



SIMON SINGH

***The Code Book***

Simon Singh received his Ph.D. in physics from Cambridge University. A former BBC producer, he directed an award-winning documentary film on Fermat’s Last Theorem that aired on PBS’s *Nova* series and wrote the bestselling book, *Fermat’s Enigma*. He lives in London, England.

**Also by Simon Singh**

 *Fermat’s Enigma*



FIRST ANCHOR BOOKS EDITION, SEPTEMBER 2000

*Copyright © 1999 by Simon Singh*

All rights reserved under International and Pan-American Copyright Conventions. Published in the United States by Anchor Books, a division of Random House, Inc., New York, and simultaneously in Canada by Random House of Canada Limited, Toronto. Originally published in hardcover in the United States by Doubleday, a division of Random House, Inc., New York, and in the United Kingdom by the Fourth Estate, London, in 1999.

Anchor Books and colophon are registered trademarks of Random House, Inc.

The Library of Congress has cataloged the Doubleday edition as follows:
Singh, Simon.
The code book : the evolution of secrecy from Mary Queen of Scots to quantum cryptography / Simon Singh. –1st ed.
p. cm.
1. Cryptography–History.   2. Data encryption (Computer science)–History.   I. Title.
Z103.S56    1999
652′.8′09–dc21          99-35261

*Author photo © Nigel Spalding*

For my mother and father,

Sawaran Kaur and Mehnga Singh

The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others. Some are fortunate enough to find a job which consists in the solution of mysteries, but most of us are driven to sublimate this urge by the solving of artificial puzzles devised for our entertainment. Detective stories or crossword puzzles cater for the majority; the solution of secret codes may be the pursuit of a few.

John Chadwick
The Decipherment of Linear B

**Introduction**

For thousands of years, kings, queens and generals have relied on efficient communication in order to govern their countries and command their armies. At the same time, they have all been aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rival nations and betraying vital information to opposing forces. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.

The desire for secrecy has meant that nations have operated codemaking departments, responsible for ensuring the security of communications by inventing and implementing the best possible codes. At the same time, enemy codebreakers have attempted to break these codes, and steal secrets. Codebreakers are linguistic alchemists, a mystical tribe attempting to conjure sensible words out of meaningless symbols. The history of codes and ciphers is the story of the centuries-old battle between codemakers and codebreakers, an intellectual arms race that has had a dramatic impact on the course of history.

In writing *The Code Book*, I have had two main objectives. The first is to chart the evolution of codes. Evolution is a wholly appropriate term, because the development of codes can be viewed as an evolutionary struggle. A code is constantly under attack from codebreakers. When the codebreakers have developed a new weapon that reveals a code’s weakness, then the code is no longer useful. It either becomes extinct or it evolves into a new, stronger code. In turn, this new code thrives only until the codebreakers identify its weakness, and so on. This is analogous to the situation facing, for example, a strain of infectious bacteria. The bacteria live, thrive and survive until doctors discover an antibiotic that exposes a weakness in the bacteria and kills them. The bacteria are forced to evolve and outwit the antibiotic, and, if successful, they will thrive once again and reestablish themselves. The bacteria are continually forced to evolve in order to survive the onslaught of new antibiotics.

The ongoing battle between codemakers and codebreakers has inspired a whole series of remarkable scientific breakthroughs. The codemakers have continually striven to construct ever-stronger codes for defending communications, while codebreakers have continually invented more powerful methods for attacking them. In their efforts to destroy and preserve secrecy, both sides have drawn upon a diverse range of disciplines and technologies, from mathematics to linguistics, from information theory to quantum theory. In return, codemakers and codebreakers have enriched these subjects, and their work has accelerated technological development, most notably in the case of the modern computer.

History is punctuated with codes. They have decided the outcomes of battles and led to the deaths of kings and queens. I have therefore been able to call upon stories of political intrigue and tales of life and death to illustrate the key turning points in the evolutionary development of codes. The history of codes is so inordinately rich that I have been forced to leave out many fascinating stories, which in turn means that my account is not definitive. If you would like to find out more about your favorite tale or your favorite codebreaker then I would refer you to the list of further reading, which should help those readers who would like to study the subject in more detail.

Having discussed the evolution of codes and their impact on history, the book’s second objective is to demonstrate how the subject is more relevant today than ever before. As information becomes an increasingly valuable commodity, and as the communications revolution changes society, so the process of encoding messages, known as encryption, will play an increasing role in everyday life. Nowadays our phone calls bounce off satellites and our e-mails pass through various computers, and both forms of communication can be intercepted with ease, so jeopardizing our privacy. Similarly, as more and more business is conducted over the Internet, safeguards must be put in place to protect companies and their clients. Encryption is the only way to protect our privacy and guarantee the success of the digital marketplace. The art of secret communication, otherwise known as cryptography, will provide the locks and keys of the Information Age.

However, the public’s growing demand for cryptography conflicts with the needs of law enforcement and national security. For decades, the police and the intelligence services have used wire-taps to gather evidence against terrorists and organized crime syndicates, but the recent development of ultra-strong codes threatens to undermine the value of wire-taps. As we enter the twenty-first century, civil libertarians are pressing for the widespread use of cryptography in order to protect the privacy of the individual. Arguing alongside them are businesses, who require strong cryptography in order to guarantee the security of transactions within the fast-growing world of Internet commerce. At the same time, the forces of law and order are lobbying governments to restrict the use of cryptography. The question is, which do we value more—our privacy or an effective police force? Or is there a compromise?

Although cryptography is now having a major impact on civilian activities, it should be noted that military cryptography remains an important subject. It has been said that the First World War was the chemists’ war, because mustard gas and chlorine were employed for the first time, and that the Second World War was the physicists’ war, because the atom bomb was detonated. Similarly, it has been argued that the Third World War would be the mathematicians’ war, because mathematicians will have control over the next great weapon of war—information. Mathematicians have been responsible for developing the codes that are currently used to protect military information. Not surprisingly, mathematicians are also at the forefront of the battle to break these codes.

While describing the evolution of codes and their impact on history, I have allowed myself a minor detour. [Chapter 5](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_027.html#filepos469476) describes the decipherment of various ancient scripts, including Linear B and Egyptian hieroglyphics. Technically, cryptography concerns communications that are deliberately designed to keep secrets from an enemy, whereas the writings of ancient civilizations were not intended to be indecipherable: it is merely that we have lost the ability to interpret them. However, the skills required to uncover the meaning of archaeological texts are closely related to the art of codebreaking. Ever since reading *The Decipherment of Linear B*, John Chadwick’s description of how an ancient Mediterranean text was unraveled, I have been struck by the astounding intellectual achievements of those men and women who have been able to decipher the scripts of our ancestors, thereby allowing us to read about their civilizations, religions and everyday lives.

Turning to the purists, I should apologize for the title of this book. *The Code Book* is about more than just codes. The word “code” refers to a very particular type of secret communication, one that has declined in use over the centuries. In a code, a word or phrase is replaced with a word, number or symbol. For example, secret agents have codenames, words that are used instead of their real names in order to mask their identities. Similarly, the phrase **Attack at dawn** could be replaced by the codeword **Jupiter**, and this word could be sent to a commander in the battlefield as a way of baffling the enemy. If headquarters and the commander have previously agreed on the code, then the meaning of Jupiter will be clear to the intended recipient, but it will mean nothing to an enemy who intercepts it. The alternative to a code is a cipher, a technique that acts at a more fundamental level, by replacing letters rather than whole words. For example, each letter in a phrase could be replaced by the next letter in the alphabet, so that **A** is replaced by **B, B** by **C**, and so on. **Attack at dawn** thus becomes **Buubdl bu ebxo**. Ciphers play an integral role in cryptography, and so this book should really have been called *The Code and Cipher Book*. I have, however, forsaken accuracy for snappiness.

As the need arises, I have defined the various technical terms used within cryptography. Although I have generally adhered to these definitions, there will be occasions when I use a term that is perhaps not technically accurate, but which I feel is more familiar to the non-specialist. For example, when describing a person attempting to break a cipher, I have often used *codebreaker* rather than the more accurate *cipherbreaker*. I have done this only when the meaning of the word is obvious from the context. There is a glossary of terms at the end of the book. More often than not, though, crypto-jargon is quite transparent: for example, *plaintext* is the message before encryption, and *ciphertext* is the message after encryption.

Before concluding this introduction, I must mention a problem that faces any author who tackles the subject of cryptography: the science of secrecy is largely a secret science. Many of the heroes in this book never gained recognition for their work during their lifetimes because their contribution could not be publicly acknowledged while their invention was still of diplomatic or military value. While researching this book, I was able to talk to experts at Britain’s Government Communications Headquarters (GCHQ), who revealed details of extraordinary research done in the 1970s which has only just been declassified. As a result of this declassification, three of the world’s greatest cryptographers can now receive the credit they deserve. However, this recent revelation has merely served to remind me that there is a great deal more going on, of which neither I nor any other science writer is aware. Organizations such as GCHQ and America’s National Security Agency continue to conduct classified research into cryptography, which means that their breakthroughs remain secret and the individuals who make them remain anonymous.

Despite the problems of government secrecy and classified research, I have spent the final chapter of this book speculating about the future of codes and ciphers. Ultimately, this chapter is an attempt to see if we can predict who will win the evolutionary struggle between codemaker and codebreaker. Will codemakers ever design a truly unbreakable code and succeed in their quest for absolute secrecy? Or will codebreakers build a machine that can decipher any message? Bearing in mind that some of the greatest minds work in classified laboratories, and that they receive the bulk of research funds, it is clear that some of the statements in my final chapter may be inaccurate. For example, I state that quantum computers—machines potentially capable of breaking all today’s ciphers—are at a very primitive stage, but it is possible that somebody has already built one. The only people who are in a position to point out my errors are also those who are not at liberty to reveal them.

**1 The Cipher of Mary Queen of Scots**

On the morning of Saturday, October 15, 1586, Queen Mary entered the crowded courtroom at Fotheringhay Castle. Years of imprisonment and the onset of rheumatism had taken their toll, yet she remained dignified, composed and indisputably regal. Assisted by her physician, she made her way past the judges, officials and spectators, and approached the throne that stood halfway along the long, narrow chamber. Mary had assumed that the throne was a gesture of respect toward her, but she was mistaken. The throne symbolized the absent Queen Elizabeth, Mary’s enemy and prosecutor. Mary was gently guided away from the throne and toward the opposite side of the room, to the defendant’s seat, a crimson velvet chair.

Mary Queen of Scots was on trial for treason. She had been accused of plotting to assassinate Queen Elizabeth in order to take the English crown for herself. Sir Francis Walsingham, Elizabeth’s Principal Secretary, had already arrested the other conspirators, extracted confessions, and executed them. Now he planned to prove that Mary was at the heart of the plot, and was therefore equally culpable and equally deserving of death.

Walsingham knew that before he could have Mary executed, he would have to convince Queen Elizabeth of her guilt. Although Elizabeth despised Mary, she had several reasons for being reluctant to see her put to death. First, Mary was a Scottish queen, and many questioned whether an English court had the authority to execute a foreign head of state. Second, executing Mary might establish an awkward precedent—if the state is allowed to kill one queen, then perhaps rebels might have fewer reservations about killing another, namely Elizabeth. Third, Elizabeth and Mary were cousins, and their blood tie made Elizabeth all the more squeamish about ordering her execution. In short, Elizabeth would sanction Mary’s execution only if Walsingham could prove beyond any hint of doubt that she had been part of the assassination plot.



**Figure 1** Mary Queen of Scots.([photo credit 1.1](file:///C%3A%5C%5CUsers%5C%5CJoseph%5C%5CAppData%5C%5CRoaming%5C%5CMozilla%5C%5CFirefox%5C%5CProfiles%5C%5Coyrwwab4.default%5C%5Cepub%5C%5C19%5C%5Cdummy_split_069.html%22%20%5Cl%20%22filepos930085))

The conspirators were a group of young English Catholic noblemen intent on removing Elizabeth, a Protestant, and replacing her with Mary, a fellow Catholic. It was apparent to the court that Mary was a figurehead for the conspirators, but it was not clear that she had actually given her blessing to the conspiracy. In fact, Mary had authorized the plot. The challenge for Walsingham was to demonstrate a palpable link between Mary and the plotters.

