1. Kryptologie und öffentliche Schlüssel

1.1. Verschlüsselung mit Alphabeten

Eine beliebte Methode der Verschlüsselung (vor allem unter Kindern) ist es, sich ein neues Alphabet zu geben. Schon Caesar benutzte diese Methode, indem er das Alphabet um 5 Buchstaben verschob. Um miteinander kommunizieren zu können, muss jeder Eingeweihte einen Schlüssel haben. Diese Methode lässt sich zum Beispiel auf dem Internet nicht anwenden, da vor einer Komminikation der Schlüssel übermittelt werden müsste, und dabei abgefangen werden könnte. Aber auch für den privaten Gebrauch ist die Methode nicht sicher.

Nehmen wir an, wir haben folgdende Meldung abgefangen:

```
jgoioworjyebgivwgvogeowarxdacovlopifdryoiiorvjaiwafdvoiogeuaf
djoeypixpyoebrgfdoevomvhyoevhguuopewaewyiieypjgocyfdivacoedao
yugbnogvoecoafdvoeywogeoebpziioevogrjoivomvoiroioehynzoeeoe
```

Wir vermuten, dass die Nachricht in deutscher Sprache ist. Eine Schwierigkeit besteht darin, dass keine Lehrzeichen verwendet wurden. Zählen wir die Buchstaben, erhalten wir folgende Häufigkeiten:

Buchstabe	o	e	i	v	g	y	a	d	r	w	f	j	p	b	c	u
Häufigkeit	35	20	16	14	13	11	9	8	7	7	6	6	6	4	4	4

Zählen wir Buchstabenpaare, erhalten wir

Buchstabenpaar	oe	vo	fd	oi	og	io
Häufigkeit	12	8	6	6	5	5

In der deutschen Sprache haben wir folgende Häufigkeiten in Promille:

Buchstabe	e	n	i	r	s	a	t	d	u	h	l	g	o	c
Häufigkeit	180	106	79	72	69	58	56	51	46	41	33	33	31	25
Paar	en	er	ch	de	nd	ei	te	ie	in	ge	es	un	he	ne
Häufigkeit	43	39	26	23	21	20	19	18	17	17	15	14	12	13

Wir vermuten, dass o=e und e=n. Das einzige Paar, wo kein e vorkommt, ist fd. Wir vermuten, dass dies ch ist. Wir vermuten weiter, dass v=d und i=r. Dann lautet unser Text:

```
..ere.e...n..rd..de.ne....h..ed.e.rch..erre.d..r..chdere.n..c
h.en..r...en...chende.d..end....e.n..n..rrn....e..chrd..enh.e
.....e.den.e.chden..e.nen...rrende...erde.der.eren....ennen
```

Die Buchstabenfolge `rrn` scheint nicht wahrscheinlich. Weiter muss bei `e.rch` ein Vokal dazwischen stehen. Da `sch` ein oft im Deutschen vorkommendes Tripel ist,

könnte es sein, dass r nicht so oft vorkommt, wie wir erwarten, und i=s die richtige Lösung wäre. Dann lautet der Text

```
..ese.e...n..sd..de.ne....h..ed.e.sch..esse.d..s..chdese.n..c
h.en..s...en...chende.d..end....e.n..n..ssn....e..chsd..enh.e
.....e.den.e.chden..e.nen...ssende...esde.des.esen....ennen
```

Es scheint keine sinnvollen Wörter mit `.rese` zu geben. Das nächste Paar `e.` ist `ei`. Also versuchen wir g=i:

```
.iese.e...n.isd.ideine....h..ed.e.sch..esse.d..s..chdesein..c
h.en..s...en..ichende.d..end.i..e.n..n..ssn...ie..chsd..enh.e
..i..eiden.e.chden..einen...ssendei..esde.des.esen....ennen
```

Der erste Buchstabe könnte ein j=d sein. Dann müsste aber v=d falsch sein. Da wir i auch schon haben, könnte v=t gelten, da de und te etwa gleich oft vorkommen:

```
diese.e.d.n.ist.iteine....h..et.e.sch..esse.td.s..chtesein..c
hden..s...en..ichente.t..ent.i..e.n..n..ssn..die..chst..enh.e
..i..eiten.e.chten..einen...ssentei.deste.tes.esen....ennen
```

