Einführung in die Kryptologie

Horst Gierhardt
horst@gierhardt.de

06.09.2015

Inhaltsverzeichnis

1 Allgemeines

Die Kryptologie lässt sich in drei Teilbereiche aufgliedern:

- Kryptographie,
- Kryptoanalyse und
- Steganographie.

Die Begriffe Kryptologie und Kryptographie sind aus den griechischen Wörtern *kryptos* (geheim), *logos* (das Wort, der Sinn) und *graphein* (schreiben) gebildet.

Die **Kryptographie** ist die Wissenschaft von der Datenverschlüsselung. Eine Nachricht wird unverständlich gemacht. Obwohl der verschlüsselte Text noch buchstabenweise lesbar ist, ist aber inhaltlich nur noch „Kauderwelsch“ erkennbar. Man spricht von „offenen Geheimschriften“.

Die Hauptaufgabe besteht darin, dass aus einem Geheimtext G der Klartext K für Dritte nicht oder nur schwer rekonstruierbar wird. Mathematisch ist die Verschlüsselung V eine Funktion, die einem Klartext K einen Geheimtext G zuordnet:

$$G = V(K).$$

Entsprechend ist die Entschlüsselung E eine Funktion, die den Geheimtext in den Klartext überführt:

$$K = E(G).$$

Entsprechend muss gelten

$$E(V(K)) = K.$$

Wird zum Chiffrieren (Verschlüsseln) und Dechiffrieren (Entschlüsseln) der gleiche Schlüssel benutzt, so spricht man von einem *symmetrischen* Verfahren. Bei *asymmetrischen Verfahren* unterscheiden sich Chiffrier- und Dechiffrierschlüssel.

Die **Kryptoanalyse** beschäftigt sich mit dem Aufbrechen der Verschlüsselung ohne Kenntnis des Schlüssels. Eine versuchte Kryptoanalyse eines Dritten heißt *Angriff*. Der bekannteste Angriff war wohl die Entschlüsselung der *Enigma* durch ein Team des Informatikers Alan Turing, was wohl mitenscheidend für den Verlauf des zweiten Weltkrieges war.

Die Aufgabe der **Steganographie** ist, es, die Existenz einer Nachricht zu verbergen. Deshalb spricht man in diesem Zusammenhang von „verdeckten Geheimschriften“. Zu den klassischen Verfahren zählen unter anderem:

- unsichtbare Tinte,
- Zitronensaft,

- Mikrofilme,
- doppelte Böden oder hohe Schuhabsätze,
- Semagramme (das Verstecken von Informationen in Bildern).

Beispiel 1:

Die folgende Zeitungsanzeige ist auch nicht auf den ersten Blick als Träger einer geheimen Botschaft erkennbar[1]

8-ung!!!
Umzüge, Haushaltsauflösungen,
Räumungsverkäufe -
Bieten eine intelligente Lösung all Ihrer Lagerprobleme an.
Tel.: 0123-456 789

Beispiel 2:

Das Rezept für deutsche Geheimtinte

LOS ANGELES, 12. Juli.

Fast 95 Jahre nach der Erfindung von Geheimtinte durch deutsche Wissenschaftler werden die Rezepturen jetzt in den Vereinigten Staaten zum ersten Mal öffentlich gezeigt. Im Washingtoner Nationalarchiv ist unter anderem ein Dokument vom 14. Juni 1918 in französischer Sprache zu sehen, das eine Mixtur aus „einer Tablette Pyramidon, einer Tablette Aspirin und 400 Milliliter reinem Wasser“ beschreibt. Wie das historische Dokument belegt, hatten die Franzosen die Kommunikation ihrer deutschen Feinde längst durchschaut, als während des Ersten Weltkriegs Briefe mit der vermeintlichen Geheimtinte an die Front geschickt wurden. Die in den vergangenen Wochen durch den amerikanischen Geheimdienst CIA freigegebenen Rezepte zählen zu den Dokumenten der National Archives, die am längsten geheim gehalten wurden.

(aus: Frankfurter Allgemeine Zeitung, Nr. 160, Seite 7, 13. Juli 2011)

Beispiel 3:

Im alten Griechenland soll es eine ganz besondere Art der Steganographie gegeben haben. Um eine Nachricht zu versenden, wurde zunächst einem Sklaven der Kopf kahlgeschoren. Dann wurde die geheime Nachricht auf seiner Kopfhaut eintätowiert. Nach kurzer Zeit war von der Nachricht nichts mehr zu sehen. Der Sklave wurde nun zum Empfänger gesandt. Dieser scherte die Haare des Überbringers ab und erhielt die Nachricht.

Manchen Überlieferungen zufolge wurden den Sklaven nach Empfang der Nachricht nicht nur die Haare, sondern gleich der ganze Kopf abgetrennt, um die Geheimhaltung der Nachricht zu gewährleisten.

[1] Lösung: Man lese nur die Anfangsbuchstaben.

2 Einige Beispiele

2.1 U-Sprache

Jedes Wort beginnt mit einem „u“. Wenn das Wort mit einem Vokal beginnt, wird dieser durch „u“ ersetzt. *Udies ust uin ugeheimer Ubrief..*

2.2 I-Sprache

Jeder Vokal wird durch ein „i“ ersetzt: *Drii Chinisin mit dim Kintribiss.*

2.3 Bi-Sprache

Nach jedem Vokal wird ein „bi“ eingefügt: *Dabis ibist nibicht schwebir.* Der Schriftsteller Joachim Ringelnatz (1883-1934) hat in dieser Sprache ein Gedicht gemacht:

> Ibich habibebi dibich,
> Lobittebi, sobi liebib.
>
> Habist aubich dubi mibich
> Liebib? Neibin, vebirgibib.
>
> Nabih obidebir febirn
> Gobitt seibi dibir gubit.
> Meibin Hebirz habit gebirn
> Abin dibir gebirubiht.