On the morning of her trial, Mary sat alone in the dock, dressed in sorrowful black velvet. In cases of treason, the accused was forbidden counsel and was not permitted to call witnesses. Mary was not even allowed secretaries to help her prepare her case. However, her plight was not hopeless because she had been careful to ensure that all her correspondence with the conspirators had been written in cipher. The cipher turned her words into a meaningless series of symbols, and Mary believed that even if Walsingham had captured the letters, then he could have no idea of the meaning of the words within them. If their contents were a mystery, then the letters could not be used as evidence against her. However, this all depended on the assumption that her cipher had not been broken.

Unfortunately for Mary, Walsingham was not merely Principal Secretary, he was also England’s spymaster. He had intercepted Mary’s letters to the plotters, and he knew exactly who might be capable of deciphering them. Thomas Phelippes was the nation’s foremost expert on breaking codes, and for years he had been deciphering the messages of those who plotted against Queen Elizabeth, thereby providing the evidence needed to condemn them. If he could decipher the incriminating letters between Mary and the conspirators, then her death would be inevitable. On the other hand, if Mary’s cipher was strong enough to conceal her secrets, then there was a chance that she might survive. Not for the first time, a life hung on the strength of a cipher.

**2 Le Chiffre Indéchiffrable**

For centuries, the simple monoalphabetic substitution cipher had been sufficient to ensure secrecy. The subsequent development of frequency analysis, first in the Arab world and then in Europe, destroyed its security. The tragic execution of Mary Queen of Scots was a dramatic illustration of the weaknesses of monoalphabetic substitution, and in the battle between cryptographers and cryptanalysts it was clear that the cryptanalysts had gained the upper hand. Anybody sending an encrypted message had to accept that an expert enemy codebreaker might intercept and decipher their most precious secrets.

The onus was clearly on the cryptographers to concoct a new, stronger cipher, something that could outwit the cryptanalysts. Although this cipher would not emerge until the end of the sixteenth century, its origins can be traced back to the fifteenth-century Florentine polymath Leon Battista Alberti. Born in 1404, Alberti was one of the leading figures of the Renaissance-a painter, composer, poet and philosopher, as well as the author of the first scientific analysis of perspective, a treatise on the housefly and a funeral oration for his dog. He is probably best known as an architect, having designed Rome’s first Trevi Fountain and having written *De re aedificatoria*, the first printed book on architecture, which acted as a catalyst for the transition from Gothic to Renaissance design.

Sometime in the 1460s, Alberti was wandering through the gardens of the Vatican when he bumped into his friend Leonardo Dato, the pontifical secretary, who began chatting to him about some of the finer points of cryptography. This casual conversation prompted Alberti to write an essay on the subject, outlining what he believed to be a new form of cipher. At the time, all substitution ciphers required a single cipher alphabet for encrypting each message. However, Alberti proposed using two or more cipher alphabets, switching between them during encipherment, thereby confusing potential cryptanalysts.



For example, here we have two possible cipher alphabets, and we could encrypt a message by alternating between them. To encrypt the message hello, we would encrypt the first letter according to the first cipher alphabet, so that h becomes A, but we would encrypt the second letter according to the second cipher alphabet, so that e becomes F. To encrypt the third letter we return to the first cipher alphabet, and to encrypt the fourth letter we return to the second alphabet. This means that the first l is enciphered as P, but the second l is enciphered as A. The final letter, o, is enciphered according to the first cipher alphabet and becomes D. The complete ciphertext reads AFPAD. The crucial advantage of Alberti’s system is that the same letter in the plaintext does not necessarily appear as the same letter in the ciphertext, so the repeated l in hello is enciphered differently in each case. Similarly, the repeated A in the ciphertext represents a different plaintext letter in each case, first h and then l.

Although he had hit upon the most significant breakthrough in encryption for over a thousand years, Alberti failed to develop his concept into a fully formed system of encryption. That task fell to a diverse group of intellectuals, who built on his initial idea. First came Johannes Trithemius, a German abbot born in 1462, then Giovanni Porta, an Italian scientist born in 1535, and finally Blaise de Vigenère, a French diplomat born in 1523. Vigenère became acquainted with the writings of Alberti, Trithemius and Porta when, at the age of twenty-six, he was sent to Rome on a two-year diplomatic mission. To start with, his interest in cryptography was purely practical and was linked to his diplomatic work. Then, at the age of thirty-nine, Vigenère decided that he had accumulated enough money for him to be able to abandon his career and concentrate on a life of study. It was only then that he examined in detail the ideas of Alberti, Trithemius and Porta, weaving them into a coherent and powerful new cipher.



**Figure 11** Blaise de Vigenère. ([photo credit 2.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos930632))

Although Alberti, Trithemius and Porta all made vital contributions, the cipher is known as the Vigenère cipher in honor of the man who developed it into its final form. The strength of the Vigenère cipher lies in its using not one, but 26 distinct cipher alphabets to encrypt a message. The first step in encipherment is to draw up a so-called Vigenère square, as shown in [Table 3](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_015.html#filepos146469), a plaintext alphabet followed by 26 cipher alphabets, each shifted by one letter with respect to the previous alphabet. Hence, row 1 represents a cipher alphabet with a Caesar shift of 1, which means that it could be used to implement a Caesar shift cipher in which every letter of the plaintext is replaced by the letter one place further on in the alphabet. Similarly, row 2 represents a cipher alphabet with a Caesar shift of 2, and so on. The top row of the square, in lower case, represents the plaintext letters. You could encipher each plaintext letter according to any one of the 26 cipher alphabets. For example, if cipher alphabet number 2 is used, then the letter a is enciphered as C, but if cipher alphabet number 12 is used, then a is enciphered as M.

**Table 3** A Vigenère square.



If the sender were to use just one of the cipher alphabets to encipher an entire message, this would effectively be a simple Caesar cipher, which would be a very weak form of encryption, easily deciphered by an enemy interceptor. However, in the Vigenère cipher a different row of the Vigenère square (a different cipher alphabet) is used to encrypt different letters of the message. In other words, the sender might encrypt the first letter according to row 5, the second according to row 14, the third according to row 21, and so on.

To unscramble the message, the intended receiver needs to know which row of the Vigenère square has been used to encipher each letter, so there must be an agreed system of switching between rows. This is achieved by using a keyword. To illustrate how a keyword is used with the Vigenère square to encrypt a short message, let us encipher divert troops to east ridge, using the keyword WHITE. First of all, the keyword is spelled out above the message, and repeated over and over again so that each letter in the message is associated with a letter from the keyword. The ciphertext is then generated as follows. To encrypt the first letter, d, begin by identifying the key letter above it, W, which in turn defines a particular row in the Vigenère square. The row beginning with W, row 22, is the cipher alphabet that will be used to find the substitute letter for the plaintext d. We look to see where the column headed by d intersects the row beginning with W, which turns out to be at the letter Z. Consequently, the letter d in the plaintext is represented by Z in the ciphertext.



To encipher the second letter of the message, i, the process is repeated. The key letter above i is H, so it is encrypted via a different row in the Vigenère square: the H row (row 7) which is a new cipher alphabet. To encrypt i, we look to see where the column headed by i intersects the row beginning with H, which turns out to be at the letter P. Consequently, the letter i in the plaintext is represented by P in the ciphertext. Each letter of the keyword indicates a particular cipher alphabet within the Vigenère square, and because the keyword contains five letters, the sender encrypts the message by cycling through five rows of the Vigenère square. The fifth letter of the message is enciphered according to the fifth letter of the keyword, E, but to encipher the sixth letter of the message we have to return to the first letter of the keyword. A longer keyword, or perhaps a keyphrase, would bring more rows into the encryption process and increase the complexity of the cipher. [Table 4](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_015.html#filepos149836) shows a Vigenère square, highlighting the five rows (i.e., the five cipher alphabets) defined by the keyword WHITE.

**Table 4** A Vigenère square with the rows defined by the keyword WHITE highlighted. Encryption is achieved by switching between the five highlighted cipher alphabets, defined by W, H, I, T and E.



The great advantage of the Vigenère cipher is that it is impregnable to the frequency analysis described in [Chapter 1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_009.html#filepos25656). For example, a cryptanalyst applying frequency analysis to a piece of ciphertext would usually begin by identifying the most common letter in the ciphertext, which in this case is Z, and then assume that this represents the most common letter in English, e. In fact, the letter Z represents three different letters, d, r and s, but not e. This is clearly a problem for the cryptanalyst. The fact that a letter which appears several times in the ciphertext can represent a different plaintext letter on each occasion generates tremendous ambiguity for the cryptanalyst. Equally confusing is the fact that a letter which appears several times in the plaintext can be represented by different letters in the ciphertext. For example, the letter o is repeated in troops, but it is substituted by two different letters—the oo is enciphered as HS.

As well as being invulnerable to frequency analysis, the Vigenère cipher has an enormous number of keys. The sender and receiver can agree on any word in the dictionary, any combination of words, or even fabricate words. A cryptanalyst would be unable to crack the message by searching all possible keys because the number of options is simply too great.

Vigenère’s work culminated in his *Traicté des Chiffres* (“A Treatise on Secret Writing”), published in 1586. Ironically, this was the same year that Thomas Phelippes was breaking the cipher of Mary Queen of Scots. If only Mary’s secretary had read this treatise, he would have known about the Vigenère cipher, Mary’s messages to Babington would have baffled Phelippes, and her life might have been spared.

Because of its strength and its guarantee of security, it would seem natural that the Vigenère cipher would be rapidly adopted by cipher secretaries around Europe. Surely they would be relieved to have access, once again, to a secure form of encryption? On the contrary, cipher secretaries seem to have spurned the Vigenère cipher. This apparently flawless system would remain largely neglected for the next two centuries.

**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](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_056.html#filepos875608)).

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 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.



**Figure 26** Lieutenant Georges Painvin. ([photo credit 3.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos931081))

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 Uboats 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 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](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_020.html#filepos289013) shows the encrypted telegraph; the actual message is as follows:



**Figure 27** Arthur Zimmermann. ([photo credit 3.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos931202))

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.



**Figure 28** The Zimmermann telegram, as forwarded by von Bernstorff, the German Ambassador in Washington, to Eckhardt, the German Ambassador in Mexico City. ([photo credit 3.2](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos931313))

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



**Figure 29** “Exploding in his Hands,” a cartoon by Rollin Kirby published on March 3, 1917, in *The World*.([photo credit 3.3](file:///C%3A%5C%5CUsers%5C%5CJoseph%5C%5CAppData%5C%5CRoaming%5C%5CMozilla%5C%5CFirefox%5C%5CProfiles%5C%5Coyrwwab4.default%5C%5Cepub%5C%5C19%5C%5Cdummy_split_069.html%22%20%5Cl%20%22filepos931434))

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.

**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 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.



**Figure 41** Hans-Thilo Schmidt. ([photo credit 4.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos931979))

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:



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):



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:





**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:



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:



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](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_023.html#filepos396928). 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 chance to try and build on it. Perhaps Britain and France, with their extra resources, could fully exploit the concept of the bombe.

**Table 10** Possible arrangements with five scramblers.





**Figure 43** General Heinz Guderian’s command post vehicle. An Enigma machine can be seen in use in the bottom left. ([photo credit 4.2](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos932100))

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.

**5 The Language Barrier**

While British codebreakers were breaking the German Enigma cipher and altering the course of the war in Europe, American codebreakers were having an equally important influence on events in the Pacific arena by cracking the Japanese machine cipher known as Purple. For example, in June 1942 the Americans deciphered a message outlining a Japanese plan to draw U.S. Naval forces to the Aleutian Islands by faking an attack, which would allow the Japanese Navy to take their real objective, Midway Island. Although American ships played along with the plan by leaving Midway, they never strayed far away. When American cryptanalysts intercepted and deciphered the Japanese order to attack Midway, the ships were able to return swiftly and defend the island in one of the most important battles of the entire Pacific war. According to Admiral Chester Nimitz, the American victory at Midway “was essentially a victory of intelligence. In attempting surprise, the Japanese were themselves surprised.”

Almost a year later, American cryptanalysts identified a message that showed the itinerary for a visit to the northern Solomon Islands by Admiral Isoruko Yamamoto, Commander-in-Chief of the Japanese Fleet. Nimitz decided to send fighter aircraft to intercept Yamamoto’s plane and shoot him down. Yamamoto, renowned for being compulsively punctual, approached his destination at exactly 8:00 A.M., just as stated in the intercepted schedule. There to meet him were eighteen American P-38 fighters. They succeeded in killing one of the most influential figures of the Japanese High Command.

