Leseprobe aus:

## Rudolf Kippenhahn

# Verschlüsselte Botschaften


Mehr Informationen zum Buch finden Sie auf rowohlt.de.

# Inhalt

Im Gedenken an Arno Gutberlet (1906–1996),
den Lehrer meiner Schulzeit, den wir «Scheich» nannten
und dessen Unterricht in den Fächern Mathematik
und Physik mein Leben bestimmte.

# Vorwort zur Neuauflage 2012

Fünfzehn Jahre nachdem die englischsprachige Auflage dieses Buches im New Yorker Verlag Overlook Press erschienen war, erhielt ich von Peter Mayer, dem Gründer des Verlages, eine E-Mail mit dem Vorschlag, eine Neuauflage herauszubringen, die das Buch auf den neuesten Stand bringt. Und auch der Rowohlt Verlag hatte Interesse an einer Neuauflage.

Natürlich hat es mich gefreut, dass an meinem vor Jahren erschienenen Buch weiterhin Interesse besteht. Inzwischen hatte ich mich aber anderen Dingen zugewandt, astronomische und mathematische Bücher geschrieben und auch zwei Kinderbücher. Da ich nicht annahm, mich in meinem Leben noch einmal so intensiv mit Geheimschriften zu beschäftigen, hatte ich den größten Teil meiner Bücher darüber verschenkt. Ich begann, nach jemandem Ausschau zu halten, der mir bei der Aktualisierung und Erweiterung des Buches helfen könnte. Schließlich stieß ich auf Manfred Eyßell, der im Göttinger von Universität und Max-Planck-Gesellschaft betriebenen Rechenzentrum arbeitet. Er kennt die neuen Entwicklungen im Internet- und E-Mail-Betrieb, die ich nur noch als Zuschauer verfolgt hatte.

Manfred Eyßell schrieb den Beitrag über die Navajo-Indianer und war wesentlich an den Kapiteln 14, 15, dem Anhang B und dem Register beteiligt. Ohne seine Hilfe wäre die vorliegende Neuauflage nicht entstanden. Wir danken den Mitarbeitern des Rowohlt Verlages, vor allem unserem Lektor Frank Strickstrock, unserem Korrektor Volker Rippe und Daniel Sauthoff von der Herstellung für ihre Geduld und Aufmerksamkeit.

*Göttingen, im Frühjahr 2012* *Rudolf Kippenhahn*

# Vorwort

In meiner Jugend habe ich mich nicht mehr für Geheimschriften interessiert als andere Jungen, die das Geheimnisvolle anzieht. Natürlich hatte ich die Sherlock-Holmes-Geschichte von den «Tanzenden Männchen» gelesen, doch kann ich mich nicht erinnern, dass mich Geheimschriften besonders faszinierten. Auch während meines Mathematikstudiums war mir nicht bewusst, wie eng die Beziehungen zwischen meinem Fach und der Kunst der Ver- und der Entschlüsselung sind. Erst als mir in den siebziger Jahren ein Freund von einer völlig neuen Entwicklung in der Kryptologie erzählte, begann ich mich mit ihr zu befassen – und fühlte mich unversehens von der Faszination gefesselt, die von ihr ausgeht. Ich lernte die Schicksale von Menschen kennen, deren Leben die Kryptologie geprägt hatte, sei es, weil sie sich der Ver- und Entschlüsselung verschrieben hatten, sei es, weil Geheimschriften sie schützten oder ihnen entzifferte Geheimschriften zum Verhängnis wurden.

Irgendwann hatte ich dann das Bedürfnis, etwas von dieser Faszination mitzuteilen. So entstand *Verschlüsselte Botschaften*. Je mehr ich mich mit dem Thema beschäftigte, umso tiefer wurde ich auch emotional in die Ereignisse des Zweiten Weltkriegs hineingezogen. Deshalb handelt ein Teil meines Buches von der deutschen Chiffriermaschine Enigma und von den Leuten, denen es gelang, ihre Verschlüsselung zu brechen.

