow Bletchley codebreaker, “Alan Turing was obviously a genius, but he was an approachable, friendly genius. He was always willing to take time and trouble to explain his ideas; but he was no narrow specialist, so that his versatile thought ranged over a vast area of the exact sciences.”

However, everything at the Government Code and Cypher School was top secret, so nobody outside of Bletchley Park was aware of Turing’s remarkable achievement. For example, his parents had absolutely no idea that Alan was even a codebreaker, let alone Britain’s foremost cryptanalyst. He had once told his mother that he was involved in some form of military research, but he did not elaborate. She was merely disappointed that this had not resulted in a more respectable haircut for her scruffy son.

Although Bletchley was run by the military, they had conceded that they would have to tolerate the scruffiness and eccentricities of these “professor types.” Turing rarely bothered to shave, his nails were stuffed with dirt, and his clothes were a mass of creases. Whether the military would also have tolerated his homosexuality remains unknown. Jack Good, a veteran of Bletchley, commented: “Fortunately the authorities did not know that Turing was a homosexual. Otherwise we might have lost the war.”

The first prototype bombe, christened Victory, arrived at Bletchley on March 14, 1940. The machine was put into operation immediately, but the initial results were less than satisfactory. The machine turned out to be much slower than expected, taking up to a week to find a particular key. There was a concerted effort to increase the bombe’s efficiency, and a modified design was submitted a few weeks later. It would take four more months to build the upgraded bombe. In the meantime, the cryptanalysts had to cope with the calamity they had anticipated. On May 1, 1940, the Germans changed their key exchange protocol. They no longer repeated the message key, and thereupon the number of successful Enigma decipherments dropped dramatically. The information blackout lasted until August 8, when the new bombe arrived. Christened Agnus Dei, or Agnes for short, this machine was to fulfill all Turing’s expectations.

Within eighteen months there were fifteen more bombes in operation, exploiting cribs, checking scrambler settings and revealing keys, each one clattering like a million knitting needles. If everything was going well, a bombe might find an Enigma key within an hour. Once the plugboard cablings and the scrambler settings (the message key) had been established for a particular message, it was easy to deduce the day key. All the other messages sent that same day could then be deciphered.

Even though the bombes represented a vital breakthrough in cryptanalysis, decipherment had not become a formality. There were many hurdles to overcome before the bombes could even begin to look for a key. For example, to operate a bombe you first needed a crib. The senior codebreakers would give cribs to the bombe operators, but there was no guarantee that the codebreakers had guessed the correct meaning of the ciphertext. And even if they did have the right crib, it might be in the wrong place—the cryptanalysts might have guessed that an encrypted message contained a certain phrase, but associated that phrase with the wrong piece of the ciphertext. However, there was a neat trick for checking whether a crib was in the correct position.

In the following crib, the cryptanalyst is confident that the plaintext is right, but he is not sure if he has matched it with the correct letters in the ciphertext.

Guessed plaintext: wetternullsechs
Known ciphertext: IPRENLWKMJJSXCPLEJWQ

One of the features of the Enigma machine was its inability to encipher a letter as itself, which was a consequence of the reflector. The letter a could never be enciphered as A, the letter b could never be enciphered as B, and so on. The particular crib above must therefore be misaligned, because the first e in wetter is matched with an E in the ciphertext. To find the correct alignment, we simply slide the plaintext and the ciphertext relative to each other until no letter is paired with itself. If we shift the plaintext one place to the left, the match still fails because this time the first s in sechs is matched with S in the ciphertext. However, if we shift the plaintext one place to the right there are no illegal encipherments. This crib is
therefore likely to be in the right place, and could be used as the basis for
a bombe decipherment:

Guessed plaintext \texttt{wettternullsechs}
Known ciphertext \texttt{lPRENLWKMQJSXCPLEJWQ}

