

Geheimschreibekunst

(Übersetzung von [Hedda Eulenberg](#), Erstveröffentlichung 1901 bei J.C.C.Brunns /Minden © [Thomas Eulenberg](#) 1999)

Da wir uns die Zeit nicht vorstellen können, in der sich nicht die Notwendigkeit oder zum mindesten der Wunsch herausgestellt hätte, von Individuum zu Individuum Nachrichten zu übermitteln, die sich dem Verständnis der anderen entzogen, dürfen wir wohl annehmen, daß die Gepflogenheit, durch Geheimschriften miteinander zu verkehren, eine sehr alte ist. Die Behauptung, daß die Spartaner die Erfinder der Kryptographie gewesen seien, beruht also offenbar auf einem Irrtum. De la Guilletiere behauptet, die scytala bedeute den Ursprung dieser Kunst, sie ist aber nur als das früheste Beispiel ihrer Anwendung anzuführen. Die scytalae bestanden aus zwei in jeder Hinsicht genau gleichen Zylindern. Wenn der Anführer eines Heeres in den Kampf hinauszog, empfing er von den Ephoren einen dieser Zylinder, während der andere in ihrem Besitze blieb. Wenn nun eine der Parteien der anderen etwas mitzuteilen hatte, wurde ein schmaler Pergamentstreifen so um den Zylinder gewunden, daß sich seine Ränder ganz genau aneinander anschlossen. Dann wurde das Papier der Länge nach beschrieben, wieder abgerollt und verschickt. Wurde die Botschaft nun auch aufgefangen, so war sie doch niemandem verständlich. Erreichte sie glücklich ihren Bestimmungsort, so brauchte der Benachrichtigte den Streifen nur um seinen Zylinder zu wickeln und konnte die Inschrift entziffern. Daß die Kenntnis gerade dieser Art von Kryptographie bis auf uns gekommen, ist wohl nur dem Umstände zu verdanken, daß sie bei geschichtlichen Ereignissen angewendet wurde. Ähnliche Mittel geheimen schriftlichen Verkehrs sind gewiß fast zu gleicher Zeit mit dem Briefschreiben überhaupt entdeckt worden. Beiläufig sei hier bemerkt, daß in keiner der unseren Gegenstand betreffenden Abhandlungen, die mir zu Gesicht gekommen sind, jemals von einer anderen als einer zufälligen Lösung durch eben die passende scytala die Rede gewesen ist. Und doch wäre in allen Fällen eine Entzifferung mit absoluter Sicherheit zu bewerkstelligen gewesen. Man muß, ist ein Pergamentstreifen aufgefangen worden, sich einen verhältnismäßig sehr langen – sagen wir einmal sechs Fuß langen – Kegel herstellen, dessen Umfang an der Basis wenigstens der Länge des Streifens gleichkommt. Nun rollt man denselben unten nahe an der Basis um den Kegel, so daß sich Rand dicht an Rand schließt, wie es oben beschrieben ist; dann immer fest Rand an Rand und den Streifen fest auf den Kegel drückend, führt man ihn langsam bis zur Spitze hinauf. Auf diesem Wege werden einige der Wörter, Silben oder Buchstaben, deren Verbindung bezweckt ist, gewiß zusammenkommen – an dem Punkte des Kegels nämlich, dessen Durchmesser dem der scytala, auf welcher die Nachricht geschrieben worden ist, gleichkommt, und da von der Basis des Kegels bis zu seiner Spitze alle möglichen Durchmesser vorhanden sind, ist ein Mißlingen ausgeschlossen. Hat man so den Umfang der scytala festgestellt, ist es ein leichtes, sich eine solche zu verschaffen und die Schrift in aller Ruhe zu lesen. Es werden sich nun wenige überzeugen lassen, daß es gar nicht so einfach ist, eine Geheimschrift zu erfinden, deren Auflösung dem Unberufenen unmöglich ist. Und doch darf man rundweg versichern, daß der menschliche Scharfsinn keine Geheimschrift ersinnen kann, die menschlicher Scharfsinn nicht auch zu lesen vermöchte. Die Schwierigkeit jedoch, die das Entziffern solch einer Schrift bereitet, ist je nach der besonderen Veranlagung des Lösenden außerordentlich verschieden. Von zwei Personen, deren geistige Kraft sich bei anderer Gelegenheit als durchaus gleich herausgestellt hat, kann die eine unter Umständen nicht die allereinfachste Chiffre lesen, während die andere die allerverwickeltste schnell entziffert. Hier haben nämlich die analytischen Fähigkeiten des Menschen hauptsächlich zu wirken; es wäre deshalb gar nicht so unangebracht, die Lösung von Geheimschriften in den Lehrplan unserer Hochschulen aufzunehmen, um der wichtigsten aller Geisteskräfte Spielraum zur Entfaltung zu geben. Kämen zwei Personen, die gar keine Übung im Geheimschreiben hätten, auf den Gedanken, sich Mitteilungen zukommen zu lassen, die nur ihnen verständlich wären, so würden sie wahrscheinlich zuallererst daran denken, sich ein besonderes Alphabet, zu dem jeder von ihnen den Schlüssel haben sollte, zu machen. Sie könnten zuerst übereinkommen: a sollte für z, b für y, c für x, d für w und so weiter stehen, das heißt, sie würden die Reihenfolge der Buchstaben umkehren. Da ihnen aber bei längerem Nachdenken dies Vorgehen als zu durchsichtig erscheinen wird, werden sie vielleicht nach etwas Komplizierterem suchen. Sie schreiben die ersten dreizehn Buchstaben des Alphabets unter die letzten dreizehn:

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

so daß a für n und n für a, b für o und o für b steht. Da diese Regelmäßigkeit aber auch noch zu leicht herausgefunden werden möchte, könnte man sich auch ein ganz durcheinandergeschütteltes Alphabet herstellen, zum Beispiel:

a	stände für p
b	x
c	u
d	o etc.

Viele Briefschreiber würden sich nun nach dieser Übereinkunft ganz sicher fühlen und erstaunt sein, wenn ein Geheimschriftenleser den Schlüssel zu ihrem Alphabet im Handumdrehen finden würde. Vorsichtigere würden an Stelle unserer gewöhnlichen Schriftzeichen überhaupt andere, selbst zu wählende, setzen:

(könnte a heißen
.	b
:	c
;	d
)	e etc

Ein mit derartigen Zeichen geschriebener Brief würde gewiß ganz unentzifferbar aussehen. Wem aber auch dies noch nicht genügende Sicherheit böte, käme vielleicht auf die Idee, sich eines stetig wechselnden Alphabetes zu bedienen, und könnte es sich folgendermaßen herstellen. Er nimmt zwei kreisrunde Scheiben Pappdeckel, von denen eine einen halben Zoll im Durchmesser kleiner ist als die andere. Der Mittelpunkt der kleineren wird auf den Mittelpunkt der größeren gelegt und einen Augenblick dort festgehalten. Dann zieht er von dem gemeinsamen Mittelpunkt Radien über die Umrißlinien des kleinen Kreises bis zur Umrißlinie des großen. Im ganzen sollen es sechsundzwanzig Radien sein, die jeden Kreis in sechsundzwanzig Flächen einteilen. Auf jede der Flächen des unteren Kreises schreibt er einen Buchstaben des Alphabetes und zwar je willkürlicher durcheinander um so besser. Dasselbe geschieht mit dem oberen Kreise. Nun steckt er eine Nadel durch das gemeinsame Zentrum und versetzt den oberen Kreis in Drehung, während der untere unbeweglich bleibt. Darauf hemmt er die Drehung des oberen Kreises wieder und liest das Ergebnis, das heißt: für a nimmt er den Buchstaben, der in dem Teil des kleineren Kreises steht, der sich mit dem mit a bezeichneten des größeren deckt, für b den Buchstaben, der im kleinen Kreis über der mit b bezeichneten Abteilung des großen steht, etc. Damit die Person, für die der Brief geschrieben ist, denselben lesen kann, muß sie ebenfalls zwei der eben beschriebenen Pappdeckelkreise besitzen und wissen, welche beiden Buchstaben sich auf dem oberen und unteren Kreise gerade deckten, als ihr Korrespondent die Chiffre schrieb. Dies letztere erfährt sie durch die beiden Anfangsbuchstaben des Briefes, die als Schlüssel dienen. Beginnt das Schreiben mit a m, so schließt daraus, daß sie, wenn seine beiden Kreise so legt, daß diese beiden Buchstaben übereinander stehen, das angewandte Alphabet erhält. Auf den ersten Blick möchte es scheinen, diese verzwickte Art und Weise, eine Geheimschrift zu verfertigen, böte absolute Gewähr für ihre Unlesbarkeit durch Dritte und als sei es ganz unmöglich, ein Rätsel zu raten, dessen Lösung auf so vielfach gewundenen Wegen versteckt wurde. Für manchen böte es allerdings große Schwierigkeit; anderen jedoch macht die Entwirrung solcher Dinge fast gar keine Mühe. Der Leser mache sich nun klar, daß die Grundlage dieser ganzen Kunst in den allgemeinen Prinzipien der Bildung der Sprache zu finden und deshalb von den Gesetzen, nach denen die Bildung der Geheimschrift und ihres Schlüssels geschah, gänzlich unabhängig ist. Die Schwierigkeit, ein Kryptogramm zu lesen, steht durchaus nicht immer im Verhältnis zu der Mühe und dem Scharfsinn, den seine Zusammenstellung erfordert hat. Man hat gewiß bemerkt, daß bei den eben erwähnten Methoden, ein Kryptogramm zu verfassen, diese von Fall zu Fall verzwickter wurden. Doch ist diese Verzwicktheit nur eine scheinbare, sie hat für die Lösung des Rätsels keinerlei Bedeutung; die letzterwähnte Art und Weise macht das Lesen nicht im geringsten schwerer als die erste einfachste.