2.4 Das Große Lalulã

Christian Morgenstern (1871-1914) schreibt in seinen *Galgenliedern* das folgende Gedicht.

> Das Große Lalulã
>
> Kroklokwafzi? Semememi!
> Seiokrontro - prafriplo:
> Bifzi, bafzi; hulalemi:
> quasti basti bo...
> Lalu, lalu lalu lalu la!
>
> Hontraruru miromente
> zasku zes rü rü?
> Entepente, leiolente
> klekwapufzi lü?
> Lalu lalu lalu lalu la!
>
> Simarar kos malzipempu

silzuzankunkrei (;)!
Marjomar dos: Quempu Lempu
Siri Suri Sei []!
Lalu lalu lalu lalu la!

Ob das Gedicht etwas bedeutet, womöglich eine verschlüsselte Schachpartie darstellt o.a. ist durchaus umstritten.

2.5 Die Ror-Sprache

Nach jedem Konsonanten wird ein o eingefügt und dann der Konsonant wiederholt: *Dodasos isostot einone schoschwowerore Gogehoheimomsospoprorachoche.*

Die Ror-Sprache ist allen Kalle Blomquist[2]-Lesern aufs beste bekannt.

3 Einige Beispiele aus der Geschichte

3.1 Atbasch

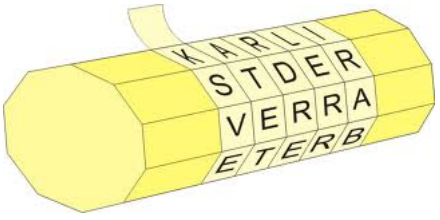
Jüdische religiöse Schreiber der Antike verbargen manchmal die Bedeutung des Geschriebenen, indem sie das Alphabet umkehrten, d.h. den letzten Buchstaben des Alphabets (Taw) anstelle des ersten (Aleph), den vorletzten (Sch) anstelle des zweiten (Beth) usw. benutzten. Dieses System, genannt **Atbasch**, ist auch in der Bibel durch ein Beispiel belegt, und zwar in Jeremia 25, 26. Dort ist „Sheshech“ für „Babel“ (Babylon) geschrieben worden. Es wurden also der zweite und der zwölfte Buchstabe des hebräischen Alphabets von hinten anstelle des zweiten und zwölften von vorn benutzt.

Eine Besonderheit ist, dass bei Atbasch Verschlüsselungs- und Entschlüsselungsmethode identisch sind. Daher genügt es, die Atbasch-Substitution ein zweites Mal auf den Geheimtext anzuwenden, um wieder den Ursprungstext zu erhalten.

Übertragen auf das lateinische Alphabet sieht die Zuordnung dann so aus:

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

3.2 Skytale von Sparta



Spartanische Ephoren[3] kommunizierten vor mehr als 2500 Jahren mit ihren Feldgenerälen, indem sie Mitteilungen quer über die nebeneinanderliegenden Ränder eines Streifens Pergament schrieben, der spiralförmig um einen Stab, genannt Skytale, gewickelt wurde. War der Streifen erst einmal abgewickelt, konnte die Mitteilung nur gelesen werden, wenn der Streifen um genau so einen Stab gewickelt wurde.

[2] von Astrid Lindgren
[3] Aufseher bzw. hohe Beamte

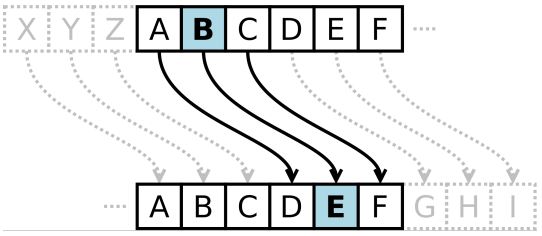
3.3 Der Polybios-Code

Polybios war ein Schriftsteller, der vor über 2000 Jahren(200 - 120 v. Chr.) in Griechenland lebte. Er erfand den durch die folgende Tabelle dargestellten Code. Die Buchstaben werden in eine 5×5-Tabelle geschrieben. Da es 26 Buchstaben gibt, müssen „I“ und „J“ in dasselbe Kästchen.

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

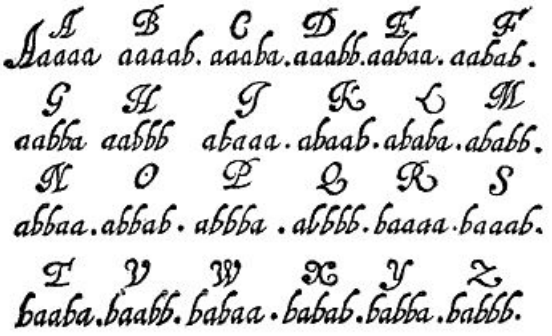
Zur Verschlüsselung hat man die links neben dem Buchstaben stehende Ziffer als Zehnerziffer und die über dem Buchstaben stehende als Einerziffer genommen. Der Buchstabe R erhielt demnach die Nr. 42. Diese Zuordnung ist wohl der Urahn unserer heutigen ASCII-Tabelle (siehe Anhang).

3.4 Die Caesar-Verschlüsselung



Der Name der Cäsar-Verschlüsselung leitet sich vom römischen Feldherrn Gaius Julius Caesar ab, der nach der Überlieferung des römischen Schriftstellers Sueton diese Art der geheimen Kommunikation für seine militärische Korrespondenz verwendet hat. Dabei benutzte Caesar eine Verschiebung des Alphabets um drei Buchstaben. Mehr dazu später.

3.5 Bacon-Code



Im Buch Nummer 6, Kapitel 1 seines Buches „The Advancement of Learning“, beschreibt Francis Bacon (1561–1626) detailliert ein Substituierungssystem: Die Buchstaben des Alphabetes wurden durchnummeriert und die zugeordnete Nummer durch eine Folge von „a“ und/oder „b“ bestehend aus 5 Zeichen derart substituiert, dass es sich effektiv um eine 5-Bit-Binärkodierung handelt. Es fällt auf, dass es noch keine klare Unterscheidung von U und V gibt, die sich erst ab dem 17. Jahrhundert durchsetzte.