The intelligence gathered at Bletchley was passed on to only the most
senior military figures and selected members of the war cabinet. Winston
Churchill was fully aware of the importance of the Bletchley decipher-
ments, and on September 6, 1941, he visited the codebreakers. On meet-
ing some of the cryptanalysts, he was surprised by the bizarre mixture of
people who were providing him with such valuable information; in addi-
tion to the mathematicians and linguists, there was an authority on porce-
lain, a curator from the Prague Museum, the British chess champion and
numerous bridge experts. Churchill muttered to Sir Stewart Menzies,

head of the Secret Intelligence Service, “I told you to leave no stone
unturbed, but I didn’t expect you to take me so literally.” Despite the
comment, he had a great fondness for the motley crew, calling them “the
geese who laid golden eggs and never cackled.”

The visit was intended to boost the morale of the codebreakers by
showing them that their work was appreciated at the very highest level. It
also had the effect of giving Turing and his colleagues the confidence to
approach Churchill directly when a crisis loomed. To make the most of
the bombes, Turing needed more staff, but his requests had been blocked
by Commander Edward Travis, who had taken over as Director of
Bletchley, and who felt that he could not justify recruiting more people.
On October 21, 1941, the cryptanalysts took the insubordinate step of
ignoring Travis and writing directly to Churchill.

Dear Prime Minister,

Some weeks ago you paid us the honor of a visit, and we believe that you
regard our work as important. You will have seen that, thanks largely to the
energy and foresight of Commander Travis, we have been well supplied
with the “bombes” for the breaking of the German Enigma codes. We
think, however, that you ought to know that this work is being held up,
and in some cases is not being done at all, principally because we cannot
get sufficient staff to deal with it. Our reason for writing to you direct is
that for months we have done everything that we possibly can through the
normal channels, and that we despair of any early improvement without
your intervention . . .

We are, Sir, Your obedient servants,

A.M. Turing
W.G. Welchman
C.H.O'D. Alexander
P.S. Milner-Barry

Churchill had no hesitation in responding. He immediately issued a
memorandum to his principal staff officer:

**ACTION THIS DAY**
Make sure they have all they want on extreme priority and report to me
that this has been done.
Henceforth there were to be no more barriers to recruitment or materials. By the end of 1942 there were 49 bombes, and a new bombe station was opened at Gayhurst Manor, just north of Bletchley. As part of the recruitment drive, the Government Code and Cypher School placed a letter in the Daily Telegraph. They issued an anonymous challenge to its readers, asking if anybody could solve the newspaper's crossword (Figure 51) in under 12 minutes. It was felt that crossword experts might also be good codebreakers, complementing the scientific minds that were already at Bletchley—but of course, none of this was mentioned in the newspaper. The 25 readers who replied were invited to Fleet Street to take a crossword test. Five of them completed the crossword within the allotted time, and another had only one word missing when the 12 minutes had expired. A few weeks later, all six were interviewed by military intelligence and recruited as codebreakers at Bletchley Park.

**Kidnapping Codebooks**

So far in this chapter, the Enigma traffic has been treated as one giant communications system, but in fact there were several distinct networks. The German Army in North Africa, for instance, had its own separate network, and their Enigma operators had codebooks that were different from those used in Europe. Hence, if Bletchley succeeded in identifying the North African day key, it would be able to decipher all the German messages sent from North Africa that day, but the North African day key would be of no use in cracking the messages being transmitted in Europe. Similarly, the Luftwaffe had its own communications network, and so in order to decipher all Luftwaffe traffic, Bletchley would have to unravel the Luftwaffe day key.

Some networks were harder to break into than others. The Kriegsmarine network was the hardest of all, because the German Navy operated a more sophisticated version of the Enigma machine. For example, the Naval Enigma operators had a choice of eight scramblers, not just five, which meant that there were almost six times as many scrambler arrangements, and therefore almost six times as many keys for Bletchley to check. The other difference in the Naval Enigma concerned the reflector, which was responsible for sending the electrical signal back through
in the scramblers. In the standard Enigma the reflector was always fixed in one particular orientation, but in the Naval Enigma the reflector could be fixed in any one of 26 orientations. Hence the number of possible keys was further increased by a factor of 26.

