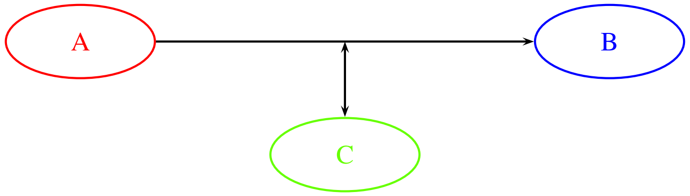
Kapitel 1
Aufgaben und Umfeld der Kryptologie

§ 1: Einsatzgebiete der Kryptographie

Kryptologie ist zusammengesetzt aus den beiden griechischen Wörtern κρυπτός = verborgen, versteckt und λόγος = Rede, Darlegung, Vernunft; sie ist also die Wissenschaft vom Geheimen. Sie besteht aus der Kryptographie (von γράφειν = schreiben), die Geheimschriften entwickelt, und der Kryptanalyse (ανάλυση = Auflösung), die versucht, letztere zu zu analysieren mit dem Ziel, sie zu knacken.

Die Grundsituation ist also die folgende:



A möchte eine Nachricht m an B übermitteln, jedoch besteht die Gefahr, daß alles, was er an B schickt auf dem Weg dorthin von C gelesen und vielleicht auch verändert wird; außerdem könnte C eventuell versuchen, sich gegenüber B als A ausgeben.

Der Ausweg besteht darin, daß A meist anstelle von m eine Nachricht c schickt, aus der B die Nachricht m und gegebenenfalls weitere Informationen rekonstruieren kann.

Aufgabe der Kryptographie ist es, in dieser oder einer ähnlichen Situation eines oder mehrere der Ziele aus folgender Liste zu erreichen; Aufgabe der Kryptanalyse ist es, dies zu verhindern.

a) Geheimhaltung: Sie muß sicherstellen, daß zwar B, nicht aber C in der Lage ist, die Originalnachricht m aus c zu rekonstruieren.

b) Verfälschungssicherheit: Sie muß sicherstellen, daß C den übertragenen Text c nicht unbemerkt durch einen Text c' ersetzen kann, den B dann als eine Nachricht m' rekonstruiert.

c) Sicherheit gegen erneutes Einspielen: Sie muß sicherstellen, daß C den übertragenen Text c nicht unbemerkt ein zweites Mal in die Übertragung einspielen kann, so daß B glaubt, A habe ihm die Nachricht m zweimal geschickt.

d) Authentizität: B muß sicher sein, daß die Nachricht m tatsächlich von A kam und nicht von C. Gelegentlich ist das sogar die einzige wesentliche Aufgabe der Kryptographie nämlich dann, wenn sie etwa bei Bankkarten oder Zugangskontrollsystemen speziell zur Identifikation berechtigter Personen eingesetzt wird.

e) Beweisbarkeit: B muß einem Dritten gegenüber beweisen können, daß die Nachricht m von A kam und nicht von C *oder ihm selbst* geschrieben wurde.

f) Urheberrechtsschutz: A muß einem Dritten gegenüber beweisen können, daß die Nachricht m ursprünglich von ihm kommt und nicht von C, der sie später kopiert hat.

g) Kopierschutz: B soll zwar in der Lage sein, die Nachricht m aus c zu rekonstruieren, er darf aber nicht in der Lage sein, m an einen Dritten weiterzugeben.

h) Dokumentation des Wissensstands: Gelegentlich soll B gar nicht in der Lage sein, die Nachricht m zu rekonstruieren, aber A möchte zu einem späteren Zeitpunkt beweisen können, daß er zum Zeitpunkt des Absendens von c die Nachricht m kannte.

Betrachten wir diese Aufgaben etwas genauer.

a) Geheimhaltung

Dies ist die älteste unter den Aufgaben der Kryptographie und zugleich auch die, für die meisten Verfahren entwickelt wurden.

Heute unterscheiden wir vor allem zwei Arten von Verschlüsselungen:

- Bei der symmetrischen Kryptographie ist die Kenntnis des Verschlüsselungsalgorithmus äquivalent zu der des Entschlüsselungsalgorithmus
- Bei der asymmetrischen Kryptographie kann der Entschlüsselungsalgorithmus nicht mit vertretbarem Aufwand aus dem Verschlüsselungsalgorithmus abgeleitet werden, so daß letzterer öffentlich bekannt sein darf.

Was das im einzelnen bedeutet und welche Vor- und Nachteile die beiden Ansätze haben, wird uns im folgenden noch ausführlich beschäftigen.

b) Verfälschungssicherheit

Im elektronischen Zahlungsverkehr zwischen Banken legen natürlich alle Beteiligten größten Wert auf Geheimhaltung; noch wichtiger ist aber, daß die übertragenen Nachrichten nicht verfälscht werden, daß also aus einem Zahlungsauftrag über zehn Euro keiner über zehn Tausend Euro werden kann. Da alles weitgehend automatisch verläuft, müssen alle übetragenen Nachrichten in einem starr vorgegebenen normierten Format abgefaßt sein, und dieses Format läßt sich schon wegen der Größe des Bankennetzwerks nicht geheimhalten. Ohne zusätzliche Sicherungsmaßnahmen würde selbst eine zufällige Veränderung dieses Felds erheblichen Schaden anrichten. Eine gewisse Verfälschungssicherheit ist gegeben, wenn das verwendete Verschlüsselungsverfahren bei Manipulationen des Chiffretexts bei Entschlüsselung mit hoher Wahrscheinlichkeit keinen vernünftigen Klartext liefert, allerdings nur dann, wenn außer Sender und Empfänger niemand in der Lage ist, einen Text zu verschlüsseln. Bei Verwendung eines asymmetrischen Kryptoverfahrens braucht man auf jeden Fall zusätzliche Maßnahmen wie etwa kryptographisch sichere Prüfsummen oder ähnliches.

c) Sicherheit gegen erneutes Einspielen

Speziell der elektronische Zahlungsverkehr bietet auch ein Beispiel dafür, daß eine Nachricht weder verstanden noch verfälscht werden muß, um damit Schaden anzurichten: Wenn etwa eine Zahlungsanweisung zugunsten des Lauschers von einer Clearingstelle an dessen

Bank geschickt wird, kann dieser sie anhand von Zeitpunkt und Absender/Empfänger mit relativ hoher Wahrscheinlichkeit identifizieren. Falls er sie unbemerkt später noch einmal einspielt, muß verhindert werden, daß ihm die Bank das Geld ein zweites Mal gutschreibt. Dazu muß die Nachricht beispielsweise eine eindeutige und nicht verfälschbare Transaktionsnummer enthalten, anhand derer Dubletten erkannt werden.

d) Authentizität

Nicht nur bei Zahlungsanweisungen ist es oft von entscheidender Bedeutung, wer der Absender der Nachricht ist. Bei einem symmetrischen Kryptoverfahren, bei dem die genaue Ver- und Entschlüsselsungsfunktion nur dem Absender und dem Empfänger bekannt sind und bei dem nur ein vernachlässigbarer Bruchteil aller theoretisch möglichen Chiffre-Nachrichten auf eine sinnvolle Entschlüsselung führt, kann sich der Empfänger einer sinnvollen Nachricht ziemlich sicher sein, daß eine nicht von ihm selbst produzierte Chiffre vom Absender stammt; bei asymmetrischen Kryptoverfahren müssen andere Wege gefunden werden.

e) Beweisbarkeit

Gelegentlich muß der Empfänger nicht nur selbst überzeugt sein, daß eine Nachricht wirklich vom angegebenen Absender stammt, sondern er muß dies auch gegenüber einem Dritten beweisen können, beispielsweise wenn der Absender eine eingegangene Verpflichtung nicht erfüllen will. Hier bietet der gerade skizzierte Einsatz eines symmetrischen Kryptoverfahrens keinen Schutz, denn der Absender kann ja jederzeit behaupten, der Empfänger habe die Nachricht selbst geschrieben. Wie wir sehen werden, kann man aber beispielsweise durch Vertauschung der Rollen von Ver- und Entschlüsselungsfunktion eines asymmetrischen Kryptosystems sogenannte *elektronische Unterschriften* erzeugen (die in Deutschland rechtsgültig sind).

f) Urheberrechtsschutz

Manchmal möchte der Absender später beweisen können, daß der Inhalt der Nachricht (etwa die Idee für ein neues Produktionsverfahren oder ein

Musikstück) von ihm stammt; insbesondere möchte er den Empfänger daran hindern, es als eigene Leistung auszugeben oder unbefugt zu verbreiten. Dazu dienen meist sogenannte „Wasserzeichen“, d.h. Zusatzinformationen, die unsichtbar mit der Nachricht verknüpft sind. Die Techniken dazu stammen oft aus der sogenannten *Steganographie,* mit der wir uns im nächsten Paragraphen beschäftigen werden.

Gelegentlich werden sie auch dazu eingesetzt, Lecks zu finden: So soll etwa die damalige britische Premierministerin MARGARET THATCHER in den achtziger Jahren angeordnet haben, die Word Prozessoren ihrer Minister und engsten Mitarbeiten so umzuprogrammieren, daß jeder durch geringfügige Variationen im Zeilenvorschub einem Fachmann den Rückschluß auf den Autor gestattete. (Word Prozessoren waren elektrische Schreibmaschinen mit einem Mikroprozessor und einem Speichermedium, die einen Teil jener Grundfunktionen beherrschten, die heute in jedem Textverarbeitungsprogramm selbstverständlich sind.) Natürlich funktionierte die Identifikation des Autors nur, wenn das Original vorlag; ein Journalist, der ein Dokument abtippen ließ und dann vernichtete, lieferte keine Informationen über seine Quelle.

Ein Hauptproblem guter Wasserzeichen besteht daher darin, daß sie robust sein müssen: Das Wasserzeichen in einem digitalen Musikstück sollte also beispielsweise im Idealfall auch in einer analogen Kopie noch nachweisbar sein.

g) Kopierschutz

Früher gab es spezielle Farbstifte, deren Schrift für Schwarz/Weiß-Kopierer nicht lesbar war; heute haben Farbkopierer spezielle Software, die dafür sorgt, daß keine Geldscheine kopiert werden. Eine Computerdatei dagegen kann beliebig oft kopiert und an andere weitergegeben werden. Die einzige Möglichkeit für einen effizienten Kopierschutz besteht daher darin, die Informationen nur in verschlüsselter Form zur Verfügung zu stellen. Da auch jedes Entschlüsselungsprogramm problemlos kopiert werden könnte, muß die Entschlüsselung durch Spezialhardware erfolgen. Diese muß auch gegen Logikanalysatoren resistent sein, beispielsweise weil kritische Schlüssel in auslesesicheren Registern

gespeichert sind. Da dies viel Aufwand erfordert, sind die meisten real existierenden Kopierschutzschemata nicht sonderlich effektiv.

h) Dokumentation des Wissensstands

Wer ein Patent anmeldet, muß sein Verfahren offenlegen, zahlt hohe Gebühren, und spätestens nach siebzehn Jahren kann es jeder frei nutzen. Wer allerdings kein Patent anmeldet, muß damit rechnen, daß ein anderer dieselbe Idee hat, diese patentieren läßt, woraufhin er selbst dann sein Verfahren nicht mehr oder nur noch nach Zahlen von Lizensgebühren anwenden darf. Ein solches Patent wird dem Konkurrenten allerdings nicht erteilt, wenn jemand nachweisen kann, daß dieser nicht der erste war, der die Idee hatte. Das sogenannte *time stamping* ist das digitale Analogon einer Stechuhr: Sie kann ein Dokument beweisbar einem Zeitpunkt zuordnen, ohne daß es einem Dritten bekanntgegeben werden muß.

§ 2: Alternativen zur Kryptographie

Am einfachsten ist diese Aufgabe, wenn schon die bloße Existenz einer Nachricht geheim gehalten werden kann; entsprechende Techniken bezeichnet man als *Steganographie* von στεγανός = schützend, verdeckt.

Über die beiden wohl ältesten bekannten Anwendungen der Steganographie berichtet HERODOT (∼484 v.Chr.–∼424 v.Chr.) in seinen *Historien.* Die erste Episode ist aus der Zeit des ionischen Aufstands (500 v.Chr.) der kleinasiatischen und der zyprischen Griechen gegen die persische Oberherrschaft. Zur Vorbereitung schickte der Extyrann von Milet, HISTIAIOS (*vor* 520 v.Chr.–493 v.Chr.), der am persischen Hof in Susa lebte, eine Nachricht an seinem Nachfolger und Schwiegersohn ARISTAGORAS (*gefallen* 497). HERODOT schreibt dazu (Buch V, 35):

> Gerade damals kam nämlich auch jener Bote mit dem beschriebenen Kopf aus Susa an, den HISTIAIOS geschickt hatte, um ARISTAGORAS zum Abfall von dem König zu bewegen. Denn HISTIAIOS fand, weil alle Straßen bewacht wurden, kein anderes sicheres Mittel, ARISTAGORAS zum Abfall zu ermutigen, als

seinem getreuesten Sklaven das Haar zu scheren, Zeichen auf seinen Kopf zu schreiben, das Haar wieder wachsen zu lassen und ihn dann nach Milet zu schicken. Der Sklave hatte bloß den Auftrag, ARISTAGORAS in Milet zu bitten, ihm das Haar zu scheren und seinen Kopf zu betrachten. Die Zeichen auf dem Kopf aber mahnten, wie ich schon sagte, zum Abfall.

Die zweite Episode ist im siebten Buch der Historien zu finden: Der 491 v.Chr. von seinem Mitkönig KLEOMENES abgesetzte und im persischen Exil lebende Ex-König DEMARATOS von Lakadaimon (Sparta) erfuhr von einer geplanten Aufrüstung der Perser für einen Feldzug gegen Griechenland. HERODOT schreibt (Buch VII, 239):

> DEMARATOS, der Sohn des ARISTON, der nach Persien entflohen war, war den Lakedaimoniern, wie ich glaube und wie die Umstände nahelegen, nicht eben wohlgesinnt; man kann daher auch annehmen, daß er nicht aus Wohlwollen, sondern aus Schadenfreude gehandelt hat. Genug, DEMARATOS, der in Susa lebte und wußte, daß XERXES den Zug gegen Hellas im Sinne hatte, wollte den Lakedaimoniern Kunde davon geben. Weil sich dies auf andere Weise nicht bewerkstelligen ließ – er mußte die Entdeckung fürchten – verfiel er auf folgenden Gedanken: Er nahm eine doppelte Schreibtafel und schabte den Wachsüberzug ab. Dann schrieb er auf das Holz des Täfelchens den Plan des Königs und überzog die Schriftzüge wieder mit dem Wachs. Das leere Täfelchen sollte den Wächtern an der Straße keinen Argwohn erwecken. Als die Tafel nach Lakedaimon gelangte, verstanden die Lakedaimonier nicht, was die leere Tafel bedeuten sollte. KLEOMENES' Tochter GORGO, LEONIDAS' Gemahlin, war es endlich, wie man mir erzählt, die den Sinn erriet. Sie sagte, man solle das Wachs abschaben; dann werde man auf dem Holz die Buchstaben finden. Sie taten es, fanden die Botschaft und lasen sie, teilten sie dann auch den übrigen Hellenen mit. So soll sich jene Kunde verbreitet haben.

(zitiert nach A. HORNEFFER*s Übersetzung der* Historien, *erschienen als* Kröners Taschenausgabe 224, *Kröner Verlag Stuttgart, 1955)*

Beides Mal war die Steganographie kriegsentscheidend: Der ionische Aufstand war erfolgreich, und die Griechen begannen nach Erhalt der Nachricht von DEMARATOS, ihrerseits eine Flotte zu bauen. Als die Flotte des Perserkönigs XERXES schließlich fertig war und er seinen vermeintlichen Überraschungsangriff startete, waren die Griechen gut vorbereitet und konnten die Perser zwar nur mit Glück (der Wind wehte in die richtige Richtung), dafür aber umso vernichtender schlagen.

Zumindest im zweiten Fall freilich hing der Erfolg davon ab, daß zwar GORKO auf die Idee kam, das Wachs von der Tafel abzukratzen, nicht aber einer der Wächter. Sobald jemand die Existenz einer Nachricht vermutet, wird er sie mit ziemlicher Sicherheit auch finden.

Aus diesem Grund wird Steganographie oft mit einer Verschlüsselung kombiniert. Ein Beispiel, das zwar eher der klassische Kryptographie als der Steganographie zuzurechnen ist, bietet das mesopotamische Arzneimittellexikon *Uruanna,* das im Auftrag des letzten assyrischen Herrschers ASSURBANIPAL (†627 *v.Chr.*) zusammengestellt wurde. Dort findet man Rezepte der Art *Menschenkot verarbeitest Du mit dem Urin eines Hundes zu einem Brei und verbindest [den Patienten] damit.* Bei Ausgrabungen wurde aber auch eine zweispalitge Tafel gefunden, die jeweils in der linken Spalte den Namen einer Pflanze enthielt und in der rechten ein Wort wie *Menschenkot, Fledermauskopf, Taubendreck,* . . . . Ganz offensichtlich waren diese Wörter also Chiffren für Heilpflanzen. Trotz des Ekels, den die wörtlich genommenen Rezepte verursachen, war der steganographische Effekt aber so groß, daß die Rezepte über die Jahrtausende tradiert und als „Weisheit der Alten“ sogar praktiziert wurden. *(s. Bild der Wissenschaft, Heft 6/2007, S. 40–41)*

Im 18. Jahrhundert sehr populär war beispielsweise KRISTIAN FRANTZ PAULINIS *Heylsame Dreck-Apothecke,* wo es unter anderem heißt:

> Im Koth und im Urin liegt GOTT und die Natur. Kuhfladen können dir weit mehr als Balsam nützen. Der blosse Gänsedreck geht Mosch und Ambra für. Was Schätze hast du offt im Kehricht und Mistpfützen. Der beste Theriak liegt draußen vor der Thür. *(zitiert nach* Deutsches Ärzteblatt **101**, *Ausgabe 47 vom 19.11.2004, Seite A-3184)*

Neu-Vermehrte/
Heylsame
Dreck-Apothecke,
Wie nemlich mit
Koth und Urin
Fast alle/ ja auch die schwerste/
gifftigste Kranckheiten, und bezauberte
Schäden vom Haupt biß zun Füssen, inn- und äusserlich, glücklich curiret worden;
Mit allerhand raren, so wohl nütz- als ergötzlichen
Historien und Anmerckungen/
Auch andern
Feinen Denckwürdigkeiten,
Nochmahls bewährt, nun zum vierdten mahl
um ein merckliches verbessert,
Und mit dem
Andern Theil
vermehrt
Von
Kristian Frantz Paulini.
Franckfurt am Mayn,
In Verlegung Friederich Daniel Knochen.
MDCCXXXIV

Auch einige heutige Bücher mit Titeln wie *Lebenssaft Urin* oder *Gesund durch Eigenharn* könnten ihren Ursprung letztlich in dieser erfolgreichen Steganographie haben.

Heute sind Nachrichten auf der Kopfhaut oder unter der Wachsschicht einer antiken Tafel sicherlich keine attraktiven Alternativen zu einer E-Mail; dafür bieten Computer aber ganz neue Möglichkeiten zur Steganographie:

Speichert man etwa Bild- oder Audiodaten in nichtkomprimierter Form, ändert es im allgemeinen den visuellen oder auditorischen Eindruck nicht, wenn man das letzte Bit des digitalisierten Werts verändert: Wie Experimente zeigen, kann unser Auge nicht mehr als etwa 64 verschiedene Grauwerte unterscheiden; da Grauwerte aber üblicherweise als Bytes und damit mit 256 möglichen Werten abgespeichert werden, läßt sich problemlos das letzte Bit oder gar Bitpaar zur Übertragung zusätzlicher Information verwenden – zumindest solange dies niemand vermutet:

Die Korrelation zwischen den Endbits benachbarter Bytes ist bei echten Bild- oder Audiodaten im Falle exakter Abtastung erheblich kleiner als beim Aufmodulieren einer steganographischen Nachricht; bei einer verrauschten Abtastung dagegen wird sie wohl eher größer sein.

Auch in Texten lassen sich Nachrichten verstecken; unter dem URL `www.spammimic.com` etwa kann man eine Nachricht in eine *spam*-Email einbetten, die sich wahrscheinlich niemand genauer ansehen möchte. Aus *Uruanna* beispielsweise wurde

```
Dear Business person ; Your email address has been
submitted to us indicating your interest in our newsletter
! If you no longer wish to receive our publications
simply reply with a Subject: of "REMOVE" and you will
immediately be removed from our database . This mail
is being sent in compliance with Senate bill 1622 ,
Title 5 , Section 305 . THIS IS NOT A GET RICH SCHEME
! Why work for somebody else when you can become rich
in 88 MONTHS ! Have you ever noticed nobody is getting
any younger plus nobody is getting any younger ! Well,
now is your chance to capitalize on this ! WE will
help YOU decrease perceived waiting time by 200% and
turn your business into an E-BUSINESS ! The best thing
about our system is that it is absolutely risk free
for you ! But don't believe us . Mr Ames of Massachusetts
tried us and says "My only problem now is where to
park all my cars" ! We are licensed to operate in all
states ! We beseech you - act now . Sign up a friend
and your friend will be rich too ! Thank-you for your
serious consideration of our offer !
```

Gibt man diese Nachricht auf `www.spammimic.com/encode.shtml` ein, erhält man wieder das Wort Uruanna.

Die Steganographie ist nicht die einzige Methode, um ohne spezielle Geheimschrift Nachrichten geheim zu halten: Auch eine den zu erwartenden Gegnern unbekannte natürliche Sprache oder Schrift kann diese Funktion erfüllen.

Im alten China beispielsweise, wo fast niemand lesen und schreiben konnte, war die gewöhnliche Schrift schon geheim genug; spezielle Geheimschriften wurden dort nie entwickelt. (Als Schutz vor Lesekundigen war allerdings eine Form der Steganographie gebräuchlich: Die Nachricht wurde auf ein Seidentuch geschrieben und dieses zusammengeknüllt und mit Wachs umhüllt, so daß es aussah wie eine einfache Wachskugel.)

Heute gibt es in jedem Staat einen nicht vernachlässigbaren Prozentsatz von Bürgern, die lesen und schreiben können; mit wenig bekannten Sprachen konnte man aber auch im zwanzigsten Jahrhundert selbst im jahrelangen Großeinsatz noch Erfolge erzielen: Der einzige amerikanische Code im zweiten Weltkrieg, den die Japaner nie knacken konnten, war der der Navajos.

Die Navajos waren einer der wenigen Stämme, die noch nie Kontakte zu deutschen Forschern gehabt hatten (Japan und Deutschland kämpften im zweiten Weltkrieg auf derselben Seite), und ihre Sprache ist mit keiner europäischen oder asiatischen Sprache verwandt. Nach damaligen Schätzungen gab es weniger als dreißig Nicht-Navajos, die diese Sprache beherrschten. Die meisten von ihnen waren als Kinder von Missionaren gemeinsam mit Navajo-Kindern aufgewachsen; keiner war Japaner oder Deutscher. Außerdem gab es zu dieser Sprache keine Schrift, und sie ist so kompliziert, daß es für einen Erwachsenen praktisch unmöglich ist, sie zu lernen: Zum einen ist die Grammatik sehr komplex, zum anderen hat – wie im Chinesischen, nicht aber im Japanischen – derselbe Laut je nach Ton völlig verschiedene Bedeutungen.

Entsprechend erwies sich 1960, beim damaligen UN-Einsatz im vormals belgischen Kongo das Gaelisch der irischen Soldaten als die effektivste Kryptographie.

Für die Hauptlast der heutigen Kryptographie freilich, die Kommunikation und den Handel über das Internet, sind diese Verfahren nicht tauglich; hier geht nichts ohne „Geheimschriften“, d.h. ohne eine algorithmische Transformation der Nachricht m in einen Chiffretext c. Dies wird daher auch den Hauptinhalt der Vorlesung ausmachen.

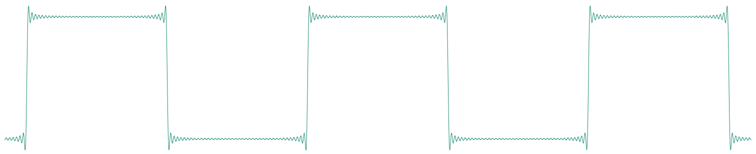
§2: Das Umfeld der Kryptologie

Auch das beste Kryptoverfahren ist nutzlos, wenn der Gegner die Entschlüsselungsfunktion kennt oder sich den Klartext auf andere Weise unabhängig vom Chiffretext verschaffen kann. Die Übertragung einer Nachricht geht über eine ganze Reihe von Schritten, und ein etwaiger Gegner kann sich aussuchen, wo er angreifen will. Natürlich wird es sich immer das aus seiner Sicht schwächste Glied der Kette aussuchen.

Zusätzlich zur Kryptanalyse hat er beispielsweise folgende Möglichkeiten:

1. Durch Bestechnung oder sogenanntes *human engineering* oder *social engineering,* d.h. durch Ausnutzen der Dummheit und/oder Naivität von Mitarbeitern im Umfeld des Absenders (oder auch von diesem selbst!) kann er versuchen, den Inhalt wichtiger Nachrichten zu erfahren, bevor diese auch nur abgeschickt werden. Auch durch Abhören von Telephonen, Einbrüche *usw.* kann er Informationen gewinnen.
2. Mit denselben Methoden oder durch klassisches Hacken kann er sich Zugriff auf den Computer des Absenders verschaffen und dafür sorgen, daß entweder die unverschlüsselte Nachricht oder alle im Computer gespeicherten Schlüssel an ihn geschickt werden. Einen gewissen Schutz dagegen bieten nur Betriebssysteme einer hohen Sicherheitsklasse, und das sind nicht die, mit denen neue Rechner standardmäßig ausgeliefert werden.
3. Auch wenn er nicht bis zum Computer vordringen kann und auch keinen freiwilligen oder unfreiwilligen Komplizen in dessen Nähe hat, kann er versuchen, den Bildschirminhalt zu lesen: Die Pixel werden im Prinzip geschaltet durch Rechteckimpulse, da Leitungen für hochfrequente Ströme jedoch nicht nur einen OHMschen Widerstand, sondern auch eine Kapazität haben, fungieren sie als RC-Kreis und damit als ein sogenannte Tiefpaßfilter. Durch das Abschneiden der hohen Frequenzen entstehen an den Flanken der Rechtecke Überschwingungen (GIBBS-Phänomen), die auch noch in einer Entfernung von etwa fünfzig Metern mit einer Antenne aufgefangen werden können und die Rekonstruktion des Bildschirminhalts gestatten. Schutz dagegen ist nur durch aufwendige physika-

lische Abschirmungsmaßnahmen möglich: Der gesamte Computer muß in einem FARADAYscher Käfig sitzen und alle Kabel müssen abgeschirmt sein.



Das Gibbs-Phänomen für Rechteckimpulse

Beim Empfänger entstehen natürlich wieder im wesentlichen genau dieselben Probleme.

Betrachten wir zur Illustration die wesentlichen Schritte auf dem Weg einer Textnachricht von einem Absender A zu einem Empfänger B im Hinblick auf Angriffsmöglichkeiten eines Gegners C:

1. Möglicherweise hat sich A bereits Notizen über den vorgesehenen Inhalt der Nachricht gemacht; fallen diese irgendwie vorher oder nachher (Suche im Abfall) in die Hände von C, kennt dieser zumindest den wesentlichen Inhalt der Nachricht.
2. Wenn A hinreichend bedeutend ist, diktiert er die Nachricht einer Sekretärin oder einem persönlichen Referenten. Falls C die Fensterscheiben mit einem Laserstrahl abtastet oder gar ein Mikrophon oder einen Spion im Raum plazieren konnte, kennt er die Nachricht.
3. Während A tippt oder tippen läßt, erscheint die Nachricht auf dem Bildschirm. Falls Bildschirm, Computer und Tastatur nicht aufwendig abgeschirmt sind, kann C mit einer nicht garzu weit entfernten Antenne die Signale auffangen und die Nachricht rekonstruieren. Falls ein Trojaner auf dem Computer aktiv ist, kann dieser den Klartext der Nachricht weiterleiten.
4. Nächster (fakultativer) Schritt ist die Quellenkodierung (oder Datenkomprimierung): Zumindest lange Nachrichten mit vielen Anhängen sollten zwecks besserer Ausnutzung der Kanalkapazität komprimiert werden; wie wir bei der Diskussion der informationstheoretischen Grundlagen der Kryptologie sehen werden, erhöht das auch zu-

mindest prinzipiell die kryptographische Sicherheit. Falls freilich das Komprimierungsprogramm ein Freeware-Programm von *Mob Enterprises Central Europe Ltd* ist, wird es vielleicht auch noch zusätzlich die Nachricht an C weiterleiten. Auch wenn das Programm während der *Woche der Sicherheit* im Rahmen der Aktion *Die Kriminalpolizei rät* erworben wurde, besteht ein gewisses Risiko, daß es sich um einen SCHÄUBLE-Trojaner handelt.
5. Nun wird die Nachricht verschlüsselt. Die Kryptologie ist für die Sicherheit des Verschlüsselungsverfahrens verantwortlich; falls diese nicht ausreicht, kann C entschlüsseln. Beim Programm, das die Verschlüsselung durchführt, hat A dieselben Probleme wie bei dem zur Quellenkodierung.
6. Da kein Übertragungskanal perfekt ist, folgt als nächstes meist noch eine Kanalkodierung, d.h. die Anwendung eines fehlerkorrigierenden oder zumindest fehlererkennenden Codes. Falls dieses Programm ein Trojaner ist, der den Computer durchsucht, haben wir auch hier dieselben Risiken; die Umsetzung selbst ist problemlos, da sie auf bereits verschlüsselten Text angewandt wird.
7. Die Nachricht wird übertragen. C kann sie auffangen und die (nicht geheime) Kanalkodierung rückgängig machen; danach hat er ein kryptanalytisches Problem zu lösen.
8. Die Nachricht kommt beim Empfänger B an, und die Schritte 1–6 werden in umgekehrter Reihenfolge rückgängig gemacht. An den Sicherheitsproblemen ändert sich dabei nichts wesentliches.

Hier in der Vorlesung geht es ausschließlich um Sicherheit gegen einen möglichen Angriff in Schritt 7, nicht aber um solche gegen die anderen Schritte oder gar die sicherlich vielfachen weiteren Möglichkeiten. Alle Hörer müssen sich daher bewußt sein, daß sie auf Kryptographie allein kein Sicherheitskonzept aufbauen können und daß auch wenn sie selbst alle Probleme perfekt gelöst haben (so dies möglich sein sollte) ein einziger Fehler beim Kommunikationspartner alle Bemühungen zunichte machen kann.

§3: Sicherheitsstandards

Unser Sicherheitsstandard sollte klar sein: Der Gegner darf nicht in der Lage sein, aus dem Chiffretext den Klartext zu rekonstruieren. Das Problem an diesem einfach klingenden Satz ist die Formulierung „darf nicht in der Lage sein“: Da der Gegner in der Wahl seiner Mittel frei ist, wissen wir nicht, was er weiß, was er kann und was er tut.

a) Was weiß der Gegner über die Nachricht?

Spontan würde man wohl sagen, daß ihm nur der Chiffretext zur Verfügung steht; in der Kryptographie redet man dann von einem *Angriff nur mit Chiffretext*.

Eine Sicherheit nur gegen diese Art von Angriffen war allerdings noch nie in der Geschichte der Kryptographie akzeptabel: Wenn sich jemand die Mühe macht, eine Nachricht abzufangen und in eine (bei guter Kryptographie) aufwendige Kryptanalyse einsteigt, wird er sicherlich gewisse Vorkenntnisse über den Inhalt der Nachricht haben. Die klassischen Anwendungen der Kryptographie beschränkten sich bis vor etwa fünfzig Jahren hauptsächlich auf den militärischen und diplomatischen Bereich; beide sind eher nicht bekannt für große Individualität und Phantasie. Ein einigermaßen mit den Verhältnissen vertrauter Gegner kann mit ziemlich hoher Sicherheit erraten, womit die Nachricht beginnt (Oberstleutnant Knedderle im Generalstab der vierunddreißigsten Infanteriedivision an . . .) und endet. Bei den heute dominierenden Anwendungen im Bankenbereich und im Internet läuft die Kryptographie weitgehend unbemerkt vom Anwender im Hintergrund ab und muß daher, um von Computern allein verstanden zu werden mit stark formalisierten Nachrichtenformaten arbeiten. Deren Spezifikation findet man in RFCs und ähnlichen Dokumenten, die sich jedermann ohne größere Mühe verschaffen kann. Man muß daher realistischerweise davon ausgehen, daß ein Gegner Teile des Klartexts kennt, und man muß fordern, daß ihm dies nicht dabei hilft, auch die restlichen Teile der Nachricht zu entschlüsseln oder gar die gesamte Entschlüsselungsfunktion zu rekonstruieren. Wir brauchen also auch *Sicherheit gegen Angriffe mit bekanntem Klartext*.

Zumindest seit der Verbreitung von Chipkarten müssen wir dem Gegner sogar noch mehr Möglichkeiten zubilligen: Die Möglichkeit, frei gewählte Chiffretexte zu entschlüsseln. Da Kryptographie heutzutage nicht mehr mit Papier und Bleistift durchgeführt wird, heißt das

konkret, daß der Gegner sich für eine gewisse Zeit in Besitz einer Entschlüsselungsmaschine oder Chipkarte setzen und frei über diese verfügen kann. Da jeder vernünftige Mensch sofort seine Schlüssel ändert sobald er so etwas bemerkt, muß der Gegner die entwendete Hardware wieder unbemerkt zurückgeben; die Kenntnis, die er zwischenzeitlich gewonnen hat, kann ihm aber niemand nehmen. Damit auch künftige verschlüsselte Nachrichten sicher sind brauchen also fast immer auch noch *Sicherheit gegen Angriffe mit frei wählbarem Chiffretext* – wobei der aktuelle Chiffretext natürlich ausgeschlossen ist: Fällt er in die Hand des Gegners, während dieser die Möglichkeit zur Entschlüsselung hat, ist er kompromittiert, aber zu jedem späteren Zeitpunkt muß er sicher sein.

b) Was weiß der Gegner über das Kryptoverfahren?

Idealerweise natürlich nichts. Aber das ist noch unrealistischer als die Annahme, daß er nichts über den Klartext weiß: Wie schon AUGUSTE KERCKHOFFS 1883 in seiner grundlegenden Arbeit *La cryptographie militaire* feststellte, muß man bei jedem in größerem Umfang eingesetzten Verfahren davon ausgehen, daß es sich nicht über einen längeren Zeitraum hinweg geheimhalten läßt. Anstelle einer einfachen Verschlüsselungsfunktion f, die jeder Nachricht m einen Chiffretext $c = f(m)$ zuordnet, soll man eine Funktion benutzen, die außer von m auch noch von einem zweiten Parameter s abhängt, dem *Schlüssel*. Somit ist also $c = f(m, s)$.

JEAN - GUILLAUME - HUBERT - VICTOR - FRANÇOIS - ALEXANDRE-AUGUSTE KERKHOFFS VON NIEUWENHOF (1835–1903) wurde in der heute niederländischen Ortschaft Nuth geboren. Er studierte an der Universität Liège, wo er mit dem Doktor der Literaturwissenschaften abschloß. Nachdem er mehrere Stellen als Lehrer in den Niederlanden und in Frankreich bekleidet hatte, wurde er schließlich Professor für Deutsch an der Ecole des Hautes Etudes Commerciales in Paris. Außer für seine Arbeit zur Militärkryptographie ist er vor allem auch noch für linguistische Studien bekannt, insbesondere auch zur heute weithin vergessenen Kunstsprache Volapük.

Im zweiten Kapitel seiner Schrift stellt er folgende Forderungen an einen Verschlüsselungsalgorithmus:

1. Das System muß praktisch, wenn schon nicht mathematisch, unentschlüsselbar sein.
2. Es darf den Schlüssel nicht preisgeben und kann ohne nachteilige Folgen in die Hand des Gegners fallen.
3. Es muß möglich sein, den Schlüssel ohne schriftliche Notitzen zu übermitteln und aufzubewahren, und er muß sich ändern lassen, wann immer die Korrespondenten dies wünschen.
4. Das System muß sich für telegraphische Übermittlung eignen.
5. Das Verschlüsselungssystem muß tragbar sein und weder seine Handhabung noch seine Funktion darf die Zusammenarbeit mehrerer Personen erfordern.
6. Schließlich ist es auf Grund der Anforderungen seiner Anwendung notwendig, daß das System leicht anwendbar ist und weder geistige Anspannung noch die Kenntnis einer langen Reihe zu beachtender Regeln erfordert.

Daran hat sich im wesentlichen bis heute nichts geändert; höchstens Regel drei muß man heute in dem Sinne abschwächen, daß der Schlüssel wohl in irgendeiner Weise elektronisch festgehalten werden muß. Anstelle telegraphischer Übermittlungen haben wir zwar heute meist Rechnernetze, aber auch da ist es aus Effiziensgründen durchaus sinnvoll, mit Standard ASCII Code zu arbeiten statt mit frei erfundenen Hyrogliphen. Auch an der Forderung nach leichten Anwendbarkeit hat sich nichts geändert: Es wäre völlig unrealistisch, vom typischen Internetbenutzen mehr Intelligenz zu erwarten als von einem Militär mitten im Gefecht. Regel 1 beschreibt ein Dilemma der Kryptographie, das auch noch heute bestimmend für das gesamte Gebiet ist und mit dem wir uns daher gleich noch viel ausführlicher befassen müssen. Die zentrale Frage ist:

c) Was kann der Gegner?

Sicher wissen wir nur, daß er es uns nicht verraten wird; meist verrät er uns schließlich nicht einmal, daß er unser Gegner ist. Wir sind daher auf Vermutungen angewiesen und sollten ihn, um mit relativ großer

Wahrscheinlichkeit auf der sicheren Seite zu sein, im Zweifelsfall eher deutlich überschätzen.

Die Kryptologie hat als Idealgestalt des überschätzten Gegners den sogenannten BAYESschen Gegner eingeführt. Er verfügt über unbegrenzte Rechenkraft, nicht aber über hellseherische Fähigkeiten. Er trifft seine Entscheidungen aufgrund der BAYESschen Statististik und stört sich nicht daran, daß die in der BAYESschen Formel auftretendend Terme in realistischen Anwendungen für alle praktischen Zwecke nicht berechenbar sind. Dies ist der Hintergrund der KERKHOFFSschen Forderung, daß das Verfahren nur praktisch, nicht aber auch mathematisch sicher sein muß.

Die Sicherheit eines Verfahrens gegen den BAYESschen Gegner kann mit informationstheoretischen Methoden ziemlich gut abgeschätzt werden; zumindest was absolute Sicherheit betrifft, ist das Ergebnis allerdings deprimierend: Wie wir im Kapitel über Informationstheorie sehen werden, ist absolute Sicherheit unmöglich, sofern der Schlüssel kürzer ist als die Gesamtheit aller je damit verschlüsselten Nachrichten.

Im nächsten Kapitel werden wir sehen, daß sich mit hinreichend langen Schlüsseln tatsächlich absolut sichere Verfahren realisieren lasen (immer vorausgesetzt natürlich, daß auch im Umfeld alles *absolut* sicher ist . . .), und im Höchstsicherheitsbereich werden diese auch tatsächlich angewendet. Für die meisten Alltagsanwendungen der Kryptographie sind sie jedoch viel zu aufwendig; hier müssen wir unsere Anforderungen deutlich zurückschrauben.

Wenn wir KERKHOFFS folgen, genügt es, daß ein Verfahren zumindest praktischen Sicherheit bietet. Wir müssen uns also überlegen, wie wir zumindest diese garantieren können.

An Ansätzen fehlt es nicht:

Der wohl erste „Sicherheitsbeweis“ geht zurück auf den GIROLAMO CARDANO: Seine Strategie bestand darin, ein Verfahren zu wählen, bei dem die Menge der möglichen Schlüssel so groß ist, daß sie unmöglich vollständig durchsucht werden kann.

GIROLAMO CARDANO (1501–1576) war einer der bedeutendsten Ärzte und Naturforscher seiner Zeit. In der Mathematik ist er vor allem bekannt für seine Arbeiten über Gleichungen dritten und vierten Grades, auch wenn wesentliche Teile dieser Arbeiten nicht auf ihn zurückgehen. Er hat allerdings als erster durch Verwendung negativer Zahlen die vielen bis dahin betrachteten Fälle auf eine einzige Formel zurückgeführt. Nach seinem Medizinstudium schlug er sich zunächst mit Glückspiel durch, wobei ihm seine Kenntnisse der Wahrscheinlichkeitstheorie sehr nützlich waren. Erst 1539 konnte er eine Stelle als Arzt antreten und wurde schnell international berühmt.

Konkret schlug CARDANO vor, zur Verschlüsselung eines Texts eine zwischen Absender und Empfänger vereinbarte Permutation der 26 Buchstaben des Alphabets durchzuführen. Dafür gibt es

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$$

Möglichkeiten, also 403 Quadrillionen 291 Trilliarden 461 Trillionen 126 Billiarden 605 Billionen 635 Milliarden und 584 Millionen. Wie er völlig zu recht bemerkt, würden „viele Bücher nicht ausreichen," um alle Möglichkeiten zu fassen.

Heute verwenden wir zum Entschlüsseln nur noch selten Bücher, aber auch Computer hätten Schwierigkeiten mit einer so großen Zahl von Möglichkeiten:

Nehmen wir an, wir hätten Tausend Chips, von denen jeder mit einer Taktfrequenz von zehn Gigahertz arbeitet und die so spezialisiert sind, daß jeder in jedem Takt eine ganze Probeentschlüsselung durchführen kann. Pro Sekunde kann also jeder Chip zehn Milliarden Möglichkeiten durchprobieren, und alle zusammen kommen auf zehn Billionen. Ein Jahr hat durchschnittlich ungefähr

$$365\frac{1}{4} \cdot 24 \cdot 60 \cdot 60 = 31\,557\,600$$

Sekunden, also schafft die Maschine pro Jahr etwas mehr als 315 Trillionen Entschlüsselungen; bis sie alle rund 403 Quadrillionen Möglichkeiten durchprobiert hat, braucht sie über eine Million Jahre; ein gewöhnlicher PC bräuchte gar weit länger als das Alter unseres Universums.

Selbst wenn wir an Stelle von Tausend Chips eine Million verwenden, bräuchte die Maschine immer noch rund 1278 Jahre, und es ist sehr unwahrscheinlich, daß der Inhalt der Nachricht auch dann noch geheim bleiben muß. Das Verfahren sollte also für alle praktischen Zwecke absolut sicher sein.

Ähnlich klingen auch die Werbeaussagen vieler heutiger Anbieter von Kryptoverfahren, obwohl nicht viele davon mit über 403 Quadrillionen Varianten aufwarten können. Was dabei meist verschwiegen wird: Durchprobieren aller Möglichkeiten ist zwar *ein* Weg zur Entschlüsselung, aber oft ist es bei weitem nicht der einzige. Wir müssen uns immer der Tatsache bewußt sein, daß es der *Angreifer* ist, der entscheidet, wie er vorgeht, nicht wir. Wenn wir unser Verfahren gegen eine Art von Attacke immunisiert haben, müssen wir stets damit rechnen, daß er einfach eine andere wählt.

Im nächsten Kapitel werden wir sehen, daß der Aufwand zum Knacken von CARDANOS Verfahren schon bei Nachrichten moderater Länge (60–100 Buchstaben) eher im Bereich von Minuten als im Bereich von Stunden liegt, und nicht viel besser sieht es aus bei modernen Kryptoverfahren, die sich nur auf die „unüberschaubar große Anzahl von Möglichkeiten" verlassen. Bevor jemand ein solches Verfahren anwendet, sollte er zum Beispiel bei `pwcrack.com` nachschauen, für welch geringe Beträge (meist 40-100 US-$) die Kryptographie heutiger Office-Programme dort geknackt wird – und das mit Erfolgsgarantie. Verglichen mit den Werten, die im kommerziellen Bereich durch solche Kryptographie geschtzt werden sollen, ist dieser Aufwand lächerlich gering. In der seriösen Kryptograhie läßt sich daher schon lange niemand mehr durch eine bloße Vielzahl von Möglichkeiten blenden.

Das zwanzigste Jahrhundert kam mit neuen Methoden wie der sogenannten Komplexitätstheorie; WHITFIELD DIFFIE, den wir in Kapitel vier als einen der beiden Väter der asymmetrischen Kryptographie kennenlernen werden und der seit 1991 als *chief security officer* bei Sun Microsystems arbeitet, schreibt dazu in seinem Buch *Privacy on the Line* (mit SUSAN LANDAU, MIT Press, ^{2}2007)

The vast number of keys was offered as an argument for the unbreakability of ciphers during the Renaissance (. . .) and probably earlier. The more general modern theories, including the theory of *non-deterministic polynomial time* or NP computing (. . .) are far more mathematical but little more satisfactory. *(Anmerkung 15 zu Kapitel 2)*

(Die beiden Auslassungen sind Verweise auf das Literaturverzeichnis)

Worum geht es? Idealerweise wüßten wir gerne, wie groß der Mindestaufwand zur Lösung eines Problems ist. Darüber läßt sich allerdings nur selten eine Aussage machen, da man dazu entweder alle möglichen Ansätze zur Lösung des Problems kennen müßte oder aber beispielsweise eine Untergrenze für die Länge des Ergebnisses. Letztere ist im Falle der Kryptographie zwar kein Problem: Fast immer ist der Klartext genauso lang wie oder nur unwesentlich länger als der Chiffretext; aUßerhalb der Steganographie dürfte es wohl kein Verfahren geben, in dem er mehr als doppelt so lang ist; dafür ist er bei Einsatz einer guten Quellenkodierung gelegentlich auch deutlich kürzer als der Klartext. Somit liefert dies keine brauchbare Untergrenze.

Die Komplexitätstheorie betrachtet daher Obergrenzen oder (seltener) obere Grenzen für den mittleren Aufwand. Es ist klar, daß diese wertlos sind, wenn es um die Beurteilung der Sicherheit einer konkreten Verschlüsselung geht.

Schlimmer noch: Da auch konkrete Obergrenzen schwer zu finden sind, begnügt man sich meist mit *asymptotischen* Aussagen über das Verhalten der Obergrenze, wenn die Länge der Eingabe (zum Beispiel die eines öffentlichen Schlüssels) gegen unendlich geht; wie jeder, der seine *Analysis I* verstanden hat, wissen sollte, folgt daraus natürlich nichts für eine konkrete vorgegebene Länge.

Da selbst asymptotische Obergrenzen nicht einfach sind, beschränken sich viele sogar noch darauf, nur zu untersuchen, ob die Obergrenze polynomial wächst oder stärker – auch hier gibt es übrigens noch viele offene Probleme. Spätestens hier werden die Ergebisse allerdings völlig bedeutungslos für praktische Anwendungen auf die Kryptographie: Die zahlentheoretischen Algorithmen, die vielen der in dieser Vorlesung behandelten Kryptoverfahren zugrunde liegen, haben typischerweise eine

asymptotische Komplexität, die für Eingabewerte der Länge n in erster Näherung durch die Funktion

$$L_{\alpha,c}(n) = e^{cn^{\alpha}(\ln n)^{1-\alpha}}$$

beschrieben werden mit reellen Konstanten $0 \leq \alpha \leq 1$ und $c > 0$. Für $\alpha = 0$ ist dies ein ein Polynom in n, für $\alpha = 1$ eine Exponentialfunktion. Für $0 < \alpha < 1$ liegt das asymptotische Verhalten zwischen diesen beiden Grenzfällen und der tatsächliche Aufwand hängt außer vom Parameter c auch noch stark von sonstigen Konstanten ab, die einer $O(\ldots)$-Abschätzung unter den Tisch fallen.

Deshalb kann die Komplexitätstheorie genauso wenig seriöse Aussagen über die Sicherheit eines konkreten Verfahrens machen wie die Mächtigkeit der Schlüsselmenge.

Wenn ein Kryptoverfahren nicht im informationstheotetischen Sinn beweisbar sicher ist, kann man nach heutigem Stand höchstens dann Vertrauen in seine Sicherheit haben, wenn sich bereits viele erfahrene Kryptologen hinreichend lange mit seiner Kryptanalyse beschäftigt haben und keine Attacke mit vertretbarem Aufwand fanden. Das gibt zwar keine Garantie, daß nicht doch einer in Kürze eine finden wird, aber damit müssen wir leben – es sei denn, wir sind bereit, den hohen Aufwand für ein beweisbar sicheres Verfahren zu tragen.