3 The Mechanization of Secrecy

At the end of the nineteenth century, cryptography was in disarray. Ever since Babbage and Kasiski had destroyed the security of the Vigenère cipher, cryptographers had been searching for a new cipher, something that would reestablish secret communication, thereby allowing businessmen and the military to exploit the immediacy of the telegraph without their communications being stolen and deciphered. Furthermore, at the turn of the century, the Italian physicist Guglielmo Marconi invented an even more powerful form of telecommunication, which made the need for secure encryption even more pressing.

In 1894, Marconi began experimenting with a curious property of electrical circuits. Under certain conditions, if one circuit carried an electric current, this could induce a current in another isolated circuit some distance away. By enhancing the design of the two circuits, increasing the power and adding aerials, Marconi could soon transmit and receive pulses of information across distances of up to 2.5 km. He had invented radio. The telegraph had already been established for half a century, but it required a wire to transport a message between sender and receiver. Marconi's system had the great advantage of being wireless–the signal traveled, as if by magic, through the air.

In 1896, in search of financial backing for his idea, Marconi emigrated to Britain, where he filed his first patent. Continuing his experiments, he increased the range of his radio communications, first transmitting a message 15 km across the Bristol Channel, and then 53 km across the English Channel to France. At the same time he began to look for commercial applications for his invention, pointing out to potential backers the two main advantages of radio: it did not require the construction of expensive telegraph lines, and it had the potential to send messages

between otherwise isolated locations. He pulled off a magnificent publicity stunt in 1899, when he equipped two ships with radios so that journalists covering the America's Cup, the world's most important yacht race, could send reports back to New York for the following day's newspapers.

Interest increased still further when Marconi shattered the myth that radio communication was limited by the horizon. Critics had argued that because radio waves could not bend and follow the curvature of the Earth, radio communication would be limited to a hundred kilometers or so. Marconi attempted to prove them wrong by sending a message from Poldhu in Cornwall to St. John's in Newfoundland, a distance of 3,500 km. In December 1901, for three hours each day, the Poldhu transmitter sent the letter S (dot-dot-dot) over and over again, while Marconi stood on the windy cliffs of Newfoundland trying to detect the radio waves. Day after day, he wrestled to raise aloft a giant kite, which in turn hoisted his antenna high into the air. A little after midday on December 12, Marconi detected three faint dots, the first transatlantic radio message. The explanation of Marconi's achievement remained a mystery until 1924, when physicists discovered the ionosphere, a layer of the atmosphere whose lower boundary is about 60 km above the Earth. The ionosphere acts as a mirror, allowing radio waves to bounce off it. Radio waves also bounce off the Earth's surface, so radio messages could effectively reach anywhere in the world after a series of reflections between the ionosphere and the Earth.

Marconi's invention tantalized the military, who viewed it with a mixture of desire and trepidation. The tactical advantages of radio are obvious: it allows direct communication between any two points without the need for a wire between the locations. Laying such a wire is often impractical, sometimes impossible. Previously, a naval commander based in port had no way of communicating with his ships, which might disappear for months on end, but radio would enable him to coordinate a fleet wherever the ships might be. Similarly, radio would allow generals to direct their campaigns, keeping them in continual contact with battalions, regardless of their movements. All this is made possible by the nature of radio waves, which emanate in all directions, and reach receivers wherever they may be. However, this all-pervasive property of radio is also its greatest military weakness, because messages will inevitably reach the enemy as

well as the intended recipient. Consequently, reliable encryption became a necessity. If the enemy were going to be able to intercept every radio message, then cryptographers had to find a way of preventing them from deciphering these messages.

The mixed blessings of radio—ease of communication and ease of interception—were brought into sharp focus at the outbreak of the First World War. All sides were keen to exploit the power of radio, but were also unsure of how to guarantee security. Together, the advent of radio and the Great War intensified the need for effective encryption. The hope was that there would be a breakthrough, some new cipher that would reestablish secrecy for military commanders. However, between 1914 and 1918 there was to be no great discovery, merely a catalogue of cryptographic failures. Codemakers conjured up several new ciphers, but one by one they were broken.

One of the most famous wartime ciphers was the German *ADFGVX cipher*, introduced on March 5, 1918, just before the major German offensive that began on March 21. Like any attack, the German thrust would benefit from the element of surprise, and a committee of cryptographers had selected the ADFGVX cipher from a variety of candidates, believing that it offered the best security. In fact, they were confident that it was unbreakable. The cipher's strength lay in its convoluted nature, a mixture of a substitution and transposition (see Appendix F).

By the beginning of June 1918, the German artillery was only 100 km from Paris, and was preparing for one final push. The only hope for the Allies was to break the ADFGVX cipher to find just where the Germans were planning to punch through their defenses. Fortunately, they had a secret weapon, a cryptanalyst by the name of Georges Painvin. This dark, slender Frenchman with a penetrating mind had recognized his talent for cryptographic conundrums only after a chance meeting with a member of the Bureau du Chiffre soon after the outbreak of war. Thereafter, his priceless skill was devoted to pinpointing the weaknesses in German ciphers. He grappled day and night with the ADFGVX cipher, in the process losing 15 kg in weight.

Eventually, on the night of June 2, he cracked an ADFGVX message. Painvin's breakthrough led to a spate of other decipherments, including a message that contained the order "Rush munitions. Even by day if not

seen." The preamble to the message indicated that it was sent from somewhere between Montdidier and Compiègne, some 80 km to the north of Paris. The urgent need for munitions implied that this was to be the location of the imminent German thrust. Aerial reconnaissance confirmed that this was the case. Allied soldiers were sent to reinforce this stretch of the front line, and a week later the German onslaught began. Having lost the element of surprise, the German army was beaten back in a hellish battle that lasted five days.

The breaking of the ADFGVX cipher typified cryptography during the First World War. Although there was a flurry of new ciphers, they were all variations or combinations of nineteenth-century ciphers that had already been broken. While some of them initially offered security, it was never long before cryptanalysts got the better of them. The biggest problem for cryptanalysts was dealing with the sheer volume of traffic. Before the advent of radio, intercepted messages were rare and precious items, and cryptanalysts cherished each one. However, in the First World War, the amount of radio traffic was enormous, and every single message could be intercepted, generating a steady flow of ciphertexts to occupy the minds of the cryptanalysts. It is estimated that the French intercepted a hundred million words of German communications during the course of the Great War.

Of all the wartime cryptanalysts, the French were the most effective. When they entered the war, they already had the strongest team of codebreakers in Europe, a consequence of the humiliating French defeat in the Franco-Prussian War. Napoleon III, keen to restore his declining popularity, had invaded Prussia in 1870, but he had not anticipated the alliance between Prussia in the north and the southern German states. Led by Otto von Bismarck, the Prussians steamrollered the French army, annexing the provinces of Alsace and Lorraine and bringing an end to French domination of Europe. Thereafter, the continued threat of the newly united Germany seems to have been the spur for French cryptanalysts to master the skills necessary to provide France with detailed intelligence about the plans of its enemy.

It was in this climate that Auguste Kerckhoffs wrote his treatise *La Cryptographie militaire*. Although Kerckhoffs was Dutch, he spent most of his life in France, and his writings provided the French with an exceptional guide to the principles of cryptanalysis. By the time the First World

Figure 26 Lieutenant Georges Painvin.

War had begun, three decades later, the French military had implemented Kerckhoffs' ideas on an industrial scale. While lone geniuses like Painvin sought to break new ciphers, teams of experts, each with specially developed skills for tackling a particular cipher, concentrated on the day-to-day decipherments. Time was of the essence, and conveyor-belt cryptanalysis could provide intelligence quickly and efficiently.

Sun-Tzu, author of the *Art of War*, a text on military strategy dating from the fourth century B.C., stated that: "Nothing should be as favorably regarded as intelligence; nothing should be as generously rewarded as intelligence; nothing should be as confidential as the work of intelligence." The French were fervent believers in the words of Sun-Tzu, and in addition to honing their cryptanalytic skills they also developed several ancillary techniques for gathering radio intelligence, methods that did not involve decipherment. For example, the French listening posts learned to recognize a radio operator's *fist*. Once encrypted, a message is sent in Morse code, as a series of dots and dashes, and each operator can be identified by his pauses, the speed of transmission, and the relative lengths of dots and dashes. A fist is the equivalent of a recognizable style of handwriting. As well as operating listening posts, the French established six direction finding stations which were able to detect where each message was coming from. Each station moved its antenna until the incoming signal was strongest, which identified a direction for the source of a message. By combining the directional information from two or more stations it was possible to locate the exact source of the enemy transmission. By combining fist information with direction finding, it was possible to establish both the identity and the location of, say, a particular battalion. French intelligence could then track its path over the course of several days, and potentially deduce its destination and objective. This form of intelligence gathering, known as traffic analysis, was particularly valuable after the introduction of a new cipher. Each new cipher would make cryptanalysts temporarily impotent, but even if a message was indecipherable it could still yield information via traffic analysis.

The vigilance of the French was in sharp contrast to the attitude of the Germans, who entered the war with no military cryptanalytic bureau. Not until 1916 did they set up the Abhorchdienst, an organization devoted to intercepting Allied messages. Part of the reason for their tardiness in establishing the Abhorchdienst was that the German army had advanced into French territory in the early phase of the war. The French, as they retreated, destroyed the landlines, forcing the advancing Germans to rely on radios for communication. While this gave the French a continuous supply of German intercepts, the opposite was not true. As the French were retreating back into their own territory, they still had access to their own landlines, and had no need to communicate by radio. With a lack of French radio communication, the Germans could not make many interceptions, and hence they did not bother to develop their cryptanalytic department until two years into the war.

The British and the Americans also made important contributions to Allied cryptanalysis. The supremacy of the Allied codebreakers and their influence on the Great War are best illustrated by the decipherment of a German telegram that was intercepted by the British on January 17, 1917. The story of this decipherment shows how cryptanalysis can affect the course of war at the very highest level, and demonstrates the potentially devastating repercussions of employing inadequate encryption. Within a matter of weeks, the deciphered telegram would force America to rethink its policy of neutrality, thereby shifting the balance of the war.