Cryptanalysis of the Naval Enigma was made even harder by the Naval operators, who were careful not to send stereotypical messages, thus depriving Bletchley of cribs. Furthermore, the Kriegsmarine also instituted a more secure system for selecting and transmitting message keys. Extra scramblers, a variable reflector, nonstereotypical messages and a new system for exchanging message keys all contributed to making German Naval communications impenetrable.

Bletchley’s failure to crack the Naval Enigma meant that the Kriegsmarine were steadily gaining the upper hand in the Battle of the Atlantic. Admiral Karl Dönitz had developed a highly effective two-stage strategy for naval warfare, which began with his U-boats spreading out and scouring the Atlantic in search of Allied convoys. As soon as one of them spotted a target, it would initiate the next stage of the strategy by calling the other U-boats to the scene. The attack would commence only when a large pack of U-boats had been assembled. For this strategy of coordinated attack to succeed, it was essential that the Kriegsmarine had access to secure communication. The Naval Enigma provided such communication, and the U-boat attacks had a devastating impact on the Allied shipping that was supplying Britain with much-needed food and armaments.

As long as U-boat communications remained secure, the Allies had no idea of the locations of the U-boats, and could not plan safe routes for the convoys. It seemed as if the Admiralty’s only strategy for pinpointing the location of U-boats was by looking at the sites of sunken British ships. Between June 1940 and June 1941 the Allies lost an average of 50 ships each month, and they were in danger of not being able to build new ships quickly enough to replace them. Besides the intolerable destruction of ships, there was also a terrible human cost—50,000 Allied seamen died during the war. Unless these losses could be drastically reduced, Britain was in danger of losing the Battle of the Atlantic, which would have meant losing the war. Churchill would later write, “Amid the torrent of violent events one anxiety reigned supreme. Battles might be won or lost, enterprises might succeed or miscarry, territories might be gained or quitted, but dom-

The Polish experience and the case of Hans-Thilo Schmidt had taught Bletchley Park that if intellectual endeavor fails to break a cipher, then it is necessary to rely on espionage, infiltration and theft in order to obtain the enemy keys. Occasionally, Bletchley would make a breakthrough against the Naval Enigma, thanks to a clever ploy by the RAF. British planes would lay mines in particular locations, provoking German vessels to send out warnings to other craft. These Enigma encrypted warnings would inevitably contain a map reference, but crucially this map reference would already be known by the British, so it could be used as a crib. In other words, Bletchley knew that a particular piece of ciphertext represented a particular set of coordinates. Sowing mines to obtain cribs, known as “gardening,” required the RAF to fly special missions, so this could not be done on a regular basis. Bletchley had to find another way of breaking the Naval Enigma.

An alternative strategy for cracking the Naval Enigma depended on stealing keys. One of the most intrepid plans for stealing keys was concocted by Ian Fleming, creator of James Bond and a member of Naval Intelligence during the war. He suggested crashing a captured German bomber in the English Channel, close to a German ship. The German sailors would then approach the plane to rescue their comrades, whereupon the aircrew, British pilots pretending to be German, would board the ship and capture its codebooks. These German codebooks contained the information that was required for establishing the encryption key, and because ships were often away from base for long periods, the codebooks would be valid for at least a month. By capturing such codebooks, Bletchley would be able to decipher the Naval Enigma for an entire month.

After approving Fleming’s plan, known as Operation Ruthless, British Intelligence began preparing a Heinkel bomber for the crash landing, and assembled an aircrew of German-speaking Englishmen. The plan was scheduled for a date early in the month, so as to capture a fresh codebook. Fleming went to Dover to oversee the operation, but unfortunately there was no German shipping in the area so the plan was postponed indefinitely. Four days later, Frank Birch, who headed the Naval section at Bletchley, recorded the reaction of Turing and his colleague Peter Twinn:
“Turing and Twinn came to me like undertakers cheated of a nice corpse two days ago, all in a stew about the cancelation of Operation Ruthless.”

