dtv

»Ein äußerst penibel recherchiertes, so spannend wie anschaulich geschriebenes Buch. Denn Singh untersucht eine über Jahrtausende währende Tradition des besonderen Gebrauchs von Zeichen und deren Dechiffrierung – die Verschlüsselungstechniken, mit deren Hilfe man bestimmte Nachrichten geheim hält, um sie nur dem Besitzer eines besonderen Codes zugänglich zu machen.«
Süddeutsche Zeitung

»Diesen Wettstreit um die Geheimhaltung hat der Bestsellerautor zu einer Wissenschaftsreportage erster Güte komponiert.«
Die Zeit

»… ein Buch, im dem jeder auch das liest, von dem er gar nicht wußte, daß es ihn interessiert.«
Albrecht Beutelspacher in *Bild der Wissenschaft*

Simon Singh, geboren 1964, studierte Physik und war bis 1997 bei der BBC tätig. Seitdem arbeitet er als freier Wissenschaftsjournalist, Produzent und Autor. Er lebt in London und hat zahlreiche Auszeichnungen erhalten, unter anderem den British Academy Award für Film und Fernsehkunst. 1997 erschien von ihm der internationale Bestseller ›Fermats letzter Satz‹ (dtv 33052).

Simon Singh

GEHEIME BOTSCHAFTEN

Die Kunst der Verschlüsselung
von der Antike bis in die Zeiten des Internet

Aus dem Englischen von
Klaus Fritz

Mit zahlreichen Schwarzweißabbildungen

dtv

Ausführliche Informationen über
unserere Autoren und Bücher
www.dtv.de

Die deutschsprachige Originalausgabe dieses Buches enthielt ein aus zehn Codes bestehendes Verschlüsselungsrätsel, das als das weltweit schwierigste galt. Verbindlich für die Richtigkeit der Aufgabenstellung war die englische Originalausgabe. Die Leser konnten ihre Fähigkeiten zum Codeknacken testen und 10 000 britische Pfund gewinnen. Die Leser der vorliegenden deutschsprachigen Taschenbuchausgabe haben diese Chance leider nicht mehr, denn sämtliche Codes wurden bis zum 7. Oktober 2000 entschlüsselt. Weitere Informationen finden Sie auf der Cipher Challenge Website, http://www.4thestate.co.uk/cipherchallenge.

Bei dtv ist von Simon Singh außerdem erschienen:
Fermats letzter Satz
Big Bang
Homers letzter Satz

14. Auflage 2017
2001 dtv Verlagsgesellschaft mbH & Co. KG, München

Titel der englischen Originalausgabe:
The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography (Fourth Estate, London 1999)

Carl Hanser Verlag, München
ISBN 3-446-19873-3
Umschlagkonzept: Balk & Brumshagen
Umschlagbild: Peter-Andreas Hassiepen
(mit freundlicher Genehmigung des Carl Hanser Verlags, München)
Satz: Fotosatz Reinhard Amann, Memmingen
Druck und Bindung: Kösel, Krugzell
Gedruckt auf säurefreiem, chlorfrei gebleichtem Papier
Printed in Germany · ISBN: 978-3-423-33071-8

Für meine Mutter und meinen Vater,
Sawaran Kaur und Mehnga Singh

Der Drang, Geheimnisse aufzudecken, ist im Wesen des Menschen tief eingewurzelt; schon die einfachste Neugier beruht ja auf der Aussicht, ein Wissen zu teilen, das andere uns vorenthalten. Einige sind glücklich genug, einen Beruf zu finden, der in der Lösung von Rätseln besteht. Aber die meisten von uns müssen diesen Drang mit der Lösung künstlich zu unserer Unterhaltung ausgedachter Rätselaufgaben stillen. Detektivgeschichten und Kreuzworträtsel werden vielen nutzen; einige wenige mögen sich der Entschlüsselung von Geheimschriften hingeben.

