

Gertrud Maria Rösch

Von der magischen Schreibkunst zur Kryptographie

Johann Ludwig Klübers *Kryptographik* (1809)
im Kontext der Geheimschriften zwischen
dem 17. und dem 19. Jahrhundert

Geheimschrift und Verschlüsselung gehören zusammen, denn durch Verschlüsselung werden Geheimschriften erzeugt, und diese wiederum sind in vielen Fällen – das zeigt der erste Blick – Bilder! Um die Fragestellung zu verfolgen, wie in der Erzeugung von Geheimtexten Bild und Schrift sich gegenseitig berühren beziehungsweise hervorbringen, seien hier vor allem Zwischenformen von Bild und Schrift ausgebreitet, wie sie zwischen dem 17. und 19. Jahrhundert historisch bedeutsam waren.

1. Begriffsklärung: Steganographie und Kryptographie

Für die beiden Formen der Geheimschrift – Steganographie und Kryptographie – fallen die reichen Varianten ins Auge.¹ Die Steganographie ist bis zum 16. Jahrhundert der umfassendere Begriff und bezeichnet den Fall, in dem das Vorhandensein einer Botschaft zunächst einmal nur versteckt wird. Die Kryptographie dagegen braucht das Vorhandensein nicht zu verheimlichen, weil sie eine Nachricht unverständlich und damit für den Gegner unbrauchbar macht. Dabei wird die Nachricht in Geheimzeichen, also Chiffren, überführt beziehungsweise durch Zahlen oder durch Buchstabenkombinationen, die durch Transposition aus dem Alphabet gewonnen wurden, ausgedrückt. Beide Geheimschriften öffnen damit einen Weg für die Erzeugung von Bildern innerhalb dieser wechselseitigen Überführung von Buchstaben- in Zahlenkombinationen und umgekehrt.

Der Idee nach sind Steganographie und Kryptographie der Kabbala verpflichtet, denn aus ihr übernahmen die Steganographen die Chiffriertechniken, d. h. die planmäßige Er- beziehungsweise Versetzung von Buchstaben und Ziffern, um einen Text zu chiffrieren und damit unleserlich zu machen. Grundlegend sind die folgenden vier Verfahren: In der ersten und einfachen Form der Metathesis, der so genannten Transposition, werden Worte, Silben oder einzelne Buchstaben versetzt oder ein Wort rückwärts gelesen (*ordo*

1. Zum historischen Kontext und den beiden Formen der Geheimschrift vgl. auch Rösch 2004, S. 9–14, ebenso Strasser 2004.

conversus beziehungsweise *inversus*), um ein anderes Wort zu substituieren, aber die Buchstaben bleiben die selben. Anagramm und Palindrom (Beispiel: leben – nebel) sind die literarischen Äquivalente dieses Verfahrens.

Die zweite Form, die Gematria, verbindet Buchstaben und Zahlen, denn sie beruht auf der Tatsache, dass die hebräischen und griechischen Buchstaben zugleich Zahlen darstellen, so dass die *supputatio numeralis* oder *transmutatio arithmetica* gelingt. Für Kabbalisten hat jedes Wort damit auch einen Zahlenwert, der sich aus der Summe seiner Buchstaben ergibt; Wörter mit dem gleichen Zahlenwert weisen daher auf eine geheime Analogie der darin bezeichneten Dinge.

Ein drittes Verfahren, das Notarikon, markiert beliebige Buchstaben eines Wortes, die dann als Abkürzung für das ganze Wort stehen. So lassen sich Wortgruppen zu einem neuen Wort zusammenziehen, beliebige Buchstaben, häufig allerdings die Anfangs- oder Endbuchstaben, können so als ein anderes Wort gelesen werden. Es ist die dem Akrostichon zugrunde liegende Technik, die in Spätantike und Mittelalter als Figuren- und Gitterakrostik verbreitet war.

Die fortgeschrittenste und zukunftsweisende Form ist die Temurah, die *commutatio literalis*, die durch Permutation und Anagramm in einem ersten Schritt die Buchstaben vertauscht und in einem zweiten Schritt die umgestellten Zeichen ersetzt. Um eine Geheimschrift zu gewinnen, werden Alphabete verschoben und bilden so einen Vorrat von Zeichen, die das ursprüngliche, das Klartext-Alphabet, substituieren können.² Diese Transposition mit folgender Substitution bildet bis heute die Grundlage der neuzeitlichen Kryptologie, während Gematria und Notarikon zum Vorbild eines spielerisch-ästhetischen Umgangs mit der Sprache wurden.

2. Der Wandel der Kryptographie

1. Johannes Trithemius: Verschlüsselungsverfahren zwischen Magie und Kombinatorik

Steganographien dienten der Geheimhaltung diplomatischer und militärischer Angelegenheiten bis in die Epoche des Absolutismus hinein; ungeachtet dieser zentralen Funktion wurde ihnen vor 1700 vielfach ein hermetischer und mitunter forciert »mystischer« Ursprung beigelegt.

Ein häufig zitiertes Beispiel für diesen auf übernatürliche Mächte zurückgehenden Ursprung lieferte der Sponheimer Abt Johannes Trithemius (1462–1516). Er schlug eine Vielzahl von kryptographischen Systemen in

2 Zur Klärung der Begriffe: Geheimtext heißt im Folgenden der zu übermittelnde vertrauliche Text; Decktext heißt der Oberflächentext, der den geheimen verdeckt beziehungsweise verbirgt.

seiner Schrift vor: *Polygraphia libri sex*. Sie wurde 1518 in Basel gedruckt und stellte die Zeitgenossen vor Rätsel, weil sie die darin vorgeschlagenen Vorgehensweisen kaum nachvollziehen konnten. Seine zweite Schrift entstand zwischen dem Ende des Jahres 1498 und dem Frühjahr 1500 und erschien erst 1606 in Frankfurt unter dem Titel *Steganographia: Hoc est: Ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*.³ Das Werk wurde sofort indiziert (bis 1609), vor allem wegen der im ersten Teil aufgelisteten Beschwörungsformeln, mit denen Engel beziehungsweise Geister gezwungen werden können, bestimmte Botschaften bestimmten Personen zu überbringen.⁴

Weil er beide Techniken – die Steganographie und die Kryptographie – in diesem Buch beschrieb, steht Trithemius historisch am Beginn der Kryptographie; er nannte seine Technik »ars sine secreti latentis suspicione scribendi«,⁵ die Kunst, ein Geheimnis mitzuteilen, ohne den Verdacht zu erregen, hier werde etwas Verborgenes weitergegeben. Daher dient sie dem Übermitteln von Ideen und Nachrichten unter den Augen von Bewachern und argwöhnischen Beobachtern, denn eine steganographische Botschaft erscheint als »harmloser« Text oder als Bild, dessen verborgene Nachricht nur der Adressat zu lesen vermag.