In einer vor achtzehn Monaten in einer hiesigen Wochenschrift erschienenen Abhandlung über einen ähnlichen Gegenstand sprach der Schreiber dieses Artikels über die starre Methode, nach der sich alle Formen des Denkens äußern, sprach von den Vorteilen, die diese gewährt, und daß selbst die anscheinend rein der Phantasie entsprungenen Vorgänge sich nach ihren Gesetzen vollziehen – also auch die Auflösung von Geheimschriften. Er wagte damals die Behauptung, jedes nach der oben erklärten Art und Weise zusammengestellte Kryptogramm lesen zu können und erregte damit ganz unerwarteterweise das größte Interesse bei dem ausgebreiteten Leserkreise des Blattes. Aus allen Teilen des Landes liefen Briefe bei dem Herausgeber ein, und viele der Schreiber waren so überzeugt von der Unlesbarkeit ihrer Geheimschriften, daß sie ihn gar zu gern zu Wetten überredet haben würden. Dabei machten sie sich nicht allzuviel Skrupel, bei der Verfassung ihrer Schriften die oben bezeichneten Grenzen zu überschreiten. Sie hatten sich fremder Sprachen bedient; einzelne Wörter und Sätze bunt durcheinander gemischt; in demselben Kryptogramm mehrere Alphabete angewandt. Ein Herr schickte gar ein Rätsel ein, das er in Krähenfüßen niedergeschrieben hatte, derengleichen in der wildesten Typographie der Redaktion nicht wiederzufinden war, und bei dem er sich sieben verschiedener Alphabete bedient hatte, ohne zwischen den Buchstaben oder zwischen den Zeilen Zwischenräume zu lassen. Von den ungefähr hundert eingelaufenen Geheimschriften gelang uns nur die Lösung einer einzigen nicht sofort, bald jedoch stellten wir sie als eine Täuschung klar – das heißt, wir bewiesen, daß sie ein Kauderwelsch zufällig zusammengestellter Buchstaben war, die absolut keinen Sinn ergaben. Den Einsender der Schrift aus sieben Alphabeten verblüfften wir zu unserem Vergnügen aufs höchste durch eine schnelle und völlige Lösung.

Die erwähnte Wochenschrift beschäftigte sich ein paar Monate lang also mit dem Entziffern der Kryptogramme, die uns aus allen Teilen des Landes zugeschickt wurden. Mit Ausnahme der Verfasser derselben aber hielt wohl kaum einer der Leser der Zeitschrift die ganze Angelegenheit für etwas anderes als für einen verwegenen Schwindel; das heißt, niemand glaubte wirklich an die Authentizität der Antworten. Eine Partei behauptete, die geheimnisvollen Zeichen seien erfunden, um die Zeitung auffällig und interessant erscheinen zu lassen. Anderen schien es wahrscheinlich, daß wir die Geheimschriften nicht nur lösten, sondern sie auch selbst zusammenstellten und so die Lösung selbstverständlich machten. Der Schreiber dieses Artikels jedoch nimmt hier noch einmal die Gelegenheit wahr, um ausdrücklich zu behaupten und in seinem eigenen Namen zu erklären, daß die Geheimschriften in gutem Glauben von Freunden des Blattes eingeschickt und von ihm durchaus selbständig gelöst worden sind.