Despite calls from politicians in Britain and America, President Woodrow Wilson had spent the first two years of the war steadfastly refusing to send American troops to support the Allies. Besides not wanting to sacrifice his nation's youth on the bloody battlefields of Europe, he was convinced that the war could be ended only by a negotiated settlement, and he believed that he could best serve the world if he remained neutral and acted as a mediator. In November 1916, Wilson saw hope for a settlement when Germany appointed a new Foreign Minister, Arthur Zimmermann, a jovial giant of a man who appeared to herald a new era of enlightened German diplomacy. American newspapers ran headlines such as OUR FRIEND ZIMMERMANN and LIBERALIZATION OF GERMANY, and one article proclaimed him as "one of the most auspicious omens for the future of German–American relations." However, unknown to the Americans, Zimmermann had no intention of pursuing peace. Instead, he was plotting to extend Germany's military aggression.

Back in 1915, a submerged German U-boat had been responsible for sinking the ocean liner *Lusitania*, drowning 1,198 passengers, including 128 U.S. civilians. The loss of the *Lusitania* would have drawn America

into the war, were it not for Germany's reassurances that henceforth U-boats would surface before attacking, a restriction that was intended to avoid accidental attacks on civilian ships. However, on January 9, 1917, Zimmermann attended a momentous meeting at the German castle of Pless, where the Supreme High Command was trying to persuade the Kaiser that it was time to renege on their promise, and embark on a course of unrestricted submarine warfare. German commanders knew that their U-boats were almost invulnerable if they launched their torpedoes while remaining submerged, and they believed that this would prove to be the decisive factor in determining the outcome of the war. Germany had been constructing a fleet of two hundred U-boats, and the Supreme High Command argued that unrestricted U-boat aggression would cut off Britain's supply lines and starve it into submission within six months.

A swift victory was essential. Unrestricted submarine warfare and the inevitable sinking of U.S. civilian ships would almost certainly provoke America into declaring war on Germany. Bearing this in mind, Germany needed to force an Allied surrender before America could mobilize its troops and make an impact in the European arena. By the end of the meeting at Pless, the Kaiser was convinced that a swift victory could be achieved, and he signed an order to proceed with unrestricted U-boat warfare, which would take effect on February 1.

In the three weeks that remained, Zimmermann devised an insurance policy. If unrestricted U-boat warfare increased the likelihood of America entering the war, then Zimmermann had a plan that would delay and weaken American involvement in Europe, and which might even discourage it completely. Zimmermann's idea was to propose an alliance with Mexico, and persuade the President of Mexico to invade America and reclaim territories such as Texas, New Mexico and Arizona. Germany would support Mexico in its battle with their common enemy, aiding it financially and militarily.

Furthermore, Zimmermann wanted the Mexican president to act as a mediator and persuade Japan that it too should attack America. This way, Germany would pose a threat to America's East Coast, Japan would attack from the west, while Mexico invaded from the south. Zimmermann's main motive was to pose America such problems at home that it could not afford to send troops to Europe. Thus Germany could win the battle

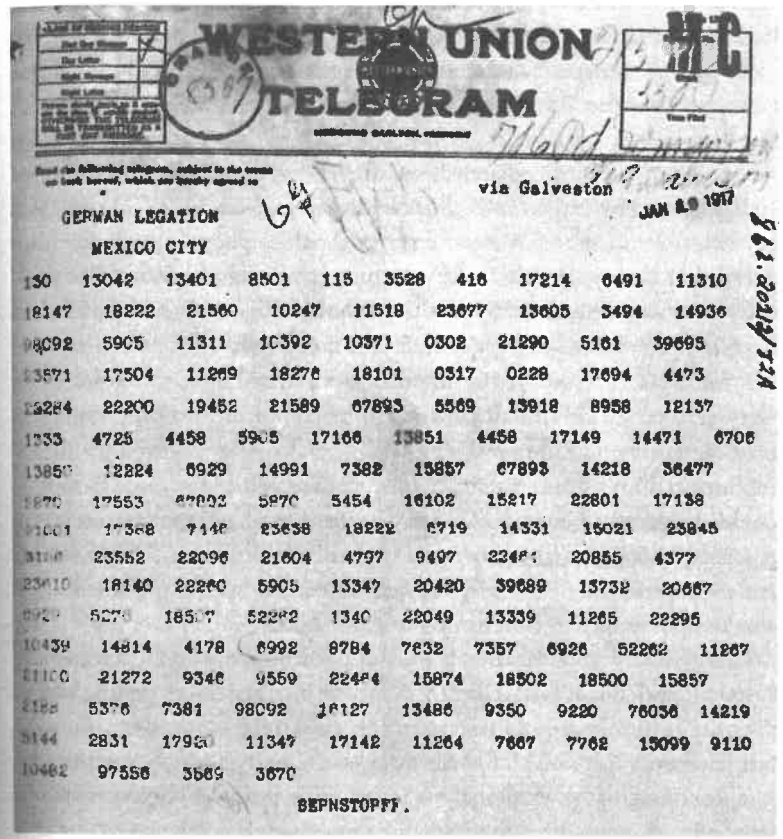
Figure 27 Arthur Zimmermann.

at sea, win the war in Europe and then withdraw from the American campaign. On January 16, Zimmermann encapsulated his proposal in a telegram to the German Ambassador in Washington, who would then retransmit it to the German Ambassador in Mexico, who would finally deliver it to the Mexican President. Figure 28 shows the encrypted telegraph; the actual message is as follows:

> We intend to begin unrestricted submarine warfare on the first of February. We shall endeavor in spite of this to keep the United States neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support, and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico and Arizona. The settlement in detail is left to you.
>
> You will inform the President [of Mexico] of the above most secretly, as soon as the outbreak of war with the United States is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves.
>
> Please call the President's attention to the fact that the unrestricted employment of our submarines now offers the prospect of compelling England to make peace within a few months. Acknowledge receipt.
>
> Zimmermann

Zimmermann had to encrypt his telegram because Germany was aware that the Allies were intercepting all its transatlantic communications, a consequence of Britain's first offensive action of the war. Before dawn on the first day of the First World War, the British ship *Telconia* approached the German coast under cover of darkness, dropped anchor, and hauled up a clutch of undersea cables. These were Germany's transatlantic cables–its communication links to the rest of the world. By the time the sun had risen, they had been severed. This act of sabotage was aimed at destroying Germany's most secure means of communication, thereby forcing German messages to be sent via insecure radio links or via cables owned by other countries. Zimmermann was forced to send his encrypted telegram via Sweden and, as a back-up, via the more direct American-owned cable. Both routes touched England, which meant that the text of the Zimmermann telegram, as it would become known, soon fell into British hands.

The intercepted telegram was immediately sent to Room 40, the Admiralty's cipher bureau, named after the office in which it was initially housed. Room 40 was a strange mixture of linguists, classical scholars and puzzle addicts, capable of the most ingenious feats of cryptanalysis. For example, the Reverend Montgomery, a gifted translator of German theological works, had deciphered a secret message hidden in a postcard addressed to Sir Henry Jones, 184 King's Road, Tighnabruaich, Scotland.


WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
13571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1733 4725 4458 5905 17166 13851 4458 17149 14471 6706
13858 12224 6929 14991 7382 15857 67893 14218 36477
17553 67893 5870 5454 16102 15217 22801 17138
7148 23638 18222 6719 14331 15021 23845
23552 22096 21604 4797 9497 20855 4377
18140 22260 5905 13347 20420 39689 13732 20667
5870 18557 52262 1340 22049 13339 11265 22295
14814 4178 6992 8784 7632 7357 6926 52262 11267
21272 9346 9559 22464 15874 18502 18500 15857
5376 7381 98092 16127 13486 9350 9220 76036 14219
2831 17934 11347 17142 11264 7667 7762 15099 9110
97556 3569 3670

BERNSTORFF.

Figure 28 The Zimmermann telegram, as forwarded by von Bernstorff, the German Ambassador in Washington, to Eckhardt, the German Ambassador in Mexico City.

The postcard had been sent from Turkey, so Sir Henry had assumed that it was from his son, a prisoner of the Turks. However, he was puzzled because the postcard was blank, and the address was peculiar–the village of Tighnabruaich was so tiny that none of the houses had numbers and there was no King's Road. Eventually, the Reverend Montgomery spotted the postcard's cryptic message. The address alluded to the Bible, First Book of Kings, Chapter 18, Verse 4: "Obadiah took a hundred prophets, and hid them fifty in a cave, and fed them with bread and water." Sir Henry's son was simply reassuring his family that he was being well looked after by his captors.

When the encrypted Zimmermann telegram arrived in Room 40, it was Montgomery who was made responsible for deciphering it, along with Nigel de Grey, a publisher seconded from the firm of William Heinemann. They saw immediately that they were dealing with a form of encryption used only for high-level diplomatic communications, and tackled the telegram with some urgency. The decipherment was far from trivial, but they were able to draw upon previous analyses of other similarly encrypted telegrams. Within a few hours the codebreaking duo had been able to recover a few chunks of text, enough to see that they were uncovering a message of the utmost importance. Montgomery and de Grey persevered with their task, and by the end of the day they could discern the outline of Zimmermann's terrible plans. They realized the dreadful implications of unrestricted U-boat warfare, but at the same time they could see that the German Foreign Minister was encouraging an attack on America, which was likely to provoke President Wilson into abandoning America's neutrality. The telegram contained the deadliest of threats, but also the possibility of America joining the Allies.

Montgomery and de Grey took the partially deciphered telegram to Admiral Sir William Hall, Director of Naval Intelligence, expecting him to pass the information to the Americans, thereby drawing them into the war. However, Admiral Hall merely placed the partial decipherment in his safe, encouraging his cryptanalysts to continue filling in the gaps. He was reluctant to hand the Americans an incomplete decipherment, in case there was a vital caveat that had not yet been deciphered. He also had another concern lurking in the back of his mind. If the British gave the Americans the deciphered Zimmermann telegram, and the Americans reacted by publicly condemning Germany's proposed aggression, then the Germans would conclude that their method of encryption had been broken. This would goad them into developing a new and stronger encryption system, thus choking a vital channel of intelligence. In any case, Hall was aware that the all-out U-boat onslaught would begin in just two weeks, which in itself might be enough to incite President Wilson into declaring war on Germany. There was no point jeopardizing a valuable source of intelligence when the desired outcome might happen anyway.