Doch ging es mir nicht darum, Geschichte und schon gar keine Kriegsgeschichte zu schreiben. Mich interessiert die Kryptologie an sich. Historische Vorgänge beschreibe ich nur, weil gerade in der Geschichte der Kryptologie offenkundig wird, wie eng Wissenschaft und menschliches Schicksal verknüpft sein können.

Ich hätte dieses Buch nicht vollenden können, wenn ich nicht

von vielen Seiten Hilfe bekommen hätte. Mit vielen Freunden, aber auch mit Menschen, die ich erst bei meiner Materialsuche kennenlernte, habe ich diskutiert und viel dabei gelernt. Ich danke allen. Besonders hervorheben möchte ich die Herren Franz-Leo Beeretz, Joachim Heinke, Reimar Lüst, Hartmut Petzold, Wolfgang Scondo und Helmut Steinwedel. Mein Dank geht ferner an die Präsidentin des Landgerichts Hamburg. Ich danke Herrn Rolf Spindler, der fotografische Arbeiten für mich ausgeführt hat. Ganz besonders aber möchte ich meinem Freund, dem Mathematiker Hans-Ludwig de Vries, danken, nicht nur weil er mich zu diesem Thema angeregt hat, sondern auch weil er, wie bei meinen früheren Büchern, den gesamten Text Seite für Seite kritisch mit mir durchgegangen ist. Schließlich danke ich den Mitarbeitern des Rowohlt Verlages für die vertrauensvolle Zusammenarbeit.

Alle Graphiken in diesem Buch sind mit dem Programm CorelDraw! angefertigt worden. Zum Teil wurden dabei Bilder aus der zugehörigen Clipart-Bibliothek übernommen.

*Göttingen, 17. März 1997* *Rudolf Kippenhahn*

# 1 Geheimschriften in Krieg und Frieden

Ich bin mit allen Arten von Geheimschriften ziemlich vertraut und habe auch selbst eine bescheidene Monographie über diesen Gegenstand verfasst, in der ich einhundertsechzig verschiedene Chiffrensysteme analysiert habe.

SHERLOCK HOLMES
(in «Die tanzenden Männchen»)

«Wenn man mich zum Tode verurteilt, Ohashi-san, werde ich dich als Gespenst heimsuchen», sagte der Häftling zum Inspektor der Geheimpolizei. Während der vielen Verhöre hatte sich zwischen den beiden ein vertraulicher Ton eingestellt. Inspektor Ohashi war schon an jenem Samstag im Oktober 1941 dabei gewesen, als am frühen Morgen Männer in das Tokioter Haus des Journalisten Richard Sorge eingedrungen waren und ihn in Schlafanzug und Pantoffeln zur Polizeiwache gebracht hatten.

Seither hatte der Gefangene Zeit genug gehabt, über sein Leben nachzudenken. Während der ersten Wochen in der Zelle hatte ihn diese neue Erfahrung des Scheiterns in die Verzweiflung getrieben. Dann war der anfangs schwache, sich allmählich verstärkende Trost in ihm erwacht, dass er ja seine Aufgabe erfolgreich abgeschlossen hatte, ein Gedanke, der ihm die Ungewissheit über sein weiteres Schicksal erträglicher machte. Nach Hitlers Angriff auf die Sowjetunion hatte Sorge dem Vierten Büro in Moskau signalisiert, dass Japan die Sowjetunion von Osten her nicht angreifen werde. Es waren seine Meldungen gewesen, die es Marschall Shukow ermöglicht hatten, Divisionen, Tanks und Flugzeuge aus Sibirien abzuziehen und vor Moskau gegen die Deutschen einzusetzen. Hatte er, Richard Sorge, nicht Weltgeschichte gemacht? Aus den Fragen seiner Vernehmer konnte er schließen, dass es den Japanern nicht

gelungen war, die chiffrierten Nachrichten zu entziffern, die sein Funker zu Tausenden an die sowjetischen Stationen in Schanghai und Wladiwostok übermittelt hatte.