3.6 Aufgaben:

1. Die folgende Buchstabenfolge ist die Aufschrift bzw. der Papierstreifen einer Skytale:

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

   Man weiß nur, dass die Skytale einen Umfang von 4 oder 5 Buchstaben hat. Welcher Klartext ergibt sich?

2. Verschlüssle den Text „V I E L G L U E C K“ mit dem Polybios-Code.

3. Im Film „2001 - Odyssee im Weltraum“ von Stanley Kubrick spielt der Computer HAL eine Hauptrolle. Der Name des Computers könnte eine Anspielung auf den Namen einer sehr großen Computerfirma sein[4]. Welche Caesar-Verschlüsselung wurde hier benutzt?

4. Entschlüssle den folgenden Text mit dem Original-Caesar-Verfahren:

   „Ghu Noxhjhuh jlew vrodqjh qdfk, elv hu ghu Gxpph lvw!“

5. Der folgende Text ist nach dem Atbasch-Verfahren codiert worden.

   „orvyvi vrmv uorvtv rn kliavoozmozwvm zoh vrm vovuzmg rm wvi hfkkv“

6. Welche Nummer hat der Buchstabe „R“ heute (siehe Anhang) und welche Nummer hätte er, wenn sich die Codierung von Bacon durchgesetzt hätte?

7. Dargestellt ist eine ganzseitige Anzeige einer Firma, die in einer Schülerzeitschrift um Schüler wirbt, die sich für Informatik interessieren. Was zeigt die Seite?

[4]Der Buchautor Arthur C. Clarke widerspricht dieser Darstellung.

4 Das System von Caesar

Der folgende Text ist nach dem Caesar-Verfahren verschlüsselt worden. Der Schlüssel ist aber nicht bekannt.

WRQRE XNAA QVR IREFPUYHRFFRYHAT IBA PNRFNE RVASNPU XANPXRA.

Buchstabe:	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
Anzahl:																										

1. Bestimme mit Hilfe der Tabelle den Buchstaben, der am häufigsten im Text vorkommt.

2. Entschlüssele dann den angegebenen Geheimtext.

Die Entschlüsselung nach diesem Verfahren der Häufigkeitsanalyse hat seine Grenzen. Der französische Schriftsteller Georges Perec hat es geschafft, sogar ein ganzes Buch mit etwa 85.000 Wörtern zu schreiben, ohne ein einziges Mal den Buchstaben „e“ zu benutzen. Noch erstaunlicher ist es, dass sogar Übersetzungen in das Spanische (der häufigste Buchstabe ist das „a“) ohne ein „a“ und auch ins Englische, Schwedische und Deutsche ohne ein „e“ auskamen. Der deutsche Übersetzer Eugen Hemlé veröffentlichte das Buch unter dem Titel „Anton Voyls Fortgang“. Das Buch fängt so an:

> *Kardinal, Pastor und Admiral, als Führungstrio null und nichtig und darum völlig abhängig vom Ami-Trust, tat durch Radionachricht und Anschlag kund, daß Nahrungsnot und damit Tod aufs Volk zukommt. Zunächst tat man das als Falschinformation ab. Das ist Propagandagift, sagt man. Doch bald schon ward spürbar, was man ursprünglich nicht glaubt. Das Volk griff zum Stock, zum Dolch. „Gib uns das täglich Brot“, hallts durch Land und „pfui auf das Patronat, auf Ordnung, Macht und Staat.“ ...*

Bemerkenswert dabei ist insbesondere, dass Autor und Übersetzer ins Deutsche mit „e“s in ihren Namen geradezu gesegnet sind.

4.1 Verschlüsselung mit einem Tabellenkalkulationsprogramm

Im Anhang findet man eine Zusammenstellung von wichtigen Funktionen einer Tabellenkalkulation.

4.1.1 Aufgaben

1. Fertige eine Tabelle zur Verschlüsselung eines eingegebenen Textes an. Es sollen nur die Buchstaben verschlüsselt werden. Ziffern und Satzzeichen sollen erhalten bleiben. Es genügt, wenn der eingegebene Text vor der Verschlüsselung in Großbuchstaben umgewandelt und dann verschlüsselt wird. Die Verschlüsselung soll in Abhängigkeit von einem einzugebenen Schlüsselbuchstaben (D für Original-Caesar-Verschlüsselung) verwirklicht werden.

   Eine Vorlage für ein solches Tabellenblatt findest du hier:

   http://www.gierhardt.de/informatik/krypto

   In dieser Datei sind auch die unten angegebenen Beispiele enthalten.

2. Schreibe das Tabellenblatt so weit um, dass damit auch die Entschlüsselung erledigt werden kann. Dazu ist es hilfreich, die Häufigkeit der Buchstaben im Text zu untersuchen.

3. Entschlüssle die folgenden Texte:

   (a) EPPIVERJERKMWXWGLAIV
   (b) XZCRPYDEFYOSLEMWPTTXSTYEPCY
   (c) XEBDYDOPSCMROCMRGSWWOXWSDNOWCDBYW
   (d) FGNRQGVFPURFTLZANFVHZONQYNNFCUR
   (e) HMENQLZSHJLZBGSROZRR
   (f) BDASDMYYUQDQZUEFEOTIQD
   (g) FKGGTFGKUVGKPGUEJGKDG
   (h) STGBDCSXHIPJHZPTHT
   (i) MGLOEQMGLWELMGLWMIKXI
   (j) WBKUSAMKDISXTKRYIJABQIIU

4. (freiwillige Zusatzaufgabe): Es soll auch noch nach Groß- und Kleinbuchstaben unterschieden werden.