Im zweiten Teil der *Steganographia* geht er über zu dem doppelten Verfahren aus Kryptographie und Steganographie. Auf einer Verschlüsselungsscheibe solle der Sender einer Botschaft seinen Text in eine Buchstabenfolge verwandeln und sie dann in einen lateinischen Text einbetten.

3 *Steganographia: Hoc est: Ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa. Authore reverendissimo et clarissimo viro, Joanne Trithemio, Abbate Spanhaimensi, & Magiae Naturalis Magistro perfectissimo. Praefixa est huic operi sua clavis, sev vera introductio ab ipso Authore concinnata; hactenus quidem a multis multum desiderata, sed a paucissimis visa: Nunc vero in gratiam secretioris Philosophiae Studiosorum publici iuris facta.* Frankfurt 1606, 2. Aufl. 1608. Für diesen Beitrag wurde die Ausgabe von 1621 herangezogen, die in Darmstadt erschien. Eine Abb. der Titelseite bei Shumaker 1982, S. 96. Abschriften des Buches kursierten hinfänglich in den hundert Jahren vor seiner Drucklegung.

4 Ein Beispiel ist die Übermittlung einer geheimen Botschaft durch einen lateinischen Gebetstext und die Beschwörungsformel *lamarton, anoyr*, mit der ein Geist zur Übermittlung der Botschaft gezwungen werden könne (vgl. Trithemius 1621, S. 3 f.); die Formel müsse mit dem Gesicht nach Osten gesprochen werden, damit der Empfänger die geheime Botschaft erhalte. Dazu Ernst 1996, S. 44–46; dort beschreibt er die Beschwörungen der Planetenengel, von denen Trithemius behauptet, mit ihrer Hilfe könne man eine Form geheimer und immaterieller Kommunikation erreichen.

5 Zitiert nach Bauer 1995, S. 5. Auf Bauers ausführliche Darstellung stützt sich die folgende Darlegung.

Ioannis Trithemij Abb, Spanh,

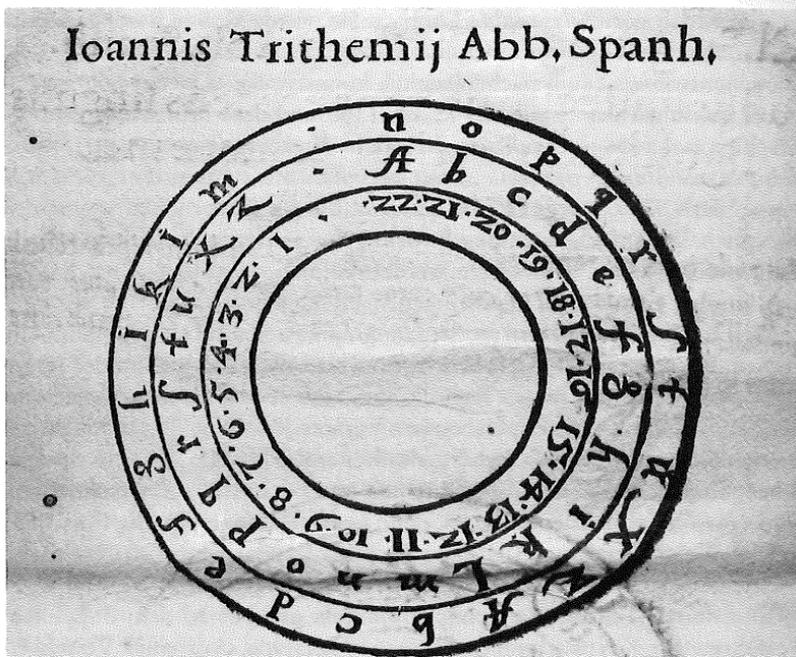


Abb. 1
Buchstaben-Ring aus Trithemius 1621. Das erste, äußerste Alphabet ist das Geheimalphabet (*literae significantes*), das zweite, innere Alphabet hingegen das Klaralphabet (*alphabetum planum*).

Rasch und ökonomisch lässt sich die Buchstabenverschiebung durch einen Buchstaben-Ring durchführen, auf dem das Klaralphabet mit einem Deckalphabet verbunden werden kann. Kryptologisch gesehen handelt es sich um eine monoalphabetische Verschlüsselung, d. h. einem Geheimalphabet wird nur ein einziges Deckalphabet zugeordnet (Abb. 1). Allerdings ist auf dem innersten Ring schon eine Zahlenreihe von eins bis zweiundzwanzig angegeben, so dass auch Ziffern die Buchstaben des Klaralphabets verschlüsseln könnten.

In einem nachfolgenden Beispiel erläutert er die Verschlüsselung mit diesem Chiffrierring. Der Geheimtext (*intentio mysteri*: Diese Bücher behalt bey dir heimlich.) werde nun durch die aus dem Geheimalphabet (*literae significantes*) genommene Buchstabenfolge verschlüsselt:

Q.r.h.r.o.k.p.v.r.g.o.r.v.n.a.i.o.x.q.g.x.v.r.x.b.a.x.p.v.v.

Diese kryptographisch über (eine monoalphabetische) Substitution ermittelte Buchstabenfolge wird nun steganographisch in einer christlichen

Lebensmaxime verborgen, dem Decktext also, wobei die Anfangsbuchstaben der Wörter jeweils die verschlüsselten Buchstaben darstellen:

»Quisque retinere humilitatis regulam optat catholica pietate vita recitundinem gubernet, oportet religiosum veritatis normam amplecti iugiter. Omnis Christianus qui Christi gloriam veraciter requirit Christi bonitatem amat Christianis pollet virtutibus. Vale.«⁶

2. Kryptographie im 17. Jahrhundert: *Diplomatie und Ars combinatoria*

Die bei Trithemius abgedruckten Ringe bilden die Vorläufer für die technisch versierteren Verschlüsselungsringe, die einen Hinweis auf die Wissenssysteme im 17. Jahrhundert liefern. Geheimschriften und Chiffrieralphabete galten als Bestandteil der allgemeinen Schreibkunst, mithin des Sekretärhandwerks. Diese zahlreiche Aspekte umfassende Schreibkunst war Thema in den *Mathematischen und Philosophischen Erquickungsstunden* von Georg Philipp Harsdörffer (1607–1658). Er sammelte im vierzehnten Teil eine ganze Reihe von »curiosen« Aufgaben, zu denen auch die Praktiken der technischen Steganographie gehörten.⁷ Auch die aus »der Ebreer Caba la« abgeleiteten anagrammatischen Spiele⁸ führte Harsdörffer an.

