Leseprobe aus: **Codes** von Simon Singh.
Abdruck erfolgt mit freundlicher Genehmigung des Verlages. Alle Rechte vorbehalten.

Hier geht’s zum Buch
>> Codes

1

Die Geheimschrift der Maria Stuart

Die Geburt der Kryptographie, das Substitutionsverfahren und die Erfindung der Entschlüsselung durch Häufigkeitsanalyse

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 befugt war, ein ausländisches Staatsoberhaupt zum Tode zu verurteilen. Zum andern würde die Hinrichtung Marias einen peinlichen Präzedenzfall schaffen – wenn

Abbildung 1: Maria Stuart.

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 Walsingham 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 Agentenfüh-

rer. 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, sporn-

ten 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 bestimm-

ten 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:

NAHT IHR EUCH WIEDER, SCHWANKENDE GESTALTEN
↓
N H I R U H I D R C W N E D G S A T N
A T H E C W E E S H A K N E E T L E
↓
NHIRUHIDRCWNEDGSATN ATHECWEESHAKNEETLE

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.

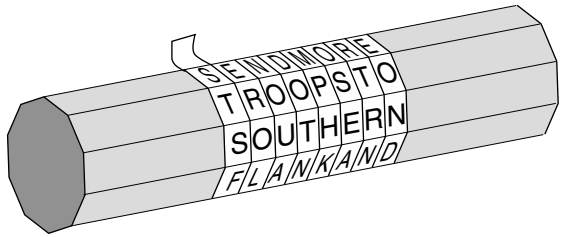

Abbildung 2: Wenn der Lederstreifen von der Skytale (Holzstab) des Absenders gelöst wird, scheint er mit einer willkürlichen Reihe von Buchstaben bedruckt; S, T, S, F, … Nur wenn der Streifen um eine andere Skytale mit dem richtigen Durchmesser gewickelt wird, taucht die Nachricht wieder auf: SEND MORE TROOPS TO SOUTHERN FLANK AND (schickt Verstärkung zur Südflanke).

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.

Die Alternative zur Transposition ist die Substitution. Eine der frühesten Beschreibungen der Verschlüsselung durch Substitution erschien im *Kāmasūtra*, einem Text, den der brahmanische Gelehrte Wātsjājana im 4. Jahrhundert n. Chr. schrieb, allerdings unter Rückgriff auf Handschriften, die auf das 4. Jahrhundert v. Chr. zurückgingen. Das *Kāmasūtra* empfiehlt, daß Frauen 64 Künste studieren sollen, darunter Kochen, Bekleidung, Massage und die Zubereitung von Parfümen. Die Liste enthält auch etwas weniger bekannte Künste, darunter Beschwörung, Schach, Buchbinderei und Teppichweberei. Die Nummer 45 auf der Liste ist *Mlecchita-vikalpā,* die Kunst der Geheimschrift, den Frauen anheimgelegt, um ihre Affären geheimzuhalten. Ein Vorschlag lautet, die Buchstaben des Alphabets nach dem Zufallsprinzip zu paaren und dann jeden Buchstaben in der Nachricht durch sein Gegenüber zu erset-

zen. Wenden wir dieses Verfahren auf das deutsche Alphabet an, könnten wir die Buchstaben wie folgt paaren:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

Dann würde der Sender statt »Treffen um Mitternacht« »zluwwus ec cgzzulsvmbz« schreiben. Dieser Geheimtext entstand mittels Substitution, denn jeder Buchstabe im Klartext wird durch einen anderen Buchstaben ersetzt, ein Verfahren, das gleichsam spiegelverkehrt zur Transposition ist. Bei dieser bleibt sich jeder Buchstabe gleich, doch er wechselt seinen Platz, während bei der Substitution jeder Buchstabe seine Gestalt wechselt, doch seinen Platz behält.