5 Die Vigenère-Methode

5.1 Erweiterung der Caesar-Verschlüsselung

Die Caesar-Verschlüsselung ist durch eine Häufigkeitsanalyse bei einem genügend langen Text fast immer sehr schnell zu knacken, weil jedem Buchstaben immer der gleiche verschlüsselte Buchstabe zugeordnet wird. Man spricht von einer *monoalphabetischen Substitution*[5].

Bereits im 16. Jahrhundert kam der französische Diplomat Blaise de Vigenère[6] auf die Idee, nach jedem verschlüsselten Buchstaben das Alphabet zu wechseln. Man spricht bei seiner Methode von *polyalphabetischer Substitution*[7]. Seine Idee war so erfolgreich, dass man bis 1917 das System für vollkommen unknackbar hielt.

Nach der Vigenère-Tabelle (siehe nächste Seite) würde man für die Original-Caesar-Verschlüsselung (Schlüssel-Buchstabe D, d.h. Verschiebung um 3 Positionen) den Klartextbuchstaben der ersten Zeile durch den Buchstaben in der vierten Zeile (beginnt mit D) ersetzen.

Wenn man nun den ersten Buchstaben des Klartextes mit dem Schlüsselbuchstaben D, den zweiten Buchstaben mit dem Schlüsselbuchstaben E und den dritten mit O verschlüsselt, hat man das Schlüsselwort DEO benutzt. Für die folgenden Buchstaben beginnt man wieder von vorne.

Beispiel:

Schlüsselwort:	D	E	O	D	E	O	D	E
Klartext:	I	N	F	O	R	A	U	M
Geheimtext:	L							

Regel: Man sucht den Buchstaben des Schlüsselwortes (z.B. D) in der ersten Spalte und den Buchstaben des Klartextes (z.B. I) in der ersten Zeile. Am Kreuzungspunkt findet man den Geheimtextbuchstaben L.

[5] von griechisch: mono = einzig, alphabeto = Alphabet sowie von lateinisch: substituere = ersetzen)
[6] Aussprache: Wischenähr
[7] von griechisch: polloi = viele

5.2 Aufgaben:

1. Vervollständige den Geheimtext zum Klartext „INFORAUM“.

Schlüsselwort:	D	E	O	D	E	O	D	E
Klartext:	I	N	F	O	R	A	U	M
Geheimtext:	L							

2. Verschlüssele den folgenden Klartext mit dem Schlüsselwort „WURST“.

Schlüssel																									
Klartext	W	E	R	B	E	I	M	M	E	T	Z	G	E	R	K	L	I	N	G	E	L	T	D	A	R
Geheimtext																									
Schlüssel																									
Klartext	F	S	I	C	H	N	I	C	H	T	W	U	N	D	E	R	N	W	E	N	N	K	E	I	N
Geheimtext																									
Schlüssel																									
Klartext	S	C	H	W	E	I	N	A	U	F	M	A	C	H	T										
Geheimtext																									

Kontrolliere das Ergebnis mit dem Programm *Cryptool*.

Stelle fest, ob das Programm *Cryptool* die Schlüssellänge errechnen und damit das Schlüsselwort bestimmen kann.

3. Formuliere eine Regel für das Entschlüsseln eines Textes.

4. Entschlüssele den folgenden Geheimtext mit dem Schlüsselwort „ICH“.

Schlüssel																									
Klartext																									
Geheimtext	W	D	D	W	J	S	L	K	L	I	N	W	P	C	I	M	V	L	E	G	J	P	U	L	T
Schlüssel																									
Klartext																									
Geheimtext	P	R	I	P	U	U	C	U	O	W	A	M	P	A	A	E	O	T	W	L	A	U	L	T	P

5.3 Das Vigenère-Quadrat

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

5.4 Kann man den Vigenère-Code knacken?

Über 300 Jahre blieb das Verfahren ungeknackt. Aber 1863 fand der preußische Infanteriemajor Friedrich Wilhelm Kasiski eine geniale Methode, um das Problem der Vigenère-Verschlüsselung zu lösen.

Seine erste Erkenntnis war:

Wenn man die Länge des Schlüsselwortes kennt, dann bekommt man auch das Schlüsselwort selbst heraus.

Wir demonstrieren das an dem im Folgenden gegebenen verschlüsselten Text. Wir nehmen an, dass der Text mit einem Schlüsselwort aus drei Buchstaben verschlüsselt wurde. Der Text wird dann in Dreierpäckchen aufgeschrieben. Wir wissen, dass jeder erste Buchstabe mit dem gleichen Schlüsselbuchstaben verschlüsselt wurde. Also bestimmen wir die Buchstabenhäufigkeit für den ersten Buchstaben eines Dreierpäckchens.

1. Häufigkeit für den **ersten** Buchstaben eines Dreierpäckchens:

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

   Am häufigsten ist der Buchstabe _____. Der Buchstabe E wurde also zu _____. Demnach muss der Schlüsselbuchstabe ein _____ sein.

2. Häufigkeit für den **zweiten** Buchstaben eines Dreierpäckchens:

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

   Am häufigsten ist der Buchstabe _____. Der Buchstabe E wurde also zu _____. Demnach muss der Schlüsselbuchstabe ein _____ sein.

3. Häufigkeit für den **dritten** Buchstaben eines Dreierpäckchens:

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

   Am häufigsten ist der Buchstabe _____. Der Buchstabe E wurde also zu _____. Demnach muss der Schlüsselbuchstabe ein _____ sein.

   Somit ist das Schlüsselwort wahrscheinlich _____. Damit soll der folgende Text entschlüsselt werden.

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

6 Gibt es unknackbare Codes?

6.1 Vorüberlegungen

Wir betrachten den folgenden Geheimtext mit 16 Buchstaben:

I C F Q D B Q D E Y Y N I G T R

1. Wir nehmen an, der Geheimtext sei mit dem Caesar-Verfahren hergestellt worden. Wie viele verschiedene Klartexte sind dann zu diesem Geheimtext möglich? Begründe!