John Chadwick
Linear B: Die Entzifferung der mykenischen Schrift

Inhalt

Einleitung

Jahrtausende schon verlassen sich Herrscher und Generäle auf schnelle und sichere Nachrichtenwege, um ihre Länder und Armeen zu führen. Und seit jeher wissen sie, welch schwerwiegende Folgen es haben könnte, sollten ihre Botschaften in die falschen Hände geraten. Dann wären den rivalisierenden Staaten oder gegnerischen Streitkräften wohlgehütete Geheimnisse und entscheidende Informationen preisgegeben. Die Gefahr, daß ein Gegner solch wichtige Nachrichten abfangen könnte, war und ist Ansporn für die Entwicklung der Verschlüsselungsverfahren. Diese Techniken des Verbergens sollen gewährleisten, daß nur der eigentliche Empfänger die Botschaft lesen kann.

Der Wunsch, bestimmte Nachrichten geheimzuhalten, führte dazu, daß Staaten ihre eigenen Verschlüsselungsdienste einrichteten, die die bestmöglichen Codes entwickeln sollten und verantwortlich waren für den sicheren Nachrichtenverkehr. Zugleich versuchten die gegnerischen Codebrecher, diese Codes zu entschlüsseln und die Geheimnisse zu stehlen. Codebrecher sind Alchemisten der Sprache, ein mythenumwobener Stamm, der versucht, sinnvolle Worte aus bedeutungslosen Symbolreihen hervorzuzaubern. Die Geschichte der Geheimschriften, der Codes und Chiffren ist die Geschichte des jahrhundertealten Kampfes zwischen Verschlüßlern und Entschlüßlern, eines geistigen Rüstungswettlaufs, der dramatische Auswirkungen auf den Gang der Geschichte hat.

Bei der Arbeit an diesem Buch verfolgte ich hauptsächlich zwei Ziele. Zum einen wollte ich die Evolution der Codes nachzeichnen. Evolution ist ein durchaus angemessener Begriff, denn die Entwick-

lung von Codes kann als evolutionärer Kampf betrachtet werden. Ein Code ist ständigen Angriffen der Codebrecher ausgesetzt. Wenn die Codebrecher eine neue Waffe entwickelt haben, die die Schwäche eines Codes bloßlegt, ist dieser nutzlos geworden. Entweder stirbt er aus oder er entwickelt sich zu einem neuen, stärkeren Code fort. Dieser neue Code wiederum wird nur so lange überdauern, bis die Codebrecher seine Schwachpunkte ausfindig gemacht haben, und so weiter. Vergleichen läßt sich diese Lage etwa mit der eines Stammes infektiöser Bakterien. Die Bakterien leben und pflanzen sich nur so lange fort, bis die Mediziner ein Antibiotikum entdecken, das einen Schwachpunkt der Bakterien angreift und sie tötet. Die Bakterien sind gezwungen, sich zu verändern und dem Antibiotikum ein Schnippchen zu schlagen, und wenn dies gelingt, werden sie sich von neuem fortpflanzen und ausbreiten können. Die Bakterien sind ständig gezwungen, sich zu verändern, um die Angriffe neuer Antibiotika zu überleben.

Der unablässige Kampf zwischen Verschlüßlern und Entschlüßlern hat zu einer Reihe bemerkenswerter wissenschaftlicher Durchbrüche geführt. Die einen sind ständig auf der Suche nach neuen Verschlüsselungsverfahren, während die anderen immer stärkere Methoden entwickeln, um sie anzugreifen. Beide Seiten, die eine um Geheimhaltung, die andere um deren Zerstörung bemüht, bedienen sich einer ganzen Reihe wissenschaftlicher Disziplinen und Verfahren, von der Mathematik bis zur Linguistik und von der Informatik bis zur Quantentheorie. Verschlüßler und Entschlüßler bereichern wiederum diese Fachgebiete, und ihre Arbeit beschleunigt die technische Entwicklung, ganz besonders die des modernen Computers.

