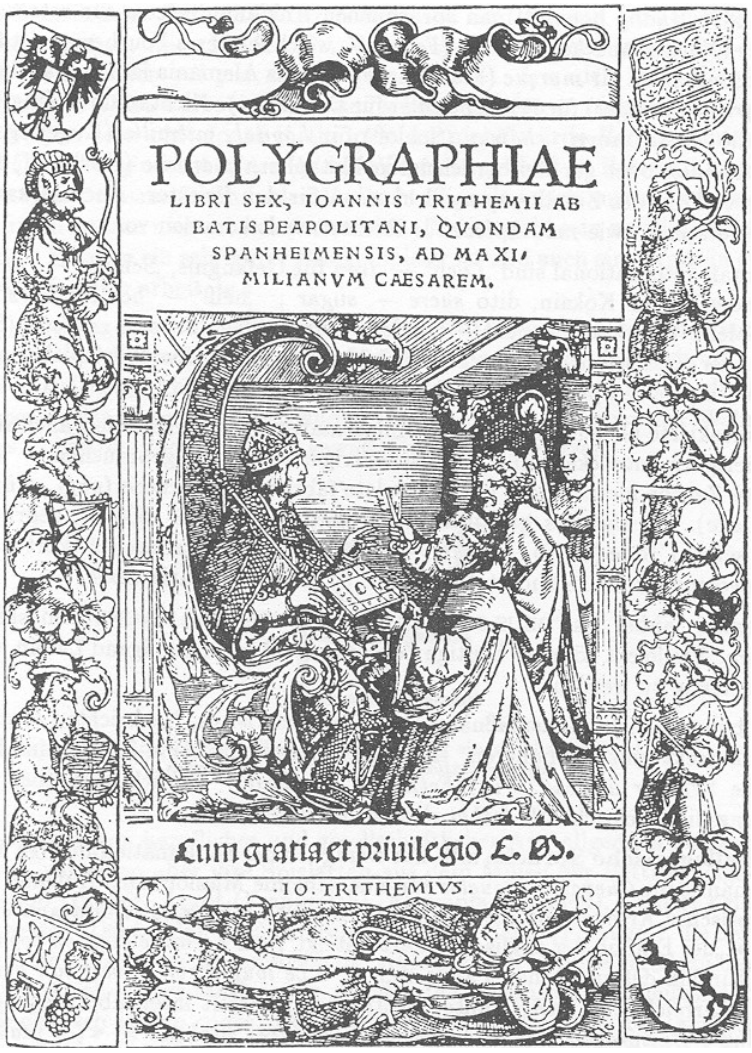
Kryptologie

von

Thomas Imboden



ZLGPXQJ:

PDUWLQD

PDULD

PDALPLOLDQ

1 Inhaltsverzeichnis

ihr professioneller webdesign und webhosting - partner

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

2 Einleitung

„Gewöhnlich glaubt der Mensch, wenn er nur Worte hört,
Es müsse sich dabei doch auch was denken lassen“.
Goethe

Seit es mit Sprache begabte Lebewesen gibt, gibt es auch vertrauliche Mitteilungen, also Mitteilungen, die nur für eine einzige Person oder nur für einen ganz bestimmten Personenkreis gedacht sind, und von denen Aussenstehenden keine Kenntnis erhalten sollten.

Wie kann eine Nachricht ‘sicher’ übermittelt werden, also so, dass *kein Unbefugter Kenntnis vom Inhalt dieser Nachricht erhält*? Eine damit zusammenhängende, fast noch wichtigere Frage ist die folgende: Wie kann man erreichen, dass die Nachricht wirklich beim Empfänger ankommt, und zwar *genauso*, wie man sie *losgeschickt* hat?

Traditionell gibt es zwei Möglichkeiten, diese Probleme zu lösen. Einmal kann man die *Existenz* der Nachricht verheimlichen (zu diesem später) oder man kann auch die Mitteilung durch eine vertrauenswürdige Person übermitteln lassen. Dies haben zu allen Zeiten heimliche Verliebte versucht.

Wir werden uns in dieser Dokumentation vornehmlich mit der Methode der *Verschlüsselung* der Nachrichten zum Zweck der Geheimhaltung beschäftigen. Historische Inforamtionen und Hintergrunde erhalten sie in Kapitel 2 und 3. Weiter geben wir ein Überblick über die Kryptographie (Kapitel 5), wo die Kryptolographie zu klassifizieren ist. Ab Kapitel 6 gehen wir auf kryptologische Methoden ein.

Beim Thema Kryptologie kommt man meistes nicht um die Verwendung einiger Fachbegriffe herum. Diese Begriffe sollen an dieser Stelle kurz erläutert werden. Zunächst aber einige Worte zur Terminologie. Die Begriffe **Kryptologie** und **Kryptographie** sind aus dem grichischen Wörtern κρυπτοσ (geheim), λογοσ (das Wort, der Sinn, und γραφειυ (schreiben) gebildet. Beide bezeichnen die Kunst und die Wissenschaft, die sich damit beschäftigt, Methoden zur Verheimlichung von Nachrichten zu entwickeln.

ihr professioneller
webdesign und
webhosting - partner

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Der Text, die Nachricht, die Buchstaben- oder Zeichenfolge, die wir übermitteln wollen, heisst der **Klartext**; wir werden den Klartext in der Regel durch kleinen Buchstaben **a, b, c, ...** darstellen. Die verschlüsselte Nachricht (also die Buchstaben- oder Zeichenfolge, die tatsächlich übermittelt wird) nennen wir den **Geheimtext** (in der älteren Litaratur wird der Geheimtext auch **Kryptogramm** genannt); ihn werden wir in Grossbuchstaben **A, B, C, ...** schreben. Den Versclüsselungsvorgang nennen wir **Chiffrieren**, den Entschlüsselungsvorgang **Dechiffrieren**. Der **Sender** chiffriert also, während der **Empfänger** dechiffrieren muss, bevor er die Nachricht lesen kann. Eine Drittperson, welche versucht, unrechtmässig einen Geheimtext abzufangen und zu dechiffrieren, nennen wir **Kryptanalytiker**. Diese beschriebenen Elemente, die bei der Schaffung eines Mittels für eine sichere Kommunikation zwischen zwei Peronen benutzt wirden, werden in ihrer Gesamtheit als **Kryptosystem** (Ver- und -Entschlüsselungssystem bezeichnet. Die prinzipielle Struktur eines typischen Kryptosystems ist in Abb. 1 schematisch dargestellt[1].

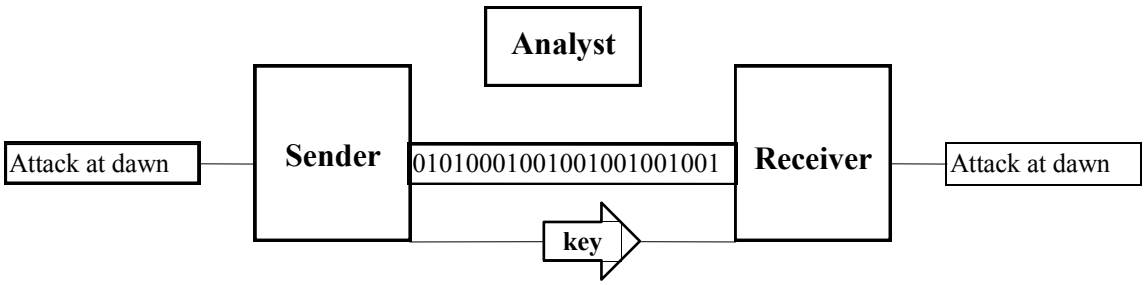


Abb. 1. Schema eines Kryptosystems

Mit diesen einleitenden Erklärungen sollte der Leser für die Lektüre der folgenden Kapitel gerüstet sein. Es ist nicht notwendig, die Kapitel der Reihe nach zu lesen. Erschrecken Sie nicht, wenn Ihnen die eine oder andere Stelle zunächst kryptisch vorkommt. Ich haben mich bemüht Fachbegriffe an der jeweiligen Stelle zu erklären, so das der Text besser verständlich ist. Ich wünsche Ihnen viel Vergnügen!

Der Autor

Thomas Imboden, itdev.ch development

[1] Diese Darstellung wurden von Buch Algorithmen Robert Sedgwick entnommen (p. 387 Abb. 23.1)

ihr professioneller webdesign und webhosting - partner

made in switzerland www.itdev.ch

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Einführung in die Kryptologie

Ziel der Kryptologie ist es, bei einem Nachrichtenaustauch zwischen einem Sender und einem Empfänger zu verhindern, dass eine dritte Person den Inhalt dieser Nachricht erfährt.

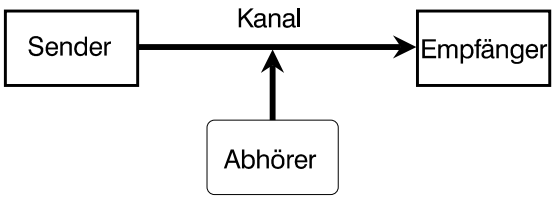


Abb. 2. Nachrichtenkanal vom Sender zum Empfänger

Nachrichten gelangen dabei vom Sender über einen Nachrichtenkanal (Kanal) zum Empfänger. Dieser Kanal ist aber in der Regel ein unsicherer Kanal, so dass eine dritte Person die Nachricht auch mithören kann. Damit auch sensible Informationen auf einem solchen Kanal übertragen werden können, nutzt man in der Regel die Errungenschaften der Kryptologie und verschlüsselt die zu übertragende Nachricht so, dass nur derjenige etwas damit anfangen kann, der den korrekten Schlüssel und das Verschlüsselungsverfahren kennt. Normalerweise werden symmetrische Verschlüsselungsverfahren angewandt, bei denen es *einen* Schlüssel gibt, der sowohl dazu dient, die Information zu verschlüsseln, als auch dazu, die verschlüsselte Information wieder in Klartext[2] zurückzuverwandeln.
Mathematisch betrachtet nimmt man einen Schlüssel K, einen Information I und ein Verschlüsselungsverfahren mit der Operation x. Wendet man das Verfahren mit dem Schlüssel K auf die Information I an, so erhält man den Geheimtext[3] (Chiffrat) C:

$$I \, x \, K \rightarrow C$$

[2] Klartext ist en unverschlüsselter Text.
[3] Geheimtext ist eine verschlüsselte Nachricht.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Dieser Geheimtext wird nun über den unsicheren Kanal übertragen, jedoch kann niemand es lesen. Nur, wer den Schlüssel *K* und das Verfahren *x* kennt, kann aus dem Geheimtext wieder in die ursprüngliche Information zurückgewinnen. Kennt der Empfänger also den Schlüssel, ergibt sich das Model

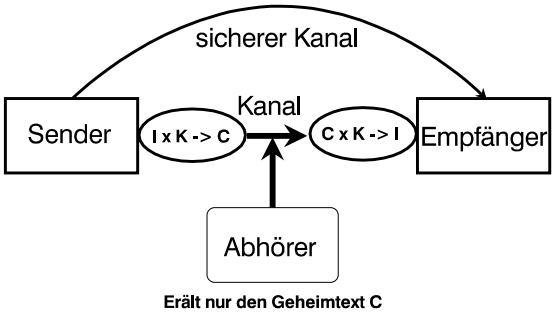


Abb. 3. Senden einer verschlüsselten Nachricht

Bei diesem System gibt es allerdings ein massives Problem: Es ist notwendig auf einem sicheren Kanal den Schlüssel vom Sender zum Empfänger zu transportieren. Denn ohne Kenntnis des Schlüssels kann den Empfänger mit dem Geheimtext ebenso wenig anfangen, wie der Analyst (Abhörer). Und würde der Schlüssel auf dem unsicheren Kanal übertragen, so fiele er dem Analyst in die Hände und die Information wäre so unsicher, als sei sie nie verschlüsselt worden.
Eigentlich jedoch ist das Modell in sich paradox, denn gäbe es einen sicheren Kanal, so könnte man auch die sensible Information dort übertragen und benötigte überhaupt keine Kryptologie.

Natürlich kann der Schlüssel auch zu einer Zeit übertragen worden sein, zu der es einen sicheren Kanal gab. Dann kann später (nach Wegfall des sicheren Kanals) die sensible Information ohne Probleme (theoretisch) über den unsicheren Kanal verschlüsselt übertragen werden. Aber der Transport des Schlüssels stellte bei nahezu allen bisherigen symmetrischen Verfahren ein wesentliches Problem dar.

Solche symmetrischen Verfahren machen aber dann Sinn, wenn es nicht darum geht, Nachrichten auf einem unsicheren Kanal zu sichern, sondern Daten auf einem Datenträger zu verschlüsseln, damit niemand anderer als der Besitzer der Daten auf diese zugreifen kann. Entsprechend gute symmetrische Verfahren können hier einen wirksamen Schutz gegen Datenmissbrauch bieten.
Was den sicheren Nachrichtenaustausch angeht, so sind inzwischen auch Verfahren entwickelt worden, die nicht symmetrisch sind. Am bekanntesten ist sicherlich das „*public key*“- Prinzip, welches wir Ihnen noch vorstellen werden.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

3 Die Wissenschaft Kryptographie

„Even in Cryptology,
silence is golden.“
Laurence D. Smith

Die Geschichte fängt vor ungefähr 2500 Jahren an. Wie wir von dem grichischen Historiker *Plutarch*[4] wissen, benutzte die Regierung von Sparta[5] folgende trickreiche Methode zur Übermittlung geheimer Nachrichten an ihre Generäle: Sender und Empfänger mussten beide eine sogenannte **Skytale** haben.

Aber eine der ersten bekannten Methoden der Kryptologie geht auf den römischen Staatsmann Gaius Julius Caesar (100-44 vC.) zurück. Es ist verständlich, dass ein Feldherr wie Caesar sich bei der Übermittlung von Botschaften an seine Offiziere im Feld nicht nur auf die Qualität seiner Boten verlassen wollte. So dachte er sich eine Möglichkeit aus, mit der eine Botschaft, auch wenn sie von seinen Feinden abgefangen werden sollte, trotzdem nicht seine Pläne durchkreuzen konnte. Dieses Verfahren besprechen wir im Kapitel monoalphabetische Chiffrierung.

Ein anderes historisches Kryptosystem stammt von Blaise de Vignère. Es handelt sich bei der Vignerère-Chiffre um ein der ersten polyalphabetischen Methoden, welche das System von Caesar in der Komplexität, aber auch in der Sicherheit, um einiges übertrifft. Tatsächlich sind, wie wir später sehen werden, ein par Trick notwendig, um eine Vigneère-Chiffre zu kancken.

Vor wenigen Jahren noch war die Kryptologie, die Lehre von den Geheimschriften und ihrer unberufenen Entzifferung, ein recht im Verborgenen blühendes Gebiet - blühend, weil von alters her ihre professionellen Vertreter gut ernährend. Denn die Kryptologie ist eine echte „Wissenschaft“: Es geht um Wissen, um erfahrenes ebenso wie um erprobtes. Ihrer Natur nach handelt sie nicht nur von Geheimschriften, sondern bleibt auch Geheimwissenschaft. Die klassische offene Literatur ist spärlich und schwierig aufzufinden: Mit dem Aufkommen allmächtiger Staatsgewalten müssen sich die professionellen Kryptologen weitgehend in die Anonymität begeben oder doch wenigstens eine Zensur ihrer Veröffentlichungen hinnehmen. Dementsprechend gab die offene Literatur nie völlig den Wissensstand wieder - man darf annehmen, dass es heute nicht anders ist. Verschiedene Staaten sind dabei verschieden zurückhaltend: Während die Vereinigten Staaten von Amerika recht grosszügig Infomationen über die Situation im 2. Weltkrieg herausliessen, hüllte sich die ehemalige Sowjetunion in Schweigen. Aber auch Grossbritannien pflegt eine Geheimniskrämerei, die manchmal unan-

[4] Plutarch griech. Schriftsteller um 46 nC.. Durch Kenntnisreichtum und sittliche Grundsätzlichkeit über alle Zeitgenossen hinausragende Persönlichkeit.
[5] Sparta (neugriech: Sparti) Hauptstadt von Lakonien. Die Stadt liegt am Fluss des Taygetosgebirges, im Tal der Eurotas. Gegründet wurde die Stadt von den Dorier Ende 2. Jahrtausend vC. Sparta oder Lacedämon galt in der Antike als typische Militärstaat.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

gemessen erscheint, so in der Sache 'COLOSSUS'[6]. Lediglich über den Stand der Kryptologie in Deutschen Reich wurde nach dem Zusammenbruch 1945 offen berichtet[7].

Die Kryptologie ist eine Jahrtausende alte Wissenschaft. Ihre Entwicklung stand mit der Entwicklung der Mathematik zumindest personell gelegentlich in Berührung - Namen wie *Viète*[8] und *Wallis*[9] tauchen auf. In einer modernen mathematischen Betrachtungsweise zeigt sie statistische (William F. Friedman, 1920), algebraisch - kombinatorische (Lester S. Hill, 1929) und stochastische Züge (Claud E. Shannon, 1941).

Der 2. Weltkrieg brachte endgültig die Mathematiker an die kryptologieshe Front: Beispielsweise standen sich gegenüber Hans Rohrbach[10] in Deutschland, Alan Turing[11] in England; in den USA waren der grosse Algebraiker A. A. Alber sowie Barkley fosser und Willard Van Orman Quine engagiert. Auch der Vater von Christopher Strachey, Oliver Strachery, war Kryptologe[12].

Mathematische Disziplinen, die nach dem heutigen Stand für die Kryptologie von Belang sind, umfassen unter anderem

- Zahlentheorie
- Gruppentheorie
- Kombinatorik
- Komplexitätstheorie
- Ergodentheorie
- Informationstheorie.

„Das Schlüssel- und Entzifferungswesen ist bereits parktisch als Untergebiet der Angewandten Matthematik anzusehen" (K. H. Kirchhofer). Für den Informatiker gewinnt die Kryptologie zusehends praktische Bedeutung in Verbindung mit Datenbasen und Datenübermittlung.

---

[6] Während des zweiten Weltkrieg entwickelten die Engländer elektromechanische und elektronische Maschine, um die deutschen verschlüsselten Nachrichten zu knacken. Die berühmteste dieser Maschinen, die Röhrenrechenanlage **COLOSSUS**, kann als der erste digitale Computer angesehen werden.

[7] Hans Rohrbach (1948), Mathematische und maschinelle Methoden beim Ciffrieren und Dechiffrieren. In: FIAT Review of German Science 1939-1941: Applied Mathematics, Part I, Wiesbaden.

[8] Francois Viète, Seigneur de la Bigotière (1540-1603), französischer Mathematiker.

[9] John Wallis (1616-1703, englischer Mathematiker.

[10] Hans Rohrbach (* 1903), deutscher Mathematiker.

[11] Alan Truing (2912-1954), britischer Logiker.

[12] Oliver Strachey ersetzte 1941 in Kanadischen Diensten den ehemaligen US Major Herbert O. Yardley, der in den Vereinigten Staaten in Ungnade gefallen war (wieso ist mir nicht bekannt).

ihr professioneller webdesign und webhosting - partner

made in switzerland www.itdev.ch

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Im allgemeinen ist es aber verständlich, wenn hoheitliche Geheimdienste selbst die Namen führender Kryptologen nicht der Öffentlichkeit preisgeben. Zu sehr lebt die professionelle Kryptologie unter den Gefahren nachrichtendienstlicher Benühungen. Es ist beduetsam, den potentiellen Gegner über die eigenen Ansichten zur Auswahl von Verfahren ebenso im unklaren zu lassen wie über die eigenen Fähigkeiten zum unbefugten entziffern. So blieben die Deutschen bis 1944 überzeugt, die Chiffrierung ihrer ENIGMA-Maschine sei nicht zu brechen. Gelingt aber eine unberufene Entzifferung - den Engländern gelang dies 1940 für die ENIGMA-Chiffrierung -, si ist es wichtig, diesen Schverhalt von dem Gegner zu verbergen und sich nicht durch Reaktionen zu verraten, wobei im Krieg Material und sogar menschen geopfert werden müssen, um anderweitig grössere Verluste zu ersparen.

ihr professioneller
webdesign und
webhosting - partner

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

4 Überblick über Geheimschriften

„En cryptographie,
aucune règle n'est absolue."
Ètienne Bazeries[13]

4.1 Kryptographie und Steganographie

Zu unterscheiden ist zwischen Kryptographie und Steganographie. Der Ausdruck **Kryptographie** (engl. cryptography, frz. cryptographie) wurde als 'cryptographia' für secrecy in writing 1641 von John Willkins, dem Gründer der Royal Society, eingeführt. Die Methoden der Kryptographie machen eine Nachricht für den Unberufenen unlesbar, unverständlich. Im Deutschen spricht man auch von offenen (d.h. offensichtlich als solchen erkennbaren) Geheimschriften. Der Ausdruck **Steganographie** (engl. Steganography, frz. stéganographie) wurde von Caspar Schott, einem Schüler von Athanasius Kircher, in dem Buchtitel Schola steganographia, Nürnberg 1665 auch für 'Kryptographie' verwendet; er findet sich schon in dem von Trithemius 1499 begonnenen ersten, noch reichlich obskuren Werke Steganographia mit der Bedeutung 'verdecktes Schreiben'. Die methoden zielen darauf ab, die blossen Existenz einer Nachricht zu verbergen. Um ein Tagebuch zu führen oder um ein Boten zu verwhren, von einer Nachricht Kenntnis zu nehmen, sind Kryptographische Metoden angebracht; um eine Nachricht durch Gefängnistore zu Schmuggeln[14], steganographische Methoden.

Die Steganographie zerfällt in zwei Baranchen, die linguistische und die technische. Nur die erstere hat mit der Kryptographie innere Berührung. Die **technische Steganographie** ist rasch erledigt. Sie arbeitet seit Plinius mit Geheimtinten. Bis heute ist Zitronensaft beliebt und bewährt. Andere Klassische Requisiten sind doppelte Böden und hohle Absätze.

Von modernen Errungenschaften seien erwähnt: Schnelltelegraphie (engl. spurts). Für schriftliche Nachrichten wurde revolutionierend die Mikrophontographie; das microdot von der Abmessung eines Fliegendrecks nimmt ein ganzer Seite auf (DIN A 4). Der russische Spion Abel stellte die Microdots auf spektroskopischem Filmmaterial her, das er unauffällig kaufen konnte. Sein Kollege Lonsdale versteckte die Microdots im Rücken gebundener Zeitschriften. Die im 2. Weltkrig von deutschen Dienststellen verwendeten Microdots schlisslich hatten gerade die Grösse, um als Schreibmaschinenpunkt verwendet zu werden.

Die **linguistische Steganographie** ('gedeckte Geheimschriften') kennt zwei Klassen von Verfahren: entweder eine geheime Nachricht als unverfängliche, offen verständliche Nachricht erscheinen zu lassen (engl. open code) oder in (eventuell winzigen, aber) sichtbaren

[13] Ètienn Bazeries (1846-1924), wohl der bedeutendste französische Kryptologe unserer Zeit.
[14] Von Sir John Trevanion unter Oliver Cromwell bis zu französischen Bankräuber Pastoure, dessen Überführung André Langie beschrieb, und zu Klaus Croissant.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

graphischen Details einer Schrift oder Zeichnung auszudrücken (**Semagramm**, engl. semagram). Die letztere Klasse ist vor allem bei Amateuren beliebt. Sie erfüllt allerdings viele Wünsche nicht. Zu verräterisch sind graphische Details einem wachsamen Auge. So hat Francis Bacon's Verwendung zweier Schriftarten (Abb. 4) aus der ersten englischen Übersetzung von De Augmentis Scientarum, 1623 keine grosse praktische Bedeutung erlangt.

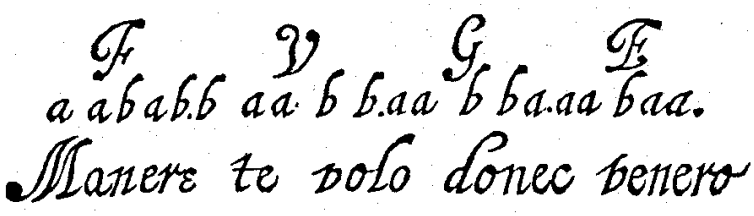


Abb. 4. Francis Bacon: Tarnung eines binären Codes ('biliteral cypher[15]') mittels zweier verschiedener Schriftzeichen - Formen. Man beachte die beiden verschiedenen |e| in Manere. Aus: [KAHN], p. 884

Dieses steganographische Prinzip scheint zur selben Zeit auch in Paris bekannt gewesen zu sein und wird auch von Vigenère 1586 erwähnt. Es scheint sich über die Jahrhunderte aber gut erhalten zu haben: die jüngsten mir bekannten Verwendungen stammen von van Wijngaarden und von einem Kollegen in einem Buch über Kombinatorik (Abb.5.).

```
In Königsberg i. Pr. gabelt sich der Pregel und umfliesst eine Insel, die
Kneiphof heisst. In den dreissiger Jahren des achtzehnten Jahrhunderts
wurde das Problem gestellt, ob es wohl möglich wäre, in einem Spaziergang
jede der sieben Königsberger Brücken genau einmal zu überschreiten.
Dass ein solcher Spaziergang unmöglich ist, war für L. EULER der Anlass,
mit seiner anno 1735 der Akademie der Wissenschaften in St. Petersburg vor-
gelegten Abhandlung Solutio problematis ad geometriam situs pertinentis
(Commentarii Academiae Petropolitanae 8 (1741) 128-140) einen der ersten
Beiträge zur Topologie zu liefern.
Das Problem besteht darin, im nachfolgend gezeichneten Grephen einen ein-
fachebn Kantenzug zu finden, der alle Kanten enthält. Dabei repräsentiert
die Ecke von Grad 5 den Kneiphof und die beiden Ecken von Grad 2 die
Krämerbrücke sowie die Grüne Brücke.
```

Abb. 5. Textsemagramm in einem Lehrbuch der Kombinatorik

Ein zweites steganographisches Prinzip besteht im Punktieren ausgewählter Zeichen in einem Buch. Es fällt sehr viel mehr auf als das obige Vorgehen[16], ist aber einfacher zu bewerkstelligen.
Ein drittes Prinzip verwendet bei Handschriften das Absetzen im Wort als Kennzeichung (Abb. 6). Im Beispiel ist allerdings nicht der Buchstabe gemeint, der vor oder nach der Unterbrechung steht, sondern es wird gezählt, nach wie vielen Buchstaben ein Buchstabe mit einem nach oben gerichteten Abschwung steht - alos 3 3 5 1 5 1 4 1 2 3 4 3 3 3 5 1 4 5 ....Dieses steganographische Prinzip wurde in Frankreich 1895 von Boetzel und O'Keenan den Autoritäten vorgeführt, ebenfalls in Verbindung mit einem numerischen Code. Es scheint jedoch in russischen Anarchistenkreisen bereits bekannt gewesen zu sein, und zwar eben im Zusammenhang mit der oben erwähnten Anarchistenchiffre. Es wurde auch von gefangenen deutscher U-Boot-Offizieren verwendet, die über alliierten U-Boot-Bekämpfungstaktik nach Hause berichteten. In all diesen Fällen handelt es sich um **Text-Semagramme** ('sichtbar getarnte Geheimschriften').

[15] Cypher ist eine veraltete Schreibweise für cipher, die aber in den USA noch verbreitet ist.
[16] Wenn es nicht mit einer Geheimtinte geschieht.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

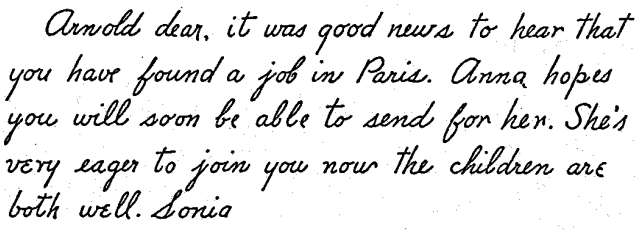


Abb. 6. Tarnung eines numerischen Codes mittels Absetzen im Schriftzug. Aus: [SMITH], p. 23

Daneben gibt es aber auch die **echten Semagramme**: Seit der Antike bekannt ist das Astragal des Aeneas, bei dem durch Löcher geschlungenes Garn Buchstaben symbolisiert. Eine Schachtel voll Dominosteine mag ebenso eine Nachricht verbergen (durch die Stellung der Steine) wie eine Sendung von Taschenuhren (durch die Stellung der Zeiger). Die tanzenden Männchen von Shelock Homes ([B-G I] p. 31) tragen ebenso Nachricht wie ein versteckter Morsecode (Abb. 7): „Compliments of CPSA MA to our chief Col. Harold R. Shaw on his visit to San Antonio May 11th 1945“. (H. R. Shaw war seit 1943 Chef der Technical Operations Division der US-Regierung.)

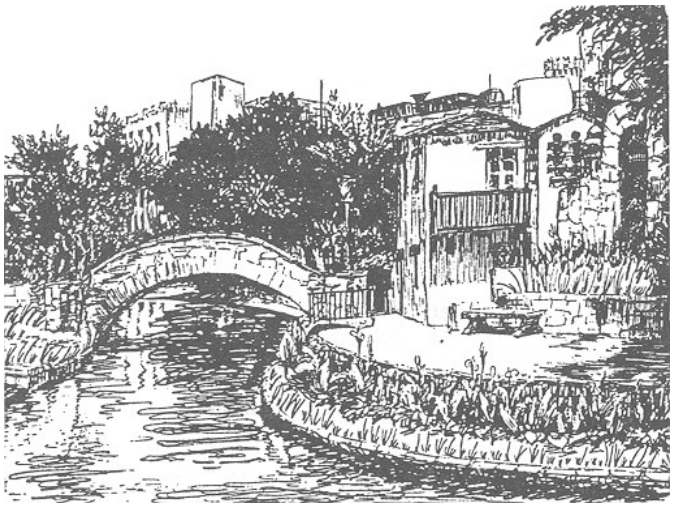


Abb. 7. Semagramm.. Die Nachricht steht im Morsecode, der aus Kurzen und langen Grashalmen links von der Brücke entlang des Flusses und auf der kleinen Mauer gebildet wird Aus: [KAHN], p. 523

Von eigentlichem Interesse für uns sind jedoch diejenigen Verfahren der linguistischen Steganographie, die eine geheime Nachricht als unverfänglich und offen verständlich ausgeben (engl. open code). Sie stehen methodisch der Kryptographie näher.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

4.2 Maskierung

Eine als offene Nachricht **maskierte Geheimschrift** erfordert vorherige Abspreche über die wahre Bedeutung unverfänglicher Floskeln. Unter Katenschwindlern soll folgendes System bekannt sein: Die Art, die Zigarette zu halten und sich zu kratzen, zeig Farbe an. Eine Hand vor die Brust gehalten, mit abgestrechtem Daumen, bedeutet „Das ist mein Spiel“. Oder der französische Zauberkünstler Houdin soll um 1845 ein ähnliches System benutzt haben, mit I, M, S, V für *coeur, carreau, trèfle, pique*; „***il** fait chaud*“ oder „***il** y a du monde*“ bedeutet I=“ich habe Herz (coeur)“.
Sondersprachen beruflicher und gesellschaftlicher Art, allgemein **Jargon** genannt, vor allem aber ihre Spielarten aus dem verschiedenen Milieus:
‘Loch’ *trou* für Gefangnis;
‘Schnee’ *neige, snow* für Kokain (oder auch *sucre, sugar*);
‘heiss’ *hot* für kürzlich gestohlene Ware;
‘abstauben’ *nettoyer* für stehlen;
‘Kies’ *galette* (frz. Kieselstein: *galet*) *rock* für Geld.
Alle Arten von Wortspielen gehören prinzipiell hierher.

4.3 Stichworte

Ein Wort oder wie die Überschrift, ein Stichwort, dass zu einem einzigen vorherbestimmten Zweck dient. Zum Beispiel sollte HIGASHI NO KAZE AME („Ostwind, Regen“), in den Wetterbericht der japanischen Überseenachrichten eingeschoben und zweimal wiederholt, ‘**Krieg mit USA**’ ankündigen. Die US Navy fing einen diesbezüglichen diplomatischen Funkspruch ab und konnte ihn im November 1941 entziffern. Zahlreiche Funkaufklärungs-stationen der USA überwachten den japanischen Radioverkehr auf das Stichwort hin. Am 7. Dezember 1941 kam es: „HIGASHI NO KAZE AME, HIGASHI NO KAZE AME“, nur Stunden nach dem Angriff auf Pearl Harbour.

4.4 Unsichtbar getarnte Geheimschrift

Regeln für getarnte Geheimschriften sind häufig von der Art „das x-te Zeichen nach einem bestimmten Zeichen“, z.B. „das erste Zeichen nach Zwischenraum“ (im 2. Weltkrieg von Soldaten gern gebraucht, zum grossen Missvergnügen des Zensors), besser schon „das dritte Zeichen nach Zwischenraum“ usw..

Es wird von einem Soldaten der US Army berichtet, der seinen Eltern das Land, in dem er sich aufhielt, durch die jeweils ersten Buchstaben (nach der Anrede) in seinen Briefen mit-teilen wollte - kryptographisch und steganographisch zunächst kein schlechter Einfall. Die Sache kam trotzdem heraus, als die Eltern schrieben: „Wo ist Nutsi - wir finden es auf unserem Atlas nicht?“.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

5 Monoalphabetische Algorithmen

Zunächst stellen wir einige klassische monoalphabetische Algorithmen über dem natürlichen Alphabet vor, wie etea die Caesar-Chiffre. Es ird sich herausstellen, dass all diese Chiffrierungen relativ leicht zu brechen sind. Bei der Darstellung dieser Algorithmen werden wir zwanglos die grundlegenden kryptologischen Begriffe und Bezeichnungen einführen können.
Eine Chiffrieung heisst **monoalphabetisch**, falls jeder Buchstabe des Alphabets stets zu demselben Buchstaben chiffriert wird. Eine monoalphabetische Chiffrieung kann man also immer so darstellen, dass man unter das „Klartextalphabet“ ein „Geheimtextalphabet“ schreibt. Zum Beispiel stellen die folgende Chiffriermethode monoalpahbetische Chiffrierungen dar:

Klartext:	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
Geheimtext:	#	%	+	^	~	£	§	«	±	×	»	¿	ª	ÿ	&	?	<	=	>	¢	÷	µ	]	_	[	/

Abb. 8. Monoalphabetische Chiffrierung. vgl. Caesars Verschlüsselungstabelle

Es ist ersichtlich, dass Klartext und Geheimtext nicht über demselben Alphabet definiert sein müssen. Ist dies jedoch der Fall, so entspricht jeder monoalphabetische chiffrierung eine Permutation der Buchstaben des Alphabets, umgekehrt kann man jeder Permutation der Buchstaben eine monoalphabetische Ciffrierung zuordnen. Darau ergibt sich insbesondere, dass es genau

$$26! = 26 * 25 *...* 2 * 1 = 403'291'461'166'605'635'584'000'000$$

monoalpabetische Chiffrierungen über dem natürlichen Alphabet {**a, b, c, ..., z**}gibt.

ihr professioneller webdesign und webhosting - partner


it development
talstrasse 98
ch 3924 st. niklaus

5.1 Die Skytale von Sparta

Wie eingangs erläutert brauchen Sender und Empfänger eine sogenannte **Skytale** ; das waren zwei Zylinder mit genau dem gleichen Radius. Der Sender wickelte ein schmales Band aus Pergament spiralförmig um seinen Zylinder und schrieb dann der Länge nach seine Nachricht auf das Band (vergleiche Abb. 9).

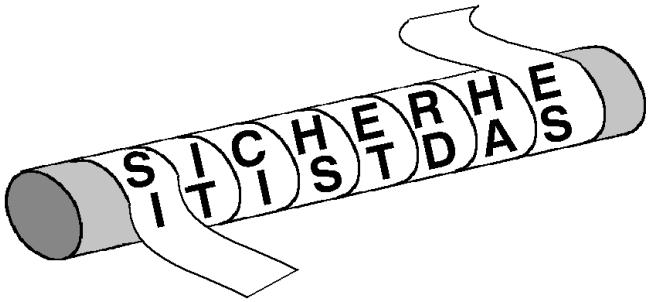


Abb. 9. Eine Skytale

War das Band abgewickelt, konnte die Nachricht nur von einer Person gelesen werden, die einen Zylinder genau desselben Umfangs hatte.
Wir betrachten nun ein Beispiel in moderner Sprache. Stellen wir uns vor, wir hätten einen Papierstreifen abgefangen, auf dem wir die folgenden Buchstabenfolge lesen:

SIEIYHITIEPICINLTEHSZDO!ETIEGRDGRRHAEKAESZRP

Die Skytaledes Senders hat einen Umfang, den wir durch die Anzahl von Buchstaben ausdrücken können. Wir können also einfach verschiedenen Umfänge u ausprobieren. Wenn wir u = 5 wählen, ergibt sich vollkommener Unsinn:

```
S H P L Z T D A S
I I I T D I G E Z
E T C E O E R K R
I I I H ! G R A P
Y E N S E R H E,
```

wenn wir aber den Text in u = 6 Spalten anordnen, wird die Botschaft klar:

```
S I C H E R H E
I T I S T D A S
E I N Z I G E Z
I E L D E R K R
Y P T O G R A P
H I E !
```

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Die Skytale ist der Prototyp eines **Transpositionsalgorithmus**[17]; dabei bleiben die Buchstaben, *was* sie sind, sie bleiben aber nicht *wo* sie sind. Ein Mathematiker würde einen Transpositionsalgorithmus beschreiben als ein Permutation der *Stellen* der Buchstaben. Transpositionsalgorithmen sind ein wichtiger Baustein für moderne Algorithmen. Die andere Komponente sind die **Substitutionsalgorithmen**[18]; bei diesen wird die Nachricht dadurch unlesbar gemacht, dass jeder Buchstabe durch einen anderen ersetzt, aber seine Position beibehält[19].

5.2 Verschiebechiffren

Die von Caesar benutzte Chiffre erhält man, wenn man unter das **Klartextalphabet** das **Geheimtextalphabet** schreibt - aber um 23 Stellen nach rechts oder, was dasselbe bedeutet, um 3 Stellen nach links versetzt:

Klartext:	**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**
Geheimtext:	**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**

Abb. 10. Caesars Verschlüsselungstabelle

Chiffriert wird, indem ein Klartextbuchstabe durch den darunterstehenden Geheimtextbuchstaben ersetzt wird. Zum Beispiel wird aus dem Wort „**klartext**“ die scheinbar sinnlose Buchstabenfolge „**NOBUWHAW**“. Die Dechiffrierung ist genauso einfach: jeder Geheitextbuschstabe wird in den darüberstehenden Klartextbuchstaben zurückübersetzt.
Sie fragen mit Recht, warum Caesar das Geheimtextalphabet gerade um 3 Stellen verschoben hat. Die Antwort ist einfach: Dafür gibt es überhaupt keine Grund, so glaube ich! In der Tat kann man das Alphabet um eine beliebige Anzahl von Stellen verschieben. Da unser Alphabet aus 26 Buchstaben besteht, gibt es genau 26 solche Chiffrierungen; man nennt sie **Verschiebechiffren** oder auch **additive** Chiffrien.

5.3 Tauschchiffren

Wenn man zum Verschlüsseln von Buchstaben Rechner verwenden will, so identifiziert man üblicherweise **a** (bzw. **A**) mit **1**, **b** (bzw. **B**) mit **2**, und se weiter; **x** identifiziert man mit **24**, **y** mit **25** und **z** mit **0**. Mit dieser Darstellung kann man eine Verschibechiffre besonders gut beschreiben: Eine Verschiebung um, sagen wir, **s** Stellen entspricht nämlich einer Addition der Zahl **s**. Konkret geht man dabei so vor:

- Zunächst wird der Klartextbuchstabe in die ihm entsprechende Zahl übersetzt;
- dann wird zu dieser Zahl die Zahl **s** addiert;
- vom Ergebnis betrachten wir nur den Rest, der sich beim Teilen durch 26 ergibt; dieser Rest wird wieder in einen Buchstaben zurückübersetzt (es handelt sich hier um **modulo** 26).

So erhält man den zugehörigen Geheimtextbuchstaben.

[17] Würfelverfahren oder Versatzverfahren.
[18] Tauschverfahren oder Ersatzverfahren.
[19] Dies sind Algorithmen wie sie C. Julius Caesar verwendet hat.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Wir wollen den Klartextbuchstaben **a** mit einer Verschiebechiffre, die um 3 (**s**) Stellen verschiebt, chiffrieren.
- **a** wird durch die Zahl **1** dargestellt;
- **1 + 3 = 4**;
- **4** ist die Darstellung des Geheimtextbuchstabens **D**.

Bei der Dechiffrierung von **B** geht man so vor:
- **B** entspricht der Zahl **2**;
- **2 - 3 = -1**;
- der Rest von -1 bei modulo 26 ist **25**;

dieser Rest entspricht dem Klartextbuchstaben **y**.

Mit dieser Methode kann man Buchstaben sozusagen *addieren*. Eine andere Methode ist das *multiplizieren* der Buchstaben. Auf diese Methode gehen wir nicht weiter ein, wir verweisen auf das Buch Kryptologie Bauer p. 35.

5.4 Schlüsselwörter

Eine riesige Menge von monoalphpbetischern Chiffren erhält man auf folgende Art und Weise: Der **Schlüssel** besteht aus zwei Komponenten, einem **Schlüsselwort** und einem **Schlüsselbuchstaben**. Zunächst mache man aus dem Schlüsselwort ein Buchstabenfolge, in der jeder Buchstabe nur **einmal** vorkommt. Dies wird dadurch erreicht, dass jeder Buchstabe bei seinem zweiten, dritten, ... Auftreten gestrichen wird. Haben wir beispielsweise des Schlüsselwort

GEHEIMSCHRIFT => GEHIMSCRFT.

Nun schreibe man diese Folge unter das Klartextalphabet, und zwar so, dass man genau unter dem Schlüsselbuchstabe beginnt. Haben wir in unserem Beispiel als Schlüsselbuchstabe **e** gewählt, so erhalten wir

Klartext: **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**
Geheimtext: **G E H I M S C R F T**

anschliessend schreibt man die restlichen Geheimtextbuchstaben in alpahbetischer Reihenfolge auf, indem man nach dem letzten Schlüsselwortbuchstaben beginnt. In unserem Beispiel ergibt sich:

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

Da man die Anzahl der Schlüsselwörter nicht genau angeben kann, kann man auch die Anzahl dieser Chiffrierungen nicht präzise bestimmen. Klar ist jedoch, dass ihre Zahl sehr gross ist. Formal könnte man sogar sagen, dass man **alle** monoalphabetischen Chiffrierungen mit Hilfe von Schlüsselwörtern erhält.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

6 Polyalphabetische Chiffrierung

„No message is safe in cipher unless
the key phrase is comparable in length
with then message itself.“
Parker Hitt[20]

In diesem Kapitel stehen die polyalphabetischen Chiffrierungen im Mittelpunkt. Bei diesen wird derselbe Klartextbuchstabe nicht stets mit demselben Geheimtextbuchstaben verschlüsselt. Eine polyalphabetische Chiffrierung kann also nicht einfach durch ein Klartextalphabet und ein daruntergeschreibenses Geheimtextalphabet beschrieben werden.
Die Zuordnung eines Klartextbuchstabens zu einem Geheimtextbuchstaben darf aber nicht willkürlich erfolgen. Die Chiffrierung muss der strengen Regel der Eindeutigkeit genügen; sonst ist kein Dechiffrierung möglich. Das Hauptproblem ist, auf einfache Weise viele verschiedene Chiffrierschritte festzulegen oder, wie man sagt, viele verschiedene Alphabete zu erzeugen. Das charakteristische Beispiel dafür ist die Verschlüsselung nach Vigenère.

[20] Colonel Parker Hitt (1877-1971) publizierte 1961 eines der ersten seriösen Bücher über Kryptologie in dern Vereinigten Staaten und beschäftigte sich darin als erster mit der systematischen Entzifferung von PLAYFAIR. Hitt war später ein Vice - Präsident von AT&T und Präsident von dessen kryptologischer Tochter *International Communication Laboratories*.

ihr professioneller
webdesign und
webhosting - partner

made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

6.1 Die Vigenère - Chiffre

Die Grundidee des Vigenère - Verschlüsselung ist, verschiedene monoalphabetische Chiffrierungen im Wechsel zu Benützen. Die Literatur spricht in diesem fall von VIGENÈRE-Chiffrierschritten[21]. Wird das Alphabet statt von a - z in der Reihenfolge z - a aufgeschrieben, so spricht man in der Literatur von der BEAUFORT-Chiffrierschritten[22].

Recta tranſpoſitionis tabula.

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

In hac tabula literarū canonica ſiue recta tot ex uno & uſuali noſtro latinarum literarum ipſarum per mutationem ſeu tranſpoſitionē habes alphabeta, quot in ea per totum ſunt monogrammata, uidelicet quater & uigeſies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per totidē multiplicata, paulo efficiunt minus q̄ quatuordecē milia.

o ij

Abb. 11. 'tabula recta' des Trithemius. Aus der Polypraphiae von 1518, 5. Buch.

Um nach dem Algorithmus von Vigenère chiffrieren zu können, braucht man das **Vigenère-Quadrat**. Dieses Quadrat besteht aus 26 Alphabeten, die so untereinander geschrieben sind, dass das erste Alphabet das gewöhnliche Alphabet ist, das zweite um einen Buchstaben verschoben ist, das dritte um zwei Buchstaben, usw.

[21] Eigentlich müsste dieser Fall nach *Trithemius* benannt werden. Die Sekundärliteratur des 19. Jahrhunderts tat Vigenère insofern Unrecht, als sie nur die verschobenen Standardalphabete mit seinem Namen belegte. Vigenère schrieb in die Kopfzeile der *tabula recta* ein permutiertes Alphabet, was gleichwertig war mit Albertis Scheibe.

[22] Schon von Giovanni Sestri 1710 betrachtet, von Admiral Sir Francis Beaufort (1774-1857, besser bekannt von der Windstärke her) 1857 wiederentdeckt. In der englischen Literatur als 'variant Beaufort', in der französischen Literatur als 'variante à l'allemande' bezeichnet.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

Klartext:	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
1.	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
2.	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	A
3.	C	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
4.	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
5.	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	D
6.	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
7.	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
8.	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
9.	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
10.	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
11.	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
12.	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13.	M	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
14.	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
15.	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	N
16.	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
17.	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
18.	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
19.	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
20.	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
21.	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
22.	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
23.	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
24.	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
25.	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
26.	Z	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

Abb. 12. Das Vigenère-Quadrat

Zur Chiffrierung eines Klartext wird der erste Buchstabe mit dem entsprechenden Buchstaben aus dem ersten Alphabet ersetzt, dann der zweite Buchstabe des Klartextes mit dem zweiten Alphabet und so weiter.
Um die Reihenfolge der Alphabete selbst zu bestimmen verwenden wir ein Schlüsselwort. Das Schlüsselwort kann jede beliebige Buchstabenfolge sein; für unser Demonstrationsbeispiel wählen wir das Wort „**GEHEIMSCHRIFT**“. Wir schreiben dieses Schlüsselwort Buchstaben für Buchstaben über den Klartext, und zwar so lange, bis die Länge des Klartexts erreicht ist.
Bei der Chiffrierung bestimmt der Schlüsselwortbuchstabe, der über einem bestimmten Buchstaben steht, das Alphabet, mit dem dieser Klartextbuchstabe zu chiffrieren ist.
Also: Um den ersten Geheimtextbuchstaben zu erhalten, müssen wir in dem Alphabet, das mit „G“ beginnt, nachsehen, was in der Spalte **w** steht; dies ist der Buchstabe **C**.

Schlüsselwort:	G	E	H	E	I	M	S	C	H	R	I	F	T	G	E	H	E	I	M	S	C	H	R			
Klartext:	w	i	r	t	s	c	h	**a**	f	t	s	i	n	f	o	r	m	**a**	t	i	k	e	r			
Geheimtext:	C	M	Y	X	A	O	Z	C	M	K	A	N	G	L	S	Y	Q	I	F	A	M	L	I			

Wir sehen, dass gleiche Buchstaben (z.B. die beiden **a**) diesmal nicht mit gleichen Buchstaben übersetzt werden. Die Häufigkeit der Buchstaben wird viel gleichmässiger verteilt. Es ist klar, dass eine solche Chiffriermethode dem **Analyst** vor erheblich grössere Probleme stellt, als dies bei einer monoalphabetischen Chiffrierung der Fall war.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

Natürlich kann mit heutigen Methoden auch ein Vigenère-chiffrierter Text geknackt werden. Der erste veröffentlichte Angriff wurde 1863 von dem preussischen Infanteriemajor Friedrich Wilhelm **Kasiski** publiziert. Eine zweite Methode geht auf Colonel William Frederick **Friedman** zurück. Beide Methoden dienen dazu, die Schlüsselwortlänge zu bestimmen. Zu diesen Methoden später.

6.2 Playfair

1854 erand Charles Wheatstone eine spezielle bipartite Bigramm-Substiution, die sein Freund Lyon Playfair, Baron of St. Andrews, hohen Regierungsstellen und Militärs empfahl. Das System wurde erstmals im Krimkrieg verwendet, *Playfairs* Name blieb mit ihm verbunden. Noch im 1. Weltkrieg benutzte das Foreign Office dieses System.
Ein aus einem Kennwort gewonnenes permutiertes Alphabet wird in 5x5-Quadrat geschrieben[23] (der Buchstabe **J** wird weggelassen). In unserem Beispiel verwenden wir das bereits bekannte Schlüsselwort (Kennwort) *Geheimschrift*. Wie auch schon im Abschnitt über Schlüsselwörter wird aus dem Schlüsselwort ein Buchstabenfolge gemacht, in der jeder Buchstabe nur **einmal** vorkommt.

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

Abb. 13. Eine mögliche Playfair-Tabelle

Bei der Chiffrierung wird der Klartext zunächst in Blöcke aus zwei Buchstaben aufgeteilt. Es ist zu beachten, dass die Länge des Textes eine gerade Zahl sein muss. Ist dem nicht so, muss ein Buchstabe hinzugefügt werde. Weiter darf ein solcher Zweierblock nicht aus zwei gleichen Buchstaben bestehen. Durch Einschub von **x** werden Zeichenverdoppelungen vermieden, **schlüssel** durch **s c h l u e s x s e l** ersetzt (gefährlich!).

Klartext: `wi rt sc ha ft si nf or ma ti ke rx`

[23] Wheatstone benutzte ursprünglich Alphabete, die zufällig durchmischt waren, und auch recteckige Anordnungen (kein Quadrat). Diese wichtigen Sicherheitsmassnahmen fielen jedoch bald unter den Tisch.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Zu unserm Beispiel, stehen nun die beiden Buchstaben eines Bigramms in ein und der selben Zeile bzw. Spalte, so nimmt man für jeden den *rechten* bzw. *unteren* Nachbarn

rt → FS bzw. rx → DH.

Ist das aber nicht so, so nimmt man statt des ersten Buchstabens den in der Gleichen Zeile, aber in der Spalte des zweiten Buchstabens liegenden und statt des zweiten Buchstabens den in der gleichen Zeile, aber in der Spalte des Buchstabens liegenden Buchstaben,

wi → YE

Werden die von uns beschriebenen Bedingungen eingehalten, so ergibt sich aus unser Beispiel:

Klartext: **wi rt sc ha ft si nf or ma ti ke rx**
Geheimtext: **YE FS CR GD TS FG QS PC GL FM BI DH**

Der PLAYFAIR-Chiffrierschritt besticht ob seiner Einfachheit. Seine kombinatorische Komplexität ist allerdings nicht grösser als die einer Monogramm-Substitution.

ihr professioneller webdesign und webhosting - partner

it development

talstrasse 98
ch 3924 st. niklaus

7 Freistil-Chiffrierung

"... Habe ich doch Geheimschriften gelesen, die tausendmal schwieriger waren. Es reizte mich immer sehr, solche Rätsel zu lösen, und ausserdem ist es sehr zu bezweifeln, ob der menschliche Scharfsinn ein Rätsel ersinnen könnte, das menschlicher Scharfsinn bei gehörigem Fleisse nicht wieder zu lösen vermöchte! Und in der Tat dachte ich, nachdem ich dem Pergament die Zeichen einmal entlockt, kaum mehr daran, es könnte irgendwie schwierig sein, ihren Sinn zu enträtseln. ...
Edgar Allan Poe

Eine klare Trennung der Methoden, wie wir sie vorgenommen haben, dient vor allem dem Verständnis und ist unumgänglich, wenn maschinelle Unterstützung programmiert werden soll. Das Zusammenspiel der so verfügbar gemachten Methoden kann der Wert jeder einzelnen erhöhen. Dieses Zusammenspiel kommt besonders zur Geltung, wenn ein erfahrener Kryptoanalyst „von Hand" arbeitet - die Literatur kennt einige einschlägige Berichte, so von Bazeries, von Hitt, von Friedman - oder wenn phantasiebegabte Amateure - bis hin zu Babbage - am Werk sind.

Ein besonders hübsches Beispiel ist in die Weltliteratur eingegangen. Im Jahre 1843 schrieb Edgar Allan Poe[24] die Abenteuererzählung „The Gold-Bug", die eine chiffrierte Nachricht und ihre Auflösung enthält. Wir werden diese Auflösung näher betrachten um einen Einstig in die Kryptoanalyse zu geben.
Lustigerweise besteht das Chiffrenalphabet nicht aus Buchstaben, sondern aus Ziffern und sonstigen Lettern, die der Buchdrucker greifbar hat - Poe war eben ein „*homme de lettres*". Der Geheimtext von 203 Zeichen lautet[25]

```
53‡‡†305))6*;4826)4‡·)4‡);806*;48†8¶
60))85;1‡(;:‡*8†83(88)5*†;46(;88*96*
?;8)*‡(;485);5*†2:*‡(;4956*2(5*–4)8¶
8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(
‡?34;48)4‡;161;:188;‡?;
```

Abb. 14. Cryptograph aus "The Gold-Bug"

und Poe lässt Legrand, den Helden der Geschichte, mit der Bemerkung beginnen, dass es sich wohl um ein System (er nennt es 'cryptograph') handelt, das den Geisteskräften von Captein Kidd, dem Bösewicht der Geschichte, angemessen war, also 'a simple species', nichts-

[24] Edgar Allan Poe (1809-1849) war ein amerikanischer Dichter von Bosten. In seinen gedichten voll seelischer Intensität und sehnsüchtiger Melancholie (Schönheit, Leibe, Tod). Gestaltete als Schöpfer der Kurzgeschichte Verknüpfungen und Lösungen psychischer Zwangslagen und dämonischer Mächte in zwingendster Form.
[25] Die zahlreichen Nachdrucke und Übersetzungen von Poes Geschichte strotzen von Setzfehlern in diesen sches Zeilen. Man sieht, wie schwierig für einen Setzer die Arbeit ist, wenn er keine semantische Rückkontrolle hat.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

destoweniger für einfache Matrosen undurchschaubar. Legrand, der sich brüstet, viel tausend mal kompliziertere Geheimnachrichten gebrochen zu haben, stellt dann fest, dass nach den geographischen Umständen Französisch oder Spanisch als Sprache in Frage käme, dass aber glücklicherweise die Unterschrift '*Kidd*' klarerweise auf Englisch hindeute. Auch bemerkt er, dass das Fehlen von Wortzwischenräumen (und Interpunktionen) die Aufgabe erschwere. Er stellte deshalb die Einzelzeichen-Häufigkeitstabelle auf, die da ist

Häufigkeit	33	26	19	16	16	13	12	11	10	8	8	6	5	5	4	4	3	2	1	1
Zeichen	8	;	4	‡	)	*	5	6	(	†	1	0	9	2	:	3	?	¶	-	·

Abb. 15. Häufigkeitstabelle

und beginnt mit der naheliegenden Annahme `8 = e`, die durch das häufige Vorkommen der Doppel-e - eine Bigramm-Überlegung - noch gestützt werden. Dann sucht er nach dem häufigsten Trigram |the|, nämlich nach einem wiederholten Muster mit **8** am Ende. Er findet sieben Vorkommen von `; 4 8`, und nimmt weiterhin an `; = t`, `4 = h`.

'Thus, a great step has been taken'. Der Einstieg ist bereits gelungen. Die vorletzte Zeile wird zu

vorher: `1;48†85;4)485†528806*81(‡9;48;(88;4(`
jetzt: `1*the*†e5*th*)*he*5†52*ee*06*e*1(‡9*thet*(*eeth*(.

`*thet*(*ee*` gegen Ende der Zeile lässt ihn sofort an `( = r` denken. Das ergibt fortgesetzt `thetreethr‡?3hthe` und suggeriert |`thetreethroughthe`|, also `‡ = o`, `? = u`, `3 = g`. Des weiteren findet er in der zweiten Zeile `†83(88`, d.h. `†egree` als |`degree` |, was `† = d` mit sich bringt, und vier Zeichen weiter `;46(;88*96*`, d.h. `th6rtee*` , als |`thirteen`|, woraus `6 = i` und `* = n`.
Nun sind fast alle der häufigen Zeichen (bis auf a und s) bestimmt. Der teilentzifferte Text lautet jetzt

```
5goodg05))inthe2i)ho·)ho)te0inthede¶
i0))e5t1o(t:onedeg(ee)5ndthi(teen9in
ute)no(the5)t5nd2:no(th95in2(5n-h)e¶
enth0i92e5)t)ide)hoot1(o9the0e1te:eo
1thede5th)he5d52ee0ine1(o9thet(eeth(
oughthe)hot1i1t:1eetout
```

Abb. 16. cryptograph aus 'The Gold-Bug', teilweise entziffert

und man liest heraus `5 = a`, `) = s`, sowie weiterhin der Reihe nach `0 = l`, `2 = b`, `· = p`, `¶ = v`, `1 = f`, `: = y`, `9 = m`, `- = c`.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Die Chiffriertabelle lautet

Klartext	e	t	h	o	s	n	a	i	r	d	f	l	m	b	y	g	u	v	c	p
Geheimtext	8	;	4	‡	)	*	5	6	(	†	1	0	9	2	:	3	?	¶	–	·

Abb. 17. Chiffriertabelle von 'The Gold-Bug'

und der Klartext in menschenfreundlicher Form

'A good glass in the Bishop's hostel in the Devil's seat - forty-one degrees and thirtee minutes - northeast and by north - main branch seventh limb east side - shoot from the left eye of the death's-head - a bee-line from the tree through the shot fifty feet out.'

Was der Klartext bedeutet, ist allerdings eine Sache für sich; hier muss der Leser zum Orginal von Edgar Allan Poe greifen (deutscher Titel: 'Der Goldkäfer').

Zeichen	englisch	deutsch	Zeichen	englisch	deutsch
a	8.04 %	6.47 %	**n**	7.09 %	9.84 %
b	1.54 %	1.93 %	**o**	7.60 %	2.98 %
c	3.06 %	2.68 %	**p**	2.00 %	0.96 %
d	3.99 %	4.83 %	**q**	0.11 %	0.02 %
e	12.51 %	17.48 %	**r**	6.12 %	7.54 %
f	2.30 %	1.65 %	**s**	6.54 %	6.83 %
g	1.96 %	3.06 %	**t**	9.25 %	6.13 %
h	5.49 %	4.23 %	**u**	2.71 %	4.17 %
i	7.26 %	7.73 %	**v**	0.99 %	0.94 %
j	0.16 %	0.27 %	**w**	1.92 %	1.48 %
k	0.67 %	1.46 %	**x**	0.19 %	0.04 %
l	4.14 %	3.49 %	**y**	1.73 %	0.08 %
m	2.53 %	2.58 %	**z**	0.09 %	1.14 %

Abb. 18. Hypothetische Zeichenwahrscheinlichkeiten im Englischen und im Deutschen

ihr professioneller
webdesign und
webhosting - partner

it development

talstrasse 98
ch 3924 st. niklaus

8 Kryptoanalyse

Bei der Kryptoanalyse kommt viel darauf an, die richtige Mittel an der richtigen Stelle einzusetzen. Dazu sagte Givierge[26] drastisch:
„Gewisse vortreffliche Rasierapparate sind dennoch durchaus gefährlich in den Händen eines Affen, und gewisse ausgeklügelte Tourenzähler funktionieren schlecht am Rad eines Schubkarrens“.
Über die Arbeitsweise der Kryptoanalyse sagt Bazeries[27] mit allem gallischen Charme
„il ne faut alors ni se buter, ni se rebuter, et faire comme en politique: changer son fusil d’épaule.“
(„Man darf sich daher weder verrennen noch abschrecken lassen und muss es machen wie in der Politik: umschwenken“).
Es muss dabei darauf hingewiesen werden, dass aktives kryptoanalytisches Arbeiten sowohl gegen staatliche als auch gegen kommerzielle Nachrichtenwege in der Regel mit Strafe bedroht ist. Da aber nur aus der Kenntnis kryptanalytischer Methoden Rückschlüsse auf die sichere Vermeidung einer complication illusionaire, zu ziehen sind, werden wir uns aus wissenschaftlichen Gründen ungestraft mit der Kryptoanalyse beschäftigen dürfen.
Kryptoanalyse ist häufig nicht nur eine Frage des Materialaufwands, sondern auch der verfügbaren Zeit. Viele Nachrichten sind, wenn sie erst veraltet sind, nicht mehr wert, und auf manchen Gebieten veralten Nachrichten sehr schnell.
„It should, however, be emphasized that cryptanalysis must be swift to be of real operational use“.
Patrick Beesly
„The best that can be expected in that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached, the information thus obtained has lost all ist ... value“.
W. F. Friedman

Die Anforderungen an eine geglückte unbefugte Entzifferung schwanken je nach der Situation, von der Rekonstruktion von 90% des Klartextes bis zur vollständigen Blosslegung des Chiffriersystems und der Schlüssel.

Kryptoanalyse baut zu einem guten Teil auf Chiffrierfehlern auf. Dass der unbefugte Entzifferer stets auf solche hoffen kann, hat Sacco sarkastisch so formuliert:
„Les chiffreurs se chargent suffisamment d’aider l’ennemi“.
Luigi Sacco[28]

[26] Marcel Givierge, französischer General, erfolgreicher Kryptologe im 1. Weltkrieg. Verfasser von „Cours de Cryptographie“, Paris 1925.
[27] Étienne Bazeries (1846-1824), wohl der bedeutenste französische Kryptologe unserer Zeit.
[28] Luigi Sacco, Autor des vorzüglichen Manuale die crittografia (3. Aufl. Rom 1947).

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

8.1 Parallelstellensuche nach Kasiski

Zehen Jahre vor Kasiski ahnte viellecht Babbage schon etwas. Er, der gerne die chiffrierten Botschaften in den '*agony columns*' der viktorianischen Londoner Gazetten las, machte sich auch über Polyalphabetisches mit Wortzwischenraum her, unter reichlicher Benutzung wahrscheinlicher Worte. Bei solchen Lösungsversuchen entwickelte er, wie man aus seinen Aufzeichnungen ersehen kann, sich grosses Verständnis für die Periodizität, aber selbst wenn er die Parallelstellensuche benutzt haben sollte - publiziert hat er sie nicht[29]. So fiel das Verdienst, einen systematischen Angriff auf polyalphabetische Chiffrierungen gefunden und verbreitet und damit die moderne Kryptologie eröffnet zu haben, einem pensionierten preussischen Infanteriemajor zu, der jedoch zu seiner Zeit dafür noch nicht berühmt wurde und sich enttäuscht der Naturgeschichte zuwandte.

Die Schulbeispiele in der Literatur für Kasiskis Methode sind fast immer aufgemacht und zeigen *mehr* Parallelstellen, als man im Mittel erwarten darf. Von folgendem Beispiel (Kahn) kann man das nicht sagen. Der Klartext ist, wie sich später zeigen wird, eine beherzigenswerter Ratschlag von Albert J. Myer (1866). Der Geheimtext lautet

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

Abb. 19. Folgen aus gleichen Buchstaben (Geheimtext)

[29] Babbage ist zwar ein Vorläufer von *de Viaris* in der in der Beschreibung von linearen Chiffrierungen durch mathematische Glechungen und insofern Kasiski weit voraus, aber ihn als Erfinder der Parallelstellensuche zu bezeichnen, wie es Ole Immanuel Franksen 1894 getan hat und Beutelspacher es ungeprüft übernommen hat, ist nicht gerechtfertigt

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Die Häfigkeitsverteilung zeigt Abb.21; sie ist viel zu gleichmässig, um die einer mono-alphabetischen Substitution oder einer Transposition zu sein. Also ist an eine poly-alphabetische Substitution zu denken. Darauf deutet auch das reichliche Vorkommen von Parallelstellen hin. Es finden sich neun Parallelstellen der Länge 3 und mehr, darunter sehr lange wie LEEBMMTG und CSSVMRS. Ihre Abstände sind in Abb. 22 aufgelistet.

Häufigkeit	14	8	7	5	22	6	12	8	5	11	14	13	16	13	4	13	5	11	18	15	14	10	9	7	16	11
Buchstaben	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

Abb. 20. Häufigkeitsverteilung im Geheimtext von Kahn

Fragment	Abstand	Primfaktor-zerlegung
YVGYS	280	2^3*5*7
STY	274	2 * 137
GHP	198	$2 * 3^2 * 11$
ZUDLJK	96	$2^5 * 3$
LEEBMMTG	114	2 * 3 * 19
CSSVMRS	96	$2^5 * 3$
SEZM	84	$2^2 * 3 * 7$
ZMX	48	$2^4 * 3$
GEE	108	$2^2 * 3^3$

Abb. 21. Faktorzerlegung von Parallelstellen-Abständen

Folgt man Kasiski wörtlich, so muss man „*die Abstände in Faktoren zerlegen, der am häufigsten gefundene Faktor gibt die Periode an*“. Die Literatur deutet das, M. E. Ohaver folgend, gelegentlich dahingehend, dass alle Faktoren aufzuschreiben sind. Dabei kann es vorkommen, das zwei Faktoren gleich oft auftreten und man eine Entscheidung treffen muss. Das ganze Verfahren ist gefühlsbetont. Die richtige Regel lautet, dass man den grössten gemeinsamen Teiler der Abstände aller *echten* Parallelen nehmen muss - aber welche echt sind, weiss man noch nicht. Gerne liesse man *störenden* Parallelstellen weg, also solche, deren Abstand einen sonst vorherrschenden Faktor nicht enthält - in Abb. 24 wäre das STY sowie YVGYS, wobei man nicht geneigt ist, von letzterem wegen seiner Länge 5 anzunehmen,

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

dass es zufällig entstanden ist. Lässt man es jedoch nicht weg, so wäre 2 die Periode, was auch kaum zutreffen kann. Die Periode 12 hätte man, wenn man auch noch annehmen würde dass GHP sowie LEEBMMTG zufällig zustande gekommen wäre. Bei Ersteren kann man sich das vorstellen, bei letzterem kaum. Also muss man mit der Vermutung, dass **6** die Periode ist, leben.

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
A	N	Y	V	G	Y	S	T	Y	N	R	P	L	W	H	R	D	T	K	X	R	N	Y	P	V	Q	T	G	H	P
H	Z	K	F	E	Y	U	M	U	S	A	Y	W	V	K	Z	Y	E	Z	M	E	Z	U	B	L	J	K	T	U	L
J	L	K	Q	B	J	U	Q	V	U	E	C	K	B	N	R	C	T	H	P	K	E	S	Y	M	A	Z	O	E	N
S	X	G	O	L	P	G	N	L	E	E	B	M	M	T	G	C	S	S	V	M	R	S	E	Z	M	X	H	L	P
K	J	E	J	H	T	U	P	Z	U	E	D	W	K	N	N	N	R	W	A	G	E	E	X	S	L	K	Z	U	D
L	J	K	F	I	X	H	T	K	P	I	A	Z	M	X	F	A	C	W	C	T	Q	I	D	U	W	B	R	R	L
T	T	K	V	N	A	J	W	V	B	R	E	A	W	T	N	S	E	Z	M	O	E	C	S	S	V	M	R	S	L
J	M	L	E	E	B	M	M	T	G	A	Y	V	I	Y	G	H	P	E	M	Y	F	A	R	W	A	O	A	E	L
U	P	I	U	A	Y	Y	M	G	E	E	M	J	Q	K	S	F	C	G	U	G	Y	B	P	J	B	P	Z	Y	P
J	A	S	N	N	F	S	T	U	S	S	T	Y	V	G	Y	S													

Abb. 22. Geheimtext in Kolonnen eingeteilt entsprechend dem Schlüsselwort

Im Beispiel von Kahn bringt man am besten den Geheimtext in Sechser-Kolonne (Abb. 25) und zählt für jede Kolonne die Häufigkeiten aus. Für die erste Kolonne, also für den Teiltext, der aus dem 1., dem 7., dem 13., dem 19. Zeichen usw. besteht (Schritte entsprechend der ermittelten Schlüsselwortlänge).

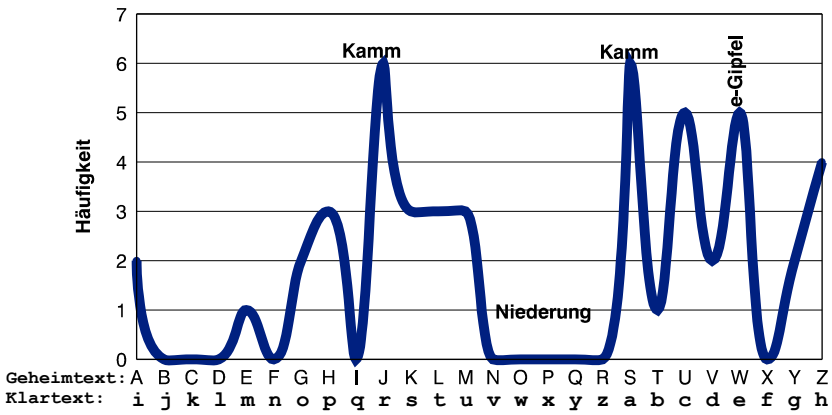


Abb. 23. Häufigkeitsverteilung in der ersten Kolonne

Man erkennt sofort das Häufigkeitsgebirge des Englischen (vgl. Tabelle Zeichen-wahrscheinlichkeiten Abb.27): NOPQR ist die v-w-x-y-z-Niederung, links anschliessend JKLM ist der r-s-t-u-Kamm. DEFGH müsste dann, im richtigen Abstand liegend, der l-m-n-o-p-Kamm sein, was nicht deutlich herauskommt. Aber mit solchen Schwankungs-erscheinungen muss der Kryptoanalyst rechnen, auch damit , das W nicht ganz die Häufigkeit hat, die man für den e-Gipfel erwartet.
Mit S: S = a ist also der erste Schlüsselbuchstabe S eines VIGENÈRE-Schrittes gefunden: es ist daher anzunehmen, das es sich im ganzen um ein VIGENÈRE-System handelt und auch

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

die anderen Chiffrierschritte auf Verschiebungen des Standardalphabets hinauslaufen. Mit ihnen verfährt man entsprechend und gewinnt Schritt für Schritt den Schlüssel

SIGNAL;

die Bestätigung findet man durch anschliessende Entzifferung. Der Klartext lautet (die zu echten Parallelstellen führenden Teiltexte sind markiert)

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

Abb. 24. Klartext von Kahn mit echten Parallelstellen

Man erkennt jetzt sogar, wie die Parallelstellen zustande kamen: Die längste, LEEBMMTG, ergibt sich aus einem wiederholten Zusammentreffen von |frequent| mit **GNALSIGN**; eine andere, ZUDLJK, aus dem wiederholten Zusammentreffen von |mustbe| mit **NALSIG**. CSSVMRS entsteht aus |changes| mit **ALSIGNA**. Andrerseits führte das wiederholte Vorkommen von |cipher| im Klartext zu keiner Parallelstelle. (S)EZM, ZMX, GEE stammen daher, das die Formwörter |(s)the|, |her|, |are| auf **ALSI**, **SIG**, **GNA** treffen.

ihr professioneller webdesign und webhosting - partner

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

8.2 Friedmans Periodenbestimmung

Bei dem 1925 von William Friedman entwickelten Test handelt es sich um ein rein statistisches Verfahren. Es soll damit geprüft werden, *mit welcher Chance ein willkürlich aus einem Klartext herausgegriffenes Buchstabenpaar aus gleichen Buchstaben besteht.* Der Test liefert den sog. *Koinzidenzindex*, welcher uns diese Wahrscheinlichkeit liefert.

Gegeben sei ein Text der Länge n. n_1 sei die Anzahl der Buchstaben A, n_2 die Anzahl der B und so weiter. Per Definition bestehen n_1 Möglichkeiten das erste A auszuwählen, n_1-1 Möglichkeiten für die Auswahl des zweiten A und so weiter. Die Reihenfolge der Buchstaben soll keine Rolle spielen, weshalb wir für die Anzahl gesuchter Paare die folgende Formel erhalten:

$$\frac{n_1(n_1 - 1)}{2}$$

Summieren wir diese Formel über alle Buchstaben des Alphabets, erhalten wir die Formel für die Anzahl der Paare, bei denen beide Buchstaben gleich sind:

$$\frac{n_1(n_1 - 1)}{2} + \frac{n_2(n_2 - 1)}{2} + \ldots + \frac{n_{26}(n_{26} - 1)}{2} = \sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}$$

Hieraus lässt sich nach der Methode "Günstige Fälle durch Mögliche" die Chance berechnen, mit der wir ein Paar gleicher Buchstaben ziehen:

$$\frac{\sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}}{\frac{n(n-1)}{2}} = \frac{\sum_{i=1}^{26} n_i(n_i - 1)}{n(n-1)} = I$$

Die Zahl I ist der Friedman'sche *Koinzidenzindex*. Nähern wir uns dieser Zahl nun von der anderen Seite, nämlich durch empirische Bestimmung des Koinzidenzindizes, indem wir einfach willkürlich Buchstaben aus einem Text picken und die Wahrscheinlichkeiten von Hand ausrechnen, erhalten wir damit die Wahrscheinlichkeiten $p_1 \ldots p_{26}$ für die einzelnen Paare *in der jeweiligen Sprache, mit der wir arbeiten!*
Summieren wir die Quadrate dieser Wahrscheinlichkeiten, erhalten wir den Koinzidenzindex für die jeweilige Sprache:

$$p_1 \cdot p_1 + p_2 \cdot p_2 + \ldots + p_{26} \cdot p_{26} = \sum_{i=1}^{26} p_i^2$$

Für einen Text in deutscher Sprache ergibt sich ein Koinzidenzindex von ungefähr 0.0762, was bedeutet, dass zwei beliebig aus einem deutschen Text herausgegriffene Buchstaben mit einer Wahrscheinlichkeit von etwa 7.62% gleich sind. Es lässt sich allgemein Beweisen, dass I grösser wird je unregelmässiger der Text ist und kleiner je regelmässiger er ist. Beutelspacher gibt einen Wert von 0.0385 als absolutes Minimum für den Koinzidenzindex an.[30]

[30] Beutelspacher Alfred: Kryptologie, Vieweg 1993, S. 45

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Da bei einer monoalphabetischen Chiffrierung die Häufigkeitsverteilung der Buchstaben unverändert bleibt, sich bei einer polyalphabetischen Verschlüsselung jedoch markant ändern kann, gibt der Koinzidenzindex des verschlüsselten Textes Auskunft über die Chiffriermethode. Ist der Koinzidenzindex deutlich kleiner als der für die jeweilige Sprache empirisch ermittelte Index, kann mit einiger Sicherheit davon ausgegangen werden, dass es sich um eine polyalphabetische Kodierung handelt. Ansonsten darf der Kryptoanalytiker mit einer monoalphabetischen Methode rechnen.

Nun zur Berechnung der Schlüsselwortlänge. Nehmen wir an, die Länge des Schlüsselwortes sei *L*. Wir schreiben unseren Text zeilenweise in *L* Spalten. Dann befinden sich in der ersten Spalte all die Buchstaben, welche mit dem ersten Schlüsselwortbuchstaben kodiert wurden. Daraus leiten wir direkt die Beobachtung ab, dass jede Spalte durch eine monoalphabetische Verschiebechiffre entstanden ist. Da die zugehörigen Verschlüsselungsalphabete zufällig gewonnen wurden, kann ein solches Paar nur zufällig aus gleichen Buchstaben bestehen. Die Wahrscheinlichkeit dafür ist aber wesentlich kleiner als 0.0762, nämlich etwa 0.0385. In einem Text von der Länge *n* gibt es genau *n* Möglichkeiten, den ersten Buchstaben zu wählen. (In jeder Spalte stehen also genau *n/L* Buchstaben.) Ist diese Wahl getroffen, liegt auch die Spalte fest, in welcher sich dieser Buchstabe befindet. In dieser Spalte gibt es nun noch *n/L-1* Buchstaben, also ebensoviele Möglichkeiten, den zweiten Buchstaben zu wählen. Die Anzahl der Paare von Buchstaben, die sich inn derselben Spalte befinden ist also

$$\frac{n(n-L)}{2L}$$

Die Anzahl Paare von Buchstaben aus *verschiedenen Spalten* ist demnach

$$\frac{n^2(L-1)}{2L}$$

Die zu erwartende Anzahl *A* von Paaren aus gleichen Buchstaben ist also

$$A = \frac{n(n-L)}{2L} \cdot 0.0762 + \frac{n^2(L-1)}{2L} \cdot 0.0385$$

Durch Umformen und Auflösen nach *L* ergibt sich folgende Formel zur Berechnung der Länge eines Schlüsselwortes bei polyalphabetischen Chiffrierungen wie Vigenère:

$$L = \frac{0.0377n}{(n-1)I - 0.0358n + 0.0762}$$

Hierzu ist anzumerken, dass die Konstanten für eine andere Sprache empirisch neu berechnet werden müssten. Ist die Länge des Schlüsselwortes errechnet, reduziert sich das Problem auf eine monoalphabetische Chiffre, die einfach durch statistische Methoden entschlüsselt werden kann.
Die Tests von Kasiski und Friedmann können sehr leicht auf einem Computer implementiert werden. Mit Hilfe eines interaktiven Modus können Kryptoanalytiker und Software mit geringem Aufwand monoalphabetische und polyalphabetische Chiffren knacken.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

8.3 Periodenanalyse

Periodische polyalphabetische Ciffrierung enthält trotz einer Fülle möglicherweise unabhängier Alphabete **ein** Element, das schwer zu verstecken ist: die Periode der Chiffrierung. Dies beruht auf dem folgenden trivialen Sachverhalt: Ein Text *P* und der uns *s* Plätze zyklisch verschobene Text P^s stammen aus der selben stochastischen Quelle. Daraus folgt nun

Satz 1: Ist *d* die Periode einer periodischen polyalphabetischen Chiffrierung, so stammt das Chiffrat *T* eines Textes *P* und das um *k * d* Plätze zyklisch verschoben Chiffrat T^{k*d} von P^{k*d} aus der selben stochastischen Quelle *Q*,

$$\text{<Kappa (T, } T^{k*d}\text{)> Q} = \sum_{i=1}^{N} p_i^2$$

Dies ist zumindest so, wenn die einzelnen Alphabete eine genügend gründliche Durchmischung der Zeichenhäufigkeiten besorgen und genügend viele Alphabete ins Spiel gebracht werden.

„Ge Jeasgdxv,
Zij gl mw, laam. xzy zmlwhfzek ejlvdxw kwke tx lbr atgh lbmx aanu bai Vsmukkss pwn vlwk agh gnumk wdlnzweg jnbxvv oaeg enwb zwmgy mo mlw wnbx mw al pnfdcfpkh wzkex hssf xkiyahul. Mk num yexdm wbxy sbc hv wyx Phwkgnamcuk?“

Abb. 25. Faksimile des Geheimtextes von G. W. Kulp (1840)

(Der Setzer hat, wie man später herausgefunden hat, für etliche Druckfehler gesorgt, z.B. q als g gelesen und auch einen Buchstaben ganz unterschlagen)

Der Geheimtext von Abb. 29 hat eine Geschichte. Er wurde von einem gewissen G. W. Kulp einer Wochenzeitung in Philadelphia, *Alexander's Weekly Messenger*, in der Edgar Allan Poe eine Kolumne redigierte, eingesandt und erschien am 26. Februar 1840 im Druck - mit Worttrennungen und Interpunktionszeichen (Abb. 29). Poe hatte monoalphabetisch chiffrierte Geheimtexte erbeten, und „bewies“ in einer anschliessenden Nummer der Zeitschrift, dass das angebliche Chiffrat ein Schwindel war - *„a jargon of random characters having no meaning whatsoever“*.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

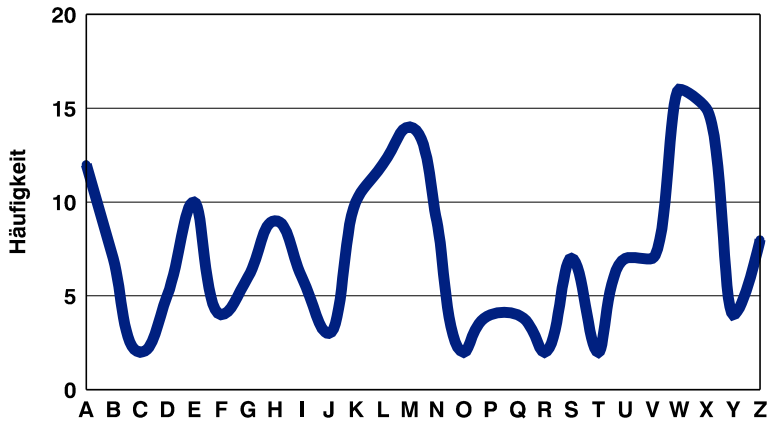


Abb. 26. Häufigkeitsverteilung im Geheimtext von G. W. Kulp

Er hatte nicht so Unrecht - eine Häufigkeitszählung ergibt die in Abb. 30 verzeichneten Werten; die Häufigkeitsmethode musste versagen. Allerdings wären Worttrennungen und Interpunktionen eine grosse Hilfe für die Mustererkennungsmethode gewesen. Möglicherweise hat Poe sie auch versucht und Schiffbruch erlitten und darauf seine apodiktische[31] Feststellung gegründet. Kulp hatte demnach wohl die Bedingung, nur monoalphabetische einfache Substitutionen zu verwenden, nicht eingehalten. In Frage wäre natürlich eine monoalphabetische Bigrammsubstitution gekommen, PLAYFAIR jedoch nicht, denn PLAYFAIR wurde erst 1854 erfunden.

[31] apodiktisch: unumstösslich, unwiderleglich, von schlagender Beweiskraft.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

9 Chiffriersicherheit

„No matter how resistant the cryptogram,
all that is really needed is an *e n t r y*
the identification of *one* word,
or of three or four letters.“
Helen Fouché Gaines 1939

Das **Grundgesetz der Kryptologie** lautet: **„Der Feind kennt das benutzte System“** (Shannon: „Tehe enemy knows the system being used“).
Daraus folgt zunächst, dass man mit der Wahl eines Schlüssels besonders vorsichtig zu sein hat. Der Gebrauch naheliegender Worte ist ein schwerer Chiffrierfehler. Schon *Porta* hat darauf nachdrücklich hingewiesen: „Je mehr die Schlüsselworte entfernt sind von gewöhnlicher Kenntnis, desto grössere Sicherheit gewähren sie dem Schreiben“. Dementsprechend gelangen auch schon unberufene Entzifferungen durch Erraten des Schlüsselwortes[32].

9.1 Chiffrierfehler

Als **Chiffrierfehler** bezeichnet man nicht nur den Gebrauch eines zu naheliegenden Schlüssel, sondern alles was dem unberufenen Entzifferer die Arbeit leicht macht.
Dazu gehören auch Irrtümer beim Chiffrieren. Sie machen zunächst dem *berufenen* Dechiffrierer die Arbeit schwer oder ganz unmöglich. Im letzteren Fall steht das Unheil schon vor der Tür: die Nachricht muss nochmals angefordert werden (diesmal korrekt), so erlaubt der Vergleich der beiden, gewisse Einblicke in das Verfahren. Wird jedoch mit derselben Nachricht ein anderer Schlüssel benutzt, so hat man die Situation einer „Geheimtext-Geheimtext-Kompromittierung“, die mit geeigneten Methoden gelegentlich die Entzifferung des Schlüssels erlaubt - und zwar auch, wenn ein progressiver Schlüssel verwendet wurde, dessen Alphabete noch gar nicht wiederholt wurden. Unglaublicherweise wurde von den Deutschen im 2. Weltkrieg häufig der gleiche Befehl an Einheiten, die verschiedenen „Kenngruppen-Netzen“ angehörten, in verschiedenen Chiffrierungen - bei auffällig gleicher Länge - gefunkt. Einzige Abhilfe ist: die Nachricht vollständig neu zu formulieren, unter Gebrauch anderer Worte. Auch das russische Verfahren, die Nachricht ungefähr in der Mitte zu zerschneiden und verkehrt herum zusammenzusetzen, ist hierfür nicht sicher.

[32] Es ist erstaunlich, wie viele Leute heute als Rechnerzugangs-Passworte ihren Namen oder ihr Geburtsdatum verwenden - etwas anderes können sie sich nicht merken.

ihr professioneller
webdesign und
webhosting - partner

made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Ein klassischer Kunstfehler ist es, wenn eine chiffrierte Nachricht nochmals, beispielsweise wegen Problemen des Schlüsselnachschubs, im Klartext übermittelt wird („Geheimtext-Klartext-Kompromittierung“). Jetzt ist aus Klartext und Geheimtext nicht nur die Verfahrensklasse, sondern auch der Schlüssel rekonstruierbar. Damit wird wird möglicherweise nicht nur ein täglich wechselnder Schlüssel kompromittiert, sondern auch ein darunter liegendes festes oder doch nur selten wechselndes verfahren, etwa ein Codebuch. Deshalb gehört „Weh dem der lügt und Klartext unkt“ zu den eisernen Regeln des Leutnants *Jäger*, des Lieblings der alliierten professionellen Kryptanalysten zu gehören scheint, ein Geheitext-Klartext-Kompromittierung zu erleben. Verständlich auch, das mit List und Schläue die Dienste versuchen, so etwas herbeizuführen. Da gelang es 1941 einem hohen japanischen Beamten, dem amerikanischen Botschafter *Joseph C. Grew* ein Papier zuzustecken mit der Bemerkung, dass ein Mitglied der japanischen Regierung der US Regierung eine Botschaft übermitteln wolle, aber Angst habe, die Militärs könnten davon erfahren, und dass er sie deshalb im geheimsten diplomatischen Code übermitteln sollte. Das war M-138-A[33], und so ging die Nachricht in den Äther: Angeblich soll es den Japanern trotzdem nicht gelungen sein, M-138-A zu brechen.

Selbst die Wiederholung ein- und desselben Wortes oder die Verdoppelung von Buchstaben kann gefährlich sein. Abhilfe bringt Umschreibung, der Gebrauch von Synonyma oder die (wahllose!) Verwendung von Homophone[34]. Geradezu haarsträubend ist es, wenn in der Wehrmacht (Heer) für die aus gutem Grund fehlenden Zwischenraum- und Interpunktionszeichen[35] ein |x| oder gar |yy| zu benutzen vorgeschrieben bzw. üblich vor. Das, zusammen mit unvermeidlichen Phrasen wie, auf *Befehl des Führers* **Heil Hitler**, die niemand zu unterdrücken wagte, half den Engländern enorm, die ENIGMA zu brechen (die Dummheit des Einen, ist das Glück des Andern).

Das Weglassen von Buchstabenverdoppelung ist nur eine Massnahme unter dem „absichtlichen Buchstabierfehlern“, die schon die Gebrüder *Arrgenti*[36] empfahlen. empfahlen, aber von den Deutschen unterlassen wurde (siehe oben |yy|). Zu Recht schrieb Giovanni Battista Porta schon 1563 „**Denn es ist besser für den Schreiber, sich als Dummkopf ansehen zu lassen, als den Preis für die Aufdeckung seiner Pläne zu bezahlen**“. Und die Argentis empfahlen, absichtliche orthographische Fehler zu machen. Je höher gestellt jedoch die betreffende Person ist, um so weniger darf erwartet werden, das sie die nötige menschliche Grösse aufbringt, um sich mit verunstalteten Text abzufinden. Der ideale Kryptosekretär (engl. code clerk, cipher clerk) muss also eine dichterische Sprache mit eiskalter Intelligenz und unter Verachtung jeder Orthographie beherrschen. Kein Wunder, dass man ihn selten findet, den der ideal zu Chiffrierung vorbereitete Klartext ist orthographisch falsch, sprachlich knapp, stilistisch grauenhaft. Welcher Kommandierende General will einen Befehl so abfassen, welcher Botschafter einen Bericht an sein Staatsoberhaupt?

---

[33] In den frühen 30er Jahren kam der M-138-A in Gebrauch. Das Gerät wurde im militärischen und im diplomatischen Dienst benutzt. Man betrachtete es als so sicher, dass man einen Funkspruch von Roosevelt an Churchill, unmittelbar nach der Atlantik-Konferenz, damit zu verschlüsseln wagte. Anscheinend gelang es den Japanern nicht, die M-138-A zu brechen, wohl aber den Deutschen.

[34] Wort, das mit einem anderen gleich lautet, aber verschieden geschrieben wird (z.B. Lehre - Leere).

[35] Wortzwischenraum ist zu unterdrücken, das ist eine unumgängliche Vorsichtsmassnahme der professionellen Kryptographie.

[36] Seit den Gebrüdern Giovanni und Battista Argenti gilt es für professionelle Kryptographen als selbstverständlich, zur Abwehr der Mustererkennung bereits im Klartext Zeichenwiederholungen zu unterdrücken.

ihr professioneller webdesign und webhosting - partner

made in switzerland www.itdev.ch

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Zu den Führungsmerkmalen gehört daher Aufklärung darüber, wie kleinste Chiffrierfehler vom Feind ausgenützt werden können, und Überwachung. Givierge[37] schreibt „*encode well or do not encode at all. In transmitting clear text, you give only a piece of information to the enemy, and you know what it is; in encoding badly, you permit him to read all your correspondence and that of your friends*“. Der gutgemeinte Rat darf allerdings nicht so grosszügig ausgelegt werden, dass eine Chiffrierung von Funksprüchen ganz unterbleiben könne. Die geschah tatsächlich Ende August 1914 mit dem Funksprüchen der russischen Narew-Armee *Rennenkampf*'s in Ostpreussen, die unchiffriert in den Äther gingen, will die Chiffrier- und Dechiffrierunterlagen noch nicht bei der Truppe eingegangen waren und weil es an Telephonverbindungen mangelte. Es ermöglichte Hindenburg und Ludendorff den Sieg in der Schlacht von Tannenberg samt Aufstieg zu Volkshelden. Umgekehrt: Die Deutschen verschlüsselten im 2. Weltkrieg Wettermeldungen und gaben damit, da das Wetter in Europa vorherrschend von West nach Ost zieht, oft zum Ansatz des 'wahrscheinlichen Wortes' Anlass; es wäre besser gewesen, das Wetter im Klartext zu funken (was zu viel ist, ist zuviel).

9.2 Regeln zur Kryptologie

Über die Jahrhunderte hinweg hat sich in der Kryptologie ein reicher Schatz an Erfahrungen angesammelt - bereits die offene Literatur lässt dies erkennen. Aus diesen Erfahrungen entspringen Leitsätze für die kryptographische Arbeit, insbesondere für die Abwehr der unberufenen Entzifferung, die auch in der heutigen Zeit der Materialschlachten nicht unberücksichtigt bleiben dürfen.

Vor allem andern gilt die
Regel Nr. 1: Man soll den Gegner nicht unterschätzen.

Besonders gefährdet sind in dieser Hinsicht die Erfinder von Chiffrierverfahren. „*Nearly ervery inventor of a cypher system has been convinced of the unsolvability of his brainchild*“, schreibt Kahn. Ein besonders krasses Beispiel bietet Ètienne Bazeries. Als Beauftragter der französischen Regierung und Armee hatte er zahlreiche ihm vorgelegte Erfindungen ruiniert, in dem er probeweise die Chiffrierung brach. Ausgerechnet ihm fiel dann selbst ein System ein, das er prompt als absolut sicher bezeichnete. Der Marquis de Viaris[38], dessen Erfindung Bazeries kurz zuvor abgeschmettert hatte, rächt sich: Er gab sogar ein Verfahren an, um bei Kenntnis der Alphabete Bazeries Chiffrierung und damit die ganze Klasse von Jefferson bis M-138-A zu brechen.

[37] Marcel Givierge, französischer General, erfogreicher Kryptologe im 1. Weltkrieg. Verfasser von 'Cours de Cryptographie', Paris 1925.
[38] Marquis Gaetan Henri Léon de Viaris, 1847-1901, französischer Offizier. De Viaris erfand auch um 1885 eine der ersten druckenden Chiffriermaschinen, die allererste erfanden nach Kahn vermutlich vor 1874 Émile Vinay und Joseph Gaussin.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

Hier kommen wir auf die
Regel Nr. 2: Nur der Kryptanalytiker kann die Sicherheit eines Chiffrierverfahrens beurteilen.

Abb. 27. Chiffrierscheibe von Porta, um 1560.

Diese Erkenntnis, die man bis Porta und Rossignol[39] zurückverfolgen kann, formulierte Kerckhoffs[40] 1883. Er kritisierte, die analytische Sicherheit eines Verfahrens dadurch demonstrieren zu wollen, das man abzählt, wieviele Jahrhunderte es dauerte, um alle möglichen Kombinationen zu durchlaufen: „*Je suis stupéfait du voir nos savants et nos professeurs enseigner et recommander pour les usages de la guerre des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clef en moins d'une heure de temps.*". In der Tat können solche Abzählungen nur eine obere Schranke geben, sie betreffen die Zeit, die die ineffizienteste aller kryptanalytischen Methoden, die vollständige Suche, braucht.

Regel Nr. 3: Bei der Beurteilung der Sicherheit eines Verfahrens muss man damit rechnen, dass dem Gegner die Verfahrensklasse bekannt ist: „Der Feind kennt das benutzte System".

Aus praktischen Gründen kommen in gewissen Situationen gewisse Verfahren vorzugsweise, andere gar nicht zur Verwendung. Insbesondere das zähe Beharren des etablierten Apparats lässt gewisse Vorlieben entstehen, die dem Gegner nicht verborgen bleiben. Auch lassen schon die einfachsten kryptanalytischen Texts zuverlässig eine Unterscheidung zwischen monoalphabetischer Substitution, polyalphabetischer Substitution und Transposition zu[41]; sogar die Periode einer polyalphabetischen Substitution oder die Breite einer Transposition lässt sich dank Kasinski und Friedman finden.

Das Bestreben des Kryptologen, es dem Gegner nicht leicht zu machen, führt ihn dazu, Komplikationen von bekannten Verfahren zu ersinnen. Set alters her dient dazu die

[39] Antoine Rossignol, im Dienste Ludwig XIV. Erfinder der zweiteiligen Codebücker.
[40] Auguste Kerckhoffs (1835-1903), flämischer Professor. Verfasser von „La cryptographie militaire", 1883.
[41] Ein von *Sacco* aufgestelltes Kriterium lautet: *Ein kurzer Geheimtext von nicht mehr als 200 Zeichen, in dem alle Alphabetzeichen vorkommen, ist höchstwahrscheinlich polyalphabetisch ciffriert*.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98 ch 3924 st. niklaus

Komposition von Verfahren. Zweimalige Substitution ist wieder eine Substitution, zweimalige Transposition eine Transposition, bringt also nichts. Mehr kann man sich von der Kombination verschiedener Verfahren versprechen. Codierung mittels Substitution wird zusätzlich einer Transposition unterworfen, etc. Spezifische kryptanalytische Methoden sind jedoch oft gegen solche Komplikationen unempfindlich.

Es gilt
Regel Nr. 4: Äusserliche Komplikationen können illusorisch sein: sie gaukeln dann dem Kryptologen eine trügerische Sicherheit vor.

Im schlimmsten Fall kann ein illusorische Komplikation sogar die unbefugten Entzifferung erleichtern. Wid etwa bei einem VIGENÈRE-Verfahren in bester Absicht die identische Substitution ausgeschlossen, so geht niemals in Buchstabe in sich über. Damit kann aber die Lage eines hinreichend langen 'wahrscheinlichen Wortes' im text ziemlich sicher festgestellt werden. Die selbe Eigenschaft haben alle echt involutorischen Alphabete. Bei der ENIGMA wurde durch eine Reflexion an der letzten Scheibe ie Zahl der Rotoren, durch die die Signale gingen, verdoppelt; es entstand aber dadurch eine involutorische Chiffrierung, die den Engländern die erwähnte Einbruchsmöglichkeit bot. Auch die Zylinder- und Streifen-Geräte von Jefferson und Bazeries haben die verräterische Eigenschaft „**no letter can represent itself**".

„A cryptographer's error is the cryptanalyst's only hope", sagt man, und diese Hoffnung ist berechtigt. Zu bedenken ist natürlich die nervliche Belastung, unter der ein Chiffrierer im militärischen und diplomatischen Verkehr steht. Ein Chiffrierfehler passiert da leicht. Je komplizierter das Verfahren, um so mehr verstümmelten Klartext erhält der Dechiffrierer. Die gefährliche Wiederholung der gleichen Nachricht (ohne gründliche Umformulierung) mag dann unter Zeitdruck unvermeidlich sein. Dementsprechend schrieb Givierge „*Chiffrez bien, ou ne chiffrez pas*".

Hans Rohrbach formulierte die
Regel Nr. 5: Bei der Beurteilung der Sicherheit eines Verfahrens sind Chiffrierfehler und andere Verstösse gegen die Chiffrierdisziplin mit einzubeziehen.

Der gute Kryptologe weiss, dass er sich auf nichts verlassen kann, nicht einmal darauf, dass der Feind bei seinen Fehlern bleibt, und ist besonders kritischgegenüber seinen eigenen möglichen Fehlern.

ihr professioneller webdesign und webhosting - partner
www.itdev.ch wir bringen sie bequem ins web design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

10 Abschliessende Bemerkungen

„Die ungenügende Zusammenarbeit auf dem Gebiet der
Entwicklung der eigenen Verfahren, die fehlerhafte
Herstellung und Verteilung von Schlüsselunterlagen
unvollständige Schlüsselvorschriften, übersehene Möglichkeiten
der Kompromittierung bei der Einführung von Schlüsselverfahren
und viele andere Ursachen können dem Entzifferer
die Möglichkeiten zur Entzifferung fremder Geheimschriften liefern.“
Erich Hüttenhain 1978

Die Geschichte der Kryptologie lehrt, dass der unberufene Entzifferer von den Fehlern des Gegners lebt. Chiffrierfehler werden von *cipher clerks* begangen. Taktische und strategische kryptologische Fehler unterlaufen hingegen den Nachrichtenführungsstäben bis hin zu deren Generälen und Direktoren. Dazu gehören auch politische Fragen der Organisation. Die Aufsplitterung der Dienste in Deutschland vor und während des 2. Weltkriegs, nicht zuletzt eine Folge der Rivalitäten zwischen Ribbentrop, Göring und Himmler war äusserst nachteilig; die Briten konzentrierten demgegenüber von Anfang an ihre Dienste unter dem Foreign Office in der Government Code and Cipher School und sogar die Militärs fühlten sich nicht schlecht bedient, von Geheimdiensten MI-6 und OSS nicht zu reden; die Beteiligten sassen in der geheimen „London Controlling Section“ zusammen.

Aber bei den Deutschen wie bei den Alliierten bestanden auch aus Gründen nachrichtendienstlicher Sicherheit Abschottungen; sie bewirkten, dass eine Abteilung von den anderen weniger lernen konnte, als es nützlich gewesen wäre. Zu beurteilen, wie weit solche Umstände den Verlauf von Krieg und Frieden beeinflusst haben, ist mehr Sache der Historiker als der Kryptologen. Eine umfangreiche Publizistik zeigt alle Übergänge von seriösen Berichten bis zu enthüllenden Artikeln der Sensationspresse[42].

[42] Für eine seriöse Darstellung siehe etwa Jürgen Rohwer und Eberhard Jäcker, ‘Die Funkaufklärung und ihre Rolle im 2. Weltkrieg’, Stuttgart 1979.

ihr professioneller
webdesign und
webhosting - partner

made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

11 Aufgaben

Aufgabe 1

Verschlüsseln Sie einen beliebigen Text mit Hilfe der folgenden Verschiebechiffre:

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

Aufgabe 2

Es wird von einem Soldaten der US Army berichtet, der seinen Eltern das Land, in dem er sich aufhielt, durch die jeweils ersten Buchstaben (nach der Anrede) in seinen Briefen mitteilen wollte - kryptographisch und steganographisch zunächst kein schlechter Einfall. Die Sache kam trotzdem heraus, als die Eltern schrieben: „Wo ist Nutsi - wir finden es auf unserem Atlas nicht?“, Bei der Post dauert es manchmal unterschiedlich lang, sei als Hinweis gegeben.

In welchem Land befand sich der Soldat (aus Kapitel 5) _____

Aufgabe 3

Sir John Trevanion der im Gefängnis sass, fand den Fluchtweg in einem Brief von seines Freundes R.T. (leider in Englisch).

```
Worthie Sir John:-Hope, that is ye best comfort of ye afflicted, cannot much, I fear me, help
you now. That I would saye to you, is this only: if ever I may be able to requite that I do
owe you, stand not upon asking me. ‘Tis not much that I can do: but what I can do, bee ye
verie sure I wille. I knowe that,, if dethe comes, if ordinary men fear it, it frights not
you, accounting if for a high honour, to have such a rewarde of your loyalty. Pray yet that
you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only
if bie submission you can turn them away, ‘tis the part of a wise man. Tell me, an if you can,
to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge
your servant to command.-R.T.
```

Aufgabe 4 (Schlüssel zu Aufgabe 3)

Der folgende Text wurde nach Caesar verschlüsselt. Dechiffrieren Sie!

G U L W W H U E X F K V W D E H Q D F K L Q W H U S X Q N W L R Q V C H L F K H Q

ihr professioneller webdesign und webhosting - partner

www.itdev.ch wir bringen sie bequem ins web design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

12 Abbildungen

ihr professioneller webdesign und webhosting - partner

made in switzerland www.itdev.ch

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

Die Abbildung auf dem Titelseite zeigt die Titelseite (Holzschnitt) des ersten gedruckten Werkes über Kryptographie (1518).

Die Abbildung in der Kopfzeile zeigt die Chiffrierscheibe von Leon Battista Alberti. Aus [KAHN], p. 128.

ihr professioneller
webdesign und
webhosting - partner

it development

talstrasse 98
ch 3924 st. niklaus

13 Literaturverzeichnis

Gute amatuerhafte Einführungen in die klassische Kryptographie geben:
[SMITH]
Smith, L.D., Crytography. Dover, New York 1955

Ein Klassiker der Kryptanalysis ist:
Friedman, W.F., Military Cryptanalysis. Part IV. Washington, 1942.

Eine umfassende geschichtliche Darlegung der Kryptologie nach dem Stand der offenen Literatur von 1967 findet sich in:
[KAHN]
Kahn, D., The Codebreakers. Mecmillan, New York 1967

Dort findet man auch Hinweise auf spezielle, schwer zugängliche, insbesondere historische Literatur von dem 19. Jahrhundert. Mit journalistischer Verve von einem Historiker geschrieben.

ihr professioneller webdesign und webhosting - partner
made in switzerland www.itdev.ch
www.itdev.ch
wir bringen sie bequem ins web
design & webhosting
it development
talstrasse 98
ch 3924 st. niklaus

14 Stichwortverzeichnis

ihr professioneller webdesign und webhosting - partner

made in switzerland www.itdev.ch

www.itdev.ch
wir bringen sie bequem ins web
design & webhosting

it development

talstrasse 98
ch 3924 st. niklaus

ihr professioneller
webdesign und
webhosting - partner

it development

talstrasse 98
ch 3924 st. niklaus