In due course Operation Ruthless was canceled, but German Naval codebooks were eventually captured during a spate of daring raids on weather ships and U-boats. These so-called “pinches” gave Bletchley the documents it needed to bring an end to the intelligence blackout. With the Naval Enigma transparent, Bletchley could pinpoint the location of U-boats, and the Battle of the Atlantic began to swing in favor of the Allies. Convoys could be steered clear of U-boats, and British destroyers could even begin to go on the offensive, seeking out and sinking U-boats.

It was vital that the German High Command never suspected that the Allies had pinched Enigma codebooks. If the Germans found that their security had been compromised, they would upgrade their Enigma machines, and Bletchley would be back to square one. As with the Zimmermann telegram episode, the British took various precautions to avoid arousing suspicion, such as sinking a German vessel after pinching its codebooks. This would persuade Admiral Dönitz that the cipher material had found its way to the bottom of the sea, and not fallen into British hands.

Once material had been secretly captured, further precautions had to be taken before exploiting the resulting intelligence. For example, the Enigma decipherments gave the locations of numerous U-boats, but it would have been unwise to have attacked every single one of them, because a sudden unexplained increase in British success would warn Germany that its communications were being deciphered. Consequently, the Allies would allow some U-boats to escape, and would attack others only when a spotter plane had been sent out first, thus justifying the approach of a destroyer some hours later. Alternatively, the Allies might send fake messages describing sightings of U-boats, which likewise provided sufficient explanation for the ensuing attack.

Despite this policy of minimizing telltale signs that Enigma had been broken, British actions did sometimes raise concerns among Germany’s security experts. On one occasion, Bletchley deciphered an Enigma message giving the exact location of a group of German tankers and supply ships, nine in total. The Admiralty decided not to sink all of the ships in case a clean sweep of targets aroused German suspicions. Instead, they informed destroyers of the exact location of just seven of the ships, which should have allowed the Gedania and the Gonzenheim to escape unharmed. The seven targeted ships were indeed sunk, but Royal Navy destroyers accidentally encountered the two ships that were supposed to be spared, and also sank them. The destroyers did not know about Enigma or the policy of not arousing suspicion—they merely believed they were doing their duty. Back in Berlin, Admiral Kurt Fricke instigated an investigation into this and other similar attacks, exploring the possibility that the British had broken Enigma. The report concluded that the numerous losses were either the result of natural misfortune, or caused by a British spy who had infiltrated the Kriegsmarine. The breaking of Enigma was considered impossible and inconceivable.

The Anonymous Cryptanalysts

As well as breaking the German Enigma cipher, Bletchley Park also succeeded in deciphering Italian and Japanese messages. The intelligence that emerged from these three sources was given the codename Ultra, and the Ultra Intelligence files were responsible for giving the Allies a clear advantage in all the major arenas of conflict. In North Africa, Ultra helped to destroy German supply lines and informed the Allies of the status of General Rommel’s forces, enabling the Eighth Army to fight back against the German advances. Ultra also warned of the German invasion of Greece, which allowed British troops to retreat without heavy losses. In fact, Ultra provided accurate reports on the enemy’s situation throughout the entire Mediterranean. This information was particularly valuable when the Allies landed in Italy and Sicily in 1943.