Codes sind in die Geschichte eingewoben, sie haben Schlachten entschieden und den Tod gekrönter Häupter herbeigeführt. Deshalb kann ich aus einer Fülle von politischen Intrigen, von Dramen um Leben und Tod schöpfen und damit die entscheidenden Wendepunkte in der evolutionären Entwicklung der Codes anschaulich machen. So ungewöhnlich reichhaltig ist die Geschichte der Verschlüsselung, daß ich viele spannende Episoden weglassen mußte und meine Darstellung also keineswegs die endgültige ist. Ich bitte um Nachsicht, sollte ich Ihre Lieblingsgeschichte oder den von Ihnen be-

sonders geschätzten Codeknacker unerwähnt lassen. Im Anhang finden Sie weiterführende Literatur, und ich hoffe, dies wird auch jene Leser besänftigen, die sich eingehender mit der Sache beschäftigen wollen.

Nach der Darstellung der Evolution der Codes und ihrer historischen Rolle ist es das zweite Ziel des Buches zu zeigen, daß dieses Thema heute bedeutsamer ist denn je. Information wird zu einer immer wertvolleren Ware, und die Kommunikationsrevolution verändert die Gesellschaft: Daher werden Techniken zur Verschlüsselung von Nachrichten eine wachsende Rolle im alltäglichen Leben spielen. Satelliten übermitteln heute unsere Telefongespräche, und unsere elektronische Post durchläuft verschiedene Computer. Und da beide ohne großen Aufwand belauscht oder abgefangen werden können, ist unsere Privatsphäre in Gefahr. Immer mehr Geschäfte werden über das Internet abgewickelt, und wenn Firmen und ihre Kunden geschützt werden sollen, müssen Sicherungen eingebaut werden. Die Verschlüsselung ist die einzige Möglichkeit, unsere Privatsphäre zu schützen und den Erfolg des digitalen Marktes zu gewährleisten. Die Kunst der geheimen Kommunikation, auch als Kryptographie bezeichnet, wird die Schlösser und die Schlüssel des Informationszeitalters bereitstellen.

Allerdings kollidiert der wachsende öffentliche Bedarf an Kryptographie mit den Notwendigkeiten der Strafverfolgung und dem Sicherheitsbedürfnis der Staaten. Seit Jahrzehnten zapfen Polizei und Geheimdienste Telefonleitungen an, um Beweismaterial gegen Terroristen und das organisierte Verbrechen zu sammeln, doch die jüngste Entwicklung ultrastarker Codes droht solche Abhörverfahren wertlos zu machen. Beim Eintritt ins 21. Jahrhundert fordern Bürgerrechtler den allgemeinen Gebrauch der Kryptographie, um das Privatleben der Bürger zu schützen. Ihr Mitstreiter ist die Wirtschaft, die starke kryptographische Verfahren braucht, um ihre Transaktionen in der rasch wachsenden Welt des Internet-Handels zu sichern. Zugleich jedoch verlangen die Sicherheitsbehörden von den Regierungen, den Gebrauch der Kryptographie einzuschränken. Die Frage lautet: Was schätzen wir höher ein, unser Privatleben oder eine wirksame Verbrechensbekämpfung, oder gibt es einen Kompromiß?

Zwar hat die Kryptographie inzwischen starken Einfluß im zivilen Leben gewonnen, doch es darf nicht unerwähnt bleiben, daß die militärische Kryptographie nach wie vor eine wichtige Rolle spielt. Es heißt, der Erste Weltkrieg sei der Krieg der Chemiker gewesen, weil zum ersten Mal Senfgas und Chlor eingesetzt wurden, der Zweite Weltkrieg der Krieg der Physiker, weil die Atombombe abgeworfen wurde. Der Dritte Weltkrieg würde der Krieg der Mathematiker werden, weil die Mathematiker die nächste große Kriegswaffe, die Information, kontrollieren würden. Mathematiker haben die Codes entwickelt, die gegenwärtig militärische Informationen schützen. Es überrascht nicht, daß sie auch an vorderster Front im Kampf um die Entschlüsselung dieser Codes stehen.