Wenngleich bei Harsdörffer die spielerischen Aspekte im Vordergrund standen, war Kryptographie weiterhin kein Teil der Ästhetik, sondern der Kanzleiwissenschaft und der Diplomatie.

3. Kryptographie im 18. Jahrhundert: *Alltägliche Praxis*

Während des ganzen 18. Jahrhunderts nimmt die Kryptographie ihren legitimen Platz in der politischen Wissenschaft ein. Sie hat sich von ihren geheimwissenschaftlichen Anfängen gelöst und gehört zur außenpolitischen Praxis der Staaten. In *Zedlers Universal-Lexikon* heißt es über die

»Schreibe-Kunst, (geheime) oder magische Schreibe-Kunst [...] wenn man durch Zeichen dasjenige, das man sagen will, zu verstecken sucht, damit es nicht ein ieder errathen kan. Diese verstehtet also niemand, als der den Schlüssel dazu hat, das ist, dem die Bedeutung eröffnet, oder

6 Geheimtext, kryptographischer und steganographischer Decktext, zit. nach Trithemius 1621, Anh. S. 63.

7 Dazu ausführlich Rösch 2004, S. 14–16.

8 Harsdörffer & Schwenter 1999, 2, S. 514. Beschrieben wird hier die anagrammatische oder transpositorische Metathesis der Kabbala.

Regeln, selbige zu entdecken, an die Hand gegeben worden, es wäre denn, dass einer die Kunst, verborgene Schreib-Arten zu eröffnen, besäße, welches sich aber wohl niemand wird rühmen können; weil man ja nach Belieben Characteres erwehlen kann, die ein anderer unmöglich versteht, wenn er nicht den Schlüssel dazu hat; oder es müssten die Zeichen so beschaffen seyn, dass ihre Bedeutung ohne Schlüssel sich heraus bringen liesse. [...] Man bedienet sich vornehmlich dieser geheimen Schreibe-Kunst in Kriegs- und Staats-Canzleyen, um Briefe zu schreiben, darinne solche Dinge enthalten, die niemand als der an den sie gerichtet, wissen soll. Die Characteres oder Ziffern, deren man sich dazu gebraucht, bestehen entweder aus verwechsellten Buchstaben, oder aus einem selbst erdichteten Alphabet, oder aus gewissen Ziffern und Zahlen, denen man die Bedeutung gewisser Buchstaben, Sylben oder gantzer Wörter giebet, solche in ein ordentliches Register verfasst, dass ein ieder eine Abschrift bey sich hat, welches Register der Schlüssel genennet wird.« (Zedler 1731–54, S. 1138 f.)⁹

Diese über das ganze 17. und 18. Jahrhundert hindurch anhaltende Aktualität der Kryptographik, die sich in Publikationen und historischen Abrissen niederschlug, belegt sehr anschaulich das Lehrbuch des Juristen Johann Ludwig Klüber (1809).¹⁰ Dessen nachdrückliches Plädoyer für praktikable Geheimschriften, die einfach anzuwenden und sicher vor schneller Auflösung sein müssten, lässt auf den anhaltenden Bedarf an diesen Techniken schließen.

Klüber war zugleich einer der wichtigen Diplomaten der Zeit; seine Kompetenz beruhte vor allem darauf, dass er zwei Rechtssysteme aus eigener Anschauung kannte und zum Teil mitgeprägt hatte. Er hatte zwischen 1780 und 1785 ein Studium der Rechte in Erlangen, Gießen und Leipzig absolviert, promovierte in Erlangen und wurde dort 1787 zum ordentlichen Professor ernannt, blieb aber nicht lange in dieser Position. 1804 berief ihn der Souverän des neu gegründeten Großherzogtums Baden (seit 1803 unter der Protektion Napoleons) in sein Kabinett und übertrug ihm zugleich die Erziehung des Erbprinzen; diesen begleitete er 1806 nach Paris, wo er die Adoptivtochter Napoleons, Stefanie, heiratete.¹¹

9 In dieser Definition ist der mystische Ursprung, wie er die Darlegungen von Trithemius durchzieht, bereits getilgt.

10 Klüber wurde geboren am 10. November 1762 in Tann (Rhön) und starb am 16. Februar 1837 in Frankfurt a. M., wo er auch begraben ist; zur Biographie vgl. Mager 1980.

11 Das neue Großherzogtum war politisch ein Vasallenstaat Napoleons und wurde nach französischem Muster organisiert. Dem Großherzog Karl Friedrich folgte 1811 sein Enkel Karl Ludwig Friedrich (1811–1818), der mit Napoleons Adoptivtochter Stephanie Beauharnais (1789–1860) vermählt

Auf die Bitte des damaligen preußischen Staatskanzlers, Karl August Freiherr von Hardenberg, nahm er am Wiener Kongress teil; von ihm erschienen die *Acten des Wiener Congresses* (8 Bde. und ein Nachtragsband 1835) wie auch eine Systematik des neuen Bundesrechts und des Staatsrechts seiner Mitgliedsstaaten (*Öffentliches Recht des Teutschen Bundes und der Bundesstaaten*, zuerst Frankfurt 1817, dann 1822, 3. Aufl. 1830, 4. Aufl. 1840) sowie ein europäisches Völkerrecht (*Droit des gens moderne de L'Europe*, 1819). Seine letzte Schrift galt dem neu gegründeten griechischen Staat.

Aus heutiger Sicht war er eine der »großen Leitfiguren des Vormärzliberalismus« (Schuck 1994, S. 93). Seine Aufgaben in der Politik verband er ohne Schwierigkeiten mit einer juristischen Professur in Heidelberg (seit 1807), wo er die *Kryptographik* verfasste, die also – das sollte der kurze Abriss seiner Laufbahn zeigen – von einem versierten Teilnehmer am zeitgenössischen politischen Leben stammte.