## Funker Klausen sendet nach Moskau

Die Luft liegt an diesem Sommertag drückend über Tokio. Max Klausen blickt auf das Blatt vor ihm auf dem Tisch. Es wird eine Weile dauern, bis der Text verschlüsselt ist. Er liest ihn – wieder eine Meldung von «Otto». Der Chef hat es ihm nie gesagt, doch Max weiß, dass «Otto» ein japanischer Mitarbeiter der Gruppe ist. Seine Nachrichten sind immer wichtig.

Seit dem 22. Juni 1941 dringen die deutschen Truppen immer tiefer in das Gebiet der Sowjetunion ein. Lange zuvor hat Max die Warnung, die sogar das richtige Datum des deutschen Angriffs enthalten hatte, nach Moskau gefunkt, doch hat dort niemand darauf reagiert. Wird sich die Sowjetunion in Kürze vielleicht nicht nur gegen Deutschland, sondern gleichzeitig – trotz des Nichtangriffsabkommens vom April – auch gegen die Japaner verteidigen müssen? Japan hat in diesen Tagen mobil gemacht. Werden die neu zusammengestellten Truppen Richtung Süden kommandiert oder nach Norden, gegen die Sowjetunion?

Die Meldung von «Otto» schafft Klarheit. Japan wird keinesfalls Russland angreifen, da es mit den chinesischen Zwischenfällen genügend zu tun hat. Solange nicht sicher ist, wie sich die Verhandlungen mit Amerika entwickeln werden, will hier in Japan niemand einen Krieg mit Russland.[1] Wenn Japan die Sowjetunion überhaupt angreifen wird, dann frühestens im nächsten Jahr.

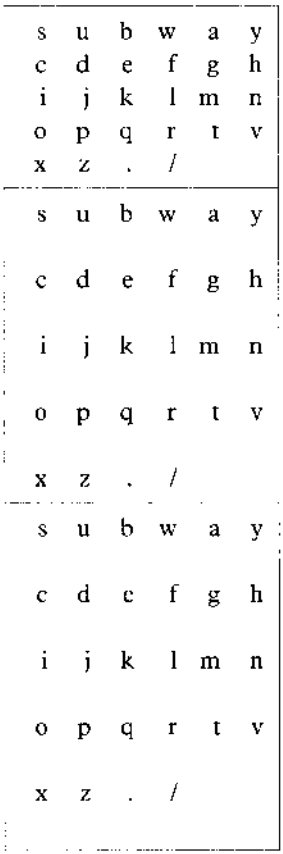
1 F. W. Deakin, G. R. Storry: Richard Sorge: *Die Geschichte eines großen Doppelspiels*, München 1965, S. 259.

Inzwischen sind die deutschen Truppen weit auf russisches Terrain vorgedrungen. Es scheint, als wolle Hitler noch vor Einbruch des Winters in Moskau sein. Die Nachricht, dass von der japanischen Seite her kein Angriff zu erwarten ist, muss den Sowjets eine große Erleichterung bringen. Funker Max Klausen beginnt mit der Verschlüsselung.

Den ersten Schritt kennt er zwar auswendig, doch diesmal nimmt er ein Blatt Papier zu Hilfe, das er anschließend vernichten wird. Es geht im ersten Schritt darum, den Buchstaben des Alphabets Zahlen zuzuordnen. Dazu muss er sein Schlüsselwort benutzen. Es ist das englische Wort für U-Bahn: *SUBWAY*. Er schreibt die sechs Buchstaben nebeneinander und ordnet vier weitere Zeilen darunter an, in die er der Reihe nach die restlichen Buchstaben des Alphabets und die Zeichen «Punkt» und «Schrägstrich» (als Zeichen der Worttrennung) einfügt. Er erhält damit die Tafel der Abbildung 1.1 oben.