Das a sollte ein Vokal sein, wahrscheinlich ein a, was mit der Häufigkeit übereinstimmt. Setzen wir also a=a:

```
diese.e.d.n.ist.iteine.a..ha.et.e.sch..esse.tdas.achtesein.ac
hden..s...en..ichente.t..ent.i..e.n.an..ssn..die..chsta.enhae
..i..eiten.eachten..einen...ssentei.deste.tes.esen....ennen
```

Als nächstes raten wir w=m:

```
dieseme.d.n.istmiteinema..ha.et.e.sch..esse.tdasmachtesein.ac
hden..s...en..ichente.t..ent.i..e.nmanm.ssn..die..chsta.enhae
..i..eiten.eachten.meinen...ssentei.deste.tes.esen....ennen
```

Wir erkennen u=f, y=u, c=b

```
dieseme.dun.istmiteinema..habet.e.sch.uesse.tdasmachteseinfac
hdenu.s..uen..ichente.t.uent.iffe.nmanmussnu.diebuchstabenhae
ufi..eitenbeachtenumeinen...ssentei.deste.tes.esen.u..ennen
```

Jetzt ist es nicht mehr schwer, r=l, b=g, x=p, l=v, p=r, m=x, h=z, n=k, z=o

```
diesemeldungistmiteinemalphabetverschluesseltdasmachteseinfac
hdenurspruenglichentextzuentziffernmanmussnurdiebuchstabenhae
ufigkeitenbeachtenumeinengrossenteildestexteslesenzukoennen
```

Jetzt haben wir den Text entschlüsselt. Hätten wir mehr Text, oder mehrere Meldungen abgefangen, wäre die Entschlüsselung noch einfacher. Wir wollen nun eine Möglichkeit entwickeln, mit einem öffentlichen Schlüssel zu verschlüsseln, so dass die Entschlüsselung schwierig wird.

1.2. Gruppentheorie

Definition 1.1. *Eine Menge $G \neq \emptyset$ mit einer Verknüpfung $\circ : G \times G \to G$ heisst* **Gruppe**, *falls*

i) $a \circ (b \circ c) = (a \circ b) \circ c$ *für alle* $a, b, c \in G$,

ii) *es gibt ein* **neutrales Element** e, *so dass* $a \circ e = a$ *für alle* $a \in G$,

iii) *für alle* $a \in G$ *gibt es ein* **inverses Element** a^{-1}, *so dass* $a \circ a^{-1} = e$.

Eine Gruppe $(G, \circ)$ heisst **kommutativ**, *falls zusätzlich gilt, dass*

iv) $a \circ b = b \circ a$ *für alle* $a, b \in G$.

Einfache Beispiele für kommutative Gruppen sind: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mit der Verknüpfung $+$, oder $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ mit der Verknüpfung $\cdot$. Ist A eine Menge, so bilden die bijektiven Abbildungen $A \to A$ ein Gruppe. Hat A drei oder mehr Elemente, so ist die Gruppe nicht kommutativ. Zum Beispiel, betrachten wir $A = [0, \infty[$. Dann sind die Abbildungen $f(x) = \mathrm{e}^x - 1$ und $g(x) = x^2$ bijektiv. Wir haben dann $f \circ g(x) = f(g(x)) = \mathrm{e}^{x^2} - 1$ und $g \circ f(x) = g(f(x)) = (\mathrm{e}^x - 1)^2$, was nicht dasselbe ist.

Wir schreiben für eine Gruppe G nun ab statt $a \circ b$. Es gilt folgendes:

$$a^{-1}a = a^{-1}a(a^{-1}(a^{-1})^{-1}) = a^{-1}e(a^{-1})^{-1} = a^{-1}(a^{-1})^{-1} = e \; .$$

Weiter erhalten wir

$$ea = (aa^{-1})a = a(a^{-1}a) = ae = a \; .$$

Wir zeigen nun: Zu jedem $a, b \in G$ gibt es ein eindeutiges x, so dass $ax = b$. Sei x eine Lösung. Dann haben wir

$$x = ex = a^{-1}ax = a^{-1}b \; .$$

Somit muss eine Lösung eindeutig sein. Da $a(a^{-1}b) = eb = b$, ist $x = a^{-1}b$ eine Lösung. Analog ist $y = ba^{-1}$ die eindeutige Lösung von $ya = b$. Insbesondere ist das neutrale und das inverse Element eindeutig. Wir schliessen insbesondere aus $a^{-1}a = e$ und der Eindeutigkeit, dass $(a^{-1})^{-1} = a$.