Although Purple and Enigma, the Japanese and German ciphers, were eventually broken, they did offer some security when they were initially implemented and provided real challenges for American and British cryptanalysts. In fact, had the cipher machines been used properly—without repeated message keys, without cillies, without restrictions on plugboard settings and scrambler arrangements, and without stereotypical messages which resulted in cribs—it is quite possible that they might never have been broken at all.

The true strength and potential of machine ciphers was demonstrated by the Typex (or Type X) cipher machine used by the British army and air force, and the SIGABA (or M-143-C) cipher machine used by the American military. Both these machines were more complex than the Enigma machine and both were used properly, and therefore they remained unbroken throughout the war. Allied cryptographers were confident that complicated electromechanical machine ciphers could guarantee secure communication. However, complicated machine ciphers are not the only way of sending secure messages. Indeed, one of the most secure forms of encryption used in the Second World War was also one of the simplest.

During the Pacific campaign, American commanders began to realize that cipher machines, such as SIGABA, had a fundamental drawback. Although electromechanical encryption offered relatively high levels of security, it was painfully slow. Messages had to be typed into the machine letter by letter, the output had to be noted down letter by letter, and then the completed ciphertext had to be transmitted by the radio operator. The radio operator who received the enciphered message then had to pass it on to a cipher expert, who would carefully select the correct key, and type the ciphertext into a cipher machine, to decipher it letter by letter. The time and space required for this delicate operation is available at headquarters or onboard a ship, but machine encryption was not ideally suited to more hostile and intense environments, such as the islands of the Pacific. One war correspondent described the difficulties of communication during the heat of jungle battle: “When the fighting became confined to a small area, everything had to move on a split-second schedule. There was not time for enciphering and deciphering. At such times, the King’s English became a last resort—the profaner the better.” Unfortunately for the Americans, many Japanese soldiers had attended American colleges and were fluent in English, including the profanities. Valuable information about American strategy and tactics was falling into the hands of the enemy.

One of the first to react to this problem was Philip Johnston, an engineer based in Los Angeles, who was too old to fight but still wanted to contribute to the war effort. At the beginning of 1942 he began to formulate an encryption system inspired by his childhood experiences. The son of a Protestant missionary, Johnston had grown up on the Navajo reservations of Arizona, and as a result he had become fully immersed in Navajo culture. He was one of the few people outside the tribe who could speak their language fluently, which allowed him to act as an interpreter for discussions between the Navajo and government agents. His work in this capacity culminated in a visit to the White House, when, as a nine-year-old, Johnston translated for two Navajos who were appealing to President Theodore Roosevelt for fairer treatment for their community. Fully aware of how impenetrable the language was for those outside the tribe, Johnston was struck by the notion that Navajo, or any other Native American language, could act as a virtually unbreakable code. If each battalion in the Pacific employed a pair of Native Americans as radio operators, secure communication could be guaranteed.

He took his idea to Lieutenant Colonel James E. Jones, the area signal officer at Camp Elliott, just outside San Diego. Merely by throwing a few Navajo phrases at the bewildered officer, Johnston was able to persuade him that the idea was worthy of serious consideration. A fortnight later he returned with two Navajos, ready to conduct a test demonstration in front of senior marine officers. The Navajos were isolated from each other, and one was given six typical messages in English, which he translated into Navajo and transmitted to his colleague via a radio. The Navajo receiver translated the messages back into English, wrote them down, and handed them over to the officers, who compared them with the originals. The game of Navajo whispers proved to be flawless, and the marine officers authorized a pilot project and ordered recruitment to begin immediately.

Before recruiting anybody, however, Lieutenant Colonel Jones and Philip Johnston had to decide whether to conduct the pilot study with the Navajo, or select another tribe. Johnston had used Navajo men for his original demonstration because he had personal connections with the tribe, but this did not necessarily make them the ideal choice. The most important selection criterion was simply a question of numbers: the marines needed to find a tribe capable of supplying a large number of men who were fluent in English and literate. The lack of government investment meant that the literacy rate was very low on most of the reservations, and attention was therefore focused on the four largest tribes: the Navajo, the Sioux, the Chippewa and the Pima-Papago.

The Navajo was the largest tribe, but also the least literate, while the Pima-Papago was the most literate but much fewer in number. There was little to choose between the four tribes, and ultimately the decision rested on another critical factor. According to the official report on Johnston’s idea:

The Navajo is the only tribe in the United States that has not been infested with German students during the past twenty years. These Germans, studying the various tribal dialects under the guise of art students, anthropologists, etc., have undoubtedly attained a good working knowledge of all tribal dialects except Navajo. For this reason the Navajo is the only tribe available offering complete security for the type of work under consideration. It should also be noted that the Navajo tribal dialect is completely unintelligible to all other tribes and all other people, with the possible exception of as many as 28 Americans who have made a study of the dialect. This dialect is equivalent to a secret code to the enemy, and admirably suited for rapid, secure communication.

At the time of America’s entry into the Second World War, the Navajo were living in harsh conditions and being treated as inferior people. Yet their tribal council supported the war effort and declared their loyalty: “There exists no purer concentration of Americanism than among the First Americans.” The Navajos were so eager to fight that some of them lied about their age, or gorged themselves on bunches of bananas and swallowed great quantities of water in order to reach the minimum weight requirement of 55 kg. Similarly, there was no difficulty in finding suitable candidates to serve as Navajo code talkers, as they were to become known. Within four months of the bombing of Pearl Harbor, 29 Navajos, some as young as fifteen, began an eight-week communications course with the Marine Corps.

Before training could begin, the Marine Corps had to overcome a problem that had plagued the only other code to have been based on a Native American language. In Northern France during the First World War, Captain E.W. Horner of Company D, 141st Infantry, ordered that eight men from the Choctaw tribe be employed as radio operators. Obviously none of the enemy understood their language, so the Choctaw provided secure communications. However, this encryption system was fundamentally flawed because the Choctaw language had no equivalent for modern military jargon. A specific technical term in a message might therefore have to be translated into a vague Choctaw expression, with the risk that this could be misinterpreted by the receiver.

The same problem would have arisen with the Navajo language, but the Marine Corps planned to construct a lexicon of Navajo terms to replace otherwise untranslatable English words, thus removing any ambiguities. The trainees helped to compile the lexicon, tending to choose words describing the natural world to indicate specific military terms. Thus, the names of birds were used for planes, and fish for ships ([Table 11](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_027.html#filepos482293)). Commanding officers became “war chiefs,” platoons were “mud-clans,” fortifications turned into “cave dwellings” and mortars were known as “guns that squat.”

Even though the complete lexicon contained 274 words, there was still the problem of translating less predictable words and the names of people and places. The solution was to devise an encoded phonetic alphabet for spelling out difficult words. For example, the word “Pacific” would be spelled out as “pig, ant, cat, ice, fox, ice, cat,” which would then be translated into Navajo as bi-sodih, wol-la-chee, moasi, tkin, ma-e, tkin, moasi. The complete Navajo alphabet is given in [Table 12](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_027.html#filepos483607). Within eight weeks, the trainee code talkers had learned the entire lexicon and alphabet, thus obviating the need for codebooks which might fall into enemy hands. For the Navajos, committing everything to memory was trivial because traditionally their language had no written script, so they were used to memorizing their folk stories and family histories. As William McCabe, one of the trainees, said, “In Navajo everything is in the memory—songs, prayers, everything. That’s the way we were raised.”

**Table 11** Navajo codewords for planes and ships.



At the end of their training, the Navajos were put to the test. Senders translated a series of messages from English into Navajo, transmitted them, and then receivers translated the messages back into English, using the memorized lexicon and alphabet when necessary. The results were word-perfect. To check the strength of the system, a recording of the transmissions was given to Navy Intelligence, the unit that had cracked Purple, the toughest Japanese cipher. After three weeks of intense cryptanalysis, the Naval codebreakers were still baffled by the messages. They called the Navajo language a “weird succession of guttural, nasal, tongue-twisting sounds … we couldn’t even transcribe it, much less crack it.” The Navajo code was judged a success. Two Navajo soldiers, John Benally and Johnny Manuelito, were asked to stay and train the next batch of recruits, while the other 27 Navajo code talkers were assigned to four regiments and sent to the Pacific.

**Table 12** The Navajo alphabet code.



Japanese forces had attacked Pearl Harbor on December 7, 1941, and not long after they dominated large parts of the western Pacific. Japanese troops overran the American garrison on Guam on December 10, they took Guadalcanal, one of the islands in the Solomon chain, on December 13, Hong Kong capitulated on December 25, and U.S. troops on the Philippines surrendered on January 2, 1942. The Japanese planned to consolidate their control of the Pacific the following summer by building an airfield on Guadalcanal, creating a base for bombers which would enable them to destroy Allied supply lines, thus making any Allied counterattack almost impossible. Admiral Ernest King, Chief of American Naval Operations, urged an attack on the island before the airfield was completed, and on August 7, the 1st Marine Division spearheaded an invasion of Guadalcanal. The initial landing parties included the first group of code talkers to see action.

Although the Navajos were confident that their skills would be a blessing to the marines, their first attempts generated only confusion. Many of the regular signal operators were unaware of this new code, and they sent panic messages all over the island, stating that the Japanese were broadcasting on American frequencies. The colonel in charge immediately halted Navajo communications until he could convince himself that the system was worth pursuing. One of the code talkers recalled how the Navajo code was eventually brought back into service:



**Figure 52** The first 29 Navajo code talkers pose for a traditional graduation photograph. ([photo credit 5.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos932700))

The colonel had an idea. He said he would keep us on one condition: that I could outrace his “white code”—a mechanical ticking cylinder thing. We both sent messages, by white cylinder and by my voice. Both of us received answers and the race was to see who could decode his answer first. I was asked, “How long will it take you? Two hours?” “More like two minutes,” I answered. The other guy was still decoding when I got the roger on my return message in about four and a half minutes. I said, “Colonel, when are you going to give up on that cylinder thing?” He didn’t say anything. He just lit up his pipe and walked away.

The code talkers soon proved their worth on the battlefield. During one episode on the island of Saipan, a battalion of marines took over positions previously held by Japanese soldiers, who had retreated. Suddenly a salvo exploded nearby. They were under friendly fire from fellow Americans who were unaware of their advance. The marines radioed back in English explaining their position, but the salvos continued because the attacking American troops suspected that the messages were from Japanese impersonators trying to fool them. It was only when a Navajo message was sent that the attackers saw their mistake and halted the assault. A Navajo message could never be faked, and could always be trusted.

The reputation of the code talkers soon spread, and by the end of 1942 there was a request for 83 more men. The Navajo were to serve in all six Marine Corps divisions, and were sometimes borrowed by other American forces. Their war of words soon turned the Navajos into heroes. Other soldiers would offer to carry their radios and rifles, and they were even given personal bodyguards, partly to protect them from their own comrades. On at least three occasions code talkers were mistaken for Japanese soldiers and captured by fellow Americans. They were released only when colleagues from their own battalion vouched for them.

The impenetrability of the Navajo code was all down to the fact that Navajo belongs to the Na-Dene family of languages, which has no link with any Asian or European language. For example, a Navajo verb is conjugated not solely according to its subject, but also according to its object. The verb ending depends on which category the object belongs to: long (e.g., pipe, pencil), slender and flexible (e.g., snake, thong), granular (e.g., sugar, salt), bundled (e.g., hay), viscous (e.g., mud, feces) and many others. The verb will also incorporate adverbs, and will reflect whether or not the speaker has experienced what he or she is talking about, or whether it is hearsay. Consequently, a single verb can be equivalent to a whole sentence, making it virtually impossible for foreigners to disentangle its meaning.

Despite its strengths, the Navajo code still suffered from two significant flaws. First, words that were neither in the natural Navajo vocabulary nor in the list of 274 authorized codewords had to be spelled out using the special alphabet. This was time-consuming, so it was decided to add another 234 common terms to the lexicon. For example, nations were given Navajo nicknames: “Rolled Hat” for Australia, “Bounded by Water” for Britain, “Braided Hair” for China, “Iron Hat” for Germany, “Floating Land” for the Philippines, and “Sheep Pain” for Spain.