Diese Form der Verschlüsselung für militärische Zwecke beschreibt erstmals Julius Caesar im *Gallischen Krieg.* Er verfaßt eine Nachricht an den mit seinen Leuten belagerten Quintus Cicero, der kurz davor ist, sich zu ergeben. Caesar ersetzt die Buchstaben des römischen Alphabets durch griechische und macht damit die Botschaft für den Gegner unlesbar. Er schildert die dramatische Überbringung: »Wenn (der gallische Bote) nicht persönlich herankommen könne, solle er, wie ich ihm riet, einen Wurfspieß mit dem am Wurfriemen befestigten Brief in das befestigte Lager schleudern … Aus Furcht vor der Gefahr schleuderte der Gallier auftragsgemäß den Wurfspieß hinein. Dieser blieb durch Zufall in einem Turme stecken, wurde zwei Tage lang von niemandem bemerkt. Erst am dritten Tag sah ein Soldat den Brief, nahm ihn ab und brachte ihn zu Cicero. Er las die Mitteilung, gab sie dann den Soldaten bekannt und löste größte Freude im Lager aus.«

Caesar benutzte so häufig Geheimschriften, daß Valerius Probus eine ganze Abhandlung darüber schrieb, die leider nicht erhalten geblieben ist. Allerdings verdanken wir dem im zweiten Jahrhundert verfaßten *Caesarenleben* des Sueton

die genaue Beschreibung der von Caesar eingesetzten Substitutions-Chiffre. Der Kaiser ersetzte einfach jeden Buchstaben der Nachricht durch den Buchstaben, der drei Stellen weiter im Alphabet folgt. Kryptographen sprechen häufig vom *Klartextalphabet,* mit dem die ursprüngliche Nachricht geschrieben ist, und dem *Geheimtextalphabet,* der Buchstabenfolge, die an die Stelle der Klarbuchstaben tritt. Wenn das Klartextalphabet über das Geheimtextalphabet gelegt wird, wie in Abbildung 3, wird deutlich, daß das Geheimtextalphabet um drei Stellen verschoben ist. Von daher wird diese Form der Substitution oft als *Caesar-Verschiebung* oder einfach als *Caesar* bezeichnet. Geheimschrift oder Chiffre nennen wir das Ergebnis einer Substitution, bei der jeder Buchstabe durch einen anderen Buchstaben oder ein Symbol ersetzt wird.

Klartextalphabet	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
Geheimtextalphabet	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Klartext	v e n i, v i d i, v i c i
Geheimtext	Y H Q L, Y L G L, Y L F L

Abbildung 3: Die Caesar-Verschiebung, angewandt auf einen kurzen Text. Der »Caesar« beruht auf einem Geheimtextalphabet, das um eine bestimmte Stellenzahl gegenüber dem Klartextalphabet verschoben ist, in diesem Falle um drei Stellen. In der Kryptographie ist es üblich, das Klartextalphabet in Kleinbuchstaben, das Geheimtextalphabet in Großbuchstaben zu schreiben, was es dem Leser erleichtert, zwischen den beiden zu unterscheiden. Auch die ursprüngliche Botschaft, der Klartext, wird klein, und die verschlüsselte Botschaft, der Geheimtext, groß geschrieben.

Obwohl Sueton nur eine Caesar-Verschiebung um drei Stellen erwähnt, liegt es auf der Hand, daß es mit Verschiebungen zwischen einer und 25 Stellen möglich ist, 25 verschiedene Geheimschriften zu erzeugen. Und wenn wir uns nicht darauf beschränken, das Alphabet zu verschieben, und als Geheimtextalphabete beliebige Umstellungen des Klartextalphabets

zulassen, dann können wir eine sehr viel größere Zahl unterschiedlicher Geheimschriften erzeugen. Es gibt über 400 000 000 000 000 000 000 000 000 000 solcher Neuanordnungen und damit eine entsprechend hohe Zahl unterschiedlicher Geheimschriften.

Jede einzelne Geheimschrift entsteht aus der Verknüpfung einer allgemeinen Verschlüsselungsmethode, dem *Algorithmus,* mit einem *Schlüssel,* der die Einzelheiten jeder bestimmten Verschlüsselung festlegt. Im vorliegenden Fall besteht der Algorithmus aus der Ersetzung jedes Buchstabens des Klartextalphabets durch einen Buchstaben eines Geheimtextalphabets, wobei letzteres eine beliebige Neuanordnung des Klartextalphabets sein kann. Der Schlüssel ist das jeweilige Geheimtextalphabet, das für eine bestimmte Verschlüsselung verwendet wird. Das Verhältnis von Algorithmus und Schlüssel ist in Abbildung 4 dargestellt.