On February 1, as ordered by the Kaiser, Germany instigated unrestricted naval warfare. On February 2, Woodrow Wilson held a cabinet meeting to decide the American response. On February 3, he spoke to Congress and announced that America would continue to remain neutral, acting as a peacemaker, not a combatant. This was contrary to Allied and German expectations. American reluctance to join the Allies left Admiral Hall with no choice but to exploit the Zimmermann telegram.

In the fortnight since Montgomery and de Grey had first contacted Hall, they had completed the decipherment. Furthermore, Hall had found a way of keeping Germany from suspecting that their security had been breached. He realized that von Bernstòrff, the German Ambassador in Washington, would have forwarded the message to von Eckhardt, the German Ambassador in Mexico, having first made some minor changes. For example, von Bernstorff would have removed the instructions aimed at himself, and would also have changed the address. Von Eckhardt would then have delivered this revised version of the telegram, unencrypted, to the Mexican President. If Hall could somehow obtain this Mexican version of the Zimmermann telegram, then it could be published in the newspapers and the Germans would assume that it had been stolen from the Mexican Government, not intercepted and cracked by the British on its way to America. Hall contacted a British agent in Mexico, known only as Mr. H., who in turn infiltrated the Mexican Telegraph Office. Mr. H. was able to obtain exactly what he needed–the Mexican version of the Zimmermann telegram.

It was this version of the telegram that Hall handed to Arthur Balfour, the British Secretary of State for Foreign Affairs. On February 23, Balfour summoned the American Ambassador, Walter Page, and presented him with the Zimmermann telegram, later calling this "the most dramatic

moment in all my life." Four days later, President Wilson saw for himself the "eloquent evidence," as he called it, proof that Germany was encouraging direct aggression against America.

The telegram was released to the press and, at last, the American nation was confronted with the reality of Germany's intentions. Although there was little doubt among the American people that they should retaliate, there was some concern within the U.S. administration that the telegram might be a hoax, manufactured by the British to guarantee American involvement in the war. However, the question of authenticity soon vanished when Zimmermann publicly admitted his authorship. At a press

Figure 29 "Exploding in his Hands," a cartoon by Rollin Kirby published on March 3, 1917, in *The World*.

conference in Berlin, without being pressured, he simply stated, "I cannot deny it. It is true."

In Germany, the Foreign Office began an investigation into how the Americans had obtained the Zimmermann telegram. They fell for Admiral Hall's ploy, and came to the conclusion that "various indications suggest that the treachery was committed in Mexico." Meanwhile, Hall continued to distract attention from the work of British cryptanalysts. He planted a story in the British press criticizing his own organization for not intercepting the Zimmermann telegram, which in turn led to a spate of articles attacking the British secret service and praising the Americans.

At the beginning of the year, Wilson had said that it would be a "crime against civilization" to lead his nation to war, but by April 2, 1917, he had changed his mind: "I advise that the Congress declare the recent course of the Imperial Government to be in fact nothing less than war against the government and people of the United States, and that it formally accept the status of belligerent which has thus been thrust upon it." A single breakthrough by Room 40 cryptanalysts had succeeded where three years of intensive diplomacy had failed. Barbara Tuchman, American historian and author of *The Zimmermann Telegram*, offered the following analysis:

> Had the telegram never been intercepted or never been published, inevitably the Germans would have done something else that would have brought us in eventually. But the time was already late and, had we delayed much longer, the Allies might have been forced to negotiate. To that extent the Zimmermann telegram altered the course of history . . . In itself the Zimmermann telegram was only a pebble on the long road of history. But a pebble can kill a Goliath, and this one killed the American illusion that we could go about our business happily separate from other nations. In world affairs it was a German Minister's minor plot. In the lives of the American people it was the end of innocence.

The Holy Grail of Cryptography

The First World War saw a series of victories for cryptanalysts, culminating in the decipherment of the Zimmermann telegram. Ever since the cracking of the Vigenère cipher in the nineteenth century, codebreakers had maintained the upper hand over the codemakers. Then, toward the end of the

war, when cryptographers were in a state of utter despair, scientists in America made an astounding breakthrough. They discovered that the Vigenère cipher could be used as the basis for a new, more formidable form of encryption. In fact, this new cipher could offer perfect security.

The fundamental weakness of the Vigenère cipher is its cyclical nature. If the keyword is five letters long, then every fifth letter of the plaintext is encrypted according to the same cipher alphabet. If the cryptanalyst can identify the length of the keyword, the ciphertext can be treated as a series of five monoalphabetic ciphers, and each one can be broken by frequency analysis. However, consider what happens as the keyword gets longer.

Imagine a plaintext of 1,000 letters encrypted according to the Vigenère cipher, and imagine that we are trying to cryptanalyze the resulting ciphertext. If the keyword used to encipher the plaintext were only 5 letters long, the final stage of cryptanalysis would require applying frequency analysis to 5 sets of 200 letters, which is easy. But if the keyword had been 20 letters long, the final stage would be a frequency analysis of 20 sets of 50 letters, which is considerably harder. And if the keyword had been 1,000 letters long, you would be faced with frequency analysis of 1,000 sets of 1 letter each, which is completely impossible. In other words, if the keyword (or keyphrase) is as long as the message, then the cryptanalytic technique developed by Babbage and Kasiski will not work.

Using a key as long as the message is all well and good, but this requires the cryptographer to create a lengthy key. If the message is hundreds of letters long, the key also needs to be hundreds of letters long. Rather than inventing a long key from scratch, it might be tempting to base it on, say, the lyrics of a song. Alternatively, the cryptographer could pick up a book on birdwatching and base the key on a series of randomly chosen bird names. However, such shortcut keys are fundamentally flawed.

In the following example, I have enciphered a piece of ciphertext using the Vigenère cipher, using a keyphrase that is as long as the message. All the cryptanalytic techniques that I have previously described will fail. None the less, the message can be deciphered.

Key	? ?
Plaintext	? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

This new system of cryptanalysis begins with the assumption that the ciphertext contains some common words, such as **the**. Next, we randomly place **the** at various points in the plaintext, as shown below, and deduce what sort of keyletters would be required to turn **the** into the appropriate ciphertext. For example, if we pretend that **the** is the first word of the plaintext, then what would this imply for the first three letters of the key? The first letter of the key would encrypt **t** into **V**. To work out the first letter of the key, we take a Vigenère square, look down the column headed by **t** until we reach **V**, and find that the letter that begins that row is **C**. This process is repeated with **h** and **e**, which would be encrypted as **H** and **R** respectively, and eventually we have candidates for the first three letters of the key, **CAN**. All of this comes from the assumption that **the** is the first word of the plaintext. We place **the** in a few other positions, and, once again, deduce the corresponding keyletters. (You can check the relationship between each plaintext letter and ciphertext letter by referring to the Vigenère square in Table 9.)

Key	C A N ? ? ? B S J ? ? ? ? ? Y P T ? ? ? ?
Plaintext	t h e ? ? ? t h e ? ? ? ? ? t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

We have tested three **the**'s against three arbitrary fragments of the ciphertext, and generated three guesses as to the elements of certain parts of the key. How can we tell whether any of the **the**'s are in the right position? We suspect that the key consists of sensible words, and we can use this to our advantage. If a **the** is in a wrong position, it will probably result in a random selection of keyletters. However, if it is in a correct position, the keyletters should make some sense. For example, the first **the** yields the keyletters **CAN**, which is encouraging because this is a perfectly reasonable English syllable. It is possible that this **the** is in the correct position. The second **the** yields **BSJ**, which is a very peculiar combination of consonants, suggesting that the second **the** is probably a mistake. The third **the** yields **YPT**, an unusual syllable but one which is worth further investigation. If **YPT** really were part of the key, it would be within a larger word, the only possibilities being **APOCALYPTIC**, **CRYPT** and **EGYPT**, and derivatives of these words. How can we find out if one of these words is part of the key? We can test each hypothesis by inserting

the three candidate words in the key, above the appropriate section of the ciphertext, and working out the corresponding plaintext:

Key	C A N ? ? ? ? ? A P O C A L Y P T I C ? ?
Plaintext	t h e ? ? ? ? ? n q c b e o t h e x g ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? ? ? ? ? ? ? C R Y P T ? ? ? ?
Plaintext	t h e ? ? ? ? ? ? ? ? ? c i t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Key	C A N ? ? ? ? ? ? ? ? ? E G Y P T ? ? ? ?
Plaintext	t h e ? ? ? ? ? ? ? ? ? a t t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

If the candidate word is not part of the key, it will probably result in a random piece of plaintext, but if it is part of the key the resulting plaintext should make some sense. With **APOCALYPTIC** as part of the key the resulting plaintext is gibberish of the highest quality. With **CRYPT**, the resulting plaintext is **cithe**, which is not an inconceivable piece of plaintext. However, if **EGYPT** were part of the key it would generate **atthe**, a more promising combination of letters, probably representing the words **at the**.

For the time being let us assume that the most likely possibility is that **EGYPT** is part of the key. Perhaps the key is a list of countries. This would suggest that **CAN**, the piece of the key that corresponds to the first **the**, is the start of **CANADA**. We can test this hypothesis by working out more of the plaintext, based on the assumption that **CANADA**, as well as **EGYPT**, is part of the key:

Key	C A N A D A ? ? ? ? ? ? E G Y P T ? ? ? ?
Plaintext	t h e m e e ? ? ? ? ? ? a t t h e ? ? ? ?
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Our assumption seems to be making sense. **CANADA** implies that the plaintext begins with **themee** which perhaps is the start of **the meeting**. Now that we have deduced some more letters of the plaintext, ting, we can deduce the corresponding part of the key, which turns out to be

BRAZ. Surely this is the beginning of **BRAZIL**. Using the combination of **CANADABRAZILEGYPT** as the bulk of the key, we get the following decipherment: **the meeting is at the ????**.

In order to find the final word of the plaintext, the location of the meeting, the best strategy would be to complete the key by testing one by one the names of all possible countries, and deducing the resulting plaintext. The only sensible plaintext is derived if the final piece of the key is **CUBA**:

Key	C A N A D A B R A Z I L E G Y P T C U B A
Plaintext	t h e m e e t i n g i s a t t h e d o c k
Ciphertext	V H R M H E U Z N F Q D E Z R W X F I D K

Table 9 Vigenère square.