The second problem concerned those words that would still have to be spelled out. If it became clear to the Japanese that words were being spelled out, they would realize that they could use frequency analysis to identify which Navajo words represented which letters. It would soon become obvious that the most commonly used word was dzeh, which means “elk” and which represents e, the most commonly used letter of the English alphabet. Just spelling out the name of the island Guadalcanal and repeating the word wol-la-chee (ant) four times would be a big clue as to what word represented the letter a. The solution was to add more words to act as extra substitutes (homophones) for the commonly used letters. Two extra words were introduced as alternatives for each of the six commonest letters (e, t, a, o, i, n), and one extra word for the six next commonest letters (s, h, r, d, l, u). The letter a, for example, could now also be substituted by the words be-la-sana (apple) or tse-nihl (axe). Thereafter, Guadalcanal could be spelled with only one repetition: klizzie, shi-da, wol-la-chee, lha-cha-eh, be-la-sana, dibeh-yazzie, moasi, tse-nihl, nesh-chee, tse-nihl, ah-jad (goat, uncle, ant, dog, apple, lamb, cat, axe, nut, axe, leg).

As the war in the Pacific intensified, and as the Americans advanced from the Solomon Islands to Okinawa, the Navajo code talkers played an increasingly vital role. During the first days of the attack on Iwo Jima, more than eight hundred Navajo messages were sent, all without error. According to Major General Howard Conner, “without the Navajos, the marines would never have taken Iwo Jima.” The contribution of the Navajo code talkers is all the more remarkable when you consider that, in order to fulfill their duties, they often had to confront and defy their own deeply held spiritual fears. The Navajo believe that the spirits of the dead, *chindi*, will seek revenge on the living unless ceremonial rites are performed on the body. The war in the Pacific was particularly bloody, with corpses strewn across the battlefields, and yet the code talkers summoned up the courage to carry on regardless of the *chindi* that haunted them. In Doris Paul’s book *The Navajo Code Talkers*, one of the Navajo recounts an incident which typifies their bravery, dedication and composure:



**Figure 53** Corporal Henry Bake, Jr. (left) and Private First Class George H. Kirk using the Navajo code in the dense jungles of Bougainville in 1943.

If you so much as held up your head six inches you were gone, the fire was so intense. And then in the wee hours, with no relief on our side or theirs, there was a dead standstill. It must have gotten so that this one Japanese couldn’t take it anymore. He got up and yelled and screamed at the top of his voice and dashed over our trench, swinging a long samurai sword. I imagine he was shot from 25 to 40 times before he fell.

There was a buddy with me in the trench. But that Japanese had cut him across the throat, clear through to the cords on the back of his neck. He was still gasping through his windpipe. And the sound of him trying to breathe was horrible. He died, of course. When the Jap struck, warm blood spattered all over my hand that was holding a microphone. I was calling in code for help. They tell me that in spite of what happened, every syllable of my message came through.

Altogether, there were 420 Navajo code talkers. Although their bravery as fighting men was acknowledged, their special role in securing communications was classified information. The government forbade them to talk about their work, and their unique contribution was not made public. Just like Turing and the cryptanalysts at Bletchley Park, the Navajo were ignored for decades. Eventually, in 1968, the Navajo code was declassified, and the following year the code talkers held their first reunion. Then, in 1982, they were honored when the U.S. Government named August 14 “National Navajo Code Talkers Day.” However, the greatest tribute to the work of the Navajo is the simple fact that their code is one of very few throughout history that was never broken. Lieutenant General Seizo Arisue, the Japanese chief of intelligence, admitted that, although they had broken the American Air Force code, they had failed to make any impact on the Navajo code.

**6 Alice and Bob Go Public**

During the Second World War, British codebreakers had the upper hand over German codemakers, mainly because the men and women at Bletchley Park, following the lead of the Poles, developed some of the earliest codebreaking technology. In addition to Turing’s bombes, which were used to crack the Enigma cipher, the British also invented another codebreaking device, Colossus, to combat an even stronger form of encryption, namely the German Lorenz cipher. Of the two types of codebreaking machine, it was Colossus that would determine the development of cryptography during the latter half of the twentieth century.

The Lorenz cipher was used to encrypt communications between Hitler and his generals. The encryption was performed by the Lorenz SZ40 machine, which operated in a similar way to the Enigma machine, but the Lorenz was far more complicated, and it provided the Bletchley codebreakers with an even greater challenge. However, two of Bletchley’s codebreakers, John Tiltman and Bill Tutte, discovered a weakness in the way that the Lorenz cipher was used, a flaw that Bletchley could exploit and thereby read Hitler’s messages.

Breaking the Lorenz cipher required a mixture of searching, matching, statistical analysis and careful judgment, all of which was beyond the technical abilities of the bombes. The bombes were able to carry out a specific task at high speed, but they were not flexible enough to deal with the subtleties of Lorenz. Lorenz-encrypted messages had to be broken by hand, which took weeks of painstaking effort, by which time the messages were largely out of date. Eventually, Max Newman, a Bletchley mathematician, came up with a way to mechanize the cryptanalysis of the Lorenz cipher. Drawing heavily on Alan Turing’s concept of the universal machine, Newman designed a machine that was capable of adapting itself to different problems, what we today would call a programmable computer.

Implementing Newman’s design was deemed technically impossible, so Bletchley’s senior officials shelved the project. Fortunately, Tommy Flowers, an engineer who had taken part in discussions about Newman’s design, decided to ignore Bletchley’s skepticism, and went ahead with building the machine. At the Post Office’s research center at Dollis Hill, North London, Flowers took Newman’s blueprint and spent ten months turning it into the Colossus machine, which he delivered to Bletchley Park on December 8, 1943. It consisted of 1,500 electronic valves, which were considerably faster than the sluggish electromechanical relay switches used in the bombes. But more important than Colossus’s speed was the fact that it was programmable. It was this fact that made Colossus the precursor to the modern digital computer.

Colossus, as with everything else at Bletchley Park, was destroyed after the war, and those who worked on it were forbidden to talk about it. When Tommy Flowers was ordered to dispose of the Colossus blueprints, he obediently took them down to the boiler room and burned them. The plans for the world’s first computer were lost forever. This secrecy meant that other scientists gained the credit for the invention of the computer. In 1945, J. Presper Eckert and John W. Mauchly of the University of Pennsylvania completed ENIAC (Electronic Numerical Integrator And Calculator), consisting of 18,000 electronic valves, capable of performing 5,000 calculations per second. For decades, ENIAC, not Colossus, was considered the mother of all computers.

Having contributed to the birth of the modern computer, cryptanalysts continued after the war to develop and employ computer technology in order to break all sorts of ciphers. They could now exploit the speed and flexibility of programmable computers to search through all possible keys until the correct one was found. In due course, the cryptographers began to fight back, exploiting the power of computers to create increasingly complex ciphers. In short, the computer played a crucial role in the postwar battle between codemakers and codebreakers.

Using a computer to encipher a message is, to a large extent, very similar to traditional forms of encryption. Indeed, there are only three significant differences between computer encryption and the sort of mechanical encryption that was the basis for ciphers like Enigma. The first difference is that a mechanical cipher machine is limited by what can be practically built, whereas a computer can mimic a hypothetical cipher machine of immense complexity. For example, a computer could be programmed to mimic the action of a hundred scramblers, some spinning clockwise, some anticlockwise, some vanishing after every tenth letter, others rotating faster and faster as encryption progresses. Such a mechanical machine would be practically impossible to build, but its “virtual” computerized equivalent would deliver a highly secure cipher.

The second difference is simply a matter of speed. Electronics can operate far more quickly than mechanical scramblers: a computer programmed to mimic the Enigma cipher could encipher a lengthy message in an instant. Alternatively, a computer programmed to perform a vastly more complex form of encryption could still accomplish the task within a reasonable time.

The third, and perhaps most significant, difference is that a computer scrambles numbers rather than letters of the alphabet. Computers deal only in binary numbers-sequences of ones and zeros known as *binary digits*, or *bits* for short. Before encryption, any message must therefore be converted into binary digits. This conversion can be performed according to various protocols, such as the American Standard Code for Information Interchange, known familiarly by the acronym ASCII, pronounced “asskey.” ASCII assigns a 7-digit binary number to each letter of the alphabet. For the time being, it is sufficient to think of a binary number as merely a pattern of ones and zeros that uniquely identifies each letter ([Table 24](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_032.html#filepos592755)), just as Morse code identifies each letter with a unique series of dots and dashes. There are 128 (27) ways to arrange a combination of 7 binary digits, so ASCII can identify up to 128 distinct characters. This allows plenty of room to define all the lowercase letters (e.g., a = 1100001), all necessary punctuation (e.g., ! = 0100001), as well as other symbols (e.g., & = 0100110). Once the message has been converted into binary, encryption can begin.

Even though we are dealing with computers and numbers, and not machines and letters, the encryption still proceeds by the age-old principles of substitution and transposition, in which elements of the message are substituted for other elements, or their positions are switched, or both. Every encipherment, no matter how complex, can be broken down into combinations of these simple operations. The following two examples demonstrate the essential simplicity of computer encipherment by showing how a computer might perform an elementary substitution cipher and an elementary transposition cipher.

First, imagine that we wish to encrypt the message HELLO, employing a simple computer version of a transposition cipher. Before encryption can begin, we must translate the message into ASCII according to [Table 24](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_032.html#filepos592755):



One of the simplest forms of transposition cipher would be to swap the first and second digits, the third and fourth digits, and so on. In this case the final digit would remain unchanged because there are an odd number of digits. In order to see the operation more clearly, I have removed the spaces between the ASCII blocks in the original plaintext to generate a single string, and then lined it up against the resulting ciphertext for comparison:



An interesting aspect of transposition at the level of binary digits is that the transposing can happen within the letter. Furthermore, bits of one letter can swap places with bits of the neighboring letter. For example, by swapping the seventh and eighth numbers, the final 0 of H is swapped with the initial 1 of E. The encrypted message is a single string of 35 binary digits, which can be transmitted to the receiver, who then reverses the transposition to re-create the original string of binary digits. Finally, the receiver reinterprets the binary digits via ASCII to regenerate the message HELLO.

**Table 24** ASCII binary numbers for the capital letters.



Next, imagine that we wish to encrypt the same message, HELLO, this time employing a simple computer version of a substitution cipher. Once again, we begin by converting the message into ASCII before encryption. As usual, substitution relies on a key that has been agreed between sender and receiver. In this case the key is the word DAVID translated into ASCII, and it is used in the following way. Each element of the plaintext is “added” to the corresponding element of the key. Adding binary digits can be thought of in terms of two simple rules. If the elements in the plaintext and the key are the same, the element in the plaintext is substituted for 0 in the ciphertext. But, if the elements in the message and key are different, the element in the plaintext is substituted for 1 in the ciphertext:



The resulting encrypted message is a single string of 35 binary digits which can be transmitted to the receiver, who uses the same key to reverse the substitution, thus recreating the original string of binary digits. Finally, the receiver reinterprets the binary digits via ASCII to regenerate the message HELLO.

Computer encryption was restricted to those who had computers, which in the early days meant the government and the military. However, a series of scientific, technological and engineering breakthroughs made computers, and computer encryption, far more widely available. In 1947, AT&T Bell Laboratories invented the transistor, a cheap alternative to the electronic valve. Commercial computing became a reality in 1951 when companies such as Ferranti began to make computers to order. In 1953 IBM launched its first computer, and four years later it introduced Fortran, a programming language that allowed “ordinary” people to write computer programs. Then, in 1959, the invention of the integrated circuit heralded a new era of computing.

During the 1960s, computers became more powerful, and at the same time they became cheaper. Businesses were increasingly able to afford computers, and could use them to encrypt important communications such as money transfers or delicate trade negotiations. However, as more and more businesses bought computers, and as encryption between businesses spread, cryptographers were confronted with new problems, difficulties that had not existed when cryptography was the preserve of governments and the military. One of the primary concerns was the issue of standardization. A company might use a particular encryption system to ensure secure internal communication, but it could not send a secret message to an outside organization unless the receiver used the same system of encryption. Eventually, on May 15, 1973, America’s National Bureau of Standards planned to solve the problem, and formally requested proposals for a standard encryption system that would allow business to speak secretly unto business.