In 1944, Ultra played a major role in the Allied invasion of Europe. For example, in the months prior to D-Day, the Bletchley decipherments provided a detailed picture of the German troop concentrations along the French coast. Sir Harry Hinsley, official historian of British Intelligence during the war, wrote:

As Ultra accumulated, it administered some unpleasant shocks. In particular, it revealed in the second half of May—following earlier disturbing indications that the Germans were concluding that the area between Le Havre and Cherbourg was a likely, and perhaps even the main, invasion
area—that they were sending reinforcements to Normandy and the Cherbourg peninsula. But this evidence arrived in time to enable the Allies to modify the plans for the landings on and behind the Utah beach; and it is a singular fact that before the expedition sailed the Allied estimate of the number, identification, and location of the enemy’s divisions in the west, fifty-eight in all, was accurate in all but two items that were to be of operational importance.

Throughout the war, the Bletchley codebreakers knew that their decipherments were vital, and Churchill’s visit to Bletchley had reinforced this point. But the cryptanalysts were never given any operational details or told how their decipherments were being used. For example, the codebreakers were given no information about the date for D-Day, and they arranged a dance for the evening before the landings. This worried Commander Travis, the Director of Bletchley and the only person on site who was privy to the plans for D-Day. He could not tell the Hut 6 Dance Committee to cancel the event because this would have been a clear hint that a major offensive was in the offing, and as such a breach of security. The dance was allowed to go ahead. As it happened, bad weather postponed the landings for twenty-four hours, so the codebreakers had time to recover from the frivolities. On the day of the landings, the French resistance destroyed landlines, forcing the Germans to communicate solely by radio, which in turn gave Bletchley the opportunity to intercept and decipher even more messages. At the turning point of the war, Bletchley was able to provide an even more detailed picture of German military operations.

Stuart Milner-Barry, one of the Hut 6 cryptanalysts, wrote: “I do not imagine that any war since classical times, if ever, has been fought in which one side read consistently the main military and naval intelligence of the other.” An American report came to a similar conclusion: “Ultra created in senior staffs and at the political summit a state of mind which transformed the taking of decisions. To feel that you know your enemy is a vastly comforting feeling. It grows imperceptibly over time if you regularly and intimately observe his thoughts and ways and habits and actions. Knowledge of this kind makes your own planning less tentative and more assured, less harrowing and more buoyant.”

It has been argued, albeit controversially, that Bletchley Park’s achieve-
ments were the decisive factor in the Allied victory. What is certain is that the Bletchley codebreakers significantly shortened the war. This becomes evident by rerunning the Battle of the Atlantic and speculating what might have happened without the benefit of Ultra intelligence. To begin with, more ships and supplies would certainly have been lost to the dominant U-boat fleet, which would have compromised the vital link to America and forced the Allies to divert manpower and resources into the building of new ships. Historians have estimated that this would have delayed Allied plans by several months, which would have meant postponing the D-Day invasion until at least the following year. According to Sir Harry Hinsley, “the war, instead of finishing in 1945, would have ended in 1948 had the Government Code and Cypher School not been able to read the Enigma cyphers and produce the Ultra intelligence.”

During this period of delay, additional lives would have been lost in Europe, and Hitler would have been able to make greater use of his V-weapons, inflicting damage throughout southern England. The historian David Kahn summarizes the impact of breaking Enigma: “It saved lives. Not only Allied and Russian lives but, by shortening the war, German, Italian, and Japanese lives as well. Some people alive after World War II might not have been but for these solutions. That is the debt that the world owes to the codebreakers; that is the crowning human value of their triumphs.”

After the war, Bletchley’s accomplishments remained a closely guarded secret. Having successfully deciphered messages during the war, Britain wanted to continue its intelligence operations, and was reluctant to divulge its capabilities. In fact, Britain had captured thousands of Enigma machines, and distributed them among its former colonies, who believed that the cipher was as secure as it had seemed to the Germans. The British did nothing to disabuse them of this belief, and routinely deciphered their secret communications in the years that followed.