Definition 1.2. *Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $\emptyset \neq U \subset G$ heisst* **Untergruppe**, *wenn U versehen mit der Verknüpfung $\circ$ auch eine Gruppe ist.*

Hilfssatz 1.3. *Sei G eine Gruppe und $\emptyset \neq U \subset G$. U ist genau dann eine Untergruppe ist, falls für alle $a, b \in U$ auch $ab^{-1} \in U$.*

Beweis. Ist U eine Untergruppe, so gibt es ein neutrales Element $f \in U$. Dann ist $ff = f$. Da in G die Lösung der Gleichung $fx = f$ die eindeutige Lösung $x = e$ hat, muss $f = e$ sein. Also ist $e \in U$. Weiter gibt es für $a \in U$ ein $b \in U$, so dass $ab = e$. Daher muss $b = a^{-1}$ sein. Also haben wir $a^{-1} \in U$. Wir erhalten somit, dass $ab^{-1} \in U$ für alle $a, b \in U$.

Sei nun $ab^{-1} \in U$ für alle $a, b \in U$. Ist $a \in U$, so ist $e = aa^{-1} \in U$ und $a^{-1} = ea^{-1} \in U$. Somit erhalten wir für $a, b \in U$, dass $ab = a(b^{-1})^{-1} \in U$. Also führt die Verknüpfung nicht aus U. Da die erste Eigenschaft trivialerweise erfüllt ist, ist U eine Untergruppe. □

Sei G eine Gruppe und $U \subset G$ eine Untergruppe. Für $a, b \in G$, so setzt man

$$aU := \{ax : x \in U\}\,, \qquad Ua := \{xa : x \in U\}\,, \qquad aUb = \{axb : x \in U\}\,.$$

aU heisst **Linksnebenklasse**, Ua heisst **Rechtsnebenklasse**.

Wir betrachten nun Linksnebenklassen. Sei $u \in U$ und $b \in aU$. Dann gibt es $x \in U$, so dass $b = ax$. Da $b = (au)(u^{-1}x)$, ist $b \in (au)U$. Sei $c \in (au)U$, so gibt es ein $y \in U$, so dass $c = (au)y = a(uy)$. Somit ist $c \in aU$. Also haben wir $aU = (au)U$.

Sei nun $a, b \in G$, so dass $a^{-1}b \in U$. Dann ist $aU = a(a^{-1}b)U = bU$. Sei $aU = bU$. Da $e \in U$ und $b = be \in bU$, ist $b \in aU$. Also gibt es $c \in U$, so dass $ac = b$. Damit ist $a^{-1}b = c \in U$. Wir haben also gezeigt, dass $aU = bU$ genau dann gilt, wenn $a^{-1}b \in U$.

Betrachten wir aU und bU. Sei $c \in aU \cap bU$, so ist $c = ax = by$ für ein $x, y \in U$. Also ist $a^{-1}b = xy^{-1} \in U$. Also sind entweder die Klassen gleich oder disjunkt.

Wir betrachten im weiteren nun endliche Gruppen. Hat eine Gruppe G nur endlich viele Elemente, so bezeichnet $\operatorname{ord} G$ (**Ordnung** von G) die Anzahl der Elemente. Ist $U \subset G$ eine Untergruppe, so nennt man die Anzahl der Linksnebenklassen als den **Index** von U in G, und wird mit $[G : U]$ bezeichnet.

Hilfssatz 1.4. *Sei G eine Gruppe und $U \subset G$ eine Untergruppe. Dann gilt* $\operatorname{ord} G = [G : U] \cdot \operatorname{ord} U$.