2. Wie viele verschiedene „Worte“ mit

   (a) 1 Buchstaben,

   (b) 2 Buchstaben,

   (c) 3 Buchstaben bzw.

   (d) 16 Buchstaben

   sind überhaupt für irgendeinen Klartext möglich, wenn wir nur mit 26 verschiedenen Buchstaben verwenden?

3. Wir nehmen nun an, der Geheimtext sei nach dem Verfahren von Vigenère hergestellt worden. In den folgenden drei Tabellen ist immer der gleiche Geheimtext zu verschiedenen Klartextvarianten angegeben. Stelle fest, ob sich immer ein Schlüsselwort angeben lässt.

Schlüssel																
Klartext	S	C	H	U	L	E	M	A	C	H	T	S	P	A	S	S
Geheimtext	I	C	F	Q	D	B	Q	D	E	Y	Y	N	I	G	T	R

Schlüssel																
Klartext	I	N	F	O	R	M	A	T	I	K	I	S	T	G	U	T
Geheimtext	I	C	F	Q	D	B	Q	D	E	Y	Y	N	I	G	T	R

Schlüssel																
Klartext	F	E	R	I	E	N	S	I	N	D	B	E	S	S	E	R
Geheimtext	I	C	F	Q	D	B	Q	D	E	Y	Y	N	I	G	T	R

   Antwort (mit Begründung):

4. Wie viele verschiedene Klartexte lassen sich aus dem gegebenen Geheimtext herstellen?

   Antwort:

6.2 Das perfekte Verfahren

Ein Verschlüsselungssystem bietet perfekte Sicherheit, wenn zu einem Geheimtext jeder mögliche Klartext gleich wahrscheinlich ist.

Das lässt sich „ganz einfach“ erreichen (**One time pad - Verfahren**):

- Man wählt einen Schlüssel, der genauso lang wie der Klartext ist.
- Der Schlüssel enthält nur rein zufällig gewählte Buchstaben.
- Man verwendet den Schlüssel nur einmal zum Entschlüsseln.

Aber manches ist dann doch nicht ganz so einfach:

- Ein Schlüssel, der genauso lang wie der Klartext ist, macht die Ver- und Entschlüsselung sehr unpraktisch, weil die gleiche Datenmenge noch einmal auf anderem Wege übertragen werden muss. Wenn dieser „andere Weg“ unsicher ist, gibt es Probleme.
- Die Herstellung von rein zufälligen Buchstaben oder Zahlen ist gar nicht so einfach, wie man im ersten Moment denkt. Schon bei einem einfachen Würfel ist nicht immer gesichert, dass jede Augenzahl mit gleicher Wahrscheinlichkeit kommt.

  Computer können sogenannte Zufallszahlen liefern. Diese Zahlen werden aber durch bestimmte Formeln bestimmt. Nach dem Start bei einer bestimmten Zahl liefert der Computer nacheinander immer die gleichen Zahlenfolge. Nur bei einem Wechsel der Startzahl erscheinen neue Zahlen. Oft wird als Startzahl einer Zufallszahlenfolge eine Uhrzeit o.a. genommen. Damit ist nicht ganz ausgeschlossen, dass die Berechnung der Zufallszahlen beeinflusst werden kann. Geheimdienste interessieren sich für Zufallsgeneratoren von Computern!

7 Public-Key-Chiffrierung

7.1 Das Prinzip des öffentlichen Schlüssels

Die bekannteste Public-Key-Kodierung geht auf die drei Mathematiker Ron Rivest, Adi Shamir und Leonard Adleman vom Massachusetts Institute of Technology (MIT) zurück und wird seit 1978 nach deren Anfangsbuchstaben als **RSA-Verfahren** bezeichnet.

Zur Erinnerung: Bei einem symmetrischen Verschlüsselungsverfahren (Caesar, Vigenère, u.a.) wird zum Ver- und Entschlüsseln derselbe Schlüssel benutzt).

Das RSA-Verschlüsselungsverfahren gehört zu der Klasse der asymmetrischen Verschlüsselungsverfahren. Beim Verschlüsseln wird ein **öffentlicher Schlüssel** und beim Entschlüsseln ein **privater Schlüssel** verwendet. Mit dem öffentlichen Schlüssel kann jeder Nachrichten verschlüsseln, aber nicht entschlüsseln. Zum Entschlüsseln benötigt man den privaten Schlüssel, und den kennt nur der Empfänger.

7.2 Das Verfahren allgemein beschrieben

1. Wähle zwei Primzahlen p und q.
2. Berechne das Produkt $n = p \cdot q$.
3. Berechne das Produkt[8] $\phi(n) = (p-1) \cdot (q-1)$.
4. Wähle eine Zahl c mit $1 < c < n$, die teilerfremd zu $\phi(n) = (p-1) \cdot (q-1)$ ist.
5. Bestimme eine Zahl d mit der Eigenschaft $(c \cdot d) \bmod \phi(n) = 1$.

   In Worten (Version 1): Dividiert man das Produkt $c \cdot d$ durch $\phi(n) = (p-1) \cdot (q-1)$, so erhält man den Rest 1.

   In Worten (Version 2): Ein Vielfaches von $(p-1) \cdot (q-1)$ ergänzt um 1 ergibt $c \cdot d$.

   Oder: Es gibt eine natürliche Zahl s mit $c \cdot d = s \cdot (p-1) \cdot (q-1) + 1$.
6. Als öffentlichen Schlüssel nimmt man die Zahlen n und c.
7. Als geheimen Schlüssel nimmt man die Zahl d.
8. **Verschlüsselung:** Ein Buchstabe b des Klartextes wird durch eine Zahl w repräsentiert. Daraus berechnet man die Zahl x mit

   $$x = w^c \bmod n.$$

   x kommt dann in die geheime Botschaft anstelle des Buchstabens b.