Plain	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

So, a key that is as long as the message is not sufficient to guarantee security. The insecurity in the example above arises because the key was constructed from meaningful words. We began by randomly inserting **the** throughout the plaintext, and working out the corresponding keyletters. We could tell when we had put a **the** in the correct place, because the keyletters looked as if they might be part of meaningful words. Thereafter, we used these snippets in the key to deduce whole words in the key. In turn this gave us more snippets in the message, which we could expand into whole words, and so on. This entire process of toing and froing between the message and the key was only possible because the key had an inherent structure and consisted of recognizable words. However, in 1918 cryptographers began experimenting with keys that were devoid of structure. The result was an unbreakable cipher.

As the Great War drew to a close, Major Joseph Mauborgne, head of cryptographic research for the U.S. Army, introduced the concept of a random key—one that consisted not of a recognizable series of words, but rather a random series of letters. He advocated employing these random keys as part of a Vigenère cipher to give an unprecedented level of security. The first stage of Mauborgne's system was to compile a thick pad consisting of hundreds of sheets of paper, each sheet bearing a unique key in the form of lines of randomly sequenced letters. There would be two copies of the pad, one for the sender and one for the receiver. To encrypt a message, the sender would apply the Vigenère cipher using the first sheet of the pad as the key. Figure 30 shows three sheets from such a pad (in reality each sheet would contain hundreds of letters), followed by a message encrypted using the random key on the first sheet. The receiver can easily decipher the ciphertext by using the identical key and reversing the Vigenère cipher. Once that message has been successfully sent, received and deciphered, both the sender and the receiver destroy the sheet that acted as the key, so that it is never used again. When the next message is encrypted, the next random key in the pad is employed, which is also subsequently destroyed, and so on. Because each key is used once, and only once, this system is known as a *onetime pad cipher*.

The onetime pad cipher overcomes all previous weaknesses. Imagine that the message **attack the valley at dawn** has been enciphered as in Figure 30, sent via a radio transmitter and intercepted by the enemy. The

ciphertext is handed to an enemy cryptanalyst, who then attempts to decipher it. The first hurdle is that, by definition, there is no repetition in a random key, so the method of Babbage and Kasiski cannot break the onetime pad cipher. As an alternative, the enemy cryptanalyst might try placing the word **the** in various places, and deduce the corresponding piece of the key, just as we did when we attempted to decipher the previous message. If the cryptanalyst tries putting **the** at the beginning of the message, which is incorrect, then the corresponding segment of key would be revealed as **WXB**, which is a random series of letters. If the cryptanalyst tries placing **the** so that it begins at the seventh letter of the message, which happens to be correct, then the corresponding segment of key would be revealed as **QKJ**, which is also a random series of letters. In other words, the cryptanalyst cannot tell whether the trial word is, or is not, in the correct place.

In desperation, the cryptanalyst might consider an exhaustive search of all possible keys. The ciphertext consists of 21 letters, so the cryptanalyst knows that the key consists of 21 letters. This means that there are roughly 500,000,000,000,000,000,000,000,000,000 possible keys to test, which is completely beyond what is humanly or mechanically feasible. However, even if the cryptanalyst could test all these keys, there is an even greater obstacle to be overcome. By checking every possible key the

Sheet 1	Sheet 2	Sheet 3
P L M O E	O I W V H	J A B P R
Z Q K J Z	P I Q Z E	M F E C F
L R T E A	T S E B L	L G U X D
V C R C B	C Y R U P	D A G M R
Y N N R B	D U V N M	Z K W Y I

Key	P L M O E Z Q K J Z L R T E A V C R C B Y
Plaintext	a t t a c k t h e v a l l e y a t d a w n
Ciphertext	P E F O G J J R N U L C E I Y V V U C X L

Figure 30 Three sheets, each a potential key for a onetime pad cipher. The message is enciphered using Sheet 1.

cryptanalyst will certainly find the right message–but every wrong message will also be revealed. For example, the following key applied to the same ciphertext generates a completely different message:

Key	M A A K T G Q K J N D R T I F D B H K T S
Plaintext	d e f e n d t h e h i l l a t s u n s e t
Ciphertext	P E F O G J J R N U L C E I Y V V U C X L

If all the different keys could be tested, every conceivable 21-letter message would be generated, and the cryptanalyst would be unable to distinguish between the right one and all the others. This difficulty would not have arisen had the key been a series of words or a phrase, because the incorrect messages would almost certainly have been associated with a meaningless key, whereas the correct message would be associated with a sensible key.

The security of the onetime pad cipher is wholly due to the randomness of the key. The key injects randomness into the ciphertext, and if the ciphertext is random then it has no patterns, no structure, nothing the cryptanalyst can latch onto. In fact, it can be mathematically proved that it is impossible for a cryptanalyst to crack a message encrypted with a onetime pad cipher. In other words, the onetime pad cipher is not merely believed to be unbreakable, just as the Vigenère cipher was in the nineteenth century, *it really is absolutely secure*. The onetime pad offers a guarantee of secrecy: the Holy Grail of cryptography.

At last, cryptographers had found an unbreakable system of encryption. However, the perfection of the onetime pad cipher did not end the quest for secrecy: the truth of the matter is that it was hardly ever used. Although it is perfect in theory, it is flawed in practice because the cipher suffers from two fundamental difficulties. First, there is the practical problem of making large quantities of random keys. In a single day an army might exchange hundreds of messages, each containing thousands of characters, so radio operators would require a daily supply of keys equivalent to millions of randomly arranged letters. Supplying so many random sequences of letters is an immense task.

Some early cryptographers assumed that they could generate huge amounts of random keys by haphazardly tapping away at a typewriter. However, whenever this was tried, the typist would tend to get into the habit of typing a character using the left hand, and then a character using the right hand, and thereafter alternate between the two sides. This might be a quick way of generating a key, but the resulting sequence has structure, and is no longer random–if the typist hits the letter D, from the left side of the keyboard, then the next letter is predictable in as much as it is probably from the right side of the keyboard. If a onetime pad key was to be truly random, a letter from the left side of the keyboard should be followed by another letter from the left side of the keyboard on roughly half the occasions.

Cryptographers have come to realize that it requires a great deal of time, effort and money to create a random key. The best random keys are created by harnessing natural physical processes, such as radioactivity, which is known to exhibit truly random behavior. The cryptographer could place a lump of radioactive material on a bench, and detect its emissions with a Geiger counter. Sometimes the emissions follow each other in rapid succession, sometimes there are long delays–the time between emissions is unpredictable and random. The cryptographer could then connect a display to the Geiger counter, which rapidly cycles through the alphabet at a fixed rate, but which freezes momentarily as soon as an emission is detected. Whatever letter is on the display could be used as the next letter of the random key. The display restarts and once again cycles through the alphabet until it is stopped at random by the next emission, the letter frozen on the display is added to the key, and so on. This arrangement would be guaranteed to generate a truly random key, but it is impractical for day-to-day cryptography.

Even if you could fabricate enough random keys, there is a second problem, namely the difficulty of distributing them. Imagine a battlefield scenario in which hundreds of radio operators are part of the same communications network. To start with, every single person must have identical copies of the onetime pad. Next, when new pads are issued, they must be distributed to everybody simultaneously. Finally, everybody must remain in step, making sure that they are using the right sheet of the onetime pad at the right time. Widespread use of the onetime pad would fill the battlefield with couriers and bookkeepers. Furthermore, if the enemy captures just one set of keys, then the whole communication system is compromised.

It might be tempting to cut down on the manufacture and distribution of keys by reusing onetime pads, but this is a cryptographic cardinal sin.

Reusing a onetime pad would allow an enemy cryptanalyst to decipher messages with relative ease. The technique used to prize open two pieces of ciphertext encrypted with the same onetime pad key is explained in Appendix G, but for the time being the important point is that there can be no shortcuts in using the onetime pad cipher. The sender and receiver must use a new key for every message.

A onetime pad is practicable only for people who need ultrasecure communication, and who can afford to meet the enormous costs of manufacturing and securely distributing the keys. For example, the hotline between the presidents of Russia and America is secured via a onetime pad cipher.

The practical flaws of the theoretically perfect onetime pad meant that Mauborgne's idea could never be used in the heat of battle. In the aftermath of the First World War and all its cryptographic failures, the search continued for a practical system that could be employed in the next conflict. Fortunately for cryptographers, it would not be long before they made a breakthrough, something that would reestablish secret communication on the battlefield. In order to strengthen their ciphers, cryptographers were forced to abandon their pencil-and-paper approach to secrecy, and exploit the very latest technology to scramble messages.

The Development of Cipher Machines–from Cipher Disks to the Enigma

The earliest cryptographic machine is the cipher disk, invented in the fifteenth century by the Italian architect Leon Alberti, one of the fathers of the polyalphabetic cipher. He took two copper disks, one slightly larger than the other, and inscribed the alphabet around the edge of both. By placing the smaller disk on top of the larger one and fixing them with a needle to act as an axis, he constructed something similar to the cipher disk shown in Figure 31. The two disks can be independently rotated so that the two alphabets can have different relative positions, and can thus be used to encrypt a message with a simple Caesar shift. For example, to encrypt a message with a Caesar shift of one place, position the outer A next to the inner B–the outer disk is the plain alphabet, and the inner disk represents the cipher alphabet. Each letter in the plaintext message is looked up on the outer disk, and the corresponding letter on the inner disk is written down as part of the ciphertext. To send a message with a Caesar shift of five places, simply rotate the disks so that the outer A is next to the inner F, and then use the cipher disk in its new setting.

Even though the cipher disk is a very basic device, it does ease encipherment, and it endured for five centuries. The version shown in Figure 31 was used in the American Civil War. Figure 32 shows a Code-o-Graph, a cipher disk used by the eponymous hero of *Captain Midnight*, one of the early American radio dramas. Listeners could obtain their own Code-o-Graph by writing to the program sponsors, Ovaltine, and enclosing a label from one of their containers. Occasionally the program would end with a secret message from Captain Midnight, which could be deciphered by loyal listeners using the Code-o-Graph.