Wenn der Gegner eine verschlüsselte Nachricht abfängt, mag er zwar plausible Vermutungen über den Algorithmus anstellen, doch besteht durchaus Hoffnung, daß er den genauen Schlüssel nicht kennt. So könnte er vermuten, daß jeder

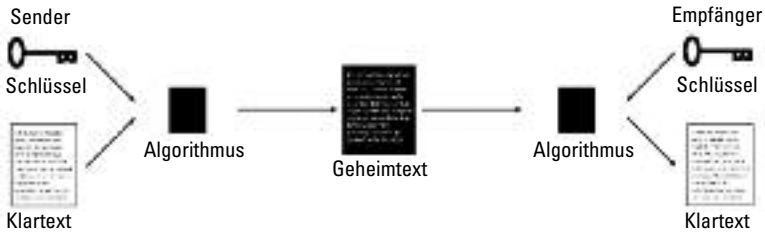

Abbildung 4: Um einen Klartext zu verschlüsseln, führt ihn der Sender durch einen Verschlüsselungs-Algorithmus. Der Algorithmus ist ein allgemeines Verfahren zur Verschlüsselung, das durch die Wahl eines Schlüssels genau bestimmt werden muß. Wendet man Schlüssel und Algorithmus zusammen auf einen Klartext an, erhält man die verschlüsselte Botschaft, die auch als Geheimtext oder als Chiffre bezeichnet wird. Der Geheimtext kann von einem Gegner abgefangen werden, doch er sollte nicht in der Lage sein, die Botschaft zu entschlüsseln. Der Empfänger jedoch kennt den Schlüssel und den Algorithmus und kann den Geheimtext in den Klartext zurückverwandeln.

Buchstabe des Klartexts durch einen anderen Buchstaben eines Geheimtextalphabets ersetzt wurde, doch wird er wahrscheinlich nicht wissen, welches bestimmte Geheimtextalphabet verwendet wurde. Wenn das Geheimtextalphabet, der Schlüssel, ein streng bewachtes Geheimnis zwischen Sender und Empfänger bleibt, dann kann der Gegner die abgefangene Nachricht nicht entschlüsseln. Die Bedeutung des Schlüssels im Gegensatz zum Algorithmus ist ein bis heute unumstrittener Grundsatz der Kryptographie, dem der holländische Linguist Auguste Kerckhoff von Nieuwenhof in seinem Buch *La Cryptograhie Militaire* die endgültige Gestalt gab. Kerckhoffs Maxime: »Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.«

Die Sicherheit eines Verschlüsselungssystems wird nicht allein durch die Geheimhaltung des jeweiligen Schlüssels gewährleistet, nötig ist auch eine Vielzahl möglicher Schlüssel. Verwendet der Sender zum Beispiel die Caesar-Verschiebung, um eine Nachricht zu verschlüsseln, dann ist die Verschlüsselung recht schwach, weil es nur 25 mögliche Schlüssel gibt. Wenn der Gegner die Nachricht abfängt und vermutet, daß die Caesar-Verschiebung als Algorithmus gebraucht wurde, muß er nur diese 25 Möglichkeiten prüfen. Verwendet der Sender jedoch den allgemeineren Substitutions-Algorithmus, bei dem das Geheimtextalphabet eine beliebige Neuanordnung des Klartextalphabets sein kann, dann gibt es 400 000 000 000 000 000 000 000 000 mögliche Schlüssel, aus denen er wählen kann. Fängt der Gegner die Nachricht ab und kennt den Algorithmus, dann steht er immer noch vor der überwältigenden Aufgabe, alle möglichen Schlüssel durchzuprobieren. Könnte ein gegnerischer Agent jede Sekunde einen der 400 000 000 000 000 000 000 000 000 möglichen Schlüssel prüfen, würde er grob gerechnet die milliardenfache Lebensdauer des Universums benötigen, um sie alle zu testen und die Nachricht zu entschlüsseln.