3.1 Chiffrieren und Dechiffrieren als Handbuchwissen

Im ganzen Buch beruft Klüber sich mehrfach auf seine Praxis und die Kenntnisse über die Verfahren der Kabinette und Generalstäbe, um die Notwendigkeit für eine zuverlässige Verschlüsselung zu beweisen. Dazu flocht er Schilderungen politischer Situationen ein, in denen geheimschriftliche Nachrichten und ihre erfolgreiche Verschlüsselung bedeutsam wurden. Der Band beginnt mit einer allgemeinen Theorie der Chiffrierkunst, handelt dann die steganographischen und kryptographischen Verfahren ab; er erklärt also zunächst einzelne Formen, die mit der Kryptographik verwandt sind: Brachygraphik, Stenographik, Tachygraphik, Okygraphik, Pasigraphik, Hieroglyphik, Telegraphik, dann die Fingersprache und Schiffsignalkunde. Insgesamt bietet sein Buch eine Übersicht der kryptographischen Praktiken, auch der historischen Erscheinungsformen, die er als obsolet und wirkungslos darstellt. Als Erfordernisse einer guten Geheimschrift zählte er auf: Einfachheit, geringe Mühe, Zuverlässigkeit und die Sicherheit des übermittelten Geheimnisses.

war. Er schloss sich nach der Schlacht bei Leipzig den Verbündeten an, bekam die Erhaltung der Souveränität und seines Gebiets zugesichert, trat 1815 in den Deutschen Bund ein, sicherte 1817 gesetzlich die Unteilbarkeit des Landes, ordnete die Erbfolge und gab seinem Land am 22. August 1818 eine Verfassung.

3.2 Sichere Verschlüsselungen für den politischen und privaten Gebrauch

Klüber bewertete die wichtigen Verschlüsselungen nach dem Grad ihrer Sicherheit und leichten Handhabe für den häufigen Gebrauch. Als zuverlässig referierte er die Transpositionschiffren, ob auf der Grundlage von Buchstaben oder Zahlen, und beschreibt detailliert die schon bei Trithemius zu findende Chiffrierscheibe (Klüber 1809, S. 165–168). Allerdings kritisiert er sie auch als leicht aufzulösende monoalphabetische Verschlüsselung (umso leichter zu entschlüsseln, wenn der Dechiffreur die Morphologie der gängigen Sprachen und die Häufigkeitsanalyse beherrscht). Sicherer sei die polyalphabetische beziehungsweise Vigenère-Verschlüsselung, die auf mehreren Alphabeten beruht, die nach den Vorgaben eines Schlüsselworts jeweils verwendet werden.

Insgesamt erstaunt die Menge der Verschlüsselungen jenseits der Vigenère-Verschlüsselung, die Klüber unter den ernstzunehmenden, d. h. sicheren Verfahren gelten ließ.

Zu ihnen gehörten die Gitterchiffre und die Linienschrift, die beide auf ihre Art graphische Gebilde erzeugen. Die Gitterchiffre ist der Steganographie zuzuordnen, denn der Decktext enthält den Geheimtext, der nur noch durch ein bestimmtes ›Gitter‹ herausgelesen werden muss (vgl. Abb. 2). Die Linienschrift gehört zu den Figuren- und Farbenchiffren, weil in dieser die Botschaft durch das beinahe abstrakt anmutende Liniengebilde übermittelt wird. Der Empfänger muss lediglich seinen Schlüssel, d. h. entweder das Gitter oder die konzentrischen Kreise mit den entsprechenden Buchstaben unterlegen, um die Linien zu verfolgen und die Buchstaben herauslesen zu können. Die Nachricht lautet in beiden Fällen: »est silentio merces« (vgl. Abb. 3). Die Buchchiffre besteht darin, auf einer gedruckten Seite eines Buches über Zahlen die Zeile, das Wort, die Silbe und den Buchstaben auf dieser Buchseite zu bezeichnen und damit die Buchstaben des Geheimworts zu chiffrieren.¹² Die Beschreibung einer Skytale ist ihm als »Lacedämonische Geheimschrift« eine Erwähnung wert und steht neben der Kartenchiffre (ebd., §§ 72–74, S. III–III3); beide beruhen sie auf dem Arrangement von Material, um eine Schrift sichtbar zu machen. Bei der Skytale ist es das umwickelte Band, bei den Spielkarten ist es deren Rand, der beschrieben wird, nachdem er mit einem Buchbinderhobel geglättet wurde. Nach dem Beschreiben

12 Beispiel einer Buchchiffre: 40, 6, 3, 1; dies würde aufgelöst heißen: »In Zeile 40 das sechste Wort, darin die dritte Silbe und der erste Buchstabe dieser Silbe«; vgl. Klüber 1809, § 219, S. 343 f.

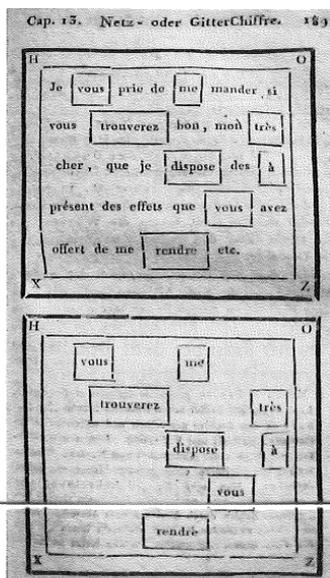


Abb. 2
Gitterchiffre aus Klüber 1809.