The cipher disk can be thought of as a "scrambler," taking each plaintext letter and transforming it into something else. The mode of operation described so far is straightforward, and the resulting cipher is

Figure 31 A U.S. Confederate cipher disk used in the American Civil War.

relatively trivial to break, but the cipher disk can be used in a more complicated way. Its inventor, Alberti, suggested changing the setting of the disk during the message, which in effect generates a polyalphabetic cipher instead of a monoalphabetic cipher. For example, Alberti could have used his disk to encipher the word **goodbye**, using the keyword **LEON**. He would begin by setting his disk according to the first letter of the keyword, moving the outer **A** next to the inner **L**. Then he would encipher the first letter of the message, **g**, by finding it on the outer disk and noting the corresponding letter on the inner disk, which is **R**. To encipher the second letter of the message, he would reset his disk according to the second letter of the keyword, moving the outer **A** next to the inner **E**. Then he would encipher **o** by finding it on the outer disk and noting the corresponding letter on the inner disk, which is **S**. The encryption process continues with the cipher disk being set according to the keyletter **O**, then **N**, then back to **L**, and so on. Alberti has effectively encrypted a message

Figure 32 Captain Midnight's Code-o-Graph, which enciphers each plaintext letter (outer disk) as a number (inner disk), rather than a letter.

using the Vigenère cipher with his first name acting as the keyword. The cipher disk speeds up encryption and reduces errors compared with performing the encryption via a Vigenère square.

The important feature of using the cipher disk in this way is the fact that the disk is changing its mode of scrambling during encryption. Although this extra level of complication makes the cipher harder to break, it does not make it unbreakable, because we are simply dealing with a mechanized version of the Vigenère cipher, and the Vigenère cipher was broken by Babbage and Kasiski. However, five hundred years after Alberti, a more complex reincarnation of his cipher disk would lead to a new generation of ciphers, an order of magnitude more difficult to crack than anything previously used.

In 1918, the German inventor Arthur Scherbius and his close friend Richard Ritter founded the company of Scherbius & Ritter, an innovative engineering firm that dabbled in everything from turbines to heated pillows. Scherbius was in charge of research and development, and was constantly looking for new opportunities. One of his pet projects was to replace the inadequate systems of cryptography used in the First World War by swapping pencil-and-paper ciphers with a form of encryption that exploited twentieth-century technology. Having studied electrical engineering in Hanover and Munich, he developed a piece of cryptographic machinery that was essentially an electrical version of Alberti's cipher disk. Called Enigma, Scherbius's invention would become the most fearsome system of encryption in history.

Scherbius's Enigma machine consisted of a number of ingenious components, which he combined into a formidable and intricate cipher machine. However, if we break the machine down into its constituent parts and rebuild it in stages, then its underlying principles will become apparent. The basic form of Scherbius's invention consists of three elements connected by wires: a keyboard for inputting each plaintext letter, a scrambling unit that encrypts each plaintext letter into a corresponding ciphertext letter, and a display board consisting of various lamps for indicating the ciphertext letter. Figure 33 shows a stylized layout of the machine, limited to a six-letter alphabet for simplicity. In order to encrypt a plaintext letter, the operator presses the appropriate plaintext letter on the keyboard, which sends an electric pulse through the central

scrambling unit and out the other side, where it illuminates the corresponding ciphertext letter on the lampboard.

The scrambler, a thick rubber disk riddled with wires, is the most important part of the machine. From the keyboard, the wires enter the scrambler at six points, and then make a series of twists and turns within the scrambler before emerging at six points on the other side. The internal wirings of the scrambler determine how the plaintext letters will be encrypted. For example, in Figure 33 the wirings dictate that:

typing in **a** will illuminate the letter **B**, which means that **a** is encrypted as **B**,
typing in **b** will illuminate the letter **A**, which means that **b** is encrypted as **A**,
typing in **c** will illuminate the letter **D**, which means that **c** is encrypted as **D**,
typing in **d** will illuminate the letter **F**, which means that **d** is encrypted as **F**,
typing in **e** will illuminate the letter **E**, which means that **e** is encrypted as **E**,
typing in **f** will illuminate the letter **C**, which means that **f** is encrypted as **C**.

The message **cafe** would be encrypted as **DBCE**. With this basic setup, the scrambler essentially defines a cipher alphabet, and the machine can be used to implement a simple monoalphabetic substitution cipher.

However, Scherbius's idea was for the scrambler disk to automatically rotate by one-sixth of a revolution each time a letter is encrypted (or one-twenty-sixth of a revolution for a complete alphabet of 26 letters). Figure 34(a) shows the same arrangement as in Figure 33; once again, typing in the letter **b** will illuminate the letter **A**. However, this time, immediately after typing a letter and illuminating the lampboard, the scrambler revolves by one-sixth of a revolution to the position shown in Figure 34(b). Typing in the letter **b** again will now illuminate a different letter, namely **C**. Immediately afterward, the scrambler rotates once more, to the position shown in Figure 34(c). This time, typing in the letter **b** will illuminate **E**. Typing the letter **b** six times in a row would generate the ciphertext **ACEBDC**. In other words, the cipher alphabet changes after each encryption, and the encryption of the letter **b** is constantly changing. With this rotating setup, the scrambler essentially defines six cipher alphabets, and the machine can be used to implement a polyalphabetic cipher.

The rotation of the scrambler is the most important feature of Scherbius's design. However, as it stands the machine suffers from one obvious weakness. Typing **b** six times will return the scrambler to its original

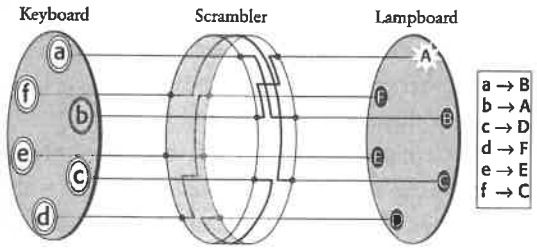


Figure 33 A simplified version of the Enigma machine with an alphabet of just six letters. The most important element of the machine is the scrambler. By typing in **b** on the keyboard, a current passes into the scrambler, follows the path of the internal wiring, and then emerges so as illuminate the **A** lamp. In short, **b** is encrypted as **A**. The box to the right indicates how each of the six letters is encrypted.

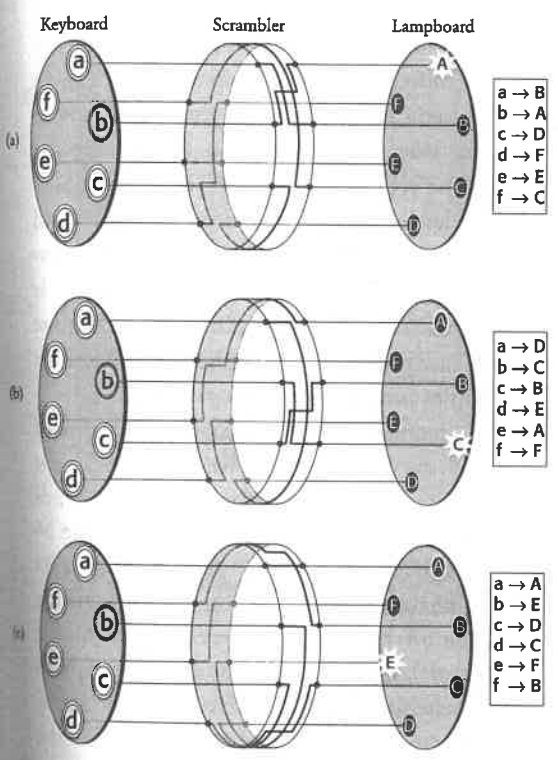


Figure 34 Every time a letter is typed into the keyboard and encrypted, the scrambler rotates by one place, thus changing how each letter is potentially encrypted. In (a) the scrambler encrypts **b** as **A**, but in (b) the new scrambler orientation encrypts **b** as **C**. In (c), after rotating one more place, the scrambler encrypts **b** as **E**. After encrypting four more letters, and rotating four more places, the scrambler returns to its original orientation.

position, and typing b again and again will repeat the pattern of encryption. In general, cryptographers are keen to avoid repetition because it leads to regularity and structure in the ciphertext, symptoms of a weak cipher. This problem can be alleviated by introducing a second scrambler disk.

Figure 35 is a schematic of a cipher machine with two scramblers. Because of the difficulty of drawing a three-dimensional scrambler with three-dimensional internal wirings, Figure 35 shows only a two-dimensional representation. Each time a letter is encrypted, the first scrambler rotates by one space, or in terms of the two-dimensional diagram, each wiring shifts down one place. In contrast, the second scrambler disk remains stationary for most of the time. It moves only after the first scrambler has made a complete revolution. The first scrambler is fitted with a tooth, and it is only when this tooth reaches a certain point that it knocks the second scrambler on one place.

In Figure 35(a), the first scrambler is in a position where it is just about to knock forward the second scrambler. Typing in and encrypting a letter moves the mechanism to the configuration shown in Figure 35(b), in which the first scrambler has moved on one place, and the second scrambler has also been knocked on one place. Typing in and encrypting another letter again moves the first scrambler on one place, Figure 35(c), but this time the second scrambler has remained stationary. The second scrambler will not move again until the first scrambler completes one revolution, which will take another five encryptions. This arrangement is similar to a car odometer–the rotor representing single miles turns quite quickly, and when it completes one revolution by reaching "9," it knocks the rotor representing tens of miles forward one place.