Eine sehr gewöhnliche aber allzuleicht lösbare Art von Geheimschriften ist auch die folgende: Eine Karte wird in unregelmäßigen Zwischenräumen mit länglichen Löchern, die ungefähr den Platz für gewöhnliche dreisilbige Worte einnehmen, versehen und eine zweite ganz gleiche hergestellt. Jede der Parteien, die miteinander korrespondieren wollen, ist im Besitze einer solchen Karte. Wenn nun ein Brief geschrieben werden soll, wird diese Schlüsselkarte auf das Briefpapier gelegt und die mitzuteilenden Worte werden in die leeren Räume geschrieben. Dann entfernt man die Karte und füllt die leeren Stellen in dem Briefe derartig aus, daß er einen ganz anderen Sinn bekommt. Wenn das Schreiben an seinem Bestimmungsorte angekommen ist, braucht der Empfänger nur seine Karte auf dasselbe zu legen, die überflüssigen Worte werden bedeckt, und er kann den beabsichtigten Sinn schnell herauslesen. Das gewichtigste Bedenken gegen diese Art Geheimschrift ist aber die Schwierigkeit, die leeren Stellen im Briefe so auszufüllen, daß das Ganze einen ungezwungenen Eindruck macht, sowohl was den Sinn als auch die Handschrift angeht. Einem gewieften Beobachter wird der Unterschied in der Schrift allerdings nie entgehen.

Zuweilen auch bedient man sich eines ganzen Kartenspiels, um sich eine Botschaft im geheimen zu überbringen. Die Parteien werden sich zum Beispiel über die besondere Lage der einzelnen Karten einig. Sie kommen zum Beispiel überein, daß zu Anfang der Schrift die Aufeinanderfolge der Buchstaben durch den Wert der Karte bestimmt werden soll. Zuerst kommen alle Piks, dann die Herzen, dann die Karos, dann die Treffs. Nun schreibt der Schreiber auf die erste Karte den ersten Buchstaben, auf die zweite den zweiten und so weiter, bis er auf alle Karten und somit zweiundfünfzig Buchstaben geschrieben hat. Nun wirft er die Karten nach einem bestimmten Plane, über den er sich mit dem Empfänger geeinigt hat, durcheinander. Er nimmt zum Beispiel die drei untersten Karten und legt sie nach oben – dann die oberste und legt sie zu unterst und so fort eine gegebene Anzahl mal weiter. Dann schreibt er wieder zweiundfünfzig Buchstaben, auf jede folgende Karte einen, und so fort, bis sein Brief geschrieben ist. Wenn sein Korrespondent das Spiel Karten nun erhält, hat er die einzelnen nach dem Übereinkommen zu legen und liest die ersten zweiundfünfzig Buchstaben der Mitteilung. Dann wirft er die Karten, wie verabredet, zur zweiten Lesung durcheinander, liest die weiteren zweiundfünfzig Buchstaben und so weiter bis zum Schluß. Der schwerste Einwand gegen diese Art Geheimschrift liegt in der Tatsache, daß die Übersendung eines Spieles Karten von einer Partei an eine andere gewiß Argwohn erregt; es ist aber viel sicherer, eine Geheimschrift so zu versenden, daß sie nicht als solche erkannt wird, als viel Zeit damit zu verschwenden, sie für den Fall, daß sie aufgefangen werde, möglichst unlösbar zu gestalten. Die Erfahrung hat übrigens gelehrt, daß das scharfsinnigst zusammengestellte Kryptogramm, sobald es erst als solches erkannt worden, gelöst werden kann und wird.

Eine ungewöhnlich sichere Art und Weise, sich geheim Mitteilungen zu machen, ist die folgende. Beide Parteien müssen sich in den Besitz derselben Ausgabe eines Buches setzen – je seltener Ausgabe und Buch ist, desto besser. Das Kryptogramm besteht in diesem Falle nur aus Zahlen, die sich auf die Stellung von Buchstaben in dem Bande beziehen. Eine Nachricht beginnt zum Beispiel: 121-6-8. Der Empfänger schlägt nun Seite 121 seines Bandes auf und sucht den sechsten Buchstaben vom linken Rande der achten Zeile von oben. Mit diesem Buchstaben beginnt der Brief und so weiter. Dies Vorgehen ist sehr sicher, doch ist es möglich, auch

den Sinn dieses Kryptogramms zu entziffern, und diese Art und Weise ist auch deshalb weniger zu empfehlen, weil zu ihrer Lösung, selbst wenn man sich im Besitze des Schlüssels befindet, ein großer Zeitaufwand erforderlich ist.