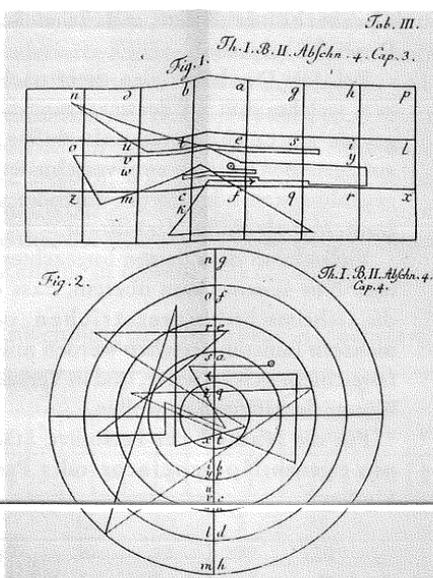


Abb. 3
Quadrat- oder Linienschiffre aus Klüber 1809.

vermischt der Sender das Kartenspiel, während der Empfänger es in der verabredeten Folge ordnet und die erscheinende Schrift liest.¹³

4. Johann Ludwig Klübers eigene Chiffriermethode

Mit großem Nachdruck kündigt Klüber eine von ihm selbst erfundene Methode als sehr sichere und mühelose Form des Chiffrierens an (ebd., §63 f.). Klübers Schlüssel beruht auf einer doppelten Kolumne von Wörtern, wie sie in Registern oder Taschenwörterbüchern zu finden ist. Sie hat viel gemeinsam mit der Wortchiffre, bei der tragende Wörter des Geheimtextes durch Deckwörter ersetzt werden und der Decktext durch bedeutungslose Wörter (»mots perdus«) vermehrt wird (ebd., §§54–62, S. 86–96):

»Jedes Wort, welches in dem Concept der Depesche vorkommt, und durch ein anderes Wort chiffriert werden soll, suche ich in dem Wörterbuche auf, und bediene mich desselben als eines chiffre chiffrant, indem ich das, demselben in der andern Columne gerade gegen-

¹³ Unter den sicheren Verschlüsselungen erscheint auch die Mnemonik, bei der ein Bote Bilder oder Zifferwörter auswendig hersagt, ohne ihren Sinn zu kennen; er kann daher auch kein Geheimnis verraten, sollte er gefangen werden, vgl. ebd., §262, S. 416f.

überstehende Wort, statt jenes ächten, als Geheimschrift in die Depesche schreibe.

Bei dem Dechiffriren dient nachher eben dieses Wort demjenigen, welches ihm auf der entgegengesetzten Columne derselben Seite gerade gegenübersteht, als *chiffre déchiffrant*. Also dienen zwei, auf derselben Seite, in zwei verschiedenen Columnen, einander gerade gegenüberstehende Wörter, einander wechselseitig als *chiffre chiffrent*, und als *chiffre déchiffrant*.

Vieles kann man dessen ungeachtet in Klarschrift (*en clair*) schreiben. Nur komme man überein, dass entweder die Klarschrift, oder die Geheimschrift unterstrichen, oder unterwärts mit einem oder mehrern Punkten versehen werden müsse, damit man bei dem Dechiffriren nicht sich verwirre, und in Versuchung gerathe, auch die ächten Wörter dechiffriren zu wollen.

Für die Namen der Personen, Städte, Staaten u. d. kann man einen eigenen Nomenclator oder *Passe-partout* verabreden.« (ebd., S. 98–99)

Als Praktiker gab er ein Beispiel einer solchen Tabelle und einer teilverschlüsselten Depesche (Klüber 1809, S. 100f.). In der Depesche bleiben die unterstrichenen Wörter als nicht sinntragend im Decktext stehen; die zentralen Begriffe sind jedoch nach einer Liste, die einem Wörterbuch entnommen sein könnte, ersetzt.

Geheimtext: »Le Ministre d'état et de cabinet Fabius a donné sa démission. Il est remplacé par Monsieur Aristides dont on sait qu'il favorise le parti grec.«

Decktext: »Le minéral débacler éteindre et de cabaner 564 abacot donné sa démonstratif illusion est rempoché paradis mont 1240 donjon on sait querelle il fauconnier le particulier 16.«

An dieser Stelle zog Klüber auch Beispiele aus der *Polygraphia* von Trithemius heran, in der dieser im ersten Teil 132 Wortalphabete aufgezeichnet hatte, bei denen ein Wort jeweils für einen Buchstaben des Geheimworts stand. Ein Beispiel eines solchen Buchstaben-Alphabets, das aus lauter Worten religiösen Inhalts bestand, führte er an und referierte kurz die Geschichte der *Polygraphia*, die gerade durch diese Alphabete, teils aus erfundenen und seltsam klingenden Wörtern, die man für die Namen von guten und bösen Geistern hielt, in den Verdacht eines ketzerischen Buches geraten war.

Erstaunlich bleibt in Klübers Repertoire die Variation und Doppelung von bekannten Codes, indem etwa eine Zahlen-Verschlüsselung durch eine weitere Zahlenoperation (Addition, Subtraktion, Multiplikation,

Division) noch einmal verschlüsselt wird. Ein Beispiel dafür ist die Notation der Zahlen als Brüche; dazu referierte Klüber die Methode, derer sich der französische Politiker und Publizist Honoré Gabriel de Riqueti, Graf von Mirabeau (1749–1791), bedient haben soll (Klüber 1809, § 50, S. 79 f.).

Dazu wird ein Alphabet willkürlich in fünf Gruppen von fünf Buchstaben aufgeteilt, die nummeriert werden, wie auch die Gruppen selbst nummeriert werden. Nun erscheint als der Zähler des Bruchs die Nummer der Buchstabengruppe, als der Nenner der Buchstabe; beide können durch »Non-valeurs« (bedeutungslose Zahlen, in diesem Fall die Zahlen von 6 bis o) vermehrt werden.

Nachfolgend ein Beispiel der Anwendung des »Mirabeau-Alphabets«:¹⁴

1					2					3					4					5				
c	f	g	u	z	x	a	m	o	k	s	e	h	n	q	d	l	y	q	w	n	i	r	t	v
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5

Decktext: $\frac{36}{44}$ $\frac{3}{72}$ $\frac{590}{840}$ $\frac{5}{29}$ $\frac{12}{30}$ $\frac{30}{92}$ $\frac{2}{290}$ $\frac{38}{120}$

Geheimtext: »Ne timeas«

4.1 Eine graphologische Vorläuferin der Chipkarte

Unter den historisch bedeutungsvollen Funktionen der Steganographie beschrieb Klüber eine graphologisch kunstvolle Vorläuferin einer Chipkarte, wie sie ihm aus der Regierung Ludwigs XVI. bekannt war. Dessen Außenminister, der Graf von Vergennes (1717–1787), hatte eine eigene Polzeischrift eingeführt, mit deren Hilfe Empfehlungskarten einreisender Fremder ausgestellt wurden. Nach außen hatten diese Karten das Ansehen von Visitenkarten, jedoch hatten die ausstellenden Agenten dazu Instruktionen für die Codierung bestimmter Angaben, so dass der Empfänger einer solchen Karte nicht wusste,

»dass er in seiner Empfehlungskarte, die in dem Aeussern den Visitenbillets ähnlich war, eine genaue Charakteristik seiner Persönlichkeit, vielleicht selbst einen Uriasbrief, offen trug. Kein Zug, kein Strich, kein Punct, keine Ziffer, keine Farbe, keine Figur war in dieser Karte ohne Bedeutung.« (ebd., S. 295)

Die Schlüssel zu diesem Chiffriersystem mussten sehr umfangreich sein, auch war das Billet nicht einfach auszustellen, wie die bei Klüber abgedruckten Beispiele zeigen (Abb. 4).