The advantage of adding a second scrambler is that the pattern of encryption is not repeated until the second scrambler is back where it started, which requires six complete revolutions of the first scrambler, or the encryption of 6 × 6, or 36 letters in total. In other words, there are 36 distinct scrambler settings, which is equivalent to switching between 36 cipher alphabets. With a full alphabet of 26 letters, the cipher machine would switch between 26 × 26, or 676 cipher alphabets. So by combining scramblers (sometimes called rotors), it is possible to build an encryption machine which is continually switching between different cipher alphabets. The operator types in a particular letter and, depending on the

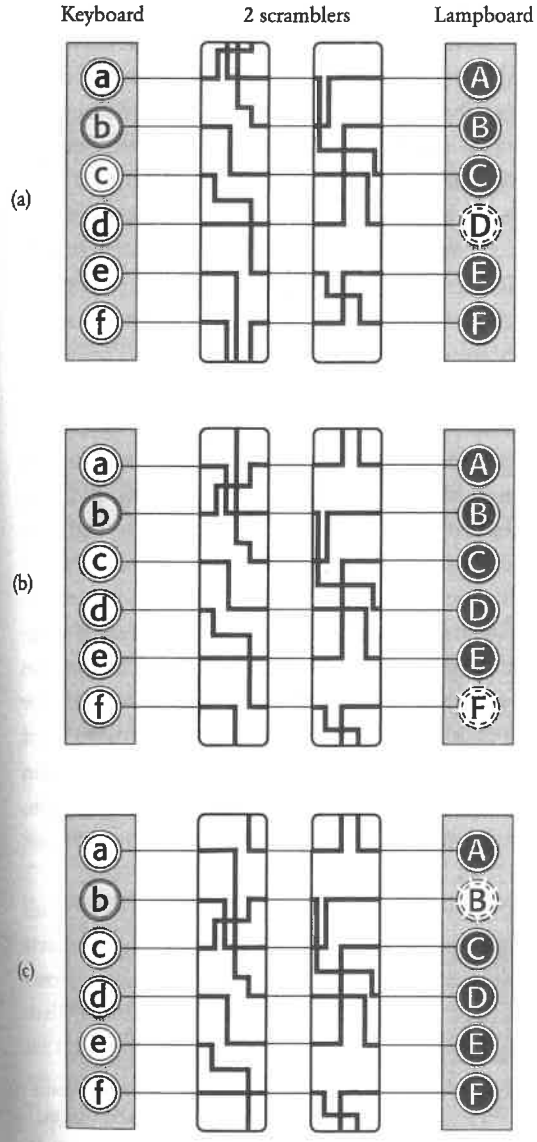


Figure 35 On adding a second scrambler, the pattern of encryption does not repeat until 36 letters have been enciphered, at which point both scramblers have returned to their original positions. To simplify the diagram, the scramblers are represented in just two dimensions; instead of rotating one place, the wirings move down one place. If a wire appears to leave the top or bottom of a scrambler, its path can be followed by continuing from the corresponding wire at the bottom or top of the same scrambler. In (a), b is encrypted as D. After encryption, the first scrambler rotates by one place, also nudging the second scrambler around one place–this happens only once during each complete revolution of the first wheel. This new setting is shown in (b), in which b is encrypted as F. After encryption, the first scrambler rotates by one place, but this time the second scrambler remains fixed. This new setting is shown in (c), in which b is encrypted as B.

scrambler arrangement, it can be encrypted according to any one of hundreds of cipher alphabets. Then the scrambler arrangement changes, so that when the next letter is typed into the machine it is encrypted according to a different cipher alphabet. Furthermore, all of this is done with great efficiency and accuracy, thanks to the automatic movement of scramblers and the speed of electricity.

Before explaining in detail how Scherbius intended his encryption machine to be used, it is necessary to describe two more elements of the Enigma, which are shown in Figure 36. First, Scherbius's standard encryption machine employed a third scrambler for extra complexity–for a full alphabet these three scramblers would provide 26 × 26 × 26, or 17,576 distinct scrambler arrangements. Second, Scherbius added a *reflector*. The reflector is a bit like a scrambler, inasmuch as it is a rubber disk with internal wirings, but it differs because it does not rotate, and the wires enter on one side and then reemerge on the same side. With the reflector in place, the operator types in a letter, which sends an electrical signal through the three scramblers. When the reflector receives the incoming signal it sends it back through the same three scramblers, but along a different route. For example, with the setup in Figure 36, typing the letter b would send a signal through the three scramblers and into the reflector, whereupon the signal would return back through the wirings to arrive at the letter D. The signal does not actually emerge through the keyboard, as it might seem from Figure 36, but instead is diverted to the lampboard. At first sight the reflector seems to be a pointless addition to the machine, because its static

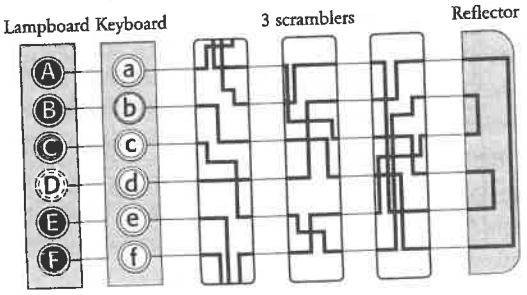


Figure 36 Scherbius's design of the Enigma included a third scrambler and a reflector that sends the current back through the scramblers. In this particular setting, typing in b eventually illuminates D on the lampboard, shown here adjacent to the keyboard.

nature means that it does not add to the number of cipher alphabets. However, its benefits become clear when we see how the machine was actually used to encrypt and decrypt a message.

An operator wishes to send a secret message. Before encryption begins, the operator must first rotate the scramblers to a particular starting position. There are 17,576 possible arrangements, and therefore 17,576 possible starting positions. The initial setting of the scramblers will determine how the message is encrypted. We can think of the Enigma machine in terms of a general cipher system, and the initial settings are what determine the exact details of the encryption. In other words, the initial settings provide the key. The initial settings are usually dictated by a codebook, which lists the key for each day, and which is available to everybody within the communications network. Distributing the codebook requires time and effort, but because only one key per day is required, it could be arranged for a codebook containing 28 keys to be sent out just once every four weeks. By comparison, if an army were to use a onetime pad cipher, it would require a new key for every message, and key distribution would be a much greater task. Once the scramblers have been set according to the codebook's daily requirement, the sender can begin encrypting. He types in the first letter of the message, sees which letter is illuminated on the lampboard, and notes it down as the first letter of the ciphertext. Then, the first scrambler having automatically stepped on by one place, the sender inputs the second letter of the message, and so on. Once he has generated the complete ciphertext, he hands it to a radio operator who transmits it to the intended receiver.

In order to decipher the message, the receiver needs to have another Enigma machine and a copy of the codebook that contains the initial scrambler settings for that day. He sets up the machine according to the book, types in the ciphertext letter by letter, and the lampboard indicates the plaintext. In other words, the sender typed in the plaintext to generate the ciphertext, and now the receiver types in the ciphertext to generate the plaintext–encipherment and decipherment are mirror processes. The ease of decipherment is a consequence of the reflector. From Figure 36 we can see that if we type in b and follow the electrical path, we come back to D. Similarly, if we type in d and follow the path, then we come back to B. The machine encrypts a plaintext letter into a ciphertext letter,

and, as long as the machine is in the same setting, it will decrypt the same ciphertext letter back into the same plaintext letter.

It is clear that the key, and the codebook that contains it, must never be allowed to fall into enemy hands. It is quite possible that the enemy might capture an Enigma machine, but without knowing the initial settings used for encryption, they cannot easily decrypt an intercepted message. Without the codebook, the enemy cryptanalyst must resort to checking all the possible keys, which means trying all the 17,576 possible initial scrambler settings. The desperate cryptanalyst would set up the captured Enigma machine with a particular scrambler arrangement, input a short piece of the ciphertext, and see if the output makes any sense. If not, he would change to a different scrambler arrangement and try again. If he can check one scrambler arrangement each minute and works night and day, it would take almost two weeks to check all the settings. This is a moderate level of security, but if the enemy set a dozen people on the task, then all the settings could be checked within a day. Scherbius therefore decided to improve the security of his invention by increasing the number of initial settings and thus the number of possible keys.

He could have increased security by adding more scramblers (each new scrambler increases the number of keys by a factor of 26), but this would have increased the size of the Enigma machine. Instead, he added two other features. First, he simply made the scramblers removable and interchangeable. So, for example, the first scrambler disk could be moved to the third position, and the third scrambler disk to the first position. The arrangement of the scramblers affects the encryption, so the exact arrangement is crucial to encipherment and decipherment. There are six different ways to arrange the three scramblers, so this feature increases the number of keys, or the number of possible initial settings, by a factor of six.

The second new feature was the insertion of a *plugboard* between the keyboard and the first scrambler. The plugboard allows the sender to insert cables which have the effect of swapping some of the letters before they enter the scrambler. For example, a cable could be used to connect the a and b sockets of the plugboard, so that when the cryptographer wants to encrypt the letter b, the electrical signal actually follows the path through the scramblers that previously would have been the path for the letter a, and vice versa. The Enigma operator had six cables, which meant

that six pairs of letters could be swapped, leaving fourteen letters unplugged and unswapped. The letters swapped by the plugboard are part of the machine's setting, and so must be specified in the codebook. Figure 37 shows the layout of the machine with the plugboard in place. Because the diagram deals only with a six-letter alphabet, only one pair of letters, a and b, have been swapped.

There is one more feature of Scherbius's design, known as the *ring*, which has not yet been mentioned. Although the ring does have some effect on encryption, it is the least significant part of the whole Enigma machine, and I have decided to ignore it for the purposes of this discussion. (Readers who would like to know about the exact role of the ring should refer to some of the books in the list of further reading, such as *Seizing the Enigma* by David Kahn. This list also includes two Web sites containing excellent Enigma emulators, which allow you to operate a virtual Enigma machine.)