[8] ϕ heißt auch Eulersche Funktion und gibt die Anzahl der zu n teilerfremden Zahlen kleiner als n an. Beispiel: $\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$ und es gibt 8 Zahlen kleiner als 15, die teilerfremd zu 15 sind: 1, 2, 4, 7, 8, 11, 13 und 14.

9. **Entschlüsselung:** Aus der Zahl x in der geheimen Botschaft wird die Zahl y berechnet nach

   $$y = x^d \bmod n.$$

   Wenn man sich nicht verrechnet hat, müsste dann $y = w$ sein, woraus sich der ursprüngliche Buchstabe b ergeben sollte.

7.3 Das Verfahren an einem Beispiel beschrieben

1. Wähle die zwei Primzahlen $p = 3$ und $q = 7$.
2. Berechne das Produkt $n = p \cdot q = 3 \cdot 7 = 21$.
3. Berechne das Produkt $\phi(n) = (p-1) \cdot (q-1) : \phi(21) = (3-1) \cdot (7-1) = 2 \cdot 6 = 12$.
4. Wähle eine Zahl c mit $1 < c < 21$, die teilerfremd zu $\phi(21) = 12$ ist. Wähle z.B. $c = 5$, weil 5 und 12 keinen Teiler gemeinsam haben.
5. Bestimme eine Zahl d mit der Eigenschaft $(5 \cdot d) \bmod 12 = 1$.

d	$5 \cdot d$	$(5 \cdot d) \bmod 12$
1	5	5
2	10	10
3	15	3
4	20	8
5	25	1

   In Worten (Version 1): Dividiert man das Produkt $5 \cdot d$ durch 12, erhält man den Rest 1.

   In Worten (Version 2): Ein Vielfaches von 12 ergänzt um 1 ergibt $5 \cdot d$.

   Es ergibt sich $d = 5$.
6. Als öffentlichen Schlüssel nimmt man die Zahlen $n = 21$ und $c = 5$.
7. Als geheimen Schlüssel nimmt man die Zahl $d = 5$ (hier zufällig identisch mit c).
8. **Verschlüsselung:** Wir geben dem Buchstaben A die Nummer 1, dem Buchstaben B die Nummer 2 usw. Nehmen wir den Buchstaben B des Klartextes, so ist $w = 2$. Daraus berechnet man die Zahl x mit

   $$x = 2^5 \bmod 21 = 32 \bmod 21 = 11.$$

   $x = 11$ kommt dann in die geheime Botschaft anstelle des Klarbuchstabens B.
9. **Entschlüsselung:** Aus der Zahl $x = 11$ in der geheimen Botschaft wird die Zahl y berechnet nach

   $$y = 11^5 \bmod 21 = 161.051 \bmod 21 = 2, \text{ weil } 161.051 = 7669 \cdot 21 + 2.$$

   2 ist die Nummer des Klarbuchstabens B.

7.4 Wie sicher ist RSA?

Im Beispiel lässt sich der geheime Schlüssel $d = 5$ sehr einfach bestimmen, weil man $n = 21$ leicht in die Primfaktoren $p = 3$ und $q = 7$ zerlegen kann. Mit der Kenntnis von p und q (und dem öffentlichen Wert von c) kann man d bestimmen und den Code knacken.

Auf den ersten Blick scheint die Primfaktorzerlegung kein großes Problem zu sein. Z.B. findet man schnell $207 = 9 \cdot 23$. Etwas länger dauert es (zumindest mit dem Taschenrechner), die Zerlegung $2773 = 47 \cdot 59$ zu finden. Für einen Computer ist das kein nennenswertes Problem. Er kann bei der Suche nach einem Teiler einer Zahl n alle Primzahlen bis $\sqrt{n}$ testen. Bei einer 200-stelligen Zahl muss er dann etwa alle Primzahlen zwischen 2 und 10^{100} als Teiler untersuchen. In diesem Bereich liegen allerdings ca. 10^{97} Primzahlen, mehr als die Anzahl der Atome im Universum. Wenn ein Computer für eine Division nur 1 Milliardstel Sekunde ($= 1 \cdot 10^{-9}$ s) benötigt, dann dauert seine Suche nach einem Primfaktor im schlimmsten Fall

$$10^{97} \cdot 1 \cdot 10^{-9}\,\text{s} = 1 \cdot 10^{88}\,\text{s} = 2{,}77 \cdot 10^{84}\,\text{h} = 3{,}17 \cdot 10^{80}\,\text{Jahre}$$

bei einem geschätzten Alter unseres Universums von ca. $14 \cdot 10^9$ Jahren.

Nun haben kluge Mathematiker und Informatiker schon Algorithmen entwickelt, die nicht jede Primzahl wie oben beschrieben als Teiler testen und damit die Primfaktorzerlegung viel schneller erledigen. Der aktuelle Stand (Meldung vom 07.01.2010): Ein internationales Team von Wissenschaftlern unter Beteiligung der Universität Bonn hat eine 232-stellige Zahl in ihre Primfaktoren zerlegt. Für ihre Berechnung nutzten sie vernetzte Computer, ein einzelner handelsüblicher Rechner wäre knapp 2.000 Jahre beschäftigt gewesen.

Auf der Seite

http://www.arndt-bruenner.de/mathe/scripts/primzahlen.htm

kann man sich RSA-Schlüssel generieren und dann nach den Primfaktoren suchen lassen.

Zusammengefasst: Das RSA-Verfahren ist nicht absolut sicher. Das Knacken des Codes dauert aber heute noch so lange, dass man sich am Ende wahrscheinlich nicht mehr für die Nachricht interessiert.

7.5 Das Rechnen mit Resten

Beim Ver- und Entschlüsseln sind gigantische Potenzen zu bearbeiten. Schon eine „kleine“ Potenz wie z.B. 61^{57} kann ein handelsüblicher Taschenrechner nicht mehr verarbeiten. Deshalb sind Methoden gefordert, um die Resteberechnung bei großen Potenzen zu vereinfachen.