Man muß nicht annehmen, daß die Kryptographie als ernsthaftes Mittel, sich Botschaften zu übermitteln, in unseren Tagen aus dem Gebrauch gekommen sei. In der Diplomatie bedient man sich ihrer noch immer und es gibt Personen im Dienste verschiedener fremder Mächte, deren Geschäft es ist, derartige Geheimschriften zu entziffern. Wir haben schon gesagt, daß bei der Lösung kryptographischer Probleme ganz besondere Fähigkeiten des Geistes in Aktion treten, besonders bei jedem verwickelteren Kryptogramm. Gute Geheimschriftleser sind sehr selten, und ihre Dienste werden, wenn auch selten verlangt, so doch gut honoriert.

Ein Beispiel für die Anwendung von Geheimschriften in neuerer Zeit ist in dem kürzlich erschienenen Werke: »Sketches of Conspicuous Living Characters of France« zu finden. Dort wird erwähnt, daß die Herzogin de Berri den Legitimisten von Paris ein langes Kryptogramm sandte, um sie von ihrer Ankunft zu benachrichtigen, dessen Schlüssel zu geben sie aber vergessen hatte. »Der durchdringende Geist Berryers«, sagt der Biograph, »entdeckte ihn aber bald.« Es war die für die vierundzwanzig Buchstaben des Alphabets stehende Phrase: Le gouvernement provisoire.

Die Behauptung, daß Berryer bald den Schlüssel entdeckte, beweist nur, daß der Schriftsteller gar keine Ahnung von der Beschaffenheit eines Kryptogramms hat. Monsieur Berryer hat gewiß den Schlüssel gefunden, aber nur, um seine Neugierde zu befriedigen, nachdem er das Rätsel bereits geraten hatte. Beim Entziffern konnte er noch gar nicht im Besitze des Schlüssels sein.

In einer in der Aprilnummer dieses Blattes erschienenen Notiz über das Buch sprachen wir folgendermaßen darüber:

Die Phrase »Le gouvernement provisoire« ist französisch und das Kryptogramm war für Franzosen bestimmt. Man kann wohl annehmen, daß die Schwierigkeit, die Schrift zu entziffern, größer gewesen, wenn der Schlüssel aus Bestandteilen einer fremden Sprache gebildet worden wäre. Wir fordern jedoch jeden, der sich die Mühe nehmen will, auf, uns eine Geheimschrift zuzusenden, deren Schlüssel aus dem Französischen, Italienischen, Spanischen, Deutschen, Lateinischen oder Griechischen (oder aus einem beliebigen Dialekt dieser Sprachen) genommen ist und wir geben unser Wort, daß es uns gelingen wird, das Rätsel zu lösen. Auf diesen Aufruf erhielten wir nur eine Antwort, die in dem folgenden Briefe enthalten ist. Das einzige, das wir an demselben auszusetzen haben, ist die Tatsache, daß uns der Schreiber nicht seinen Namen ganz mitgeteilt hat. Wir bitten ihn, dies noch recht bald zu tun, damit wir nicht wieder in den Verdacht geraten, unsere Kryptogramme selbst zu verfertigen. Der Poststempel des Briefes ist: Stonington, Coun.

An den Herausgeber von Grahams Magazine.

Sehr geehrter Herr!

In der Aprilnummer Ihrer Zeitschrift laden Sie anläßlich einer Besprechung von Mr. Walshs Übersetzung »Sketches of Conspicuous Living Characters of France« Ihre Leser ein, Ihnen eine Geheimschrift zuzuschicken, deren Schlüssel der französischen, lateinischen oder griechischen Sprache entlehnt sein dürfe und gaben Ihr Wort, daß Sie imstande sein würden, sie zu lösen. Da verschiedene Ihrer Anmerkungen mein Interesse erregten, stellte ich zu meinem Vergnügen folgende beiden Schriften zusammen. Der Schlüssel der ersten ist der englischen, der der zweiten der lateinischen Sprache entnommen. Da ich aus der Mainummer Ihres Blattes nicht entnehmen, daß irgendeiner Ihrer Leser Ihrem Aufruf Folge geleistet hat, nehme ich mir die Freiheit, Ihnen die beiden Chiffren zuzusenden, an denen Sie, wenn Sie es der Mühe wert erachten, Ihren Scharfsinn erproben können. Hochachtungsvoll ergebenst

S.D.L

Nr. 1.