Now that we know all the main elements of Scherbius's Enigma machine, we can work out the number of keys, by combining the number of possible plugboard cablings with the number of possible scrambler

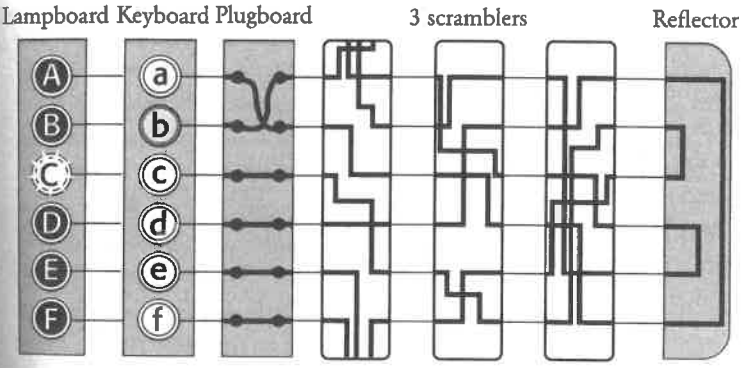


Figure 37 The plugboard sits between the keyboard and the first scrambler. By inserting cables it is possible to swap pairs of letters, so that, in this case, b is swapped with a. Now, b is encrypted by following the path previously associated with the encryption of a. In the real 26-letter Enigma, the user would have six cables for swapping six pairs of letters.

arrangements and orientations. The following list shows each variable of the machine and the corresponding number of possibilities for each one:

Scrambler orientations. Each of the 3 scramblers can be set in one of 26 orientations. There are therefore $26 \times 26 \times 26$ settings: 17,576

Scrambler arrangements. The three scramblers (1, 2 and 3) can be positioned in any of the following six orders: 123, 132, 213, 231, 312, 321. 6

Plugboard. The number of ways of connecting, thereby swapping, six pairs of letters out of 26 is enormous: 100,391,791,500

Total. The total number of keys is the multiple of these three numbers: $17,576 \times 6 \times 100,391,791,500$

$\approx 10,000,000,000,000,000$

As long as sender and receiver have agreed on the plugboard cablings, the order of the scramblers and their respective orientations, all of which specify the key, they can encrypt and decrypt messages easily. However, an enemy interceptor who does not know the key would have to check every single one of the 10,000,000,000,000,000 possible keys in order to crack the ciphertext. To put this into context, a persistent cryptanalyst who is capable of checking one setting every minute would need longer than the age of the universe to check every setting. (In fact, because I have ignored the effect of the rings in these calculations, the number of possible keys is even larger, and the time to break Enigma even longer.)

Since by far the largest contribution to the number of keys comes from the plugboard, you might wonder why Scherbius bothered with the scramblers. On its own, the plugboard would provide a trivial cipher, because it would do nothing more than act as a monoalphabetic substitution cipher, swapping around just 12 letters. The problem with the plugboard is that the swaps do not change once encryption begins, so on its own it would generate a ciphertext that could be broken by frequency analysis. The scramblers contribute a smaller number of keys, but their setup is continually changing, which means that the resulting ciphertext cannot be broken by frequency analysis. By combining the scramblers with the plugboard, Scherbius protected his machine against frequency analysis, and at the same time gave it an enormous number of possible keys.

Scherbius took out his first patent in 1918. His cipher machine was contained in a compact box measuring only $34 \times 28 \times 15$ cm, but it weighed a hefty 12 kg. Figure 39 shows an Enigma machine with the outer lid open, ready for use. It is possible to see the keyboard where the plaintext letters are typed in, and, above it, the lampboard which displays the resulting ciphertext letter. Below the keyboard is the plugboard; there are more than six pairs of letters swapped by the plugboard, because this particular Enigma machine is a slightly later modification of the original model, which is the version that has been described so far. Figure 40 shows an Enigma with the cover plate removed to reveal more features, in particular the three scramblers.

Scherbius believed that Enigma was impregnable, and that its cryptographic strength would create a great demand for it. He tried to market the cipher machine to both the military and the business community,

Figure 38 Arthur Scherbius.

offering different versions to each. For example, he offered a basic version of Enigma to businesses, and a luxury diplomatic version with a printer rather than a lampboard to the Foreign Office. The price of an individual unit was as much as $30,000 in today's prices.

Unfortunately, the high cost of the machine discouraged potential buyers. Businesses said that they could not afford Enigma's security, but Scherbius believed that they could not afford to be without it. He argued that a vital message intercepted by a business rival could cost a company a fortune, but few businessmen took any notice of him. The German military were equally unenthusiastic, because they were oblivious to the damage caused by their insecure ciphers during the Great War. For example, they had been led to believe that the Zimmermann telegram had been stolen by American spies in Mexico, and so they blamed that failure on Mexican security. They still did not realize that the telegram had in fact been intercepted and deciphered by the British, and that the Zimmermann debacle was actually a failure of German cryptography.

Scherbius was not alone in his growing frustration. Three other inventors in three other countries had independently and almost simultaneously hit upon the idea of a cipher machine based on rotating scramblers. In the Netherlands in 1919, Alexander Koch took out patent No. 10,700, but he failed to turn his rotor machine into a commercial success and eventually sold the patent rights in 1927. In Sweden, Arvid Damm took out a similar patent, but by the time he died in 1927 he had also failed to find a market. In America, inventor Edward Hebern had complete faith in his invention, the so-called Sphinx of the Wireless, but his failure was the greatest of all.

In the mid-1920s, Hebern began building a $380,000 factory, but unfortunately this was a period when the mood in America was changing from paranoia to openness. The previous decade, in the aftermath of the First World War, the U.S. Government had established the American Black Chamber, a highly effective cipher bureau staffed by a team of twenty cryptanalysts, led by the flamboyant and brilliant Herbert Yardley. Later, Yardley wrote that "The Black Chamber, bolted, hidden, guarded, sees all, hears all. Though the blinds are drawn and the windows heavily curtained, its far-seeking eyes penetrate the secret conference chambers at Washington, Tokyo, London, Paris, Geneva, Rome. Its sensitive ears catch the faintest whisperings in the foreign capitals of the world." The

Figure 39 An army Enigma machine ready for use.

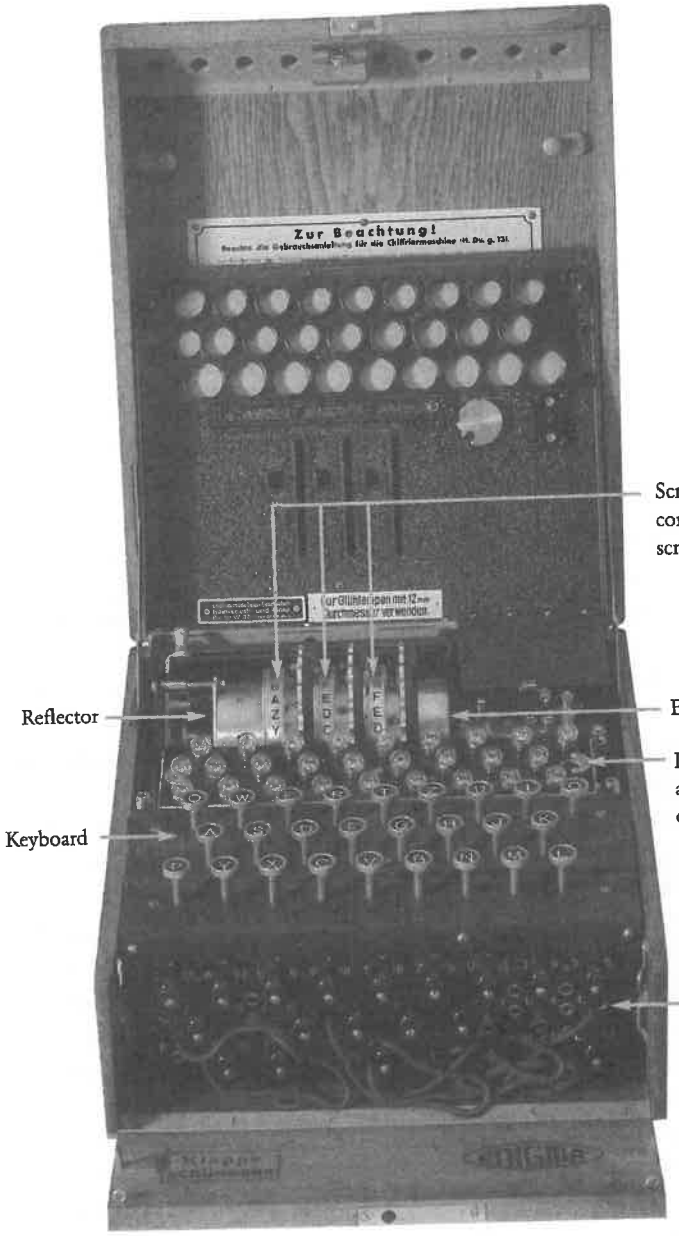


Figure 40 An Enigma machine with the inner lid opened, revealing the three scramblers.

American Black Chamber solved 45,000 cryptograms in a decade, but by the time Hebern built his factory, Herbert Hoover had been elected President and was attempting to usher in a new era of trust in international affairs. He disbanded the Black Chamber, and his Secretary of State, Henry Stimson, declared that "Gentlemen should not read each other's mail." If a nation believes that it is wrong to read the messages of others, then it also begins to believe that others will not read its own messages, and it does not see the necessity for fancy cipher machines. Hebern sold only twelve machines at a total price of roughly $1,200, and in 1926 he was brought to trial by dissatisfied shareholders and found guilty under California's Corporate Securities Act.

Fortunately for Scherbius, however, the German military were eventually shocked into appreciating the value of his Enigma machine, thanks to two British documents. The first was Winston Churchill's *The World Crisis*, published in 1923, which included a dramatic account of how the British had gained access to valuable German cryptographic material:

> At the beginning of September 1914, the German light cruiser *Magdeburg* was wrecked in the Baltic. The body of a drowned German under-officer was picked up by the Russians a few hours later, and clasped in his bosom by arms rigid in death, were the cipher and signal books of the German navy and the minutely squared maps of the North Sea and Heligoland Bight. On September 6 the Russian Naval Attaché came to see me. He had received a message from Petrograd telling him what had happened, and that the Russian Admiralty with the aid of the cipher and signal books had been able to decode portions at least of the German naval messages. The Russians felt that as the leading naval Power, the British Admiralty ought to have these books and charts. If we would send a vessel to Alexandrov, the Russian officers in charge of the books would bring them to England.

This material had helped the cryptanalysts in Room 40 to crack Germany's encrypted messages on a regular basis. Finally, almost a decade later, the Germans were made aware of this failure in their communications security. Also in 1923, the British Royal Navy published their official history of the First World War, which reiterated the fact that the interception and cryptanalysis of German communications had provided the Allies with a clear advantage. These proud achievements of British Intelligence were a stark

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 Chiffrierstelle, 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

Figure 41 Hans-Thilo Schmidt.