Da er seine Texte immer in Englisch abschickt, nehmen bei ihm die in dieser Sprache am häufigsten vorkommenden Buchstaben a, s, i, n, t, o, e und r eine Sonderrolle ein. Der Spruch «a sin to err» (eine Sünde zu irren) besteht aus genau diesen Buchstaben – eine Merkhilfe, die Klausen nicht nötig hat. Diesen acht Buchstaben sollen die Zahlen 0, …, 7 zugewiesen werden. Dazu fügt er sie in diese Tabelle, Spalte für Spalte, von links beginnend. Sobald er auf einen Buchstaben von asintoer trifft, schreibt er eine der Zahlen von 0 bis 7 der Reihe nach darunter. Nunmehr gleicht seine Tabelle der in der Abbildung 1.1 Mitte. Jetzt schreibt er unter die restlichen Buchstaben spaltenweise die Zahlen von 80 bis 99 und erhält die Tabelle der Abbildung 1.1 unten.

Nun hat jeder Buchstabe des Alphabets seine Zahl. Damit kann Klausen die Buchstaben der Nachricht in eine Zahlenfolge übertragen. Nehmen wir zur Veranschaulichung einen einfachen Funkspruch: Aus der Wortfolge «kein Angriff», also aus «no attack» im Englischen, wird 729456658088. Die zwölfstellige Ziffern-



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

**Abb. 1.1: Wie Max Klausen mit dem Schlüsselwort *SUBWAY* und dem Merkwort asintoer in drei Schritten eine Schlüsseltafel herstellte, mit der er die Buchstaben des Alphabets in Zahlen umwandeln konnte.**

gruppe lässt sich ohne Mühe wieder in Zahlen oder Zahlenpaare auflösen, die Buchstaben oder Ziffern entsprechen. Ziffern, denen keine 8 oder 9 vorangeht, entsprechen einzeln einem Buchstaben der Tabelle. Tritt eine 8 oder eine 9 auf, so steht sie zusammen mit der nachfolgenden Ziffer für jeweils einen Buchstaben der Tabelle. Bei 729456658088 entsprechen 7, 2, 94 und 5 den Buchstaben (beziehungsweise Zeichen) n, o, / und a. Die zwei Sechsen sind das doppelte t. Die 80 stellt das c, die 88 den Buchstaben k dar. Damit ist

«no attack» verschlüsselt. Das aber ist nur der erste Schritt, Klausen hat jetzt erst den *vorläufig* verschlüsselten Text vor sich.

Damit ist noch nicht viel gewonnen. Jeder Anfänger kann herausfinden, dass in längeren auf diese Weise chiffrierten Nachrichten die Zahl 3 am häufigsten vorkommt. Sie entspricht dem sowohl im Deutschen als auch im Englischen häufigsten Buchstaben e. Damit hätte jeder Unbefugte den ersten Schritt zu einer Entschlüsselung getan. Deshalb beginnt Max Klausen nunmehr mit der eigentlichen Verschlüsselung. Er nimmt aus seinem Bücherregal das Statistische Jahrbuch für das Deutsche Reich vom Jahr 1935 und schlägt eine der mit Zahlen angefüllten Seiten auf. Er notiert sich die Seitenzahl sowie Zeile und Spalte in der Tabelle, in der die Zahl steht, mit der er beginnen will; es handelt sich um Angaben zur Tabakproduktion verschiedener Staaten. Dort steht die Zahl 4230, darunter 5166, 7821, 9421 und so weiter. Es besteht eine alte Vereinbarung zwischen Moskau und ihm, dass er mit der dritten und vierten Ziffer der ersten Zahl beginnen muss, um dann die anderen Zahlen anzufügen: 30516678219421 … Diese Ziffernfolge ist sein eigentlicher Schlüssel. Also schreibt Klausen seinen vorläufig verschlüsselten Text hin und darunter den Schlüssel:

729456658088
*305166782194 …*

Jetzt addiert er, wobei er, wenn eine Summe die 9 überschreitet, den Zehner nicht auf die vorangehende Stelle überträgt, also nicht 7 + 8 = 15, sondern 7 + 8 = 5 rechnet. In Abbildung 1.2 oben ist seine Rechnung vorgeführt. Nun muss er noch Seitenzahl sowie Zeile und Spalte des Jahrbuches mitteilen, damit der Empfänger den Schlüssel dem gleichen Buch entnehmen kann. Für die Seitenzahl genügen zwei Ziffern, denn wenn 34 angegeben ist, so kann es entweder 34, 134 oder 234 sein. Welches die richtige Seite ist, kann der Empfänger leicht selbst entscheiden. Für Zeile und Spalte genügen drei Zif-

fern, 236 für Zeile 23 und Spalte 6, sodass insgesamt die fünf Ziffern 34236 ausreichen, um den Anfang des Schlüssels zu kennzeichnen. Diese fünf Zahlen setzt Klausen an den Anfang seiner Nachricht, aber er verschlüsselt sie, indem er die erste Fünfergruppe des chiffrierten Textes hinzuaddiert, wieder ohne Zehnerübertragung, also 34236 + 02451 = 36687. Damit lautet seine Nachricht, in Gruppen zu je fünf Ziffern unterteilt, 36687 02451 23301 72. Diese Zifferngruppen funkt er in den Äther. Er weiß, dass der Empfänger als Erstes die zweite Fünfergruppe von der ersten ohne Zehnerübertragung abziehen wird: 36687 – 02451 = 34236. Damit hat er die Seitenzahl (34 oder 134 oder 234) und die Zeilen- und Spaltennummern (23 und 6), also alle Information, die er braucht, um den Schlüssel zu bestimmen. Er muss ihn nun von der empfangenen Nachricht (ohne die erste zum Auffinden des Schlüssels nötige Fünfergruppe) abziehen, so wie es in Abbildung 1.2 unten gezeigt ist.

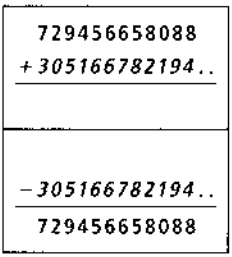



**Abb. 1.2, *oben:* Von einem numerischen, das heißt in Ziffern umgewandelten Klartext über einen Schlüssel (kursiv) zu einem numerischen Geheimtext. *Unten:* Vom numerischen Geheimtext zum numerischen Klartext.**

Damit hat er den mit der Tabelle verschlüsselten Text, den er leicht in den Klartext zurückübersetzen kann, denn auch er hat ja die Tabelle der Abbildung 1.1 unten.

Jede neue Nachricht sendete Max Klausen von einem anderen Ort. Einmal funkte er von seiner Wohnung aus, das nächste Mal vom Haus eines jugoslawischen Mitglieds des Spionagerings, und auch in

den Wohnungen anderer Freunde baute er gelegentlich seinen Sender samt Antenne auf. So gelang es dem japanischen Geheimdienst nicht, den Sender inmitten der dichtbesiedelten Stadt anzupeilen und aufzuspüren, obwohl ihm längst die zahlreichen Funksprüche aufgefallen waren, die von Tokio aus in den Äther gingen.

Um nicht von Peilwagen lokalisiert zu werden, wechselte Klausen oft auch während einer Sendung die Position. Ständig musste er das Funkgerät von einem Ort zum anderen schleppen und hätte dabei leicht einer Polizeikontrolle in die Arme laufen können. Aber es waren nicht die Funksprüche, die den Spionagering schließlich verrieten. Die Enttarnung gelang dem japanischen Geheimdienst zufällig, als er frühere Sympathisanten der kommunistischen Partei Japans näher unter die Lupe nahm.