Cauhiif aud ftd sdtfirf ithot tacd wdde rdchfdr tiu fuaefshfftheo fdoudf hetiusafhie tuis ied herhchriai fi aeiftdu wn sdaef it iuhftheo hiidohwid fi aen deodsf ths tiu itis hf iaf iuhoheaim rdff hedr; aer ftd auf it ftif fdoudfin oissiehoaftheo hefdiihodeod taf wdde odeduaiin fdusdr ounsfiouastn. Saen fsdohdf it fdoudf iuhftheo idud weiie fi ftd aeohdeff; fisdfhsdf a fiacdf tdar iaf ftacdr aer ftd ouiiie iuhffde isie ihft fisd herdihwid oiiiuiheo tiuhr, atfdu ithot ftd tahu wdheo sdushffdr fi ouii aoahe hetiusafhie oiiir wd fuaefshffdr ihft ihffid raeodu ftaf rhfoicdun iiiir defid iefhi ftd aswiiafinn, dshiffid fatdin udaotdr hff rdffheafie. Ounsfiouastn tiidcdu siud suisduin dswuaodf ftifd sirdf it iuhftheo ithot aud uderdudr idohwid iein wn sdaef it fisd desiaefiun wdn ithot sawdf weiie ftd udai fhoehthoafhie it ftd ohstduf dssiindr fi hff siffdffiu.

Nr. 2.

Ofoiioiiaso ortsiir sov eodisoioe af duiostifoi ft iftvi si tri oistoiv oiniafetsorit ifeov rsri afotiiiiv ridliot irio rivvio eovit atrotfetsoria aiortiti iitri tf, oitovin tri aetifei ioreitit sov usttoi oioittstifo dfti afdooitior trso ifeov tri dfit otftfeov softriedi ft oistoiv oriofiforiti suitteii viireiititfioi ft tri iarfoisiti iiti trir uet otiiotiv uitf ti rid io tri eoviiieiiiv rfasueostr ft rii dftrit tfoeei.

Die Lösung der ersten Geheimschrift machte uns nicht mehr als durchschnittliche Mühe. Die zweite stellte sich als außerordentlich schwer heraus, und nur mit Aufbietung aller Kräfte gelang es uns, sie überhaupt zu lesen. Die erste bedeutet:

Various are the methods which have been devised for transmitting secret information from one individual to another by means of writing, illegible to any except him for whom it was originally destined; and the art of

thus secretly communicating intelligence has been generally termed cryptography. Many species of secret writing were known to the ancients. Sometimes a slave's head was shaved and the crown written upon with some indelible colouring fluid; after which the hair being permitted to grow again information could be transmitted with little danger that discovery would ensue until the ambulatory epistle savely reached its destination. Cryptography, however pure, properly embraces those modes of writing which are rendered legible only by means of some explanatory key which makes known the real signification of the ciphers employed to its possessor.

Der Schlüssel zu diesem Kryptogramm ist:

A word to the wise is sufficient.

Der Schlüssel zu diesem Kryptogramm lautet zu deutsch:

Dem Weisen genügt ein Wort.

Man hat verschiedene Methoden erfunden, um von einer Person zur anderen geheime Schriften zu überbringen, die für niemand anderen als für die zum Empfang bestimmte lesbar waren; die Kunst, solch geheime Botschaften anfertigen zu können, ist gewöhnlich Kryptographie genannt worden. Den Alten waren viele Arten von Geheimschriften bekannt. Manchmal wurde ein Sklave geschoren und sein Kopf mit irgendeiner unauslöschlichen farbigen Flüssigkeit beschrieben. Dann ließ man das Haar wieder wachsen und konnte den wandelnden Brief verschicken, ohne fürchten zu müssen, daß er vor seinem Bestimmungsorte aufgefangen werde. Zur eigentlichen Kryptographie jedoch gehören nur die Schriften, die mittels eines erklärenden Schlüssels, der die wirkliche Bedeutung der Chiffren dem Empfänger bekannt macht, lesbar sind.