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 mathematical cryptanalyst put it, the creative codebreaker must "perforce 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
4th letter	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

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, and 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:

A→ F →W→ A	3 links
B→ Q → Z → K → V → E → L → R → I → B	9 links
C→ H → G → O → Y → D → P → C	7 links
J → M → X → S → T → N → U → J	7 links

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 characteristics 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:

A→ F →W→ A	3 links
B→ Q → Z → T → V → E → L → R → I → B	9 links
C→ H → S → O → Y → D → P → C	7 links
J → M → X → G → K → N → U → J	7 links

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 cablings were unknown and missing. However, every so often vaguely recognizable phrases would appear, such as **alliveinbelrin**–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, codenamed "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 *bombes*, 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 cafe eating a *bombe*, an ice cream shaped into a hemisphere. The bombes 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 bombes, 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, shortcutting the necessity for bombes 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 bombes, each representing a different scrambler arrangement. The sheer cost of building such a battery of bombes 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.

In 1938 Polish interceptions and decipherments had been at their peak, but by the beginning of 1939 the new scramblers and extra plugboard cables stemmed 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.

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

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 telegraphed 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 bombes. 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 bombes, 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 straining 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

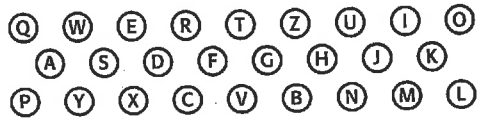


Figure 46 Layout of the Enigma keyboard.

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 bombes, 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

Figure 47 Alan Turing.

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 cablings. For example, if he could find something in the crib that had nothing to do with the plugboard cablings, 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 cablings.

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.

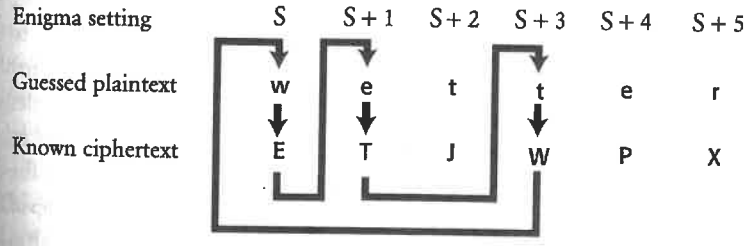


Figure 48 One of Turing's cribs, showing a loop.

Remember, cribs are only guesses, but if we assume that this crib is correct, we can link the letters w→E, e→T, t→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 cablings, 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 cablings.

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

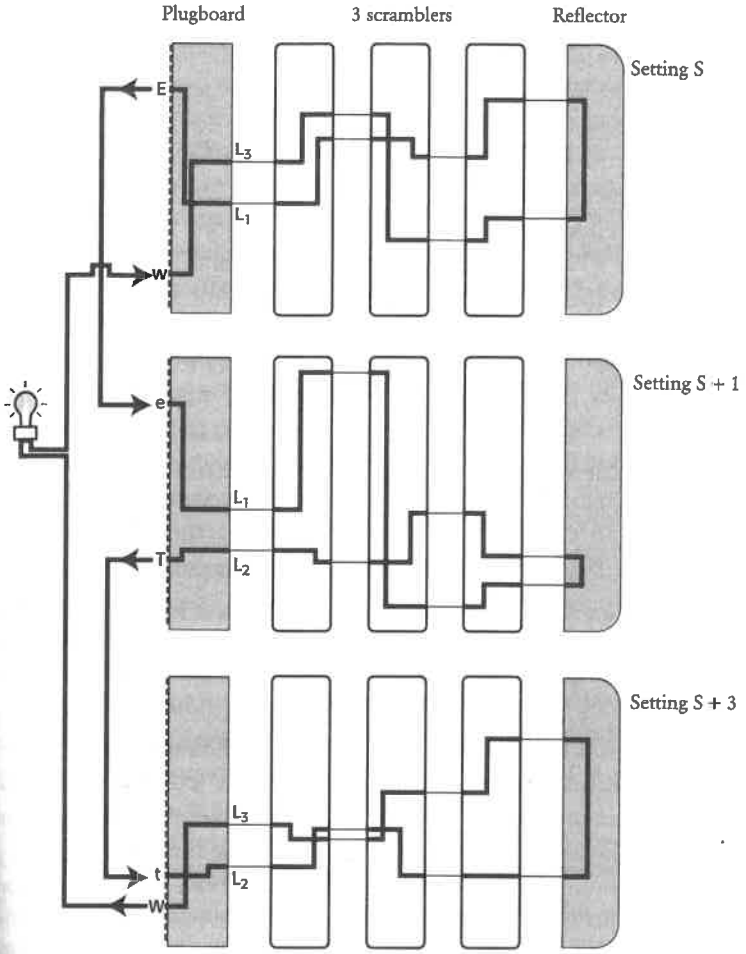


Figure 49 The loop in the crib can be paralleled by an electrical loop. Three Enigma machines are set up in identical ways, except that the second one has its first scrambler moved forward one place (setting S + 1), and the third has its scrambler moved forward two further places (setting S + 3). The 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	w e t t e r n u l l s e c h s
Known ciphertext	I P R E N L W K M J J S X C P L E J W Q

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	w e t t e r n u l l s e c h s
Known ciphertext	I P R E N L W K M J J S X C P L E J W Q

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 decipherments, and on September 6, 1941, he visited the codebreakers. On meeting some of the cryptanalysts, he was surprised by the bizarre mixture of people who were providing him with such valuable information; in addition to the mathematicians and linguists, there was an authority on porcelain, a curator from the Prague Museum, the British chess champion and numerous bridge experts. Churchill muttered to Sir Stewart Menzies,

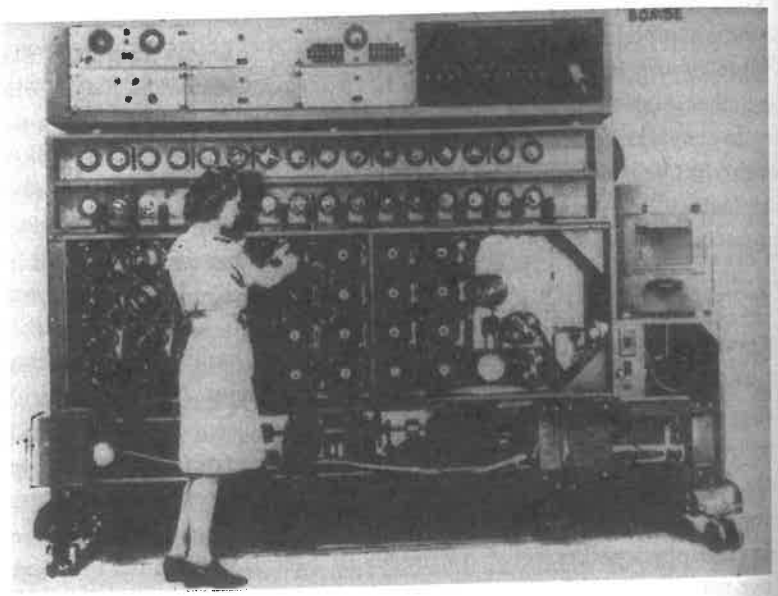


Figure 50 A bombe in action.

head of the Secret Intelligence Service, "I told you to leave no stone unturned, 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,

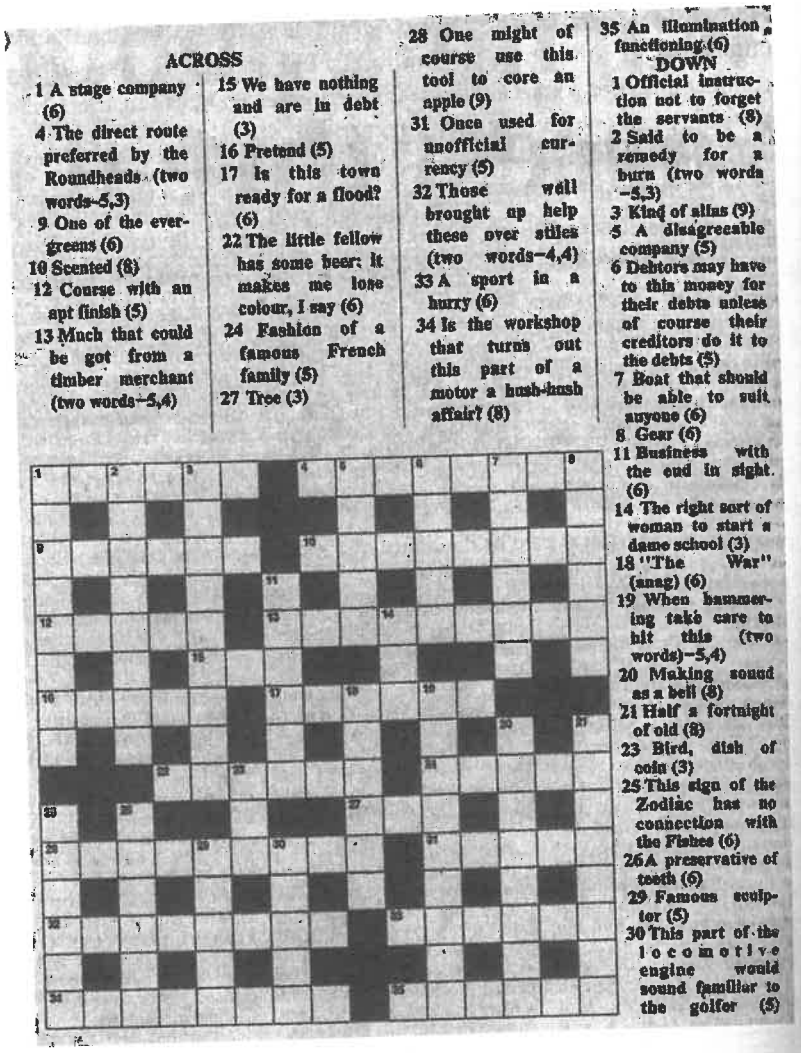
Some weeks ago you paid us the honor of a visit, and we believe that you regard our work as important. You will have seen that, thanks largely to the energy and foresight of Commander Travis, we have been well supplied with the "bombes" for the breaking of the German Enigma codes. We think, however, 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.



ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words–5,3)
9 One of the evergreens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (two words–5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words–4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (two words–5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight. (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (anag) (6)
19 When hammering take care to hit this (two words)–5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

Figure 51 The *Daily Telegraph* crossword used as a test to recruit new codebreakers (the solution is in Appendix H).

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

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 dominating all our power to carry on war, or even keep ourselves alive, lay our mastery of the ocean routes and the free approach and entry to our ports."

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 a particular location, 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 achievements 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 bombes 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't 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 Boxmoor, 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.