Bei der Darstellung der Evolution von Codes und ihrer Auswirkungen auf die Geschichte erlaube ich mir einen kleinen Abstecher. Kapitel 5 behandelt die Entzifferung verschiedener antiker Schriften, darunter Linear B und die ägyptischen Hieroglyphen. Technisch gesehen, geht es in der Kryptographie um Botschaften, die absichtlich so gestaltet sind, daß ihre Geheimnisse einem Gegner verborgen bleiben. Dagegen waren die Schriften der alten Kulturen nicht absichtlich unentzifferbar, allerdings hatten wir die Fähigkeit verloren, sie zu verstehen. Und doch ist die Kunst der Entschlüsselung archaischer Texte eng verwandt mit der Kunst des Codebrechens. Seit ich John Chadwicks Buch *Linear B: Die Entzifferung der mykenischen Schrift* gelesen habe, verblüffen mich immer wieder die erstaunlichen intellektuellen Leistungen jener Männer und Frauen, die in der Lage waren, die Schriften unserer Vorfahren zu entziffern, und uns damit die Möglichkeit gaben, etwas über ihre Kulturen, ihre Religionen und ihr alltägliches Leben zu erfahren.

Bei den Puristen möchte ich mich für meinen recht lockeren Sprachgebrauch in dieser Einleitung entschuldigen. In diesem Buch geht es um mehr als nur um Codes. Das Wort *Code* bezeichnet eigentlich einen besonderen Fall der geheimen Kommunikation, der seit Jahrhunderten im Niedergang begriffen ist. Dabei wird ein Wort oder Satz durch ein anderes Wort, eine Zahl oder ein Symbol ersetzt. So besitzen etwa Geheimagenten Codenamen, also Tarnnamen an Stelle ihrer richtigen Namen. Auch kann der Satz Angriff bei Morgengrauen

durch das Codewort Jupiter ersetzt werden, und dieses Wort könnte einem Befehlshaber auf dem Schlachtfeld übermittelt werden, um den Gegner, der es abhört, zu verwirren. Wenn das Hauptquartier und der Kommandeur sich zuvor abgesprochen haben, wird dem eigentlichen Empfänger die Bedeutung von Jupiter klar sein, dem Gegner jedoch wird die Meldung unverständlich bleiben. Die Alternative zum Code ist die Chiffre, ein Verfahren, das auf tieferer Ebene ansetzt und zum Beispiel Buchstaben statt ganzer Wörter ersetzt. So kann jeder Buchstabe in einem Satz durch den nächsten Buchstaben im Alphabet ersetzt werden, A durch B, B durch C und so weiter. Dann wird Angriff bei Morgengrauen zu Bohsjgg cfj Npshfohsbvfo. Chiffren spielen in der Kryptographie eine wesentliche Rolle, und so sollte dieses Buch eigentlich *Das Buch der Codes und Chiffren* heißen. Ich habe jedoch die Genauigkeit der Griffigkeit geopfert und hoffe, Sie verzeihen mir die Wahl des Titels.

Je nach Bedarf erläutere ich die verschiedenen Fachbegriffe, die in der Kryptographie verwendet werden. Zwar halte ich mich im allgemeinen an diese Definitionen, doch gebrauche ich gelegentlich auch einen Begriff, der technisch vielleicht nicht ganz treffend ist, von dem ich jedoch glaube, daß er den Laien vertrauter ist. Geht es etwa um jemanden, der versucht, eine Chiffre zu entschlüsseln, verwende ich häufig das Wort *Codebrecher* und nicht das genauere *Chiffrenbrecher.* Ich tue dies nur dann, wenn die Bedeutung des Wortes klar aus dem Zusammenhang hervorgeht. Am Schluß des Buches findet sich ein Glossar, doch häufig ist die kryptographische Fachsprache selbsterklärend; so ist der *Klartext* die Botschaft vor, der *Geheimtext* die Botschaft nach der Verschlüsselung.