Die zweite Chiffre bedeutet:

Nonsensical phrases and unmeaning combinations of words as the learned lexicographer would have confessed himself when hidden under cryptographic ciphers serve to perplex the curious enquirer, and baffle penetration more completely than would the most profound apothegms of learned philosophers. Abstruse disquisitions of the scholiasts were they but presented before him in the undisguised vocabulary of his mother tongue –

Zu deutsch:

Sinnlose Phrasen und bedeutungslose Wortverbindungen dienen, wenn sie unter Geheimchiffren verborgen sind, wie der gelehrte Lexicograph selbst zugeben wird, mehr dazu, den neugierigen Entzifferer zu verblüffen und seinen Scharfsinn zu äffen, als die tiefsten Lehrsprüche der Philosophen. Kämen ihm die widersinnigsten Erörterungen der Scholastiker in dem unverkleideten Vokabular seiner Muttersprache vor die Augen –

Der letzte Satz ist also abgebrochen. Das d ist wohl irrtümlicherweise statt l in das Wort perplex gekommen.

Der Schlüssel zu dieser Chiffre heißt:

Suaviter in modo, fortiter in re.

Im gewöhnlichen Kryptogramm wird, wie wir bei dem eben erwähnten gesehen haben, ein künstliches, selbst bestimmtes Alphabet Buchstabe für Buchstabe für das natürliche allbekannte gebraucht. Zum Beispiel: zwei Parteien wünschen einen geheimen schriftlichen Verkehr und kommen überein, daß

(stehen soll für	a
)		b
-		c
*		d
;		e
:		f
?		i und j
!		k
&		l
o		m

'		n
+		o
#		p
,		q
%		r
]		s
[t
£		u und v
§		w
~		x
i		y
@		z

Nun soll die folgende Nachricht übermittelt werden:

»We must see you immediately upon a matter of great importance. Plots have been discovered and the conspirators are in our hands. Hasten!«

»Wir müssen Sie sofort in einer sehr wichtigen Angelegenheit sprechen. Verschwörer sind in unseren Händen. Eilen Sie!«

Diese Worte würden also so aussehen:

§ . O £] [] . . i + £ ? O O . * ?) [. & i £ # + ') O) [[. % + ' ; % .) [? O # + % [) ' . # & + [] :) £ . (. . ' * .] - + £ . % . *) ' * [: . - + '] # ? %) [+ %]) % . ? ' + £ % :) ' *] :] [. ' .

Dies sieht gewiß außerordentlich verzwickelt aus und wird von jedem, der in der Kryptographie nicht bewandert ist, für sehr schwer lesbar gehalten werden. Man sieht jedoch, daß a niemals durch ein anderes Zeichen als) , b niemals anders als durch (ausgedrückt worden ist und so weiter. Wenn man nun durch Zufall oder auf anderem Wege einen dieser Buchstaben errät, hat man einen großen Schritt zur Lösung der Chiffre gemacht und die Erklärung für alle gleichen Zeichen der ganzen Schrift.

Die Kryptogramme jedoch, die uns von unserem Korrespondenten aus Stonington geschickt worden sind, und die nach denselben Prinzipien wie das von Berryer entzifferte abgefaßt waren, boten dem Entzifferer diesen Vorteil nicht.

Wenden wir uns jetzt dem zweiten Rätsel zu. Der Schlüssel heißt:

Suaviter in modo

fortiter in re.

Wir wollen nun das Alphabet unter diesen Satz setzen:

s	u	a	v	i	t	e	r	i	n	m	o	d	o	f	o	r	t	i	t	e	r	i	n	r	e
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

Es steht also

a	für	c	
---	-----	---	--

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

n kann also eine doppelte, e, o, t eine dreifache, i, r eine vierfache Bedeutung haben. Dreizehn Buchstaben stehen für das ganze Alphabet. Es liegt also an diesem speziellen Schlüssel, daß die zu ihm passende Chiffre wie ein Gemengsel der Buchstaben e o t r und i aussieht. Der letzte Buchstabe herrscht sogar ganz besonders vor, da er zufällig für die beiden Charaktere steht, die in den meisten Sprachen am öftesten vorkommen, für e und i. Wenn ein derartig geschriebener Brief aufgefangen wird und die Person, in deren Hände er gerät, den Schlüssel nicht kennt, so könnte sie, durch Raten vielleicht, auf den Gedanken kommen, ein gewisser Buchstabe, i zum Beispiel, bedeute e. Wenn sie nun aber das Kryptogramm daraufhin durchsähe, würde sie nur Widerlegungen dieser Meinung begegnen, weil das betreffende Zeichen sich an Orten befindet, an denen es unmöglich e bedeuten kann. Er könnte zum Beispiel verblüfft sehen, daß vier i für sich allein, ohne anderes Zeichen, ein Wort ausmachen. In diesem Falle können sie natürlich nicht immer e bedeuten. In unserem Falle würde das Wort wise so aussehen:

iiii

Das erkennen wir jetzt, da wir im Besitze des Schlüssels sind und fragen uns, wie wir ohne Schlüssel und ohne Kenntnis eines einzigen Buchstaben des Sinn des Wortes iiii hätten herausfinden können.