Klartextalphabet	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
Geheimtextalphabet	J L P A W I Q B C T R Z Y D S K E G F X H U O N V M

Klartext	e t t u, b r u t u s ?
Geheimtext	W X X H, L G H X H F ?

Abbildung 5: Ein Beispiel für den Substitutions-Algorithmus, ein monoalphabetisches Verfahren, bei dem jeder Buchstabe des Klartexts durch einen anderen Buchstaben gemäß einem Schlüssel ersetzt wird. Dieser Schlüssel ist das Geheimtextalphabet.

Das Schöne an dieser Verschlüsselung ist, daß sie leicht anzuwenden ist und zugleich ein hohes Maß an Sicherheit gewährleistet. Für den Sender ist es einfach, den Schlüssel festzulegen, er muß nur die Reihenfolge der 26 Buchstaben im Geheimtextalphabet bestimmen. Und doch ist es für den Gegner praktisch unmöglich, mit der sogenannten Exhaustionsmethode, also buchstäblich bis zur Erschöpfung, alle möglichen Schlüssel durchzuprobieren. Wichtig ist, daß der Schlüssel einfach ist, weil Sender und Empfänger sich über den Schlüssel verständigen müssen, und je simpler er ist, desto geringer ist die Gefahr von Mißverständnissen.

Tatsächlich ist es möglich, einen noch einfacheren Schlüssel zu erzeugen, wenn der Sender bereit ist, eine leichte Verringerung der Zahl möglicher Schlüssel in Kauf zu nehmen. Anstatt die Buchstaben des Klartextalphabets einfach zufällig anzuordnen, wählt der Sender ein *Schlüsselwort* oder einen *Schlüsselsatz.* Wenn wir zum Beispiel »Julius Caesar« als Schlüsselwort nehmen, lassen wir im ersten Schritt die Wortzwischenräume und die wiederholten Buchstaben weg (JULISCAER). Dann verwenden wir das Wort als Beginn des Geheimtextalphabets. Die restliche Buchstabenfolge ist nichts weiter als ein verschobenes Alphabet, das dort beginnt, wo das Schlüsselwort endet, wobei die Buchstaben, die schon im Schlüsselwort vorkommen, weggelassen werden. Das Geheimtextalphabet würde daher wie folgt aussehen:

Klartextalphabet 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
Geheimtextalphabet J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

Dies hat den Vorteil, daß man sich das Schlüsselwort oder den Schlüsselsatz und damit das ganze Geheimtextalphabet leicht einprägen kann. Wenn der Sender das Geheimtextalphabet auf einem Blatt Papier aufbewahren muß, könnte es dem Gegner in die Hände fallen, dem dann alle Geheimbotschaften preisgegeben wären.

Diese Verbindung von Einfachheit und Stärke ließ das Substitutionsverfahren im ersten Jahrtausend zur Königin der Verschlüsselungskunst werden. Die Verschlüßler hatten ein Verfahren entwickelt, das den sicheren Nachrichtenverkehr gewährleistete, und weil man damit gute Erfahrungen machte, fehlte der Druck, etwas Besseres zu erfinden. Den Schwarzen Peter hatte man den Codebrechern zugeschoben, die versuchen mußten, diese Verschlüsselung zu knacken. Hatte ein Gegner überhaupt die Chance, eine chiffrierte Botschaft zu entschlüsseln? Viele Gelehrte der alten Zeit hielten die Substitution dank der gigantischen Zahl möglicher Schlüssel für unüberwindlich, und über die Jahrhunderte schien sich diese Annahme zu bestätigen. Allerdings sollten die Codebrecher schließlich doch einen Weg finden, der ihnen die erschöpfende Prüfung aller Schlüssel ersparte. Es würde nun nicht mehr Milliarden von Jahren dauern, bis eine Geheimschrift geknackt war, sondern ein paar Minuten. Der Durchbruch gelang im Orient und verdankte sich einer genialen Mischung aus Sprachwissenschaft, Statistik und religiöser Hingabe.