Zum Schluß möchte ich Ihre Aufmerksamkeit auf ein Problem lenken, vor dem jeder Autor steht, der sich mit dem Thema Kryptographie befaßt, die Tatsache nämlich, daß sie eine weitgehend geheime Wissenschaft ist. Viele Helden dieses Buches fanden zu ihren Lebzeiten nie Anerkennung für ihre Arbeit, weil ihre Leistungen öffentlich nie dargestellt werden durften, während ihre Erfindungen gleichwohl von diplomatischem oder militärischem Wert waren. Während der Recherchen für dieses Buch konnte ich mit Fachleuten im britischen Government Communications Headquarters (GCHQ)

sprechen, die mir Einzelheiten erstaunlicher Forschungsarbeiten aus den siebziger Jahren enthüllten, die erst vor kurzem freigegeben wurden. Dank dieser Aufhebung der Geheimhaltung können jetzt drei der besten Kryptographen der Welt die Anerkennung erhalten, die sie verdienen. Allerdings hat mir diese jüngste Enthüllung nur deutlich gemacht, daß noch eine Menge mehr vor sich geht, von dem weder ich noch irgendein anderer Wissenschaftsautor Ahnung haben. Organisationen wie das GCHQ und die amerikanische National Security Agency (NSA) betreiben auch weiterhin geheime kryptographische Forschung, und das heißt, ihre bahnbrechenden Erkenntnisse bleiben geheim und die Menschen, denen sie gelingen, bleiben anonym. Trotz dieser Probleme mit staatlich verfügter Geheimhaltung und geheimer Forschung mutmaße ich im letzten Kapitel des Buches ausgiebig über die Zukunft der Codes und Chiffren. Im Grunde geht es darum, abzuschätzen, wer den evolutionären Kampf zwischen Verschlüßlern und Entschlüßlern gewinnen wird. Werden die Verschlüßler jemals einen wirklich unentschlüsselbaren Code entwickeln und in ihrem Streben nach absoluter Geheimhaltung den Sieg davontragen? Oder werden die Codebrecher eines Tages eine Maschine bauen, die jede Botschaft entschlüsseln kann? Wenn wir uns vor Augen halten, daß einige der besten Köpfe in geheimen Forschungsstätten arbeiten und daß sie auch den Großteil der Forschungsmittel erhalten, ist klar, daß einige der Thesen im letzten Kapitel vielleicht unzutreffend sind. So behaupte ich etwa, daß Quantencomputer – Maschinen, die potentiell in der Lage sind, alle heutigen Chiffren zu entschlüsseln – noch in einem sehr frühen Entwicklungsstadium sind, doch ist es durchaus möglich, daß die NSA bereits einen gebaut hat. Die einzigen Menschen, die mir meine Irrtümer nachweisen könnten, sind dieselben, die nicht frei sind, es zu tun.

1
Die Geheimschrift der Maria Stuart

Am Morgen des 15. Oktober 1586 betrat die schottische Königin Maria Stuart den überfüllten Gerichtssaal von Fotheringhay Castle. Jahrelange Haft und eine beginnende rheumatische Erkrankung hatten ihr schwer zugesetzt, doch ihre Würde, ihre Fassung und ihr unverkennbar herrschaftliches Auftreten hatte sie nicht verloren. Gestützt auf ihren Arzt, schritt sie an den Richtern, Hofbeamten und Zuschauern vorbei auf den Thron in der Mitte des langen, schmalen Saals zu. Sie hielt ihn für eine Geste der Hochachtung, doch sie irrte. Der leere Thron vertrat die abwesende Königin Elisabeth, Marias Gegnerin und Anklägerin. Mit sanfter Gewalt führte man Maria weiter auf die andere Seite des Saals, zu dem scharlachroten Samtstuhl, der für die Angeklagten bestimmt war.