Zur Vereinfachung wird für Reste die folgende Schreibweise verwendet:

Definition: Mit $R_n(m)$ wird der Rest bei der Division von m durch n bezeichnet. Andere Schreibweise:

$$R_n(m) = m \bmod n$$

Beispiele:

1. $R_3(17) = 2,$ weil $17 = 5 \cdot 3 + 2.$

2. $R_3(27) = 0,$ weil $27 = 9 \cdot 3 + 0.$

3. $R_5(38) = 3,$ weil $38 = 7 \cdot 5 + 3.$

7.5.1 Addition

Zuerst ein Beispiel zur Demonstration:

$$\begin{aligned} R_3(7) &= 1 \\ R_3(17) &= 2 \\ R_3(7+17) &= R_3(24) = 0 \neq R_3(7) + R_3(17), \text{ aber} \\ R_3(7+17) &= R_3\left[R_3(7) + R_3(17)\right] = R_3(1+2) = R_3(3) = 0 \end{aligned}$$

Es gilt allgemein (ohne Beweis): $\boxed{R_n(a+b) = R_n\left(R_n(a) + R_n(b)\right)}$

7.5.2 Multiplikation

Und wieder zuerst ein Beispiel zur Demonstration:

$$\begin{aligned} R_5(7) &= 2 \\ R_5(14) &= 4 \\ R_5(7 \cdot 14) &= R_5(98) = 3 \neq R_5(7) \cdot R_5(14) = 8, \text{ aber} \\ R_5(7 \cdot 17) &= R_5\left[R_5(7) \cdot R_5(14)\right] = R_4(2 \cdot 4) = R_5(8) = 3 \end{aligned}$$

Es gilt allgemein (ohne Beweis): $\boxed{R_n(a \cdot b) = R_n\left(R_n(a) \cdot R_n(b)\right)}$

7.5.3 Potenzierung

Zuerst ein Beispiel:

$$\begin{aligned} R_3(17^5) &= R_3(1.419.857) = R_3(473.285 \cdot 3 + 2) = 2(\text{ direkt berechnet}) \\ R_3(17^5) &= R_3(17 \cdot 17 \cdot 17 \cdot 17 \cdot 17) \\ &= R_3(R_3(17) \cdot R_3(17) \cdot R_3(17) \cdot R_3(17) \cdot R_3(17))(\text{ Multiplikationsregel}) \\ &= R_3(R_3^5(17)) \\ &= R_3(2^5) = R_3(32) = 2 \end{aligned}$$

Es gilt allgemein (ohne Beweis): $\boxed{R_n(a^m) = R_n\left(R_n^m(a)\right)}$

7.5.4 Wir machen große Potenzen klein!

Mit einem Taschenrechner ist z.B. $R_26(85^{10})$ nicht berechenbar. Ein übliches Tabellenkalkulationsprogramm liefert das falsche Ergebnis 6.

Mit den Rechenregeln:

$$
\begin{aligned}
R_{26}(85^{10}) &= R_{26}(R_{26}^{10}(85)) \\
&= R_{26}(R_{26}^{10}(3 \cdot 26 + 7)) \\
&= R_{26}(7^{10}) \\
&= R_{26}(282.475.249) \\
&= R_{26}(10.864.432 \cdot 26 + 17) \\
&= 17 \quad \text{oder} \\
R_{26}(85^{10}) &= R_{26}\left[85^3 \cdot 85^3 \cdot 85^4\right] \\
&= R_{26}\left[R_{26}(85^3) \cdot R_{26}(85^3) \cdot R_{26}(85^4)\right] \\
&= R_{26}\left[R_{26}(R_{26}^3(85)) \cdot R_{26}(R_{26}^3(85)) \cdot R_{26}(R_{26}^4(85))\right] \\
&= R_{26}\left[R_{26}(7^3) \cdot R_{26}(7^3) \cdot R_{26}(7^4)\right] \\
&= R_{26}\left[R_{26}(343) \cdot R_{26}(343) \cdot R_{26}(2401)\right] \\
&= R_{26}\left[5 \cdot 5 \cdot 9\right] \\
&= R_{26}\left[225\right] \\
&= 17
\end{aligned}
$$

8 Anhang

8.1 Tabellenkalkulationsfunktionen

8.1.1 Funktionen für Texte

1. **=GROSS(Text)** wandelt den Text komplett in Großbuchstaben um.

   Beispiel: `=GROSS("Ene mene mu")` liefert „ENE MENE MU“.

2. **=VERKETTEN(Text1;Text2;...** liefert die Verkettung der Texte.

   Beispiel: `=VERKETTEN("Ene"; "Mene"; "MU")` liefert „Ene Mene Mu“.

3. **=TEIL(Text; Startposition; Anzahl)** liefert ab der Startposition Anzahl Buchstaben des Textes.

   Beispiel: `=TEIL("Quatschkopf"; 8; 1)` liefert „k“.

8.1.2 Allgemeine Funktionen

1. **=WENN(Bedingung; Dann-Ergebnis; Sonst-Ergebnis)** liefert das Dann-Ergebnis, wenn die Bedingung erfüllt ist, sonst das Sonst-Ergebnis.

   Beispiel: `=WENN(REST(A3;2)=0;"Zahl ist gerade"; "Zahl ist ungerade.")`

2. **=ZÄHLENWENN(Bereich; Kriterium)** liefert die Anzahl der Zellen, die im Bereich dem Kriterium entsprechen.

   Beispiel: `=ZÄHLENWENN(A1:A10;67)` liefert die Anzahl der Zellen von A1 bis A10, die den Wert 67 enthalten.

8.1.3 Funktionen zum Rechnen

1. **=GANZZAHL(Zaehler/Nenner)** liefert den Wert einer ganzzahligen Division.

   Beispiel: `=GANZZAHL(35/11)` liefert 3, weil 35:11 = 3 Rest 2.

2. **=REST(Zaehler; Nenner)** liefert den Rest bei einer ganzzahligen Division.