One of the more established cipher algorithms, and a candidate for the standard, was an IBM product known as Lucifer. It had been developed by Horst Feistel, a German émigré who had arrived in America in 1934. He was on the verge of becoming a U.S. citizen when America entered the war, which meant that he was placed under house arrest until 1944. For some years after, he suppressed his interest in cryptography to avoid arousing the suspicions of the American authorities. When he did eventually begin research into ciphers, at the Air Force’s Cambridge Research Center, he soon found himself in trouble with the National Security Agency (NSA), the organization with overall responsibility for maintaining the security of military and governmental communications, and which also attempts to intercept and decipher foreign communications. The NSA employs more mathematicians, buys more computer hardware, and intercepts more messages than any other organization in the world. It is the world leader when it comes to snooping.

The NSA did not object to Feistel’s past, they merely wanted to have a monopoly on cryptographic research, and it seems that they arranged for Feistel’s research project to be canceled. In the 1960s Feistel moved to the Mitre Corporation, but the NSA continued to apply pressure and forced him to abandon his work for a second time. Feistel eventually ended up at IBM’s Thomas J. Watson Laboratory near New York, where for several years he was able to conduct his research without being harassed. It was there, during the early 1970s, that he developed the Lucifer system.

Lucifer encrypts messages according to the following scrambling operation. First, the message is translated into a long string of binary digits. Second, the string is split into blocks of 64 digits, and encryption is performed separately on each of the blocks. Third, focusing on just one block, the 64 digits are shuffled, and then split into two half-blocks of 32, labeled Left0 and Right0. The digits in Right0 are then put through a “mangler function,” which changes the digits according to a complex substitution. The mangled Right0 is then added to Left0 to create a new halfblock of 32 digits called Right1. The original Right0 is relabeled Left1. This set of operations is called a “round.” The whole process is repeated in a second round, but starting with the new half-blocks, Left1 and Right1, and ending with Left2 and Right2. This process is repeated until there have been 16 rounds in total. The encryption process is a bit like kneading a slab of dough. Imagine a long slab of dough with a message written on it. First, the long slab is divided into blocks that are 64 cm in length. Then, one half of one of the blocks is picked up, mangled, folded over, added to the other half and stretched to make a new block. Then the process is repeated over and over again until the message has been thoroughly mixed up. After 16 rounds of kneading the ciphertext is sent, and is then deciphered at the other end by reversing the process.

The exact details of the mangler function can change, and are determined by a key agreed by sender and receiver. In other words, the same message can be encrypted in a myriad of different ways depending on which key is chosen. The keys used in computer cryptography are simply numbers. Hence, the sender and receiver merely have to agree on a number in order to decide the key. Thereafter, encryption requires the sender to input the key number and the message into Lucifer, which then outputs the ciphertext. Decryption requires the receiver to input the same key number and the ciphertext into Lucifer, which then outputs the original message.

Lucifer was generally held to be one of the strongest commercially available encryption products, and consequently it was used by a variety of organizations. It seemed inevitable that this encryption system would be adopted as the American standard, but once again the NSA interfered with Feistel’s work. Lucifer was so strong that it offered the possibility of an encryption standard that was probably beyond the codebreaking capabilities of the NSA; not surprisingly, the NSA did not want to see an encryption standard that they could not break. Hence, it is rumored that the NSA lobbied to weaken one aspect of Lucifer, the number of possible keys, before allowing it to be adopted as the standard.

The number of possible keys is one of the crucial factors determining the strength of any cipher. A cryptanalyst trying to decipher an encrypted message could attempt to check all possible keys, and the greater the number of possible keys, the longer it will take to find the right one. If there are only 1,000,000 possible keys, a cryptanalyst could use a powerful computer to find the correct one in a matter of minutes, and thereby decipher an intercepted message. However, if the number of possible keys is large enough, finding the correct key becomes impractical. If Lucifer were to become the encryption standard, then the NSA wanted to ensure that it operated with only a restricted number of keys.

The NSA argued in favor of limiting the number of keys to roughly 100,000,000,000,000,000 (technically referred to as 56 bits, because this number consists of 56 digits when written in binary). It seems that the NSA believed that such a key would provide security within the civilian community, because no civilian organization had a computer powerful enough to check every possible key within a reasonable amount of time. However, the NSA itself, with access to the world’s greatest computing resource, would just about be able to break into messages. The 56-bit version of Feistel’s Lucifer cipher was officially adopted on November 23, 1976, and was called the Data Encryption Standard (DES). A quarter of a century later, DES remains America’s official standard for encryption.

The adoption of DES solved the problem of standardization, encouraging businesses to use cryptography for security. Furthermore, DES was strong enough to guarantee security against attacks from commercial rivals. It was effectively impossible for a company with a civilian computer to break into a DES-encrypted message because the number of possible keys was sufficiently large. Unfortunately, despite standardization and despite the strength of DES, businesses still had to deal with one more major issue, a problem known as *key distribution*.

Imagine that a bank wants to send some confidential data to a client via a telephone line, but is worried that there might be somebody tapping the wire. The bank picks a key and uses DES to encrypt the data message. In order to decrypt the message, the client needs not only to have a copy of DES on its computer, but also to know which key was used to encrypt the message. How does the bank inform the client of the key? It cannot send the key via the telephone line, because it suspects that there is an eavesdropper on the line. The only truly secure way to send the key is to hand it over in person, which is clearly a time-consuming task. A less secure but more practical solution is to send the key via a courier. In the 1970s, banks attempted to distribute keys by employing special dispatch riders who had been vetted and who were among the company’s most trusted employees. These dispatch riders would race across the world with padlocked briefcases, personally distributing keys to everyone who would receive messages from the bank over the next week. As business networks grew in size, as more messages were sent, and as more keys had to be delivered, the banks found that this distribution process became a horrendous logistical nightmare, and the overhead costs became prohibitive.

The problem of key distribution has plagued cryptographers throughout history. For example, during the Second World War the German High Command had to distribute the monthly book of day keys to all its Enigma operators, which was an enormous logistical problem. Also, Uboats, which tended to spend extended periods away from base, had to somehow obtain a regular supply of keys. In earlier times, users of the Vigenère cipher had to find a way of getting the keyword from the sender to the receiver. No matter how secure a cipher is in theory, in practice it can be undermined by the problem of key distribution.

To some extent, government and the military have been able to deal with the problem of key distribution by throwing money and resources at it. Their messages are so important that they will go to any lengths to ensure secure key distribution. The U.S. Government keys are managed and distributed by CO MS EC, short for Communications Security. In the 1970s, COMSEC was responsible for transporting tons of keys every day. When ships carrying COMSEC material came into dock, crypto-custodians would march onboard, collect stacks of cards, paper tapes, floppy disks, or whatever other medium the keys might be stored on, and then deliver them to the intended recipients.

Key distribution might seem a mundane issue, but it became the overriding problem for postwar cryptographers. If two parties wanted to communicate securely, they had to rely on a third party to deliver the key, and this became the weakest link in the chain of security. The dilemma for businesses was straightforward-if governments with all their money were struggling to guarantee the secure distribution of keys, then how could civilian companies ever hope to achieve reliable key distribution without bankrupting themselves?

Despite claims that the problem of key distribution was unsolvable, a team of mavericks triumphed against the odds and came up with a brilliant solution in the mid-1970s. They devised an encryption system that appeared to defy all logic. Although computers transformed the implementation of ciphers, the greatest revolution in twentieth-century cryptography has been the development of techniques to overcome the problem of key distribution. Indeed, this breakthrough is considered to be the greatest cryptographic achievement since the invention of the monoalphabetic cipher, over two thousand years ago.

**7 Pretty Good Privacy**

Just as Whit Diffie predicted in the early 1970s, we are now entering the Information Age, a postindustrial era in which information is the most valuable commodity. The exchange of digital information has become an integral part of our society. Already, tens of millions of e-mails are sent each day, and electronic mail will soon become more popular than conventional mail. The Internet, still in its infancy, has provided the infrastructure for the digital marketplace, and e-commerce is thriving. Money is flowing through cyberspace, and it is estimated that every day half the world’s Gross Domestic Product travels through the Society for Worldwide Interbank Financial Telecommunications network. In the future, democracies that favor referenda will begin to have on-line voting, and governments will use the Internet to help administer their countries, offering facilities such as on-line tax declarations.

However, the success of the Information Age depends on the ability to protect information as it flows around the world, and this relies on the power of cryptography. Encryption can be seen as providing the locks and keys of the Information Age. For two thousand years encryption has been of importance only to governments and the military, but today it also has a role to play in facilitating business, and tomorrow ordinary people will rely on cryptography in order to protect their privacy. Fortunately, just as the Information Age is taking off, we have access to extraordinarily strong encryption. The development of public key cryptography, particularly the RSA cipher, has given today’s cryptographers a clear advantage in their continual power struggle against cryptanalysts. If the value of *N* is large enough, then finding *p* and *q* takes Eve an unreasonable amount of time, and RSA encryption is therefore effectively unbreakable. Most important of all, public key cryptography is not weakened by any key distribution problems. In short, RSA guarantees almost unbreakable locks for our most precious pieces of information.



**Figure 70** Phil Zimmermann. ([photo credit 7.1](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_069.html#filepos934272))

However, as with every technology, there is a dark side to encryption. As well as protecting the communications of law-abiding citizens, encryption also protects the communications of criminals and terrorists. Currently, the police use wiretapping as a way of gathering evidence in serious cases, such as organized crime and terrorism, but this would be impossible if criminals used unbreakable ciphers. As we enter the twenty-first century, the fundamental dilemma for cryptography is to find a way of allowing the public and business to use encryption in order to exploit the benefits of the Information Age without allowing criminals to abuse encryption and evade arrest. There is currently an active and vigorous debate about the best way forward, and much of the discussion has been inspired by the story of Phil Zimmermann, a man whose attempts to encourage the widespread use of strong encryption have panicked America’s security experts, threatened the effectiveness of the billion-dollar National Security Agency, and made him the subject of an FBI inquiry and a grand jury investigation.

Phil Zimmermann spent the mid-1970s at Florida Atlantic University, where he studied physics and then computer science. On graduation he seemed set for a steady career in the rapidly growing computer industry, but the political events of the early 1980s transformed his life, and he became less interested in the technology of silicon chips and more worried about the threat of nuclear war. He was alarmed by the Soviet invasion of Afghanistan, the election of Ronald Reagan, the instability caused by an aging Brezhnev and the increasingly tense nature of the Cold War. He even considered taking himself and his family to New Zealand, believing that this would be one of the few places on Earth that would be habitable after a nuclear conflict. But just as he had obtained passports and the necessary immigration papers, he and his wife attended a meeting held by the Nuclear Weapons Freeze Campaign. Rather than flee, the Zimmermanns decided to stay and fight the battle at home, becoming front-line antinuclear activists-they educated political candidates on issues of military policy, and were arrested at the Nevada nuclear testing grounds, alongside Carl Sagan and four hundred other protesters.

A few years later, in 1988, Mikhail Gorbachev became head of state of the Soviet Union, heralding perestroika, glasnost and a reduction in tension between East and West. Zimmermann’s fears began to subside, but he did not lose his passion for political activism, he merely channeled it in a different direction. He began to focus his attentions on the digital revolution and the necessity for encryption:

Cryptography used to be an obscure science, of little relevance to everyday life. Historically, it always had a special role in military and diplomatic communications. But in the Information Age, cryptography is about political power, and in particular, about the power relationship between a government and its people. It is about the right to privacy, freedom of speech, freedom of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone.

These views might seem paranoid, but according to Zimmermann there is a fundamental difference between traditional and digital communication which has important implications for security:

In the past, if the government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, or listen to and possibly transcribe spoken telephone conversations. This is analogous to catching fish with a hook and a line, one fish at a time. Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale. Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm for everyone, not the novelty it is today. Unlike paper mail, e-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing-making a quantitative and qualitative Orwellian difference to the health of democracy.

The difference between ordinary and digital mail can be illustrated by imagining that Alice wants to send out invitations to her birthday party, and that Eve, who has not been invited, wants to know the time and place of the party. If Alice uses the traditional method of posting letters, then it is very difficult for Eve to intercept one of the invitations. To start with, Eve does not know where Alice’s invitations entered the postal system, because Alice could use any postbox in the city. Her only hope for intercepting one of the invitations is to somehow identify the address of one of Alice’s friends, and infiltrate the local sorting office. She then has to check each and every letter manually. If she does manage to find a letter from Alice, she will have to steam it open in order to get the information she wants, and then return it to its original condition to avoid any suspicion of tampering.