Maria Stuart, Königin von Schottland, war des Verrats angeklagt. Sie wurde beschuldigt, an einer Verschwörung zur Ermordung von Königin Elisabeth I. beteiligt gewesen zu sein, mit dem Ziel, selbst die englische Krone an sich zu reißen. Sir Francis Walsingham, der für die Sicherheit zuständige Minister Elisabeths, hatte die anderen Verschwörer bereits verhaften lassen, ihnen Geständnisse abgepreßt und sie hingerichtet. Nun wollte er beweisen, daß Maria das Herz des Komplotts war, damit gleichermaßen schuldig und des Todes würdig.

Walsingham wußte genau, daß er Königin Elisabeth von der Schuld Marias überzeugen mußte, wenn er sie hinrichten lassen wollte. Zwar verabscheute Elisabeth Maria, doch sie hatte gute Gründe, vor einem Todesurteil zurückzuschrecken. Zum einen war Maria eine schottische Königin, und viele bezweifelten, daß ein englisches Gericht be-

fugt war, ein ausländisches Staatsoberhaupt zum Tode zu verurteilen. Zum andern würde die Hinrichtung Marias einen peinlichen Präzedenzfall schaffen – wenn es dem Staat erlaubt war, diese Königin zu töten, dann würden die Aufständischen vielleicht weniger Skrupel haben, eine andere Monarchin zu töten, nämlich Elisabeth selbst. Zudem waren Elisabeth und Maria Kusinen, und diese Blutsverwandtschaft ließ Elisabeth erst recht vor der letzten Konsequenz zurückscheuen. Kurz, Elisabeth würde Marias Hinrichtung nur gutheißen, wenn Wal-

Abbildung 1: Maria Stuart.

singham ohne einen Hauch des Zweifels beweisen konnte, daß sie in die Mordverschwörung verstrickt war.

Die Verschwörer waren eine Gruppe junger katholischer englischer Adliger, die Elisabeth, eine Protestantin, beseitigen und an ihrer Stelle die Katholikin Maria auf den Thron setzen wollten. Für das Gericht stand außer Zweifel, daß Maria für die Verschwörer eine Lichtgestalt war, doch daß sie dem Vorhaben wirklich ihren Segen erteilt hatte, war nicht bewiesen. Tatsächlich hatte Maria das Mordkomplott abgesegnet. Walsingham stand nun vor der Aufgabe, eine greifbare Verbindung zwischen Maria und den Verschwörern nachzuweisen.

Maria, in trauerschwarze Seide gekleidet, saß allein vor ihren Richtern. In Verratsfällen waren den Angeklagten weder Rechtsbeistände erlaubt, noch durften sie Zeugen benennen. Zur Vorbereitung ihrer Verteidigung war Maria nicht einmal die Hilfe eines Sekretärs zugestanden worden. Allerdings wußte sie, daß ihre Lage nicht hoffnungslos war, denn umsichtigerweise hatte sie die gesamte Korrespondenz mit den Verschwörern in Geheimschrift geführt. Diese Geheimschrift verwandelte Wörter in Ketten von Symbolen, die keinen Sinn ergaben. Walsingham mochte die Briefe erbeutet haben, doch Maria war fest davon überzeugt, daß er die Symbolfolgen niemals würde entziffern können. Wenn ihr Sinn verborgen blieb, dann konnten die Briefe nicht als Beweise gegen sie verwendet werden. Allerdings beruhte all dies auf der Voraussetzung, daß die Geheimschrift nicht entziffert worden war.

Zu Marias Unglück war Walsingham nicht nur der Erste Minister Elisabeths, sondern auch Englands oberster Agentenführer. Er hatte Marias Briefe an die Verschwörer abgefangen und wußte genau, wer das Zeug dazu hatte, sie zu entziffern. Thomas Phelippes war der beste Fachmann des Landes für die Entschlüsselung chiffrierter Texte; seit Jahren bereits entzifferte er die Botschaften der Verschwörer und trug die Beweise für ihre Verurteilung zusammen. Wenn er auch die belastenden Briefe zwischen Maria und den Verschwörern entschlüsseln konnte, dann war sie dem Tode geweiht. Wenn Marias Geheimschrift jedoch stark genug war, um ihre Geheimnisse zu bewahren, dann konnte sie vielleicht mit dem Leben davonkommen. Nicht zum ersten Mal entschied die Stärke einer Geheimschrift über Leben und Tod.