Am Abend des 14. Oktober 1941 wollte sich Richard Sorge mit seinem japanischen Mitarbeiter Hotsumi Ozaki treffen – dem Gewährsmann «Otto» –, doch dieser erschien nicht zur verabredeten Zeit und war auch in den nächsten Tagen telefonisch nicht zu erreichen. Klausen wurde in der Nacht vom 17. auf den 18. Oktober verhaftet, und bei Sorge klopften die Männer vom Geheimdienst am frühen Morgen an die Tür. Der Prozess gegen ihn und seine Genossen zog sich über drei Jahre hin. Ozaki und Sorge wurden am 7. November 1944 gehenkt, während Klausen zu lebenslänglicher Haft verurteilt wurde und seine Frau eine Gefängnisstrafe von drei Jahren erhielt. Beide wurden nach der Kapitulation Japans von den Alliierten befreit und in die Sowjetunion geflogen. Dann hörte man lange Zeit nichts von ihnen.

Erst im Oktober 1964, also nahezu zwanzig Jahre danach, meldete eine Ostberliner Zeitung[2] unter der Überschrift «Max Klausen lebt», dass der Berliner Korrespondent der Moskauer *Iswestija* das «bescheiden und zurückgezogen lebende Ehepaar Klausen mit

2 *Neues Deutschland* vom 29. Oktober 1964.

Hilfe deutscher Genossen in der Hauptstadt der DDR aufgespürt» habe. Nunmehr überschlugen sich die Meldungen. Das Ehepaar war 1946 nach einem Genesungs- und Erholungsurlaub in die damalige sowjetische Besatzungszone gekommen und hatte dort unter dem Namen «Christiansen» gelebt. Später waren sie nach Berlin gezogen. Die Ostberliner Zeitungen schilderten die beiden als aufrechte Kommunisten und DDR-Bürger. Erst jetzt entdeckten die Medien der DDR, dass Max Klausen schon einmal wegen seines «vorbildlichen Aufbauwillens» aufgefallen war. Das *Neue Deutschland* grub in seinen Archiven eine bereits neun Jahre alte Meldung aus, in der vom Aktivisten «Maxe» Christiansen, Kaderinstrukteur der Köpenicker Yachtwerft, die Rede ist, der, wie ein Foto zeigt, mit einer Spitzhacke Trümmern zu Leibe rückt. Damals hatte das Blatt noch nicht gewusst, um wen es sich bei dem Porträtierten handelte.

Angeblich war es nur seine Bescheidenheit gewesen, die ihn über seine Verdienste hatte schweigen lassen. Doch im Jahr 1964 war der Bann auf einmal gebrochen. Klausen gab Interviews und berichtete von der Arbeit mit Sorge in Japan. Plötzlich waren die Klausen-Christiansens aus der Versenkung aufgetaucht. Offensichtlich war die Nachricht von der Vergangenheit des Aktivisten Maxe Christiansen erst 1964 freigegeben worden, denn jede historische Auseinandersetzung mit der Arbeit des Spionagerings um Sorge musste notgedrungen auch Stalins Fehler erwähnen, der ja schließlich Sorges Meldung über Hitlers Angriff auf die Sowjetunion in den Wind geschlagen hatte. Doch 1964 war das kein Tabu mehr. Nun war es dem Altkommunisten Gerhart Eisler, Mitglied des Zentralkomitees der SED und Vorsitzender des staatlichen Rundfunkkomitees der DDR, erlaubt, sich zu erinnern, dass er Sorge früher einmal begegnet war, dem Parteiveteranen Hermann Siebler fielen seine Treffen mit dem bisher totgeschwiegenen Richard Sorge wieder ein, und der Held der Arbeit Ehrenfried Navarra von der Werkzeugmaschinenfabrik in Gera verpflichtete seine Brigade anlässlich des Geburtstages von Sorge zu einem Leistungswettbewerb. Als Max

Klausen am 15. September 1979 im Alter von einundachtzig Jahren starb, war er längst Träger des Karl-Marx-Ordens, des Rotbannerordens der Sowjetunion und anderer hoher Auszeichnungen.

Es war den Japanern nicht gelungen, die von Richard Sorges treuem Funker verschlüsselten Nachrichten zu entziffern. Das Verschlüsselungsverfahren war schon recht raffiniert und beruhte vor allem auf der Benutzung eines an sich harmlosen Buches. Das Statistische Jahrbuch wäre bei einer Hausdurchsuchung nicht aufgefallen.