Meanwhile, the Government Code and Cypher School at Bletchley Park was closed and the thousands of men and women who had contributed to the creation of Ultra were disbanded. The bombs were dismantled, and every scrap of paper that related to the wartime decipherments was either locked away or burned. Britain’s codebreaking activities were officially transferred to the newly formed Government
Communications Headquarters (GCHQ) in London, which was moved to Cheltenham in 1952. Although some of the cryptanalysts moved to GCHQ, most of them returned to their civilian lives, sworn to secrecy, unable to reveal their pivotal role in the Allied war effort. While those who had fought conventional battles could talk of their heroic achievements, those who had fought intellectual battles of no less significance had to endure the embarrassment of having to evade questions about their wartime activities. Gordon Welchman recounted how one of the young cryptanalysts working with him in Hut 6 had received a scathing letter from his old headmaster, accusing him of being a disgrace to his school for not being at the front. Derek Taunt, who also worked in Hut 6, summed up the true contribution of his colleagues: “Our happy band may not have been with King Harry on St. Crispin’s Day, but we had certainly not been abed and have no reason to think ourselves accurs’d for having been where we were.”

After three decades of silence, the secrecy over Bletchley Park eventually came to an end in the early 1970s. Captain F.W. Winterbotham, who had been responsible for distributing the Ultra intelligence, began to badger the British Government, arguing that the Commonwealth countries had stopped using the Enigma cipher and that there was now nothing to be gained by concealing the fact that Britain had broken it. The intelligence services reluctantly agreed, and permitted him to write a book about the work done at Bletchley Park. Published in the summer of 1974, Winterbotham’s book The Ultra Secret was the signal that Bletchley personnel were at last free to discuss their wartime activities. Gordon Welchman felt enormous relief: “After the war I still avoided discussions of wartime events for fear that I might reveal information obtained from Ultra rather than from some published account . . . I felt that this turn of events released me from my wartime pledge of secrecy.”

Those who had contributed so much to the war effort could now receive the recognition they deserved. Possibly the most remarkable consequence of Winterbotham’s revelations was that Rejewski realized the staggering consequences of his prewar breakthroughs against Enigma. After the invasion of Poland, Rejewski had escaped to France, and when France was overrun he fled to Britain. It would seem natural that he should have become part of the British Enigma effort, but instead he was relegated to tackling menial ciphers at a minor intelligence unit in Bovingdon, near Hemel Hempstead. It is not clear why such a brilliant mind was excluded from Bletchley Park, but as a result he was completely unaware of the activities of the Government Code and Cypher School. Until the publication of Winterbotham’s book, Rejewski had no idea that his ideas had provided the foundation for the routine decipherment of Enigma throughout the war.

For some, the publication of Winterbotham’s book came too late. Many years after the death of Alastair Denniston, Bletchley’s first director, his daughter received a letter from one of his colleagues: “Your father was a great man in whose debt all English-speaking people will remain for a very long time, if not forever. That so few should know exactly what he did is the sad part.”

Alan Turing was another cryptanalyst who did not live long enough to receive any public recognition. Instead of being acclaimed a hero, he was persecuted for his homosexuality. In 1952, while reporting a burglary to the police, he naively revealed that he was having a homosexual relationship. The police felt they had no option but to arrest and charge him with “Gross Indecency contrary to Section 11 of the Criminal Law Amendment Act 1885.” The newspapers reported the subsequent trial and conviction, and Turing was publicly humiliated.

Turing’s secret had been exposed, and his sexuality was now public knowledge. The British Government withdrew his security clearance. He was forbidden to work on research projects relating to the development of the computer. He was forced to consult a psychiatrist and had to undergo hormone treatment, which made him impotent and obese. Over the next two years he became severely depressed, and on June 7, 1954, he went to his bedroom, carrying with him a jar of cyanide solution and an apple. Twenty years earlier he had chanted the rhyme of the Wicked Witch: “Dip the apple in the brew, Let the sleeping death seep through.” Now he was ready to obey her incantation. He dipped the apple in the cyanide and took several bites. At the age of just forty-two, one of the true geniuses of cryptanalysis committed suicide.