Die Entwicklung der Geheimschriften

Die ersten Beschreibungen von Geheimschriften finden sich schon bei Herodot, dem »Vater der Geschichtsschreibung«, wie ihn der römische Philosoph und Staatsmann Cicero nennt. Der Autor der *Historien* war Chronist der Kriege zwischen Griechenland und Persien im 5. Jahrhundert v. Chr., die er als Auseinandersetzung zwischen Freiheit und Sklaverei verstand. Herodot zufolge rettete die Kunst der Geheimschrift Griechenland vor der Eroberung durch Xerxes, den König der Könige und despotischen Führer der Perser.

Der weit zurückreichende Zwist zwischen Griechenland und Persien erreichte seinen Höhepunkt, als Xerxes begann, bei Persepolis eine neue Stadt zu bauen, die künftige Hauptstadt seines Königreichs. Aus dem ganzen Reich und den angrenzenden Staaten trafen Abgaben und Geschenke ein, nur Athen und Sparta hielten sich auffällig zurück. Entschlossen, diese Überheblichkeit zu rächen, verkündete Xerxes: »Wir werden den Himmel des Zeus zur Grenze des Perserreichs machen; denn dann soll die Sonne kein Land, das an unseres grenzt, mehr bescheinen.« Während der nächsten fünf Jahre stellte er die größte Streitmacht der Geschichte zusammen, und 480 v. Chr. schließlich war er zu einem Überraschungsangriff bereit.

Einem Griechen jedoch, der aus seiner Heimat verstoßen worden war und der in der persischen Stadt Susa lebte, war die Aufrüstung der Perser nicht entgangen. Demaratos lebte zwar im Exil, doch tief in seinem Herzen fühlte er sich Griechenland noch immer verbunden. So beschloß er, den Spartanern eine Nachricht zu schicken und sie vor Xerxes' Invasion zu warnen. Die Frage war nur, wie er diese Botschaft übermitteln sollte, ohne daß sie in die Hände der persischen Wachen gelangen würde. Herodot schreibt:

> Da er das auf andere Weise nicht konnte – er mußte fürchten, dabei ertappt zu werden –, half er sich durch eine List. Er nahm nämlich eine zusammengefaltete kleine Schreibtafel, schabte das Wachs ab und schrieb auf das Holz der Tafel, was der König vorhatte. Darauf goß er wieder Wachs über die Schrift, damit die Wachen an den

> Straßen die leere Tafel unbedenklich durchließen. Sie kam auch an, doch man wußte nicht, was man damit anfangen sollte, bis, wie man sagt, Kleomenes' Tochter Gorgo, die Gemahlin des Leonidas, dahinterkam und riet, das Wachs abzukratzen, damit man dann die Schrift auf dem Holz fände. Das tat man, und nachdem man die Nachricht gefunden und gelesen hatte, schickte man diese auch den anderen Griechen.

Aufgrund dieser Warnung begannen die bis dahin wehrlosen Griechen, sich zu bewaffnen. So wurden etwa die Erträge der athenischen Silberbergwerke nicht unter den Bürgern verteilt, sondern verwendet, um eine Flotte von 200 Kriegsschiffen zu bauen.