## Das Geheimnis der Wachstäfelchen

Die Art, wie der Funker Max Klausen in einer für Nichteingeweihte unleserlichen Form Meldungen nach Moskau funkte, erscheint dem Verschlüssler von heute recht primitiv. Der lässt den Brief an einen Partner in Australien von seinem Computer chiffrieren und sendet ihn dann über das Internet. Aber im Vergleich zu den Anfängen der Verschlüsselung von Nachrichten, die geheim bleiben sollen, benutzte Klausen schon ein sehr gutes System.

Die ersten Geheimnachrichten wurden bereits vor Jahrtausenden ausgetauscht: Um viele Ereignisse der Weltgeschichte ranken sich Legenden von geheimen Botschaften, zum Beispiel um die berühmte Schlacht bei den Thermopylen im Jahr 480 vor Christus.

Wer heute auf der Europastraße 75 von Thessaloniki nach Athen fährt, kommt, nachdem er den Olymp hinter sich gelassen hat, am Golf von Lamir vorbei, dort, wo die Autobahn nahe der Küste verläuft. Ein Gedenkstein auf einem Hügel erinnert an die Schlacht, in welcher der Spartanerkönig Leonidas vergeblich versucht hatte, sich gegen die persische Übermacht unter König Xerxes zu verteidigen. Leonidas hatte das Heer der Perser erwartet, denn ihr Kommen war ihm durch eine geheime Nachricht angekündigt worden.

Wie der griechische Geschichtsschreiber Herodot berichtet, schickte ein Grieche in persischem Exil Wachstäfelchen in seine Heimat, genauer Holztäfelchen mit einer Wachsschicht, wie man sie damals zum Schreiben benutzte. Der Mann entfernte die Schicht, schrieb die Botschaft von der bevorstehenden Invasion der Perser auf das Holz, bestrich die Täfelchen wieder mit Wachs und sandte sie an Leonidas. Die Nachricht war nun nicht mehr zu lesen und konnte ungehindert nach Griechenland gelangen. Sie wäre allerdings verborgen geblieben, hätte nicht zufällig Gorgo, die Frau des Leonidas, die Schrift unter der Wachsschicht entdeckt. So wurde Leonidas gewarnt.

Doch wie so oft in der Geschichte hatte die geheime Botschaft keinen entscheidenden Einfluss auf den Ausgang der Schlacht. Auf einem Schleichweg über die Berge führte ein griechischer Verräter die Perser zu Leonidas' Stellung am Thermopylenpass, und seine Truppen wurden nun von zwei Seiten angegriffen. Sie kämpften bis zum letzten Mann.

In dem von Herodot überlieferten Fall wurde die geheime Nachricht so übermittelt, dass den Täfelchen niemand die brisante Information ansehen konnte, die sie enthielten. Wahrscheinlich war auf dem Wachs darüber ein belangloser Text eingeritzt, der von der eigentlichen Botschaft ablenken sollte.

## Die geheime Botschaft an den Grafen Sandorf

Triest war 1867 eine österreichische Stadt, und in ihrem Norden sollte der größte Hafen der Habsburgermonarchie entstehen. Doch im Frühling jenes Jahres standen die Zeichen für die Verwirklichung des Planes nicht besonders günstig. Österreich hatte wenige Monate zuvor die Schlacht bei Königgrätz gegen Preußen verloren, und die ungarische Freiheitsbewegung war seit dem von Lajos

