HANSER

Simon Singh

Geheime Botschaften

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

ISBN-10: 3-446-19873-3
ISBN-13: 978-3-446-19873-9

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 wartete 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 erwärmen, gekochte Eier schälen, Köpfe scheren und so weiter, und bisweilen wird er eine geheime Botschaft entdecken.
Daher entstand zugleich mit der Steganographie auch die Kryptographie, abgeleitet vom griechischen kryptos, verborgen. Nicht die Existenz einer Botschaft zu verschleiern ist Ziel der Kryptographie, sondern ihren Sinn zu verbergen, und dies mittels

eines Verfahrens der Verschlüsselung. Um eine Nachricht unverständlich zu machen, muß sie nach einem bestimmten Verfahren "verwürfelt" werden, das zuvor zwischen dem Sender und dem Empfänger abgesprochen wurde. Dann kann der Empfänger dieses Verfahren umgekehrt anwenden und die Botschaft lesbar machen. Der Vorteil einer kryptographisch verschlüsselten Botschaft ist, daß der Gegner, der sie abfängt, nichts damit anfangen kann. Ohne Kenntnis des Verschlüsselungsverfahrens wird es ihm schwerfallen oder gar unmöglich sein, aus dem Geheimtext die ursprüngliche Nachricht herauszulesen.
In der Kryptographie gebraucht man hauptsächlich zwei Verfahren, die Transposition und die Substitution. Bei der Transposition werden die Buchstaben einer Botschaft einfach anders angeordnet, was nichts anderes ergibt als ein Anagramm. Bei sehr kurzen Mitteilungen, etwa einem einzigen Wort, ist dieses Verfahren relativ unsicher, weil es nur eine begrenzte Zahl von Möglichkeiten gibt, einige wenige Buchstaben umzustellen. Ein Wort mit drei Buchstaben etwa kann nur auf sechs verschiedene Weisen umgestellt werden, zum Beispiel nur, nru, rnu, run, urn, unr. Steigert man jedoch die Zahl der Buchstaben allmählich, explodiert gleichsam die Zahl der möglichen neuen Anordnungen, und es wird fast unmöglich, die ursprüngliche Botschaft wiederherzustellen, wenn man das Umstellungsverfahren nicht genau kennt. Betrachten wir zum Beispiel diesen Satz. Er enthält nur 34 Buchstaben, und doch gibt es mehr als 14 830 000 000 000 000 000 000 000 000 000 verschiedene Anordnungsmöglichkeiten. Könnte ein Mensch eine Anordnung pro Sekunde prüfen, und arbeiteten alle Menschen der Erde Tag und Nacht, dann würde immer noch die fünfhundertfache Lebensspanne des Universums nötig sein, um alle Möglichkeiten durchzuprüfen. Eine Zufallstransposition von Buchstaben scheint ein sehr hohes Maß an Sicherheit zu bieten, weil es für einen gegnerischen Abhörer praktisch unmöglich wäre, selbst einen kurzen Satz wiederherzustellen. Doch die Sache hat einen Haken. Die Transposition erzeugt im Grunde ein unglaublich schwieriges Anagramm, und wenn die Buchstaben einfach ohne Sinn und Verstand nach dem Zufallsprinzip durcheinandergewürfelt werden, dann kann der eigentliche Empfänger ebensowenig wie der gegnerische Abhörer die Nachricht entschlüsseln. Damit eine

Transposition brauchbar ist, müssen die Buchstaben nach einem handhabbaren System umgestellt werden, über das sich Sender und Empfänger zuvor geeinigt haben. Schulkinder zum Beispiel schicken sich manchmal Botschaften mittels der "Gartenzaun"- Transposition. Dabei werden die Buchstaben des Texts abwechselnd auf zwei Zeilen geschrieben. Um die endgültige Geheimbotschaft herzustellen, wird die Reihe der Buchstaben auf der unteren Zeile an die Buchstabenreihe der oberen Zeile angehängt. Zum Beispiel:
Eine andere Form der Transposition ist das erste militärische Kryptographie-Verfahren, die Skytale, wie sie schon im 5. Jahrhundert die Spartaner gebrauchten. Die Skytale ist ein Holzstab, um den ein Streifen Leder oder Pergament gewickelt wird (Abbildung 2). Der Sender schreibt die Nachricht der Länge des Stabes nach auf den Streifen und wickelt ihn dann ab. Danach scheint er nur eine sinnlose Aufreihung von Buchstaben zu enthalten. Der Nachrichtentext wurde also durcheinandergewirbelt. Der Bote übernahm den Streifen und gab der Sache vielleicht noch einen kleinen steganographischen Dreh, indem er ihn als Gürtel mit nach innen gekehrten Buchstaben benutzte. Um die Nachricht wiederherzustellen, wickelte der Empfänger den Lederstreifen einfach um eine Skytale mit demselben Durchmesser, den der Sender benutzt hatte. Im Jahre 404 v. Chr. traf Lysander von Sparta auf einen blutig geschundenen Boten, einen von nur fünfen, die den kräftezehrenden Marsch von Persien überlebt hatten. Der Bote überreichte Lysander seinen Gürtel, der ihn um seine Skytale wickelte und sogleich erfuhr, daß Pharnabasus von Persien einen Angriff gegen ihn plante. Dank der Skytale konnte sich Lysander auf den Angriff vorbereiten und wehrte ihn ab.