In comparison, Eve’s task is made considerably easier if Alice sends her invitations by e-mail. As the messages leave Alice’s computer, they will go to a local server, a main entry point for the Internet; if Eve is clever enough, she can hack into that local server without leaving her home. The invitations will carry Alice’s e-mail address, and it would be a trivial matter to set up an electronic sieve that looks for e-mails containing Alice’s address. Once an invitation has been found, there is no envelope to open, and so no problem in reading it. Furthermore, the invitation can be sent on its way without it showing any sign of having been intercepted. Alice would be oblivious to what was going on. However, there is a way to prevent Eve from reading Alice’s e-mails, namely encryption.

More than a hundred million e-mails are sent around the world each day, and they are all vulnerable to interception. Digital technology has aided communication, but it has also given rise to the possibility of those communications being monitored. According to Zimmermann, cryptographers have a duty to encourage the use of encryption and thereby protect the privacy of the individual:

A future government could inherit a technology infrastructure that’s optimized for surveillance, where they can watch the movements of their political opposition, every financial transaction, every communication, every bit of e-mail, every phone call. Everything could be filtered and scanned and automatically recognized by voice recognition technology and transcribed. It’s time for cryptography to step out of the shadows of spies and the military, and step into the sunshine and be embraced by the rest of us.

In theory, when RSA was invented in 1977 it offered an antidote to the Big Brother scenario because individuals were able to create their own public and private keys, and thereafter send and receive perfectly secure messages. However, in practice there was a major problem because the actual process of RSA encryption required a substantial amount of computing power in comparison with symmetric forms of encryption, such as DES. Consequently, in the 1980s it was only government, the military and large businesses that owned computers powerful enough to run RSA. Not surprisingly, RSA Data Security, Inc., the company set up to commercialize RSA, developed their encryption products with only these markets in mind.

In contrast, Zimmermann believed that everybody deserved the right to the privacy that was offered by RSA encryption, and he directed his political zeal toward developing an RSA encryption product for the masses. He intended to draw upon his background in computer science to design a product with economy and efficiency in mind, thus not overloading the capacity of an ordinary personal computer. He also wanted his version of RSA to have a particularly friendly interface, so that the user did not have to be an expert in cryptography to operate it. He called his project Pretty Good Privacy, or PGP for short. The name was inspired by Ralph’s Pretty Good Groceries, a sponsor of Garrison Keillor’s *Prairie Home Companion*, one of Zimmermann’s favorite radio shows.

During the late 1980s, working from his home in Boulder, Colorado, Zimmermann gradually pieced together his scrambling software package. His main goal was to speed up RSA encryption. Ordinarily, if Alice wants to use RSA to encrypt a message to Bob, she looks up his public key and then applies RSA’s one-way function to the message. Conversely, Bob decrypts the ciphertext by using his private key to reverse RSA’s one-way function. Both processes require considerable mathematical manipulation, so encryption and decryption can, if the message is long, take several minutes on a personal computer. If Alice is sending a hundred messages a day, she cannot afford to spend several minutes encrypting each one. To speed up encryption and decryption, Zimmermann employed a neat trick that used asymmetric RSA encryption in tandem with old-fashioned symmetric encryption. Traditional symmetric encryption can be just as secure as asymmetric encryption, and it is much quicker to perform, but symmetric encryption suffers from the problem of having to distribute the key, which has to be securely transported from the sender to the receiver. This is where RSA comes to the rescue, because RSA can be used to encrypt the symmetric key.

Zimmermann pictured the following scenario. If Alice wants to send an encrypted message to Bob, she begins by encrypting it with a symmetric cipher. Zimmermann suggested using a cipher known as IDEA, which is similar to DES. To encrypt with IDEA, Alice needs to choose a key, but for Bob to decrypt the message Alice somehow has to get the key to Bob. Alice overcomes this problem by looking up Bob’s RSA public key, and then uses it to encrypt the IDEA key. So, Alice ends up sending two things to Bob: the message encrypted with the symmetric IDEA cipher and the IDEA key encrypted with the asymmetric RSA cipher. At the other end, Bob uses his RSA private key to decrypt the IDEA key, and then uses the IDEA key to decrypt the message. This might seem convoluted, but the advantage is that the message, which might contain a large amount of information, is being encrypted with a quick symmetric cipher, and only the symmetric IDEA key, which consists of a relatively small amount of information, is being encrypted with a slow asymmetric cipher. Zimmermann planned to have this combination of RSA and IDEA within the PGP product, but the user-friendly interface would mean that the user would not have to get involved in the nuts and bolts of what was going on.

Having largely solved the speed problem, Zimmermann also incorporated a series of handy features into PGP. For example, before using the RSA component of PGP, Alice needs to generate her own private key and public key. Key generation is not trivial, because it requires finding a pair of giant primes. However, Alice only has to wiggle her mouse in an erratic manner, and the PGP program will go ahead and create her private key and public key-the mouse movements introduce a random factor which PGP utilizes to ensure that every user has their own distinct pair of primes, and therefore their own unique private key and public key. Thereafter Alice merely has to publicize her public key.

Another helpful aspect of PGP is its facility for digitally signing an email. Ordinarily e-mail does not carry a signature, which means that it is impossible to verify the true author of an electronic message. For example, if Alice uses e-mail to send a love letter to Bob, she normally encrypts it with his public key, and when he receives it he decrypts it with his private key. Bob is initially flattered, but how can he be sure that the love letter is really from Alice? Perhaps the malevolent Eve wrote the e-mail and typed Alice’s name at the bottom. Without the reassurance of a handwritten ink signature, there is no obvious way to verify the authorship. Alternatively, imagine that a bank receives an e-mail from a client, which instructs that all the client’s funds should be transferred to a private numbered bank account in the Cayman Islands. Once again, without a handwritten signature, how does the bank know that the e-mail is really from the client? The e-mail could have been written by a criminal attempting to divert the money to his own Cayman Islands bank account. In order to develop trust on the Internet, it is essential that there is some form of reliable digital signature.

The PGP digital signature is based on a principle that was first developed by Whitfield Diffie and Martin Hellman. When they proposed the idea of separate public keys and private keys, they realized that, in addition to solving the key distribution problem, their invention would also provide a natural mechanism for generating e-mail signatures. In [Chapter 6](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_032.html#filepos582977) we saw that the public key is for encrypting and the private key for decrypting. In fact the process can be swapped around, so that the private key is used for encrypting and the public key is used for decrypting. This mode of encryption is usually ignored because it offers no security. If Alice uses her private key to encrypt a message to Bob, then everybody can decrypt it because everybody has Alice’s public key. However, this mode of operation does verify authorship, because if Bob can decrypt a message using Alice’s public key, then it must have been encrypted using her private key-only Alice has access to her private key, so the message must have been sent by Alice.

In effect, if Alice wants to send a love letter to Bob, she has two options. Either she encrypts the message with Bob’s public key to guarantee privacy, or she encrypts it with her own private key to guarantee authorship. However, if she combines both options she can guarantee privacy and authorship. There are quicker ways to achieve this, but here is one way in which Alice might send her love letter. She starts by encrypting the message using her private key, then she encrypts the resulting ciphertext using Bob’s public key. We can picture the message surrounded by a fragile inner shell, which represents encryption by Alice’s private key, and a strong outer shell, which represents encryption by Bob’s public key. The resulting ciphertext can only be deciphered by Bob, because only he has access to the private key necessary to crack the strong outer shell. Having deciphered the outer shell, Bob can then easily decipher the inner shell using Alice’s public key-the inner shell is not meant to protect the message, but it does prove that the message came from Alice, and not an impostor.

By this stage, sending a PGP encrypted message is becoming quite complicated. The IDEA cipher is being used to encrypt the message, RSA is being used to encrypt the IDEA key, and another stage of encryption has to be incorporated if a digital signature is required. However, Zimmermann developed his product in such a way that it would do everything automatically, so that Alice and Bob would not have to worry about the mathematics. To send a message to Bob, Alice would simply write her e-mail and select the PGP option from a menu on her computer screen. Next she would type in Bob’s name, then PGP would find Bob’s public key and automatically perform all the encryption. At the same time PGP would do the necessary jiggery-pokery required to digitally sign the message. Upon receiving the encrypted message, Bob would select the PGP option, and PGP would decrypt the message and verify the author. Nothing in PGP was original-Diffie and Hellman had already thought of digital signatures and other cryptographers had used a combination of symmetric and asymmetric ciphers to speed up encryption-but Zimmermann was the first to put everything together in one easy-to-use encryption product, which was efficient enough to run on a moderately sized personal computer.

By the summer of 1991, Zimmermann was well on the way to turning PGP into a polished product. Only two problems remained, neither of them technical. A long-term problem had been the fact that RSA, which is at the heart of PGP, is a patented product, and patent law required Zimmermann to obtain a license from RSA Data Security, Inc. before he launched PGP. However, Zimmermann decided to put this problem to one side. PGP was intended not as a product for businesses, but rather as something for the individual. He felt that he would not be competing directly with RSA Data Security, Inc., and hoped that the company would give him a free license in due course.

A more serious and immediate problem was the U.S. Senate’s 1991 omnibus anticrime bill, which contained the following clause: “It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.” The Senate was concerned that developments in digital technology, such as cellular telephones, might prevent law enforcers from performing effective wiretaps. However, as well as forcing companies to guarantee the possibility of wiretapping, the bill also seemed to threaten all forms of secure encryption.

A concerted effort by RSA Data Security, Inc., the communications industry, and civil liberty groups forced the clause to be dropped, but the consensus was that this was only a temporary reprieve. Zimmermann was fearful that sooner or later the government would again try to bring in legislation that would effectively outlaw encryption such as PGP. He had always intended to sell PGP, but now he reconsidered his options. Rather than waiting and risk PGP being banned by the government, he decided that it was more important for it to be available to everybody before it was too late. In June 1991 he took the drastic step of asking a friend to post PGP on a Usenet bulletin board. PGP is just a piece of software, and so from the bulletin board it could be downloaded by anyone for free. PGP was now loose on the Internet.

Initially, PGP caused a buzz only among aficionados of cryptography. Later it was downloaded by a wider range of Internet enthusiasts. Next, computer magazines ran brief reports and then full-page articles on the PGP phenomenon. Gradually PGP began to permeate the most remote corners of the digital community. For example, human rights groups around the world started to use PGP to encrypt their documents, in order to prevent the information from falling into the hands of the regimes that were being accused of human-rights abuses. Zimmermann began to receive e-mails praising him for his creation. “There are resistance groups in Burma,” says Zimmermann, “who are using it in jungle training camps. They’ve said that it’s helped morale there, because before PGP was introduced captured documents would lead to the arrest, torture and execution of entire families.” In 1991, on the day that Boris Yeltsin was shelling Moscow’s Parliament building, Zimmerman received this e-mail via someone in Latvia: “Phil, I wish you to know: let it never be, but if dictatorship takes over Russia, your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks.”

While Zimmermann was gaining fans around the world, back home in America he had been the target of criticism. RSA Data Security, Inc. decided not to give Zimmermann a free license, and was enraged that its patent was being infringed. Although Zimmermann released PGP as freeware (free software), it contained the RSA system of public key cryptography, and consequently RSA Data Security, Inc. labeled PGP as “banditware.” Zimmermann had given something away which belonged to somebody else. The patent wrangle would continue for several years, during which time Zimmermann encountered an even greater problem.

In February 1993, two government investigators paid Zimmermann a visit. After their initial enquiries about patent infringement, they began to ask questions about the more serious accusation of illegally exporting a weapon. Because the U.S. Government included encryption software within its definition of munitions, along with missiles, mortars and machine guns, PGP could not be exported without a license from the State Department. In other words, Zimmermann was accused of being an arms dealer because he had exported PGP via the Internet. Over the next three years Zimmermann became the subject of a grand jury investigation and found himself pursued by the FBI.

**8 A Quantum Leap into the Future**

For two thousand years, codemakers have fought to preserve secrets while codebreakers have tried their best to reveal them. It has always been a neck-and-neck race, with codebreakers battling back when codemakers seemed to be in command, and codemakers inventing new and stronger forms of encryption when previous methods had been compromised. The invention of public key cryptography and the political debate that surrounds the use of strong cryptography bring us up to the present day, and it is clear that the cryptographers are winning the information war. According to Phil Zimmermann, we live in a golden age of cryptography: “It is now possible to make ciphers in modern cryptography that are really, really out of reach of all known forms of cryptanalysis. And I think it’s going to stay that way.” Zimmermann’s view is supported by William Crowell, Deputy Director of the NSA: “If all the personal computers in the world-approximately 260 million computers-were to be put to work on a single PGP encrypted message, it would take on average an estimated 12 million times the age of the universe to break a single message.”