Beweis. Sei $a \in G$ und $f : U \to aU$, $x \mapsto ax$. Nach der Definition ist die Abbildung surjektiv. Sei $f(x) = f(y)$. Dann ist $ax = ay$, und wegen der Eindeutigkeit der Lösung der Gleichung, ist $x = y$. Also ist f bijektiv, und aU besitzt $\operatorname{ord} U$ Elemente. Zwei verschiedene Nebenklassen sind disjunkt. Da $e \in U$, ist $a \in aU$. Also ist jedes Element in genau einer Nebenklasse. Daraus folgt die Behauptung. □

Für $a \in G$ bezeichnet man mit $\langle a \rangle = \{a^n : n \in \mathbb{N}\}$ die von a erzeugte Untergruppe. In der Tat ist $\langle a \rangle$ eine Untergruppe. Wir können $a \neq e$ annehmen. Da G $\operatorname{ord} G$ Elemente hat, existiert

$$m = \inf\{n \in \mathbb{N} : \exists k \in \mathbb{N} \ , \ k < n \ , \ a^n = a^k\} \ .$$

Sei $k < m$ mit $a^k = a^m$. Dann ist $a^{m-1} = a^{-1}a^m = a^{-1}a^k = a^{k-1}$. Somit muss $k = 1$ gelten, und $a^{m-1} = e$. Für $n \in \mathbb{N}$ mit $n < m - 1$, ist $a^n a^{m-n-1} = a^{m-1} = e$. Also haben wir für $k, n < m - 1$, $a^n(a^k)^{-1} = a^n a^{m-k-1} = a^{m+n-k-1} \in \langle a \rangle$. Damit ist $\langle a \rangle$ eine Untergruppe.

Wir schreiben dann $\operatorname{ord} a = \operatorname{ord}\langle a \rangle$. Es folgt, dass $\operatorname{ord} a$ ein Teiler von $\operatorname{ord} G$ ist. Eine Gruppe heisst **zyklisch**, wenn es ein $a \in G$ gibt, so dass $G = \langle a \rangle$. Insbesondere ist jede Gruppe von Primzahlordnung zyklisch. In der Tat ist für $a \neq e$ $\operatorname{ord} a \geq 2$. Da $\operatorname{ord} a$ ein Teiler von $\operatorname{ord} G$ ist, muss $\operatorname{ord} a = \operatorname{ord} G$ gelten.

1.3. Teilen mit Rest und Multiplikationsgruppen

Sei $m \in \mathbb{N}$ eine Zahl mit $m \geq 2$. Zu jeder Zahl $n \in \mathbb{N}$ gibt es genau ein Paar $k, r \in \mathbb{N}$, so dass $n = km + r$ mit $0 \leq r < m$. Wir sagen $n = r \pmod m$. Mit den Zahlen $0, 1, \ldots, m - 1$ können wir auch rechnen. Wir zeigen zuerst, dass es nicht davon abhängt, ob wir vor der Rechnung r bestimmen oder erst nachher.

Beginnen wir mit der Addition. Sei $n_1 = k_1 m + r_1$ und $n_2 = k_2 m + r_2$. Dann haben wir

$$n_1 + n_2 = (k_1 m + r_1) + (k_2 m + r_2) = (k_1 + k_2)m + (r_1 + r_2) \ .$$

Somit ist $n_1 + n_2 = r_1 + r_2 \pmod m$. Bei der Multipikation ergibt sich

$$n_1 n_2 = (k_1 m + r_1)(k_2 m + r_2) = [(k_1 m + r_1)k_2 + k_1 r_2] + r_1 r_2 \ .$$

Somit ist $n_1 n_2 = r_1 r_2 \pmod m$.

Proposition 1.5. *$G = \{0, 1, \ldots, m - 1\}$ ist modulo m eine kommutative Gruppe bezüglich der Addition.*

Beweis. Für natürliche Zahlen gilt $n_1 + (n_2 + n_3) = (n_1 + n_2) + n_3$. Da es keine Rolle spielt, ob wir vorher oder nachher den Rest bestimmen, muss diese Eigenschaft auch für die Addition modulo m gelten. Analog folgt auch, dass $r_1 + r_2 = r_2 + r_1$.

Da $r + 0 = r$, gibt es ein neutrales Element.