14 Das Beispiel findet sich bei Klüber 1809, S. 79 f., § 50.



Abb. 4
Polizeischrift nach dem Außenminister Vergennes in französischem Gebrauch aus Klüber 1809.

»Esquire de Gray 1) ein Engländer – denn die Farbe des Papiers ist gelb; 2) 35 Jahre alt – denn die Einfassung bildet ein Oval; 3) groß von Person – denn die Einfassungslinien stehen weit auseinander; 4) schön gewachsen – denn die Linien der Einfassung sind wellenförmig; 5) schön von Gesicht, aber ernsthaft – denn oben in der Einfassung ist eine Tulpe; 6) verheuratet – denn die Einfassung ist mit einem Bande umwunden; 7) sehr reich – denn auf dem Oval stehen zwölf Knöpfe; 8) er trägt eine Perücke – denn hinter dem Gesichtszeichen (der Tulpe) ragt eine Muschel hervor; 9) er reiset als Gelehrter, seine Kenntnisse zu erweitern – denn zwischen den Einfassungslinien stehen zwei kleine Ovale, oben auf beiden Seiten der Tulpe; 10) evangelisch (der A. C. V.) – denn hinter seinem Namen steht ein Semicolon; 11) besitzt viele Kenntnisse – denn unter seinem Namen steht das Schlusszeichen (liegende Klammer); 12) redlich – denn über dem Schlusszeichen stehen zwei Striche („ „); 13) verschwiegen – denn das Schlusszeichen ist in Doppelstriche („ „) eingeschlossen; 14) liebt das Spiel – denn über dem Schlusszeichen steht neben den zwei Strichen noch ein Punct; 15) versteht Rechtsgelehrsamkeit und Staatskunde – denn oben, linker Hand, stehen die Ziffern 2 und 5; 16) kennt Wahrheit – denn die Zahlen sind mit (liegende Klammer) unterzeichnet.« (ebd., S. 305 f.)

Diese Methode, so Klüber, sei zu aufwendig gewesen, sie erfordere etwa zeichnerische Fähigkeiten. Vergennes sei daher zu einer anderen Methode übergegangen, »in welcher er fast Alles durch blosse Ziffern auszudrücken suchte.« (ebd., S. 306)

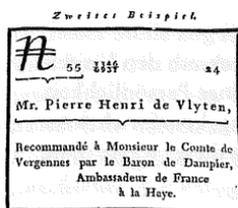


Abb. 5
Polizeischrift in französischem Gebrauch aus Klüber 1809.

»Hr. Pierre Henri de Vlyten ist 1) klein von Statur – das zeigt dieses n an; 2) verheuratet – die zwei Striche durch das n; 3) trägt eigenes Haar – unter dem n steht (liegende Klammer); 4) ein Holländer – die 5 gleich nach dem n, in der Zahl 55; 5) unbekannt ist sein Grad von Einsicht – die 1 in dem Zähler des Bruchs; 6) leichtsinnig – die 3 in dem Zähler; 7) verliebt – die 4 in dem Zähler; 8) reich – die 6 in dem Zähler; 9) schief gewachsen – die 6 in dem Nenner; 10) schön von Gesicht – die 9 in dem Nenner; 11) von

freundlicher Miene – die 3 in dem Nenner; 12) hat Wechselgeschäfte – die 7 in dem Nenner; 13) versteht Rechtsgelehrsamkeit – die 2 rechter Hand des Billiets; 14) macht aber den Kaufmann – die 4 rechter Hand; 15) unbekannt ist, ob er die Wahrheit kenne? – denn unter den Zahlen der Kenntnisse und des Standes fehlt das Zeichen (liegende Klammer); 16) unbekannt ist, ob er verschwiegen sey? – denn die Zahlen sind nicht mit „ „ eingeschlossen; 17) reformirt – das Comma hinter seinem Namen; 18) ehrlich – das Zeichen unter seinem Namen (liegende Klammer).« (ebd., S. 316)

4.2 Kuriose Phänomene – und die (noch) nicht entzifferten Hieroglyphen!

Aus der Erklärung dieser ›graphologischen Chip-Karte‹ geht hervor, dass in diesem Code Elemente kombiniert wurden, die den Charakter von Kuriositäten haben. Dazu gehören die verwendeten Zierteile (Tulpe, Muschel) des Rahmens. Klüber referiert solche Formen der geheimen Mitteilung durchaus unter der Rubrik ›Hieroglyphenschrift‹, darunter auch die Blumenschrift der Orientalen¹⁵ als ein erwähnenswertes Phänomen:

»Die Morgenländer sprechen und schreiben gern in Bildern und Allegorien. Sie besitzen, besonders für die Sprache des Herzens, die Kunst, Gedanken, ingeheim [sic], ohne alle Charaktere, durch Blumen mitzutheilen. Es ist die Kunst, ein Selam, d. h. ein Bouquet von natürlichen Blumen zu binden, die alle nach einer geheimen Bedeutung gewählt und geordnet sind. [...] Die Aster bedeutet Mutter oder Vater, die rothe, gut oder lieb; die weisse, gestorben; die violette, böse, streng.« (ebd., S. 282)

In die Nähe dieser Spielerei geraten aber auch – und hier beginnt wiederum eine kulturhistorisch interessante Spur – die Hieroglyphen, die ebenfalls als Bilderschrift angesehen wurden. Die Hieroglyphen waren noch nicht entziffert und bildeten eine Nagelprobe der frühen Kryptologie, wenngleich eine asymmetrische, weil die Verschlüsselung ja keineswegs absichtlich geschehen war; vergleichbar ist jedoch der Prozess