Previous experience, however, tells us that every so-called unbreakable cipher has, sooner or later, succumbed to cryptanalysis. The Vigenère cipher was called “le chiffre indéchiffrable,” but Babbage broke it; Enigma was considered invulnerable, until the Poles revealed its weaknesses. So, are cryptanalysts on the verge of another breakthrough, or is Zimmermann right? Predicting future developments in any technology is always a precarious task, but with ciphers it is particularly risky. Not only do we have to guess which discoveries lie in the future, but we also have to guess which discoveries lie in the present. The tale of James Ellis and GCHQ warns us that there may already be remarkable breakthroughs hidden behind the veil of government secrecy.

This final chapter examines a few of the futuristic ideas that may enhance or destroy privacy in the twenty-first century. The next section looks at the future of cryptanalysis, and one idea in particular that might enable cryptanalysts to break all today’s ciphers. In contrast, the final section of the book looks at the most exciting cryptographic prospect, a system that has the potential to guarantee absolute privacy.

**The Cipher Challenge**

The Cipher Challenge is a set of ten encrypted messages, which I placed at the end of *The Code Book* when it was first published in 1999. In addition to the intellectual reward of cracking all ten messages, there was a prize of $15,000 for the first person to solve the Challenge. The Challenge was eventually solved on October 7, 2000, after one year and one month of arduous effort by codebreakers, amateur and professional, around the world.

The Cipher Challenge remains as part of this book. There is no longer a prize associated with its solution, but I would encourage readers to decipher some of the messages. The ten stages were intended to grow in difficulty, although many codebreakers have felt that stage 3 is harder than stage 4. The ciphers used in the stages differ and progress through the ages, so the early ciphers are ancient and easy to break, whereas the latter stages employ modern ciphers and require a great deal more effort. In short, stages 1 to 4 are for the amateur, stages 5 to 8 are for the real enthusiast, and 9 and 10 are for those who are dedicated codebreakers.

If you want to know more about the Cipher Challenge, you can visit my own Web site ([www.simonsingh.com](http://www.simonsingh.com)), which offers a variety of information, including a link to a report written by the Cipher Challenge winners, Fredrik Almgren, Gunnar Andersson, Torbjorn Granlund, Lars Ivansson and Staffan Ulfberg. The report makes excellent reading, but please be aware that it, and other material on the Web site, does include spoilers that you might not want to see just yet.

The main aim of the Cipher Challenge was to excite people, to get them interested in cryptography and codebreaking. The fact that thousands of people took up the challenge is tremendously satisfying. Officially the Cipher Challenge is now over, but I hope that it will continue to generate some interest among new readers who want to test their codebreaking skills.

Good luck,
Simon Singh

# Appendices

**Glossary**

**ASCII** American Standard Code for Information Interchange, a standard for turning alphabetic and other characters into numbers.

**asymmetric key cryptography** A form of cryptography in which the key required for encrypting is not the same as the key required for decrypting. Describes public key cryptography systems, such as RSA.

**Caesar-shift substitution cipher** Originally a cipher in which each letter in the message is replaced with the letter three places further on in the alphabet. More generally, it is a cipher in which each letter in the message is replaced with the letter *x* places further on in the alphabet, where *x* is a number between 1 and 25.

**cipher** Any general system for hiding the meaning of a message by replacing each letter in the original message with another letter. The system should have some built-in flexibility, known as the key.

**cipher alphabet** The rearrangement of the ordinary (or plain) alphabet, which then determines how each letter in the original message is enciphered. The cipher alphabet can also consist of numbers or any other characters, but in all cases it dictates the replacements for letters in the original message.

**ciphertext** The message (or plaintext) after encipherment.

**code** A system for hiding the meaning of a message by replacing each word or phrase in the original message with another character or set of characters. The list of replacements is contained in a codebook. (An alternative definition of a code is any form of encryption which has no built-in flexibility, i.e., there is only one key, namely the codebook.)

**codebook** A list of replacements for words or phrases in the original message.

**cryptanalysis** The science of deducing the plaintext from a ciphertext, without knowledge of the key.

**cryptography** The science of encrypting a message, or the science of concealing the meaning of a message. Sometimes the term is used more generally to mean the science of anything connected with ciphers, and is an alternative to the term cryptology.

**cryptology** The science of secret writing in all its forms, covering both cryptography and cryptanalysis.

**decipher** To turn an enciphered message back into the original message. Formally, the term refers only to the intended receiver who knows the key required to obtain the plaintext, but informally it also refers to the process of cryptanalysis, in which the decipherment is performed by an enemy interceptor.

**decode** To turn an encoded message back into the original message.

**decrypt** To decipher or to decode.

**DES** Data Encryption Standard, developed by IBM and adopted in 1976.

**Diffie-Hellman-Merkle key exchange** A process by which a sender and receiver can establish a secret key via public discussion. Once the key has been agreed, the sender can use a cipher such as DES to encrypt a message.

**digital signature** A method for proving the authorship of an electronic document. Often this is generated by the author encrypting the document with his or her private key.

**encipher** To turn the original message into the enciphered message.

**encode** To turn the original message into the encoded message.

**encrypt** To encipher or encode.

**encryption algorithm** Any general encryption process which can be specified exactly by choosing a key.

**homophonic substitution cipher** A cipher in which there are several potential substitutions for each plaintext letter. Crucially, if there are, say, six potential substitutions for the plaintext letter a, then these six characters can only represent the letter a. This is a type of monoalphabetic substitution cipher.

**key** The element that turns the general encryption algorithm into a specific method for encryption. In general, the enemy may be aware of the encryption algorithm being used by the sender and receiver, but the enemy must not be allowed to know the key.

**key distribution** The process of ensuring that both sender and receiver have access to the key required to encrypt and decrypt a message, while making sure that the key does not fall into enemy hands. Key distribution was a major problem in terms of logistics and security before the invention of public key cryptography.

**key escrow** A scheme in which users lodge copies of their secret keys with a trusted third party, the escrow agent, who will pass on keys to law enforcers only under certain circumstances, for example if a court order is issued.

**key length** Computer encryption involves keys which are numbers. The key length refers to the number of digits or bits in the key, and thus indicates the biggest number that can be used as a key, thereby defining the number of possible keys. The longer the key length (or the greater the number of possible keys), the longer it will take a cryptanalyst to test all the keys.

**monoalphabetic substitution cipher** A substitution cipher in which the cipher alphabet is fixed throughout encryption.

**National Security Agency (NSA)** A branch of the U.S. Department of Defense, responsible for ensuring the security of American communications and for breaking into the communications of other countries.

**onetime pad** The only known form of encryption that is unbreakable. It relies on a random key that is the same length as the message. Each key can be used once and only once.

**plaintext** The original message before encryption.

**polyalphabetic substitution cipher** A substitution cipher in which the cipher alphabet changes during the encryption, for example the Vigenère cipher. The change is defined by a key.

**Pretty Good Privacy (PGP)** A computer encryption algorithm developed by Phil Zimmermann, based on RSA.

**private key** The key used by the receiver to decrypt messages in a system of public key cryptography. The private key must be kept secret.

**public key** The key used by the sender to encrypt messages in a system of public key cryptography. The public key is available to the public.

**public key cryptography** A system of cryptography which overcomes the problems of key distribution. Public key cryptography requires an asymmetric cipher, so that each user can create a public encryption key and a private decryption key.

**quantum computer** An immensely powerful computer that exploits quantum theory, in particular the theory that an object can be in many states at once (superposition), or the theory that an object can be in many universes at once. If scientists could build a quantum computer on any reasonable scale, it would jeopardize the security of all current ciphers except the onetime pad cipher.

**quantum cryptography** An unbreakable form of cryptography that exploits quantum theory, in particular the uncertainty principle-which states that it is impossible to measure all aspects of an object with absolute certainty. Quantum cryptography guarantees the secure exchange of a random series of bits, which is then used as the basis for a onetime pad cipher.

**RSA** The first system that fitted the requirements of public key cryptography, invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977.

**steganography** The science of hiding the existence of a message, as opposed to cryptography, which is the science of hiding the meaning of a message.

**substitution cipher** A system of encryption in which each letter of a message is replaced with another character, but retains its position within the message.

**symmetric key cryptography** A form of cryptography in which the key required for encrypting is the same as the key required for decrypting. The term describes all traditional forms of encryption, i.e. those in use before the 1970s.

**transposition cipher** A system of encryption in which each letter of a message changes its position within the message, but retains its identity.

**Vigenère cipher** A polyalphabetic cipher which was developed around 1500. The Vigenère square contains 26 separate cipher alphabets, each one a Caesar-shifted alphabet, and a keyword defines which cipher alphabet should be used to encrypt each letter of a message.

**Acknowledgments**

While writing this book I have had the privilege of meeting some of the world’s greatest living codemakers and codebreakers, ranging from those who worked at Bletchley Park to those who are developing the ciphers that will enrich the Information Age. I would like to thank Whitfield Diffie and Martin Hellman, who took the time to describe their work to me while I was in sunny California. Similarly, Clifford Cocks, Malcolm Williamson and Richard Walton were enormously helpful during my visit to cloudy Cheltenham. In particular, I am grateful to the Information Security Group at Royal Holloway College, London, who allowed me to attend the M.Sc. course on information security. Professor Fred Piper, Simon Blackburn, Jonathan Tuliani, and Fauzan Mirza all taught me valuable lessons about codes and ciphers.

While I was in Virginia, I was fortunate to be given a guided tour of the Beale treasure trail by Peter Viemeister, an expert on the mystery. Furthermore, the Bedford County Museum and Stephen Cowart of the Beale Cypher and Treasure Association helped me to research the subject. I am also grateful to David Deutsch and Michele Mosca of the Oxford Centre for Quantum Computation, Charles Bennett and his research group at IBM’s Thomas J. Watson Laboratories, Stephen Wiesner, Leonard Adleman, Ronald Rivest, Paul Rothemund, Jim Gillogly, Paul Leyland and Neil Barrett.

Derek Taunt, Alan Stripp and Donald Davies kindly explained to me how Bletchley Park broke Enigma, and I was also helped by the Bletchley Park Trust, whose members regularly give enlightening lectures on a variety of topics. Dr. Mohammed Mrayati and Dr. Ibrahim Kadi have been involved in revealing some of the early breakthroughs in Arab cryptanalysis, and were kind enough to send me relevant documents. The periodical *Cryptologia* also carried articles about Arabian cryptanalysis, as well as many other cryptographic subjects, and I would like to thank Brian Winkel for sending me back issues of the magazines.

I would encourage readers to visit the National Cryptologic Museum near Washington, D.C. and the Cabinet War Rooms in London, and I hope that you will be as fascinated as I was during my visits. Thank you to the curators and librarians of these museums for helping me with my research. When I was pressed for time, James Howard, Bindu Mathur, Pretty Sagoo, Anna Singh and Nick Shearing all helped me to uncover important and interesting articles, books and documents, and I am grateful to them for their efforts. Thanks also go to Antony Buonomo at [www.vertigo.co.uk](http://www.vertigo.co.uk) who helped me to establish my Web site.

As well as interviewing experts, I have also depended on numerous books and articles. The list of further reading contains some of my sources, but it is neither a complete bibliography nor a definitive reference list. Instead, it merely includes material that may be of interest to the general reader. Of all the books I have come across during my research, I would like to single out one in particular: *The Codebreakers* by David Kahn. This book documents almost every cryptographic episode in history, and as such it is an invaluable resource.

Various libraries, institutions and individuals have provided me with photographs. All the sources are listed in the picture credits, but particular thanks go to Sally McClain, for sending me photographs of the Navajo code talkers; Professor Eva Brann, for discovering the only known photo of Alice Kober; Joan Chadwick, for sending me a photo of John Chadwick; and Brenda Ellis, for allowing me to borrow photos of James Ellis. Thanks also go to Hugh Whitemore, who gave me permission to use a quote from his play *Breaking the Code*, based on Andrew Hodges’ book *Alan Turing-The Enigma*.