Doch weiter. Es wäre ganz leicht, sich einen Schlüssel zu konstruieren, bei dem ein Buchstabe für sieben, acht oder zehn des gewöhnlichen Alphabets gelte. Stellen wir uns dann einmal vor, das Wort iiiiiiiiii präsentierte sich in einem Kryptogramm einer Person, die nicht im Besitze des Schlüssels wäre, oder, wenn diese Annahme zu verblüffend ist, meinetwegen auch einer Person, die den Schlüssel hat, was soll sie mit einem Worte wie iiiiiiiiii anfangen? Jeder Leser kann sich nun vorstellen, wie zahlreich die Buchstabenverbindungen sind, die er aus diesen zehn i zusammenstellen kann. Und doch müßte der Korrespondent, wenn er nicht zufällig die richtige Bedeutung erriete, all diese Verbindungen niederschreiben, um zu dem richtigen Worte zu gelangen, und wenn er sie niedergeschrieben, stände er erst recht vor der Schwierigkeit, festzustellen, welches von diesen Wörtern nun das beabsichtigte gewesen.

Um diese Schwierigkeit beim Entziffern zu beheben und die Lösung des Rätsels doch für jeden anderen als den Besitzer des Schlüssels nicht zu erleichtern, müssen die beiden Parteien sich über eine gewisse Ordnung klar werden, in der die Zeichen, die mehr als einen Buchstaben des gewöhnlichen Alphabetes bedeuten, zu lesen sind. Sie können zum Beispiel übereinkommen, daß i, wenn es zum ersten Male in der Chiffre vorkommt, den Buchstaben im Alphabet, der sich mit dem ersten im Schlüssel deckt, bedeuten soll, beim zweiten Male mit dem zweiten und so weiter, so daß also die Stellung jedes Buchstaben in Verbindung mit ihm selbst seine wahre Bedeutung erkennen hilft.

Wir behaupten also, daß eine übereingekommene Ordnung der Art nötig ist, damit sich ein Kryptogramm nicht

selbst dem Besitzer des passenden Schlüssels als unleserlich erweise. Bei genauerem Nachsehen aber wird sich herausstellen, daß unser Korrespondent aus Stonington uns ein Kryptogramm zugesandt hat, in dem eine Ordnung überhaupt nicht beobachtet worden ist, in dem ein Buchstabe ganz nach Belieben bald für diesen, bald für jenen steht. Wenn nun auch jemand geneigt wäre, aus unserer Herausforderung im April halber einen Prahlers zu nennen, wird er doch zugeben müssen, daß wir mehr als das Versprochene vollbracht haben. Wenn wir das, was wir da sagten, auch nicht suaviter in modo aussprachen, haben wir es wenigstens fortiter in re getan.

Wir haben durchaus nicht versucht, in diesen flüchtigen Bemerkungen unseren Gegenstand zu erschöpfen, dazu wäre ein Folioband kaum ausreichend gewesen. Wir haben hier nur ein paar der gewöhnlichsten Arten der Geheimschrift erwähnt. Vor zweitausend Jahren schon spricht Aeneas Tacticus von zwanzig verschiedenen Methoden, und seit der Zeit hat der menschliche Scharfsinn diese Wissenschaft noch viel weiter ausgedehnt. Allen, die weitere Aufklärung über diesen Gegenstand wünschen, empfehle ich die eingehenden Abhandlungen von Trithemius, Cap. Porta, Vignere und P. Nicéron. Wer jedoch in diesen oder irgendwelchen anderen Werken nach Regeln zur Lösung von Kryptogrammen sucht, wird sehr enttäuscht werden. Außer einigen Winken über die allgemeine Struktur der Sprache und einigen eingehenden Übungen zu ihrer praktischen Anwendung wird er keine anderen Erklärungen finden, als die ihm sein eigener Verstand vermittelt.