¹⁵ Als Quelle für die Blumensprache nennt er: *Mysterienbuch alter und neuer Zeit, oder Anleitung geheime Schriften lesen zu können, ingleichen Chiffren aufzulösen. Nebst einem Anhang, die Blumenchiffren der Morgenländerinnen zu verstehen und nachzuahmen*. Leipzig 1797. – Allerdings war diese Symbolsprache, so kurios sie heute erscheint, damals weit verbreitet. Dies bezeugen noch Ende des 19. Jahrhunderts zahlreiche Neu-Ruppiner Bilderbögen; vgl. dazu Riedel & Hirte 1995.

der Entschlüsselung. Aufbauend auf Arbeiten des Engländers Thomas Young gelang sie schließlich dem französischen Linguisten Jean-François Champollion, der diese Entdeckung in seinem Buch *Précis du système hiéroglyphique* 1824 veröffentlichte.¹⁶

So bewandert der Jurist und Diplomat Klüber in der Politik und Geschichte seiner Zeit war, in dieser Frage der Hieroglyphen vertrat er eine ähnlich verzerrte Meinung wie viele seiner Zeitgenossen, wenn er darüber schreibt:

»Die Hieroglyphenschrift der alten Aegyptier, bei welcher die Gelehrsamkeit Monopol für eine Kaste war, ist eine Art der Figurenschrift, in deren Entzifferung man, so vieler Versuche ungeachtet, bis jetzt noch wenig Fortschritte gemacht hat.

Diese Bilderschrift, ursprünglich eine Folge der Noth und der Unwissenheit in der Buchstabenschrift (wie bei den alten Chinesen, Mexikanern, Scythen, Indianern, Phönicern, Aethiopiern und Etruskern), ward, als Geheimschrift, abgekürzt, zusammengesetzt, und mit willkürlichen Zeichen verbunden. Die Gilde der Geheimniskrämer dichtete ihr endlich sogar göttliches Ansehen an.

[...]

Da man vier Arten hieroglyphischer Schrift zählt, so ward wahrscheinlich nur eine derselben zu der Geheimschrift gebraucht, vermuthlich die symbolisch-hieroglyphische. Man vermischte Figuren mit hierographischen Charakteren, die vielleicht ursprünglich auch Figuren gewesen, aber wahrscheinlich dadurch, dass man diese nur mit Grundstrichen zu zeichnen anfieng (wie die Charaktere der Sinesen), ausgeartet waren. Dieser bediente sich die Regierung zu geheimen Befehlen und Nachrichten.« (ebd., S. 279 f.)

4.3 Die Kunst des Dechiffrierens

Der zweite Teil bringt eine Einführung in die Morphologie der wichtigen europäischen Sprachen und leitet an, ausgehend von Häufigkeit und Kombination der Buchstaben sowie von der morphologischen Gestalt der Wörter, mindestens monoalphabetische Verschlüsselungen – »chiffres à simple clé« (ebd., S. 434) – zu dechiffrieren. Was Klüber am Ende an »Eigenschaften eines Dechiffreurs« nennt, klingt dennoch stark ambivalent und relativiert den anfangs behaupteten Charakter als erlernbare Technik:

»Soll die Dechiffirkunst mit Erfolg geübt werden, so wird eine ganz eigene Subjectivität erfordert. Daher, dass die Ausübung verhältnismäßig nur wenigen gelingt. Ein zweiter Dädalus, muss ein

¹⁶ Dargestellt ist die Geschichte der Entdeckung u. a. bei Singh 2000, S. 247–265.

Dechiffreur vollkommene Kenntniss der Theorie der Dechiffirkunst, besonders der verschiedenen ChiffirirMethoden, besitzen, und selbst gute Chiffres zu componiren verstehen. Es muss Fertigkeit in Ausübung der Chiffirirkunst besitzen. Er muss genaue Kenntniss derjenigen Sprachen, worin chiffirt wird, besonders der Wortbildung und Rechtschreibung, sich eigen gemacht haben. Je besser er die allgemeine Sprachlehre kennt, je mehr Sprachen er versteht, desto leichter geht die Arbeit von statten. Hierzu müssen noch kommen, lebhaftes Einbildungskraft, Gewandtheit, treues Gedächtnis, ausdauernde Geduld und Unverdrossenheit, Lust und Liebe. Ohne diese Eigenschaften wird Niemand den ariadneischen Faden auffassen, an dem man aus dem Labyrinth symbolischer Charaktere sich herausleiten muss.« (ebd., S. 430)

3 Fazit

Blickt man auf Klübers Compendium und ebenso auf die Vorläuferwerke, die er zitiert, so kann man sich eines Eindrucks nicht erwehren: Chiffrieren und Dechiffrieren war ein Alltagsphänomen. Nur so erklärt sich die Vielfalt der Formen, unter denen offenbar die Teilverschlüsselungen und Mischformen an der Tagesordnung waren. Diese Hybridformen überraschen angesichts der Tatsache, dass ja ein komplexes und jahrhundertlang geprüftes Verfahren wie die Vigenère-Chiffre zur Verfügung stand. Die Politik und die Kriege machten Kryptographie in jeder Form unentbehrlich. Jedoch war sie keine Geheimwissenschaft mehr, sondern ein lernbares Geschäft, das nur einen Maßstab der Qualität kannte: Sie musste sicher sein und eine Nachricht gegen unerwünschte Mitwisser schützen. Auf welchem Weg dies gelang, blieb eine nachrangige Frage.

Literatur

- Bauer, Friedrich L. (1995): *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*, Berlin, Heidelberg u. a.: Springer-Verlag.
- Byerer, Klaus (Hg., 2000): *Streng geheim. Die Welt der verschlüsselten Kommunikation*, Heidelberg: Umschau.
- Ernst, Thomas (1996): »Schwarzweiße Magie. Der Schlüssel zum dritten Buch der »Steganographie« des Trithemius«, in: *Daphnis* 25, S. 1–205.
- Harsdörffer, Georg Ph. & Daniel Schwenter (1999): *Deliciae Physico-Mathematicae oder Mathematische und Philosophische Erquickungsstunden*, 3 Bde., Neudruck der Ausgabe Nürnberg 1636, hg. und eingeleitet von Jörg Jochen Berns, Frankfurt a. M.: Endter.