On a personal note, I would like to thank friends and family who put up with me over the two years while I was writing this book. Neil Boynton, Dawn Dzedzy, Sonya Holbraad, Tim Johnson, Richard Singh and Andrew Thompson all helped me to keep sane while I was struggling with convoluted cryptographic concepts. In particular, Bernadette Alves supplied me with a rich mixture of moral support and perceptive criticism. Traveling back in time, thanks also go to all the people and institutions that have shaped my career, including Wellington School, Imperial College and the High Energy Physics Group at Cambridge University; Dana Purvis, at the BBC, who gave me my first break in television; and Roger Highfield, at the *Daily Telegraph*, who encouraged me to write my first article.

Finally, I have had the enormous good fortune to work with some of the best people in publishing. Patrick Walsh is an agent with a love of science, a concern for his authors and a boundless enthusiasm. He has put me in touch with the kindest and most capable publishers, most notably Fourth Estate, whose staff endure my constant stream of queries with great spirit. Last, but certainly not least, my editors, Christopher Potter, Leo Hollis and Peternelle van Arsdale, have helped me to steer a clear path through a subject that twists and turns its way across three thousand years. For that I am tremendously grateful.

# Further Reading

The following is a list of books aimed at the general reader. I have avoided giving more detailed technical references, but several of the texts listed contain a detailed bibliography. For example, if you would like to know more about the decipherment of Linear B ([Chapter 5](file:///C%3A%5CUsers%5CJoseph%5CAppData%5CRoaming%5CMozilla%5CFirefox%5CProfiles%5Coyrwwab4.default%5Cepub%5C19%5Cdummy_split_027.html#filepos469476)), then I would recommend The Decipherment of Linear B by John Chadwick. However, if this book is not detailed enough, then please refer to the references it contains.

There is a great deal of interesting material on the Internet relating to codes and ciphers. In addition to the books, I have therefore listed a few of the Web sites that are worth visiting.

#### ****General****

Kahn, David, The Codebreakers (New York: Scribner, 1996).
A 1,200-page history of ciphers. The definitive story of cryptography up until the 1950s.

Newton, David E., Encyclopedia of Cryptology (Santa Barbara, CA: ABC-Clio, 1997).
A useful reference, with clear, concise explanations of most aspects of ancient and modern cryptology.

Smith, Lawrence Dwight, Cryptography (New York: Dover, 1943).
An excellent elementary introduction to cryptography, with more than 150 problems. Dover publishes many books on the subject of codes and ciphers.

Beutelspacher, Albrecht, Cryptology (Washington, D.C.: Mathematical Association of America, 1994).
An excellent overview of the subject, from the Caesar cipher to public key cryptography, concentrating on the mathematics rather than the history. It is also the cryptography book with the best subtitle: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding, Described Without any Arcane Skullduggery but not Without Cunning Waggery for the Delectation and Instruction of the General Public.

#### ****Chapter 1****

Gaines, Helen Fouché, Cryptanalysis (New York: Dover, 1956).
A study of ciphers and their solution. An excellent introduction to cryptanalysis, with many useful frequency tables in the appendix.

Al-Kadi, Ibraham A., “The origins of cryptology: The Arab contributions,”
Cryptologia, vol. 16, no. 2 (April 1992), pp. 97–126.
A discussion of recently discovered Arab manuscripts, and the work of al-Kindī.

Fraser, Lady Antonia, Mary Queen of Scots (London: Random House, 1989).
A highly readable account of the life of Mary Queen of Scots.

Smith, Alan Gordon, The Babington Plot (London: Macmillan, 1936).
Written in two parts, this book examines the plot from the points of view of both Babington and Walsingham.

Steuart, A. Francis (ed.), Trial of Mary Queen of Scots (London: William Hodge, 1951).
Part of the Notable British Trials series.

#### Chapter 2

Standage, Tom, The Victorian Internet (London: Weidenfeld & Nicolson, 1998). The remarkable story of the development of the electric telegraph.

Franksen, Ole Immanuel, Mr Babbage’s Secret (London: Prentice-Hall, 1985). Contains a discussion of Babbage’s work on breaking the Vigenère cipher.

Franksen, Ole Immanuel, “Babbage and cryptography. Or, the mystery of Admiral Beaufort’s cipher,” Mathematics and Computer Simulation, vol. 35, 1993, pp. 327–67.
A detailed paper on Babbage’s cryptological work, and his relationship with Rear Admiral Sir Francis Beaufort.

Rosenheim, Shawn, The Cryptographic Imagination (Baltimore, MD: Johns Hopkins University Press, 1997).
An academic assessment of the cryptographic writings of Edgar Allan Poe and their influence on literature and cryptography.

Poe, Edgar Allan, The Complete Tales and Poems of Edgar Allan Poe (London: Penguin, 1982).
Includes “The Gold Bug.”

Viemeister, Peter, The Beale Treasure: History of a Mystery (Bedford, VA: Hamilton’s, 1997).
An in-depth account of the Beale ciphers written by a respected local historian. It includes the entire text of the Beale pamphlet, and is most easily obtained directly from the publishers; Hamilton’s, P.O. Box 932, Bedford, VA, 24523, USA.

#### ****Chapter 3****

Tuchman, Barbara W., The Zimmermann Telegram (New York: Ballantine, 1994). A highly readable account of the most influential decipherment in the First World War.

Yardley, Herbert O., The American Black Chamber (Laguna Hills, CA: Aegean Park Press, 1931).
A racy history of cryptography, which was a controversial best-seller when it was first published.

#### ****Chapter 4****

Hinsley, F.H., British Intelligence in the Second World War: Its Influence on Strategy and Operations (London: HMSO, 1975).
The authoritative record of intelligence in the Second World War, including the role of Ultra intelligence.

Hodges, Andrew, Alan Turing: The Enigma (London: Vintage, 1992). The life and work of Alan Turing. One of the best scientific biographies ever written.

Kahn, David, Seizing the Enigma (London: Arrow, 1996).
Kahn’s history of the Battle of the Atlantic and the importance of cryptography. In particular, he dramatically describes the “pinches” from U-boats which helped the codebreakers at Bletchley Park.

Hinsley, F.H., and Stripp, Alan (eds), The Codebreakers: The Inside Story of Bletchley Park (Oxford: Oxford University Press, 1992).
A collection of illuminating essays by the men and women who were part of one of the greatest cryptanalytic achievements in history.

Smith, Michael, Station X (London: Channel 4 Books, 1999).
The book based on the British Channel 4 TV series of the same name, containing anecdotes from those who worked at Bletchley Park, otherwise known as Station X.

Harris, Robert, Enigma (London: Arrow, 1996).
A novel revolving around the codebreakers at Bletchley Park.

#### ****Chapter 5****

Paul, Doris A., The Navajo Code Talkers (Pittsburgh, PA: Dorrance, 1973).
A book devoted to ensuring that the contribution of the Navajo code talkers is not forgotten.

McClain, S., The Navajo Weapon (Boulder, CO: Books Beyond Borders, 1994).
A gripping account that covers the entire story, written by a woman who has spent much time talking to the men who developed and used the Navajo code.

Pope, Maurice, The Story of Decipherment (London: Thames & Hudson, 1975).
A description of various decipherments, from Hittite hieroglyphs to the Ugaritic alphabet, aimed at the layperson.

Davies, W.V., Reading the Past: Egyptian Hieroglyphs (London: British Museum Press, 1997).
Part of an excellent series of introductory texts published by the British Museum. Other authors in the series have written books on cuneiform, Etruscan, Greek inscriptions, Linear B, Maya glyphs, and runes.

Chadwick, John, The Decipherment of Linear B (Cambridge: Cambridge University Press, 1987).
A brilliant description of the decipherment.

#### Chapter 6

Data Encryption Standard, FIPS Pub. 46–1 (Washington, D.C.: National Bureau of Standards, 1987).
The official DES document.

Diffie, Whitfield, and Hellman, Martin, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. IT-22 (November 1976), pp. 644–54.
The classic paper that revealed Diffie and Hellman’s discovery of key exchange, opening the door to public key cryptography.

Gardner, Martin, “A new kind of cipher that would take millions of years to break,” Scientific American, vol. 237 (August 1977), pp. 120–24.
The article which introduced RSA to the world.

Hellman, M.E., “The mathematics of public key cryptography,” Scientific American, vol. 241 (August 1979), pp. 130–39.
An excellent overview of the various forms of public key cryptography. Schneier, Bruce, Applied Cryptography (New York: John Wiley & Sons, 1996)
An excellent survey of modern cryptography. A definitive, comprehensive, and authoritative introduction to the subject.

#### ****Chapter 7****

Zimmermann, Philip R., The Official PGP User’s Guide (Cambridge, MA: MIT Press, 1996).
A friendly overview of PGP, written by the man who developed it.

Garfinkel, Simson, PGP: Pretty Good Privacy (Sebastopol, CA: O’Reilly & Associates, 1995).
An excellent introduction to PGP and the issues surrounding modern cryptography.

Bamford, James, The Puzzle Palace (London: Penguin, 1983).
Inside the National Security Agency, America’s most secret intelligence organization.

Koops, Bert-Jaap, The Crypto Controversy (Boston, MA: Kluwer, 1998).
An excellent survey of the impact of cryptography on privacy, civil liberty, law enforcement and commerce.

Diffie, Whitfield, and Landau, Susan, Privacy on the Line (Cambridge, MA: MIT Press, 1998).
The politics of wiretapping and encryption.

#### Chapter 8

Deutsch, David, The Fabric of Reality (London: Allen Lane, 1997).
Deutsch devotes one chapter to quantum computers, in his attempt to combine quantum physics with the theories of knowledge, computation and evolution.

Bennett, C. H., Brassard, C., and Ekert, A., “Quantum Cryptography,” Scientific American, vol. 269 (October 1992), pp. 26–33.
A clear explanation of the evolution of quantum cryptography.

Deutsch, D., and Ekert, A., “Quantum computation,” Physics World, vol. 11, no. 3 (March 1998), pp. 33–56.
One of four articles in a special issue of Physics World. The other three articles discuss quantum information and quantum cryptography, and are written by leading figures in the subject. The articles are aimed at physics graduates and give an excellent overview of the current state of research.

#### ****Internet Sites****

The Mystery of the Beale Treasure
<http://www.roanokeva.com/stories/beale.html>
A collection of sites relating to the Beale ciphers. The Beale Cypher and Treasure Association is currently in transition, but it hopes to be active soon.

Bletchley Park
<http://www.cranfield.ac.uk/ccc/bpark/>
The official Web site, which includes opening times and directions.

The Alan Turing Homepage
<http://www.turing.org.uk/turing/>

Enigma emulators
<http://www.attlabs.att.co.uk/andyc/enigma/enigma_j.html>
<http://www.izzy.net/~ian/enigma/applet/index.html>
Two excellent emulators that show how the Enigma machine works. The former allows you to alter the machine settings, but it is not possible to track the electrical path through the scramblers. The latter has only one setting, but has a second window that shows the scramblers moving and the subsequent effect on the electrical path.

Phil Zimmermann and PGP
<http://www.nai.com/products/security/phil/phil.asp>

Electronic Frontier Foundation
<http://www.eff.org/>
An organization devoted to protecting rights and promoting freedom on the Internet.

Centre for Quantum Computation
<http://www.qubit.org/>

Information Security Group, Royal Holloway College
<http://isg.rhbnc.ac.uk/>

National Cryptologic Museum
<http://www.nsa.gov:8080/museum/>

American Cryptogram Association (ACA)
<http://www.und.nodak.edu/org/crypto/crypto/>
An association which specializes in setting and solving cipher puzzles. Cryptologia
[http://www.dean.usma.edu/math/
resource/pubs/cryptolo/index.htm](http://www.dean.usma.edu/math/resource/pubs/cryptolo/index.htm)
A quarterly journal devoted to all aspects of cryptology.

Cryptography Frequently Asked Questions
<http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html>

RSA Laboratories’ Frequently Asked Questions About Today’s Cryptography
<http://www.rsa.com/rsalabs/faq/html/questions.html>

Yahoo! Security and Encryption Page
[http://www.yahoo.co.uk/Computers\_and\_Internet/
Security\_and\_Encryption/](http://www.yahoo.co.uk/Computers_and_Internet/Security_and_Encryption/)

Crypto Links
<http://www.ftech.net/~monark/crypto/web.htm>

The End