Xerxes hatte den entscheidenden Vorteil des Überraschungsangriffs verloren, und als die persische Flotte am 23. September 480 v. Chr. auf die Bucht von Salamis bei Athen zulief, spornten die Griechen die persischen Schiffe auch noch an, in die Bucht einzufahren. Die Griechen wußten, daß ihre Schiffe, kleiner und der Zahl nach unterlegen, auf offener See zerstört worden wären, doch im Schutz der Bucht konnten sie die Perser möglicherweise ausstechen. Als nun noch der Wind drehte, sahen sich die Perser plötzlich in die Bucht getrieben, und jetzt mußten sie sich auf einen Kampf nach den Spielregeln der Griechen einlassen. Das Schiff der persischen Prinzessin Artemisia, von drei Seiten eingeschlossen, wollte zurück auf die offene See, doch es rammte dabei nur eines der eigenen Schiffe. Daraufhin brach Panik aus, noch mehr persische Schiffe stießen zusammen, und die Griechen starteten einen erbitterten Angriff. Binnen eines Tages wurde die gewaltige Streitmacht der Perser auf demütigende Weise geschlagen.

Demaratos' Verfahren der geheimen Nachrichtenübermittlung bestand einfach darin, die Botschaft zu verbergen. Bei Herodot findet sich auch eine andere Episode, bei der das Verbergen der Nachricht ebenfalls genügte, um ihre sichere Übermittlung zu gewährleisten. Er schildert die Geschichte des Histiaeus, der Aristagoras von Milet zum Aufstand gegen den persischen König anstacheln wollte. Um seine Botschaft sicher zu übermitteln, ließ Histiaeus den Kopf des Boten rasieren, brannte die Nachricht auf seine Kopfhaut und war-

tete dann ab, bis das Haar nachgewachsen war. Offensichtlich haben wir es mit einer historischen Epoche zu tun, in der man es nicht so eilig hatte. Der Bote jedenfalls hatte dem Augenschein nach nichts Verdächtiges bei sich und konnte ungehindert reisen. Als er am Ziel ankam, rasierte er sich den Kopf und hielt ihn dem Empfänger der Botschaft hin.

Die Übermittlung geheimer Nachrichten, bei der verborgen wird, daß überhaupt eine Botschaft existiert, heißt *Steganographie,* abgeleitet von den griechischen Wörtern *steganos,* bedeckt, und *graphein,* schreiben. In den zwei Jahrtausenden seit Herodot wurden rund um den Globus mannigfaltige Spielarten der Steganographie eingesetzt. Die alten Chinesen etwa schrieben Botschaften auf feine Seide, rollten sie zu Bällchen und tauchten sie in Wachs. Diese Wachskügelchen schluckte dann der Bote. Im 15. Jahrhundert beschrieb der italienische Wissenschaftler Giovanni Porta, wie man eine Nachricht in einem hartgekochten Ei verbergen kann. Man mische eine Unze Alaun in einen Becher Essig und schreibe mit dieser Tinte auf die Eischale. Die Lösung dringt durch die poröse Schale und hinterläßt eine Botschaft auf der Oberfläche des gehärteten Eiweißes, die nur gelesen werden kann, wenn die Schale entfernt wird. Zur Steganographie gehört auch der Gebrauch unsichtbarer Tinte. Schon im 1. Jahrhundert n. Chr. erläutert Plinius der Ältere, wie die »Milch« der Thithymallus-Pflanze als unsichtbare Tinte verwendet werden kann. Sie ist nach dem Trocknen durchsichtig, doch durch leichtes Erhitzen verfärbt sie sich braun. Viele organische Flüssigkeiten verhalten sich ähnlich, weil sie viel Kohlenstoff enthalten und daher leicht verrußen. Tatsächlich weiß man von einigen Spionen des 20. Jahrhunderts, daß sie, wenn ihnen die gewöhnliche unsichtbare Tinte ausgegangen war, ihren eigenen Urin verwendet haben.

Daß sich die Steganographie so lange gehalten hat, zeigt, daß sie immerhin ein gewisses Maß an Sicherheit bietet. Doch leidet sie unter einer entscheidenden Schwäche. Wenn der Bote durchsucht und die Nachricht entdeckt wird, liegt der Inhalt der geheimen Mitteilung sofort zutage. Wird die Botschaft abgefangen, ist alle Sicherheit dahin. Ein gewissenhafter Grenzposten wird routinemäßig alle Personen durchsuchen, alle Wachstäfelchen abschaben, leere Blätter erwär-