- Klüber, Joh[ann] L. (1809): *Kryptographik. Lehrbuch der Geheimschreibekunst (Chiffri- und Dechiffri- und Kunst) in Staats- und Privatgeschäften. Mit vier Tabellen und sechs Kupfertafeln*, Tübingen: Cotta.
- Klüber, Johann L. (1835): *Pragmatische Geschichte der nationalen und politischen Wiedergeburt Griechenlands bis zum Regierungsantritt des Königs Otto*, Frankfurt a. M.: Varrentrapp.
- Mager, Wolfgang (1980): Art. »Johann Heinrich Klüber«, in: *Neue Deutsche Biographie* 12, Berlin: Duncker & Humblot, S. 133 f.
- Riedel, Lisa & Werner Hirte (Hg., 1995): *Der neue Blumengarten. Stadt und Land auf Neuruppiner Bilderbogen*, 2. Aufl., Berlin: Eulenspiegel-Verlag.
- Rösch, Gertrud M. (2004): *Clavis Scientiae. Studien zum Verhältnis von Faktizität und Fiktionalität am Fall der Schlüssel- und Verschlüsselungsliteratur* (= Studien zur deutschen Literatur 170), Tübingen: Niemeyer.
- Schuck, Gerhard (1994): *Rheinbundpatriotismus und politische Öffentlichkeit zwischen Aufklärung und Frühliberalismus. Kontinuitätsdenken und Diskontinuitäts- und Erfahrung in den Staatsrecht- und Verfassungsdebatten der Rheinbundpublizistik*, Stuttgart: Steiner.
- Singh, Simon (2000): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München, Wien: Hanser.
- Shumaker, Wayne (1982): *Renaissance Curiosa. John Dee's Conversations with Angels, Girolamo Cardano's Horoscope of Christ, Johannes Trithemius and Cryptography, George Dalgarno's Universal Language* (= Medieval and Renaissance Texts and Studies 8), Binghampton: Center for Medieval and Early Renaissance Studies.
- Strasser, Gerhard F. (2004): »Magia naturalis« in der Kryptographie, oder »Wie man über 100. oder 1000. Meilen einem etwas entdecken soll«, in: Barbara Mahlmann-Bauer (Hg.), *Scientiae et artes. Die Vermittlung alten Wissens in Literatur, Kunst und Musik*, Bd. 2, Wiesbaden: Harrassowitz, S. 693–700.
- Trithemius, Johannes (1621): *Steganographia: Hoc est: Ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa [...]*, Darmstadt: Johann Berner.
- Zedler, Johann H. (Hg., 1731–54): *Grosses vollständiges Universal-Lexicon Aller Wissenschaften und Künste*, 64 + 4 Bde., Halle etc.: Zedler

Anhang

Kryptographik. Lehrbuch der Geheimschreibekunst (Chiffrir- und Dechiffrirkunst) in Staats- und Privatgeschäften. Von D. Joh[ann] Ludw[ig] Klüber. Mit vier Tabellen und sechs Kupfertafeln. Tübingen, in der J. G. Cotta'schen Buchhandlung 1809.

Im Einzelnen enthält sein Band folgende Teile und Kapitel:

Erster Theil. ChiffrirKunst.

Erstes Buch. Allgemeine Theorie.

Zweites Buch. Specielle Theorie.

Erster Abschnitt. Zifferschrift oder ZahlenChiffre.

Zweiter Abschnitt. Buchstabenschrift. [Darunter stehen:]

- I. Einleitung
- II. WortChiffre
- III. KartenChiffre
- IV. Lacedämonische Geheimschrift
- V. VermehrungsChiffre
- VI. ReversionsChiffre
- VII. SylbenChiffre
- VIII. Einfache BuchstabenChiffre
- IX. MultiplicationsChiffre
- X. QuadratLinienChiffre
- XI. WinkelChiffre
- XII. Transpositions- oder VersetzungsChiffre
- XIII. Netz- oder Gitterschrift
- XIV. Versschrift

Dritter Abschnitt. Zeichenschrift.

- I. Einleitung. Insbesondere Hand- oder Fingerschrift und Geberdensprache
- II. PunctirChiffre
- III. LinienChiffre.
- IV. Winkel- oder QuadratChiffre
- V. Notenschrift oder MusikChiffre, und CirkularscheibenSchrift

Vierter Abschnitt. Figuren- und FarbenChiffre.

- I. Einleitung.
- II. Hieroglyphenschrift.
- III. Quadrat- und Linienschrift.
- IV. Cirkel- und gerade Linienschrift
- V. Cirkel- und krumme Linienschrift
- VI. Geheime Polizeischrift

Fünfter Abschnitt. Abbreviaturschrift oder Brachigraphie, Pasigraphie, Stenographie, Okygraphie.

Sechster Abschnitt. Vermischte Geheimschrift.

I. Einleitung.

II. Buchschrift.

III. Astronomischer Chiffre

IV. Mnemonischer Chiffre.

V. Verschiedene Arten der vermishten Geheimschrift.

VI. Geheime Schreib- und Copirmaschine, und lithographische Copirmethode.

Siebter Abschnitt. Unsichtbare oder sogenannte sympathetische Geheimschrift.

I. Einleitung.

II. Geheimschrift, welche durch aufgestreutes Pulver sichtbar wird.

III. Geheimschrift, welche durch Schaben oder Reiben lesbar wird.

IV. Geheimschrift, welche hervorkommt, wenn man sie erwärmt, oder erhitzt.

V. Geheimschrift, welche hervorkommt, wenn man sie anfeuchtet.

VI. Geheimschrift, welche lesbar wird, wenn man sie in eine Flüssigkeit taucht.

VII. Tinte, welche lesbar wird, wenn man sie Dämpfen aussetzt.

Achter Abschnitt. Geheime Mittheilung geheimer Depeschen.

Zweiter Theil. Dechiffriirkunst.

Erstes Buch. Allgemeine Theorie.

Zweites Buch. Specielle Theorie.

I. Teutsche Sprache.

II. Französische Sprache.

III. Englische Sprache.

IV. Italiänische Sprache.

V. Spanische Sprache.

VI. Holländische Sprache.

VII. Lateinische Sprache.

VIII. Entzifferung einiger FigurenChiffre.

IX. Entdeckung geheimer Tinte.

Anhang. Literatur der Kryptographik.