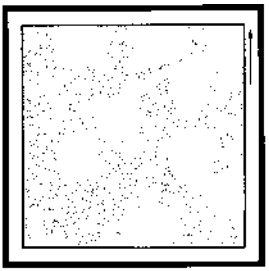


**Abb. 1.3: Die von Jules Verne in seinem Roman *Mathias Sandorf* beschriebene Chiffrierschablone. Man legt sie auf ein leeres Papier und trägt die ersten neun Buchstaben der zu verschlüsselnden Nachricht in die ausgeschnittenen (im Bild weißen) Felder des Quadrats ein. Danach dreht man die Schablone im Uhrzeigersinn um neunzig Grad und schreibt die nächsten neun Buchstaben in die offenen Felder. So fährt man fort, bis die Schablone in allen vier Stellungen benutzt wurde. Auf dem Papier füllen dann die eingeschriebenen Buchstaben ein Quadrat von sechs mal sechs Feldern, die zeilenweise gelesen den verschlüsselten Text ergeben. Ist die Nachricht länger, beginnt man mit einem neuen Quadrat. Wird ein Quadrat nicht vollständig gefüllt, ergänzt man den zu verschlüsselnden Text durch willkürlich gewählte Buchstaben, damit alle sechsunddreißig Felder vollgeschrieben sind.**

Kossuth geführten und von den Österreichern niedergeschlagenen Aufstand nicht zur Ruhe gekommen.

Diese gespannte Atmosphäre bildet den Hintergrund von Jules Vernes Roman *Mathias Sandorf*: Der ungarische Graf Sandorf lebt vorübergehend in Triest. Brieftauben bringen ihm chiffrierte Nachrichten vom Unabhängigkeitskampf zu Hause. Die Botschaft, dass man dort zum Aufstand gegen Österreich bereit sei und nur auf ein Zeichen von ihm warte, gerät in falsche Hände. Der Text:

CAELHLREENERDSSETAIISESTSNBIETZIEBIMHENUEN
WBIESENEVSRSTOIDNSCEEHNTNDERRENANLGLGAIREE
NIFUGSNUXKEAXEBXHRIATDUE

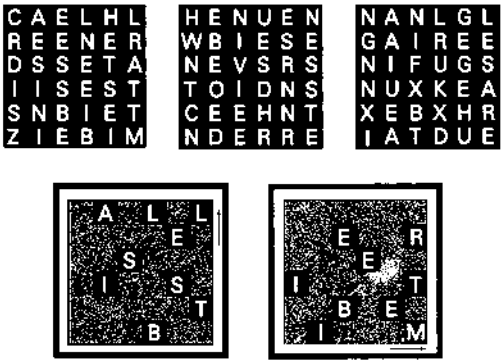



**Abb. 1.4: Wie der verschlüsselte Text von Seite 27 entschlüsselt wird. Der Geheimtext ist oben in drei Quadrate geschrieben. Die Schablone der Abbildung 1.3 ist links unten in ihrer Grundstellung auf das erste Quadrat gelegt, rechts nach einer Drehung von neunzig Grad im Uhrzeigersinn. In diesen beiden Stellungen gibt sie die ersten achtzehn Buchstaben der ursprünglichen Nachricht wieder.**

Natürlich kann das keiner der österreichischen Agenten entziffern. Erst als ein Bösewicht den Schlüssel aus dem Schreibtisch des Grafen stiehlt, ist eine Dechiffrierung möglich.

Der Schlüssel ist ein Quadrat aus sechs Zeilen und sechs Spalten. Von den sechsunddreißig quadratischen Feldern sind neun ausgeschnitten. Das ergibt eine Schablone, wie sie Abbildung 1.3 zeigt. Zur Entschlüsselung schreibt der Empfänger den Geheimtext in drei Quadrate von jeweils sechsunddreißig Feldern, so wie es in Abbildung 1.4 oben zu sehen ist. Nun legt er die Schablone auf das Quadrat der Geheimtextbuchstaben und liest durch die ausgeschnittenen Felder: allesistb (Abbildung 1.4 unten links). Dann dreht er die Schablone um neunzig Grad im Uhrzeigersinn (Abbildung 1.4 unten rechts) und liest: ereitbeim. Wieder neunzig Grad: erstenzei. Noch einmal eine Drehung: chendassi. Damit ist das erste Quadrat ausgeschöpft. Zusammen mit den anderen Quadraten folgt der Klartext: