# 1. SECRET WRITING IN WAR AND PEACE

> I am fairly familiar with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers.
>
> —SIR ARTHUR CONAN DOYLE, "The Dancing Men"

"IF I AM SENTENCED TO DEATH, Ohashi-san, I will come back to haunt you," said the prisoner to the secret police inspector. During the many interrogations a familiar tone had developed between the two men. Inspector Ohashi had been present on that Saturday in October 1941, when in the early morning his men burst into the Tokyo home of the journalist Richard Sorge and took him to the police station in his pajamas and slippers.

Since then the prisoner had had plenty of time to reflect on his life. During the first few weeks in his cell, this defeat, a new experience, drove him to despair. Then an initially feeble but gradually strengthening realization awoke in him that, after all, he had successfully accomplished his mission. This consoling thought made the uncertainty about his fate more bearable. After Hitler's attack on the Soviet Union, Sorge had signaled the Fourth Department in Moscow to the effect that Japan would not attack the Soviet Union from the east. It had been these reports that enabled Marshal Zhukov to withdraw divisions, tanks, and aircraft from Siberia and employ them against the Germans outside Moscow. Had he, Richard Sorge, not made world history? From the questions put by his interrogators he was able to conclude that the Japanese had not succeeded in deciphering the coded messages that his radio operator sent by the thousands to the Soviet stations in Shanghai and Vladivostok.

## RADIO OPERATOR KLAUSEN TRANSMITS TO MOSCOW

On this summer day the air over Tokyo is oppressive. Max Klausen glances at the sheet before him. It will take a while to encode it. He reads it—another report from "Otto." His boss never told him, but Klausen knows that Otto is a Japanese collaborator of the group. His messages are always important.

Since June 22, 1941, German troops have been pushing ever deeper into Soviet territory. Long before then, Klausen sent the warning, complete with the correct date of the German attack, to Moscow, but no one there reacted to it. Will the Soviet Union shortly have to defend itself not only against Germany but also, despite the nonaggression treaty, against Japan? Japan has been mobilizing over the past few days. Will these newly assembled troops be ordered toward the south or toward the north, against the Soviet Union?

The report from Otto holds the answer. On no account will Japan attack Russia; it has its hands full enough with the Chinese incidents. Until it is clear how the negotiations with the Americans develop, no one in Japan wants war with Russia.[1] If Japan attacks the Soviet Union at all, it will be next year at the earliest. But now the German forces have advanced far into Russian territory. It looks as if Hitler intends to be in Moscow before the onset of winter. The news that no attack should be expected from the Japanese must come as a great relief to the Soviets. Max Klausen, the radio operator, starts encoding.

He knows the first step by heart, but this time he uses a sheet of paper that he will afterward destroy. The first step requires the assigning of numbers to the letters of the alphabet. To do that he has to use his code word. It is *SUBWAY.* He writes down the six letters of the word, next to one another, then in four additional lines below he inserts the remaining letters of the alphabet, in their normal order, as well as a period and a slash (to indicate word division). He thus obtains the table in figure 1.1, top.

As he invariably sends his messages in English, the most frequent letters in that language—*a*, *s*, *i*, *n*, *t*, *o*, *e*, and *r*—play a special role. The phrase "A sin to err" consists of just these letters—a mnemonic aid that Klausen does not need. These eight letters will be assigned the numbers

| | | | | | |
|---|---|---|---|---|---|
| s | u | b | w | a | y |
| c | d | e | f | g | h |
| i | j | k | l | m | n |
| o | p | q | r | t | v |
| x | z | . | / | | |

| | | | | | |
|---|---|---|---|---|---|
| s | u | b | w | a | y |
| 0 | | | | 5 | |
| c | d | e | f | g | h |
| | | 3 | | | |
| i | j | k | l | m | n |
| 1 | | | | | 7 |
| o | p | q | r | t | v |
| 2 | | | 4 | 6 | |
| x | z | . | / | | |

| | | | | | |
|---|---|---|---|---|---|
| s | u | b | w | a | y |
| 0 | 82 | 87 | 91 | 5 | 97 |
| c | d | e | f | g | h |
| 80 | 83 | 3 | 92 | 95 | 98 |
| i | j | k | l | m | n |
| 1 | 84 | 88 | 93 | 96 | 7 |
| o | p | q | r | t | v |
| 2 | 85 | 89 | 4 | 6 | 99 |
| x | z | . | / | | |
| 81 | 86 | 90 | 94 | | |

***Fig. 1.1.* How Max Klausen, using the keyword *SUBWAY* and the mnemonic *asintoer*, in three steps sets up the key table for converting the letters of the alphabet into numbers.**

0 to 7. He enters them into this table, column by column, starting from the left. As soon as he encounters a letter from *asintoer*, he writes the numbers from 0 to 7 in sequence underneath. His table now looks like figure 1.1, center. He now writes under the remaining letters, column by column, left to right, the numbers from 80 to 99 and obtains the table in figure 1.1, bottom.

Now every letter of the alphabet has its own number. Klausen can therefore convert the letters of the message into a sequence of numbers. Let us take a simple radio message as an example. The words "no attack" become **729456658088**. This twelve-digit group can easily be reduced to numbers that correspond to pairs of numerals. Numbers not preceded by 8 or 9 correspond individually to letters in the table. If an 8 or 9 is encountered, it stands in conjunction with the number that follows it for a single letter in the table. In **729456658088** the figures 7, 2, 94 and 5 correspond to the letters (and punctuation symbol) *n*, *o*, /, and *a*. The two 6s are the double *t*. The 80 represents *c*, and the 88 the letter *k*. We now have "no attack" in encoded form. But this is only the first step. What Klausen has before him is the *provisionally* encoded text.

So far, nothing much has been gained. Any beginner can discover that in lengthy messages encoded in this manner the number 3 appears most frequently. This represents the letter *e*, the most frequent letter in English as well as in German. This would allow any unauthorized person to take the first step toward decoding the text. That is why Klausen now proceeds to the encipherment proper. From his bookshelf he takes the *Statistical Yearbook of the German Reich* for 1935 and opens it to a page filled with numbers. He notes down the page number, as well as the row and column of the table that contains the number with which he intends to start. These are data on tobacco production in different countries. They start with the number 4230, below it 5166, 7821, 9421, and so on. It has long been agreed between Moscow and himself that he must start with the third and fourth digits of the first number and then append the other figures, hence 30516678219421. . . . This numerical sequence is his real key. Klausen therefore writes down his provisionally encoded text and places his key below it:

**729456658088**

*305166782194*

He now adds, but if a sum exceeds 9, he does not carry the ten to the preceding place—hence not 7 + 8 = 15 but 7 + 8 = 5. Figure 1.2, top, demonstrates his calculation. Now he has to communicate the page number, row, and column of the annual to enable the recipient to take the same key from the book. For the page number two figures are sufficient; if 34 is transmitted, this can mean 34, or 134, or 234, but it will be easy for the recipient to decide which of them is the right page. For the row and column three figures are sufficient; 236 stands for row 23, column 6. Hence a total of five figures, 34236, is sufficient to indicate the beginning of the key. Klausen places these five figures at the beginning of his signal, but he encodes them by adding the first five-figure group of his encoded text, again without carrying; hence 34236 + 02451 = 36687. His message therefore, divided into five-figure groups, reads: 36687 02451 23301 72. He then transmits these groups of figures. He knows that the receiver will start by subtracting the second five-figure group from the first: 36687 - 02451 = 34236. This gives the receiver the page number (34, 134, or 234) and the row and column (23 and 6), that is, all the information he needs to determine the key. He now has to subtract the key from the signal as received (without the first five-figure group he used for discovering the key), as shown in figure 1.2, bottom. This gives him the text encoded with key), as shown in figure 1.2, bottom. This gives him the text encoded with the table in figure 1.1, bottom, and this he can easily convert back into the plaintext, since he, too, has the table.

```
  729456658088
 +305166782194..
 ---------------
  024512330172
 ===============
  024512330172
 -305166782194..
 ---------------
  729456658088
```

*Fig. 1.2.* **Top: from a numerical plaintext—that is, a plaintext converted into figures—via a key into a numerical ciphertext. Bottom: from the numerical ciphertext to the numerical plaintext.**

Max Klausen would transmit each signal from a different location. One time he would transmit from his room, another time from the house of a Yugoslav member of the spy ring, and sometimes he would set up his transmitter and antenna in the homes of other friends. Thus the Japanese secret service did not succeed in locating the transmitter in the middle of the densely populated metropolis, even though it had long been aware of the numerous signals emanating from Tokyo.

To avoid being discovered by direction-finding vehicles, Klausen would change his position even during a single transmission. Continually lugging his transmitter from place to place, he could easily have run into a police checkpoint. Yet it was not the radio signals that eventually betrayed the spy ring. The unmasking took place by chance, when the Japanese secret service began to take a closer look at former sympathizers with the Communist Party of Japan.

In the evening of October 14, 1941, Richard Sorge intended to meet his Japanese collaborator Hotsumi Ozaki—his source, Otto—but Ozaki failed to turn up at the agreed time. Over the next few days Sorge could not reach him by telephone either. Klausen was arrested the night of October 17, and in the early hours of the next day the secret agents knocked at Sorge's door. The trial of Sorge and his comrades dragged on over three years. Ozaki and Sorge were hanged on November 7, 1944, while Klausen was sentenced to life imprisonment and his wife to three years. Following Japan's surrender, both were freed by the Allies and flown to the Soviet Union. For a long time afterward there was no news of them.

Not until October 29, 1964, nearly twenty years later, did the East Berlin newspaper *Neues Deutschland*, under the headline "Max Klausen Alive," report that the Berlin correspondent of the Moscow *Izvestiya* had, with the help of German comrades, tracked down "the Klausen couple living modestly and quietly in the capital of the German Democratic Republic." Now one story followed another. In 1945, after a rest-and-recuperation vacation, the couple had come into the then Soviet zone of occupation and lived there under the name of Christiansen. Later they moved to Berlin. The East Berlin papers described the two as upright Communists and citizens of the German Democratic Republic. Only then did the media discover that Max Klausen had on an earlier occasion attracted attention by his "exemplary constructive determination." From its archives *Neues Deutschland* dug up a nine-year-old story about the activist Maxe Christiansen, cadre instructor at the Köpenick yacht-building yard, shown in a photograph with a pickax, attacking some rubble. At the time the paper was unaware of the identity of the man in the picture.

It was said that simple modesty had kept him silent about his merits. But in 1964 the silence was broken. Klausen gave interviews and told of his work with Sorge in Japan. All of a sudden the Klausens emerged into the limelight. Evidently the news about the activist Maxe Christiansen was released only in 1964 because any historical examination of the work of the spy ring around Sorge would have revealed Stalin's blunders. After all, Stalin had dismissed Sorge's message about Hitler's impending attack on the Soviet Union. By 1964, however, this subject was no longer taboo. Now the longtime Communist Gerhart Eisler, member of the Central Committee of the Socialist Unity Party and chairman of the State Broadcasting Committee of the German Democratic Republic, was allowed to recollect that he had once met Richard Sorge, and the Party veteran Hermann Siebler suddenly remembered his meetings with the until-then-unmentionable Sorge. And Hero of Labor Ehrenfried Navarra of the machine-tool factory in Gera pledged his brigade to a production competition in honor of Sorge's birthday. By the time Max Klausen died on September 15, 1979, at age eighty-one, he had been decorated with the Karl Marx Order, the Order of the Red Banner of the Soviet Union, and other high honors.

The Japanese never managed to decode the signals sent by Sorge and his faithful radio operator. Their encoding system was quite sophisticated and, above all, based on the use of a harmless book. A statistical yearbook would not have attracted any attention during a house search.

## THE SECRET OF THE WAX TABLETS

The method by which the radio operator Max Klausen sent a message to Moscow in a form incomprehensible to the uninitiated must seem a bit primitive to today's encoder, who has a computer encode his letter to a business partner in Australia and then sends it over the Internet. But compared to the beginnings of encoding Klausen's system was not bad at all.

The first secret messages were exchanged as long as thousands of years ago. Legends of them surround many a major event in world history, such as the famous Battle of Thermopylae in 480 B.C.

Anyone driving down European Route 75 from Thessaloniki to Athens will, after leaving Mount Olympus behind him, come to the Gulf of Lamia, where the highway runs close to the coast. A memorial stone on a hill commemorates the battle in which King Leonidas of Sparta vainly tried to defend himself against the superior forces of the Persians. Leonidas had expected the arrival of the Persian army because he was notified of it in a secret message.

As the Greek historian Herodotus reports, a Greek in Persian exile sent wax tablets to his home city; more accurately, he sent wooden tablets with a layer of wax, such as were then used for writing. The man removed the wax, wrote on the wood the message of the imminent Persian invasion, covered the tablet with a fresh layer of wax, and sent it to Leonidas.

The message, no longer legible, reached Greece without mishap. It would have remained hidden if Gogo, Leonidas's wife, had not accidentally discovered the writing underneath the wax. Thus Leonidas was warned.

But, as so often happens in history, the secret message had no effect on the outcome of the battle. A Greek traitor guided the Persians along a secret path over the mountains to Leonidas's position on the pass of Thermopylae, and his forces were attacked from two sides. They fought to the last man.

In the case reported by Herodotus, the secret message was transmitted in such a way that no one could see the wax tablets contained a vital message. Presumably there was an innocent text scratched into the wax covering the real message, designed to distract attention from it.

## THE SECRET MESSAGE TO COUNT SANDORF

Trieste in 1867 was an Austrian town, and to its north the biggest port in the Hapsburg monarchy was about to be created. But the prospects for the realization of that plan were not too favorable in the spring of that year. A few months earlier, Austria had lost the Battle of Königgrätz against Prussia, and the Hungarian freedom movement had never completely quieted down after the death of Lajos Kossuth, the leader of the rebellion crushed by the Austrians.

This tense atmosphere provides the background for Jules Verne's novel *Mathias Sandorf.* The hero, a Hungarian nobleman, is temporarily staying in Trieste. Carrier pigeons bring him encrypted messages about the liberation struggle back home in Hungary. But the message that everything is ready for a rising against Austria, and that his followers are only waiting for a signal from him, falls into the wrong hands. Here is the text:

**SETVIETGGNRIAHYSELRTYFHEOIAUDIRYSNTA**
**RSVELNERMIDTSRURYEISFOFEONSRTREEWOIE**
**RHCUENEENSGDRKAEHAPRGPYEDNNPDSOEHINN**

None of the Austrian agents is able to decode it. Only when a villain steals the key to it from Count Sandorf's writing desk is it possible to decipher it.

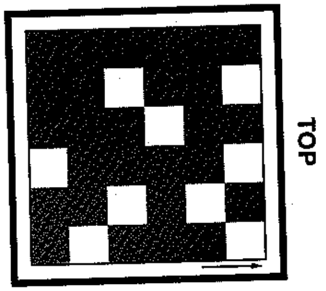
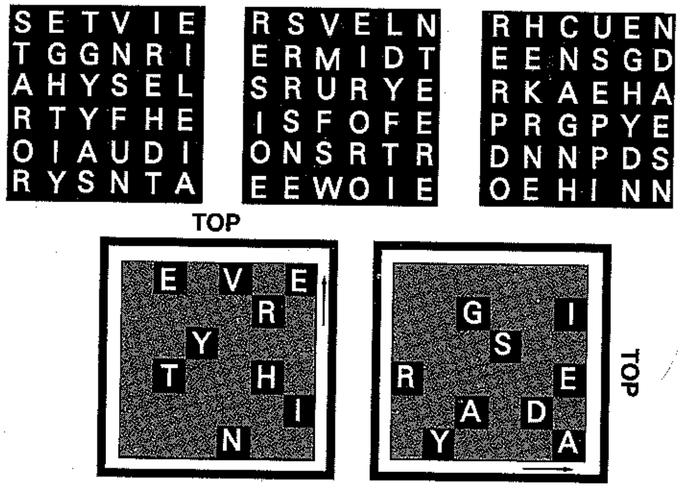


***Fig. 1.3.*** **The cipher template, or "turning grille" or "mask," described by Jules Verne in his novel *Mathias Sandorf.* It is placed on a clean sheet of paper, and the first nine letters of the message to be encrypted are entered into the cut-out fields or "cells" (white in the illustration) of the square. The grille is then rotated clockwise by ninety degrees, and the next nine letters are written into the apertures. This procedure is repeated until the grille has been used in all four positions. On the paper the letters thus entered now fill a square of six by six fields, which, read line by line, produce the encrypted text. If the message is longer, a new square is started with the same grille. Whenever a square is not completely filled, the text to be encrypted is extended by arbitrarily chosen letters to ensure all fields have letters in them.**

The key is a square of six rows and six columns. Of the thirty-six square fields, nine are cut out. The result is a grille as shown in figure 1.3. For deciphering, the recipient writes down the ciphertext in three squares of thirty-six fields each, as shown at the top of figure 1.4. He now places the grille on the square with the ciphertext and reads through the nine apertures: EVERYTHIN (fig. 1.4, bottom left). He then rotates the grille clockwise through ninety degrees (fig. 1.4, bottom right) and reads: GISREADYA. Another ninety degrees: TTHEFIRST. One more turn: SIGNALYOU. This completes the first square. With the other squares, the following plaintext emerges:

everythingisreadyatthefirstsignalyousendusfromtriesteevery
onewillriseforhungarysindependencekhpnohnreesragdp

The end of the message is extended by sixteen random letters in order to make the secret text fit into the three squares.



| | | | | | |
|---|---|---|---|---|---|
| S | E | T | V | I | E |
| T | G | G | N | R | I |
| A | H | Y | S | E | L |
| R | T | Y | F | H | E |
| O | I | A | U | D | I |
| R | Y | S | N | T | A |

| | | | | | |
|---|---|---|---|---|---|
| R | S | V | E | L | N |
| E | R | M | I | D | T |
| S | R | U | R | Y | E |
| I | S | F | O | F | E |
| O | N | S | R | T | R |
| E | E | W | O | I | E |

| | | | | | |
|---|---|---|---|---|---|
| R | H | C | U | E | N |
| E | E | N | S | G | D |
| R | K | A | E | H | A |
| P | R | G | P | Y | E |
| D | N | N | P | D | S |
| O | E | H | I | N | N |

*Fig. 1.4.* **This shows how the encrypted text on page 22 is decoded. The secret text has been written into three squares. Bottom left: the grille of figure 1.3 is placed over the first square in its basic position; bottom right: the grille has been rotated clockwise by ninety degrees. In these two positions the first eighteen letters of the original message are revealed.**

## HOW MARY, QUEEN OF SCOTS, WAS BETRAYED

In 1586, Philip II was king of Spain. He had inherited the empire of his father, Charles V, an empire comprising Spain, Sicily, Lower Italy, all the Hapsburg possessions, and the Spanish colonies scattered throughout the globe. Full of pride, Charles V had been able to exclaim: "In my empire the sun never sets!" When his son Philip was born in 1527, ten years after Luther had nailed his thesis to the door of the castle church of Wittenberg, Protestantism began to establish itself in the countries of Europe. The Zurich parish priest Ulrich Zwingli likewise opposed the papal teaching, and John Calvin followed him in the French part of Switzerland. Calvin's Reformed Church spread to France, the Netherlands, England, and Scotland. Philip II had his half brother Don John of Austria administer the Netherlands, still a Spanish possession. Previously, in the Battle of Lepanto in 1571, John had with the Italians successfully defended Catholicism against the Turks. Now, transferred to the Netherlands, he again saw it as his principal task to protect the Catholic dogma against Protestant heresy.

In England in the thirties, Henry VIII had quarreled with the pope when the pope refused to approve the annulment of his marriage to Catherine, an aunt of Charles V, and his subsequent marriage to a lady of the court. Henry thereupon declared himself head of the Church of England and compelled the clerics to recognize him instead of the pope as the supreme authority. That was the origin of the Anglican Church, which closely associated itself with the teachings of Calvin. The reform was enforced mainly under the reign of Henry's daughter, Elizabeth I. Thus England developed into the principal Protestant power.

In Scotland, too, Calvin's teachings had found followers. In a rebellion the Catholic Stuart queen, Mary, Queen of Scots, had been driven out. She found asylum in the country of her kinswoman Elizabeth, but relations between the two were tense. The English Catholics maintained that Mary was the lawful queen of England, which induced Elizabeth to put her under house arrest for twenty years.

Mary Stuart is said to have been an attractive woman, but that certainly was not the only reason why Don John considered landing his troops in England, marrying Mary, and ruling the country with her instead of Elizabeth. He confided this to others in his letters, naturally in encoded form, but apparently he did not allow for the English secret service.

There were so many intrigues and conspiracies in England during the reign of Elizabeth I that a secret police became necessary to preserve the state. Its creation was organized by Elizabeth's minister, Sir Francis Walsingham. Some years earlier, while traveling in Italy, Walsingham had come to realize the importance of ciphers, which had a long tradition there. He set up an organization that on the European continent alone maintained fifty-three secret agents. The usefulness of this was soon to become evident. A coded letter was channeled into the hands of a nobleman in the Netherlands, who had concerned himself extensively with secret writing, and within a month he succeeded in deciphering it. The letter was from Don John of Austria, and in it was revealed his dream of conquering England. One of Walsingham's men in Holland got wind of the contents of the letter and reported to the minister. Walsingham concluded that it was high time for a closer surveillance of Mary Stuart. It so happened that about the same time a petition from a prisoner, Gilbert Gifford, came into his hands, offering his services. When Gifford had completed his sentence, Walsingham took him up and employed him to observe everything that was going on around Mary Stuart.

He succeeded in infiltrating Gifford into Mary's staff as a messenger.

In 1586, when Mary had been an English prisoner for twenty years, one of her followers conceived the plan to murder Elizabeth and thereby trigger a rebellion of English Catholics, with the aim of crowning Mary queen of England. As instructed, the messenger Gifford smuggled out of the castle all letters from Mary to her followers. But before doing so he always made copies of the encoded messages and passed these on to Walsingham, who now had an experienced cryptologist able to decipher these letters quickly. In one letter to the originator of the murder conspiracy, Mary allegedly wished success to the enterprise. The decoding of this sentence sealed her fate. First Walsingham's agents seized the men who had planned the murder. Then the queen of Scots was accused of high treason. It has never been determined whether the agents who found numerous encoded letters in her rooms when they arrested her did not perhaps also plant some forged documents there. On February 8, 1586, she was taken to the scaffold. The executioner had to strike three times before severing her head from her body.

## THE RIDDLE OF THE MAN IN THE IRON MASK

The mask probably was made not of iron but of velvet, and the truth of the story has never been proven. The story is as follows. In the 1670s the inhabitants of the town of Pignerol in the duchy of Savoy noticed a prisoner who was often to be seen on the ramparts of the fortress that served as a prison. His face was covered by a black mask. The soldiers of the guard reported that the prisoner was courteously treated and even dined at the table of the fortress commandant. Supposedly the man once threw a silver tablet from the wall, with various symbols scratched into it. A citizen of the town who had happened to walk past and pick up the tablet was immediately arrested by the guards. He is said to have sat in a cold cell for weeks before he succeeded in convincing his interrogators that he could neither read nor write and that he was not involved in any conspiracy to free the prisoner. Eventually the man in the mask was taken to the Bastille in Paris, where he died in 1703, after thirty years of imprisonment.

The mysterious prisoner excited the imagination of his contemporaries and subsequent generations. Alexandre Dumas, the author of *The Three Musketeers* and *The Count of Monte Cristo,* wrote a novel about the man in the iron mask. Rumors flew about the country. Had the man in the mask been the twin brother of Louis XIV? Had he been his illegitimate son?

In 1891, a French officer named Victor Gendron in the course of some historical studies discovered a coded letter. Not knowing what to do with it, he passed it on to Etienne Bazeries of the Cipher Bureau of the foreign ministry.

Bazeries was a French officer who had come into contact with secret writing when trying to decode various personal messages in the daily papers. At that time married persons would often exchange messages with their extramarital partners; the letters were sometimes so intimate that they afforded Bazeries's comrades in the officers' mess a lot of entertainment. Bazeries was becoming increasingly skillful at reading encoded texts. On one occasion, when he was forty-four, he boasted that he would have no difficulty in reading messages encoded by the cipher system of the French military. Put to the test, he proved his ability. The war ministry thereupon changed its system, but even before the new code went into operation, Bazeries had cracked it. His fame quickly grew, and he was assigned to the Cipher Bureau of the foreign ministry. At that time he began to develop an interest in century-old messages that had remained undecoded. He uncovered the secrets of texts written at the time of Louis XIV. He was also able to read secret correspondences of the Napoleonic age. It was to him, therefore, that Gendron sent the old coded text.

This consisted of numbers between 1 and 500 that followed one another in no regular sequence. Some of the numbers occurred with special frequency. Bazeries suspected that each number represented a syllable of the French language, but that individual letters might also be expressed by one or more numbers. The number **22** was the most frequently encountered—187 times—followed by **124**. Next came **42**, **311**, and **125**. Bazeries next tried to assign these numbers to the syllables that occurred most often in a French text. He assumed that **124** could mean the article *les*, **22** *en*, and both **146** and **125** could mean *ne*; he also came to the conclusion that the letter *s* was represented by a string of various numbers. He succeeded in almost completely decoding the message. It was from the war minister Louvois and addressed to the lieutenant general de Catinat, who was commanding the army in Piedmont.

In the message Louvois reported that General Boulonde was to be punished for refusing to obey orders. The king's command was that Boulonde be arrested immediately and taken to the fortress of Pignerol. The prisoner was to be locked in a cell every night but during the day allowed to walk the battlements with **330 309**. These two numbers did not occur anywhere else in the text, which is why Bazeries was unable to guess their meaning from the context. However, he knew the story of the man in the mask in the Bastille, knew that the man had originally been imprisoned at Pignerol, and knew that the prisoner had been treated as an important personage. Bazeries concluded that **330** must mean *masque*, the French for mask, whereas **309** was probably a closing sign. He announced that the man in the mask had been General Boulonde.

Whether the brilliant Bazeries solved the mystery is doubtful. It would be surprising if *mask*, a word not part of military language, had been encoded with just a single number. The five hundred possible numbers of the code were used only for frequent words; all others had to be spelled out by strings of numbers representing letters. Moreover, Boulonde was said to have still been alive five years after the death of the man in the mask.

## THOMAS JEFFERSON'S WHEEL

Systems for the transmission of secret messages were usually invented by monks and military men, by mathematicians and secret agents, but on one occasion this brotherhood was joined by a famous politician and statesman. Thomas Jefferson, coauthor of the American Declaration of Independence, third president of the United States, invented a cipher machine, named the Jefferson wheel after him. A modern version of this is shown in plate 1.

It consists of thirty-six wooden disks of equal size, each disk divided into twenty-six equal sectors. These carry the letters of the alphabet in random sequence. The sequence is different for every disk, which presents no problem, since the number of possible arrangements of the twenty-six letters of the alphabet is enormous. The disks are marked at their apexes with the numbers 1 to 36, drilled at their center, and mounted on a metal axle—perhaps disk 27 at the extreme left, then 2, then 10, 13, and so on.

Sender and receiver must possess the same collection of disks and must have them arranged on the axle in the same order. Let us assume that the sender wishes to transmit the secret message "attacktomorrowatsunrise." He therefore holds the axle with the mounted disks horizontally before him and turns them individually so that the letters standing next to one another in a row form his text. Then he locks the disks so they can no longer turn. If he now rotates this fixed block of disks on their axle, it shows another line. Every one of the other twenty-five lines is an encoding of the message, in a form no unauthorized person can decode. Let us assume the sender chooses the line that reads **TOBQMVESBXUZKYGYMZAPXUW**. He sends this sequence of letters to the addressee, who then, on his little machine, adjusts the disks so that this same sequence of letters stands in a row. All he has to do now is look for a meaningful sequence of letters among the other twenty-five lines. Provided his disks are arranged in the same way as those of the sender, in one of the lines, he will come across "attacktomorrowatsunrise."

Whereas in Europe the art of encrypting has a long history, it seems that Jefferson thought up his invention independently. For an unauthorized person it is virtually impossible to decode a message encoded in this way, even when he has the identical thirty-six disks, if he does not know in what sequence these are threaded on the axle. Even Jefferson knew that the number of different ways of arranging the disks had forty-two digits. The Jefferson wheel provėd so successful that the United States Navy was still using it in World War II.

## SIGNS ON GRAVESTONES AND WALLS

Not far from the New York Stock Exchange on Wall Street stands Trinity Church, a church that is more than two hundred years old, tiny and lost between the skyscrapers around it. A relic of bygone centuries amidst the high tech and hubbub of New York's business district. In the churchyard beside it the visitor finds the gravestone of James Leason, who died on September 28, 1794. Leason had been a Freemason, a member of the "Jerusalem Lodge No. 4." Next to the inscription is a row of signs along the upper edge of the stone, as reproduced in figure 1.5, top. They are secret signs that can be read only by someone in possession of the key.

Each sign corresponds to a letter of the alphabet. The assignment of the letters is exceedingly simple; it can be understood from the bottom part of the figure. The inscription reads: "rememberdeath."

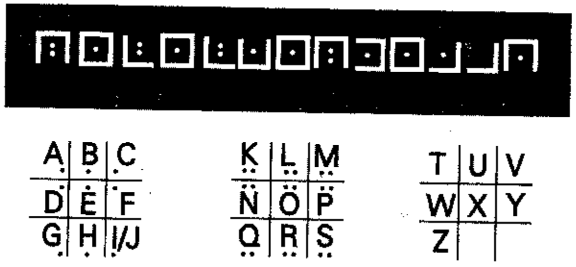


*Fig. 1.5.* **Top: the coded inscription on James Leason's grave. Bottom: twenty-five letters of the alphabet are divided among three grilles. The number of dots in each sign indicates the grille in which the letter is found. The lines of the sign indicate the position of theletter in the grille. The signs are kept so simple to allow them to be incised into the stone with a hammer and chisel (after S. B. Morris, *Cryptology*, January 1983, p. 27).**

As we will see later, this kind of code is easily deciphered. Presumably the Freemasons did not so much intend to keep the text secret by encoding it as to express the mystery of their fraternity.

|| ? 23 ⬭ ! ? § 18

§ $ ! ? ‡ ? 5 & ? ¶

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ⬭ | ‖ | 17 | 25 | ? | 18 | 10 | 2 | & | 11 | 19 | 20 | 5 | ‡ | § | 13 | 22 | ! | ¶ | 4 | $ | 15 | 23 | † | ☞ | — |

*Fig. 1.6.* **Top: a secret password of the Order of the American Union after the Civil War (1861-1865). Bottom: the cipher alphabet needed for deciphering the secret text.**

They did not very effectively encode their real secrets either, and other fraternities were no better. The Order of the American Union (OAU), founded shortly after the Civil War, also had mysterious rituals. Anyone wishing to have access to its events had to give the password twice. Members were informed of these continually changing passwords in secret writing (fig. 1.6). They were not allowed to let the key out of their hands. This, too, was a code so simple, it could be read even without the key—as we will see. In this case, it seems that the motivation was the thrill of clandestine activity rather than the need to preserve a secret.

Secret signs were used not only by societies with noble aims. The Ku Klux Klan also had its secret writing, and thieves and murderers over the past three hundred years used secret signs on walls and the sides of houses to give advice or warnings to colleagues. Figure 1.7 shows some of these signs and their meaning.

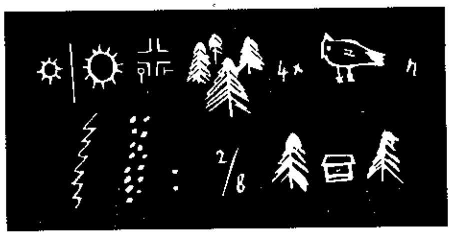


*Fig. 1.7.* **Crooks' secret marks, found in Graz about 1915. They say: "At dawn go to the crossroads by the tramcar stop at the *Volksgarten* (trees). Birdcall repeated four times. Support needed. Rich spoils. Attention (colon), meeting on 28th in the toilet at the *Volksgarten*" (from Hans Gross and Friedrich Geerds, *Handbuch der Kriminalistik*, vol. 1, Berlin 1977, p. 92).**

## THE ART OF ENCODING

The art of changing a text so that it becomes unreadable to an outsider is called *encoding, enciphering,* or *cryptography*. The science of encoding and decoding is *cryptology*. We will presently see that even with cryptographic methods that at first sight seem secure it is often possible to decode a coded message.

The example of Klausen's signals to Moscow already provided an opportunity for the explanation of a few basic concepts that will be encountered throughout this book. The message to be transmitted is the *plaintext*, which for Klausen was "no attack." He converted it into a sequence of numbers, in two separate steps. These numbers, **34236 02451 23301 72**, were the *secret text*, or *ciphertext*. In the case of James Leason's gravestone the plaintext was the warning "rememberdeath," the ciphertext the sequence of signs in figure 1.5, top. In this book all plaintexts will be printed (where possible) in lowercase letters and all ciphertexts in bold capital letters or as white letters against a black background.

The recipient of Klausen's signal in Moscow could make something of the ciphertext only because he knew the *key*. In other words, he knew how to restore the plaintext from the ciphertext. In the case of the OAU secret text, the key is reproduced in figure 1.6, bottom. For the key for James Leason's tombstone inscription, see figure 1.5, bottom. For Count Sandorf's ciphertext, the key is the template in figure 1.3. A key should be kept strictly secret, because anyone possessing it can convert a ciphertext into plaintext. In this book the keys (whenever possible) are written in capitals, and these capitals, as well as numbers if the key is a numerical sequence, are italicized. Hence:

plaintext, *KEY*, **CIPHERTEXT**

In this first chapter we already have come across two basically different kinds of encoding. The radio operator Klausen replaced the letters of his plaintext by numbers arrived at by a complicated method. Jefferson's wheel replaces the plaintext letters by other letters: *a*, *b*, *c* can become **F**, **X**, and **Y**, even if there is no *f*, *x*, or *y* in the plaintext. This type of encoding, when signs are replaced by other signs, is called *substitution*. Nearly all the chapters of this book deal with substitution procedures. In the ciphertext of Count Sandorf, however, the letters of the plaintext are preserved: they merely appear in different positions in the ciphertext. If there is no *x* or *y* in the plaintext, then neither one appears in the ciphertext. If the plaintext contains the letter *f* five times, then *f* must also occur five times in the ciphertext. This type of encoding is called *transposition*. It is discussed in chapter 8.

Whether substitution or transposition is used, the key has to be agreed upon between sender and receiver before transmission. In World War I, all naval vessels carried fat *codebooks*, comprehensive dictionary-like volumes in which every plaintext word was faced by its cipher sequence. As with a word-by-word translation into a foreign language by means of a dictionary, plaintext was converted into ciphertext. At the very beginning of World War I, the Russians got hold of one of the codebooks of the German navy (see chapter 3). It was therefore easy for Germany's opponents to decode the German naval signals.

In an effort to send as much encoded information as possible and to send it as fast as possible, and also to gain an equally fast insight into the opponent's signal traffic, encoding and decoding was not only done manually. In order to be able to read the signals encoded with the German cipher machine Enigma, which was developed in World War II (see chapters 9 and 10), and to read them with the least possible delay, British scientists and technicians developed the first electronic computers as decoding machines. After World War II, computers became an essential cryptological tool.

But better machines for ever faster code breaking were not the only development. A milestone in the history of cryptology was the development of procedures for which no secret key had to be exchanged. Until this point, anyone wishing to send a coded message also had to pass on the key, in one way or another. This involved the risk that unauthorized persons might get hold of it. Today it is possible quite publicly to send someone a ciphertext that only the authorized receiver can read, without the need also to give him the secret key.

Over the centuries increasingly sophisticated methods of encoding have been invented, but at the same time more and more sophisticated methods have been developed for reading a ciphertext without authorization. The reader will follow the development of cryptology in detail up to the present day. First, however, we will concern ourselves with the simplest forms of the transmission of secret messages. Klausen's signals consisted of numerical sequences that did not make immediate sense. Count Sandorf's ciphertexts were strings of letters. The secret texts of the Freemasons were sequences of symbols. Anyone encountering such texts would immediately assume that they were ciphertexts. Not so with the wax tablets sent to Leonidas. They got past the Persian frontier guards, because no one seeing them would suspect that a secret message might be hidden in them. This type of encoding, when an unauthorized person does not even suspect the presence of a secret message, is the subject of the next chapter.

## NOTE

[1] F. W. Deakin, and G. R. Storry, *The Case of Richard Sorge* (London: Chatto & Windus, 1966) 246ff.