   Beispiel: `=REST(35; 11)` liefert 2, weil 35:11 = 3 Rest 2.

3. **=SUMME(Bereich)** liefert die Summe der Zahlen im Bereich (z.B. A3:C7).

4. **=MITTELWERT(Bereich)** liefert den Mittelwert der Zahlen im Bereich (z.B. A3:C7).

5. **=MIN(Bereich)** liefert das Minimum der Zahlen im Bereich (z.B. A3:C7).

6. **=MAX(Bereich)** liefert das Maximum der Zahlen im Bereich (z.B. A3:C7).

7. **=ZUFALLSZAHL()** liefert eine Zufallszahl x mit $0 \leq x < 1$.

8.1.4 Funktionen für Zeichen

1. **=ZEICHEN(Zahl)** liefert das Zeichen mit der angegebenen Nummer im ASCII-Code.

   Beispiel: `=ZEICHEN(65)` liefert ein A.

2. **=CODE(Zeichen)** liefert die Nummer des Zeichens im ASCII-Code.

   Beispiel: `=CODE("A")` liefert 65.

8.1.5 Funktionen für Umwandlungen zwischen Stellenwertsystemen

1. **=DEZINHEX(Zahl; [Stellen])** liefert die Hexadezimaldarstellung der dezimalen Zahl.

   Beispiel: `=DEZINHEX(65)` liefert die Hexadezimalzahl 41.

   Beispiel: `=DEZINHEX(65; 4)` liefert die Hexadezimalzahl 0041 (4 Stellen).

2. **=HEXINDEZ(Zahl)** liefert die Dezimaldarstellung der hexadezimalen Zahl.

   Beispiel: `=HEXINDEZ(41)` liefert 65.

3. **=DEZINBIN(Zahl; [Stellen])** liefert die Binärdarstellung der dezimalen Zahl.

   Beispiel: `=DEZINBIN(7)` liefert die Binärzahl 111.

   Beispiel: `=DEZINBIN(7; 8)` liefert die Binärzahl 00000111 (8 Stellen).

4. **=BININDEZ(Zahl)** liefert die Dezimaldarstellung der Binärzahl.

   Beispiel: `=BININDEZ(111)` liefert 7.

5. **=DEZIMAL(Text; Zahlenbasis)** liefert die Dezimaldarstellung der im Text dargestellten Zahl mit der angegebenen Zahlenbasis.

   Beispiel: `=DEZIMAL(111; 2)` liefert 7.

6. **=Basis(Zahl; Zahlenbasis; [Mindestlänge])** liefert die Dezimalzahl Zahl in der angegebenen Zahlenbasis dargestellt.

   Beispiel: `=BASIS(7; 2)` liefert 111.

   Beispiel: `=BASIS(255; 16; 4)` liefert 00FF.

8.2 Die ASCII-Tabelle

Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen
0	00	NUL	32	20	SP	64	40	@	96	60	‘
1	01	SOH	33	21	!	65	41	A	97	61	a
2	02	STX	34	22	“	66	42	B	98	62	b
3	03	ETX	35	23	#	67	43	C	99	63	c
4	04	EOT	36	24	$	68	44	D	100	64	d
5	05	ENQ	37	25	%	69	45	E	101	65	e
6	06	ACK	38	26	&	70	46	F	102	66	f
7	07	BEL	39	27	’	71	47	G	103	67	g
8	08	BS	40	28	(	72	48	H	104	68	h
9	09	TAB	41	29	)	73	49	I	105	69	i
10	0A	LF	42	2A	*	74	4A	J	106	6A	j
11	0B	VT	43	2B	+	75	4B	K	107	6B	k
12	0C	FF	44	2C	,	76	4C	L	108	6C	l
13	0D	CR	45	2D	-	77	4D	M	109	6D	m
14	0E	SO	46	2E	.	78	4E	N	110	6E	n
15	0F	SI	47	2F	/	79	4F	O	111	6F	o
16	10	DLE	48	30	0	80	50	P	112	70	p
17	11	DC1	49	31	1	81	51	Q	113	71	q
18	12	DC2	50	32	2	82	52	R	114	72	r
19	13	DC3	51	33	3	83	53	S	115	73	s
20	14	DC4	52	34	4	84	54	T	116	74	t
21	15	NAK	53	35	5	85	55	U	117	75	u
22	16	SYN	54	36	6	86	56	V	118	76	v
23	17	ETB	55	37	7	87	57	W	119	77	w
24	18	CAN	56	38	8	88	58	X	120	78	x
25	19	EM	57	39	9	89	59	Y	121	79	y
26	1A	SUB	58	3A	:	90	5A	Z	122	7A	z
27	1B	ESC	59	3B	;	91	5B	[	123	7B	{
28	1C	FS	60	3C	«	92	5C	\	124	7C	|
29	1D	GS	61	3D	=	93	5D	]	125	7D	}
30	1E	RS	62	3E	»	94	5E	ˆ	126	7E	-
31	1F	US	63	3F	?	95	5F	_	127	7F	DEL

9 Quellen

Viele Inhalte und Beispiele habe ich ohne direkte Quellenangabe von diversen Autoren übernommen. Ich beanspruche keineswegs, hier eine eigene geistige Leistung dokumentiert zu haben.

- Albrecht Beutelspacher, Geheimsprachen, Verlag C. H. Beck 2002
- Albrecht Beutelspacher, Kryptologie, Vieweg 2002
- Albrecht Beutelspacher, Zeitschrift *Mathe-Welt*, Erhard Friedrich Verlag, Velber 1995 2002
- Helmut Witten und Ralph-Hardo Schulz, RSA & Co. in der Schule, LOG IN Heft Nr. 140(2006)
- Simon Singh, Geheime Botschaften, dtv 2002
- Herbert Voss, Kryptografie mit Java, Franzis Verlag 2006
- http://www.cryptool.de
- http://de.wikipedia.org