Wir haben $0 + 0 = 0$, also ist 0 das inverse Element von 0. Sei $1 \leq r \leq m - 1$. Dann ist $1 \leq m - r \leq m - 1$, und $r + (m - r) = m = 0 \pmod m$. Somit ist $m - r$ das inverse Element von r. □

Untersuchen wir die Multiplikation, so ist die Sache komplizierter. Wie für die Addition folgt $r_1(r_2r_3) = (r_1r_2)r_3 \pmod m$ und $r_1r_2 = r_2r_1 \pmod m$. Aus $r_11 = r_1$ folgt, dass 1 das neutrale Element ist. Allgemein haben wir Probleme mit der 0. Da die Gleichung $0x = r$ nur eine Lösung haben kann, wenn $r = 0$, und in diesem Fall jedes x die Gleichung erfüllt, kann 0 nie ein Element einer multiplikativen Gruppe sein. Wir müssen also $\{1, 2, \ldots, m-1\}$ betrachten.

Beispiel 1.6. Nehmen wir $m = 12$. Dann gilt zum Beispiel $4 \cdot 3 = 12 = 0 \pmod{12}$. Somit führt die Multiplikation aus der Menge $\{1, 2, \ldots, 11\}$. Betrachten wir nun aber $\{1, 2, 4, 5, 7, 8, 10, 11\}$, so ist ab nie durch 3 und damit nie durch 12 teilbar. Insbesondere führt die Multiplikation nie aus dieser Menge. Aber, $a2 \pmod{12}$ ist immer gerade. Somit kann a keine inverses Element enthalten. Entfernen wir auch noch die geraden Zahlen, erhalten wir $\{1, 5, 7, 11\}$. Da ab ungerade sein muss, führt die Multiplikation nicht aus der Menge. Die inversen Elemente finden wir durch probieren, und es stellt sich heraus, dass $aa = a \pmod{12}$. Somit ist $\{1, 5, 7, 11\}$ eine Gruppe bezüglich der Multiplikation modulo 12. ■

Allgemein hat m eine Primfaktorzerlegung. Ist p ein Primfaktor von m, so ist für jede Zahl a, die durch p teilbar ist, $ab = km + r$ mit $0 \leq r \leq m-1$. Da a und km durch p teilbar sind, muss auch r durch p teilbar sein. Da 1 nicht durch p teilbar ist, kann a kein inverses Element besitzen.

Haben zwei Zahlen a und b keinen gemeinsamen Primfaktor, so sagen wir, a und b sind relativ prim. Betrachten wir nur die Zahlen in $1, 2, \ldots, m-1$, die relativ prim zu m sind, so kann man zeigen, dass diese mit der Multiplikation modulo m eine Gruppe bilden. Wir wollen hier nur zwei Spezialfälle betrachten.

Proposition 1.7. *Ist p eine Primzahl, so ist $G = \{1, 2, \ldots, p-1\}$ eine Gruppe bezüglich der Multiplikation modulo p. Weiter gilt für $a \in G$, dass $a^{p-1} = 1 \pmod p$.*

Beweis. Nehmen wir $ab = 0 \pmod p$ an. Dann gilt $ab = kp$ für ein k, und p müsste a oder b teilen. Da $a, b < p$ ist dies nicht möglich. Somit ist $ab \in G \pmod p$. Da a^n $(n \geq 0)$ modulo p nur $p-1$ Werte annehmen kann, gibt es ein $0 \leq \ell < k$, so dass $a^\ell = a^k$. Nehmen wir an, wir hätten das minimale k gewählt. Es gilt dann, $a^k - a^\ell = qp$ für ein q. Dann ist $a^\ell(a^{k-\ell} - 1) = pq$. Da a^ℓ nicht durch p teilbar ist, muss $a^{k-\ell} - 1$ durch p teilbar sein, also $a^{k-\ell} = 1 \pmod p$. Da wir k minimal gewählt haben, ist $\ell = 1$. Somit hat a das inverse Element a^k. Insbesondere ist

G eine Gruppe. $U = \{1, a, a^2, \ldots, a^{k-1}\}$ ist dann eine Untergruppe. In der Tat ist $a^\ell a^{k-\ell} = a^k = 1 \pmod p$ für $1 \leq \ell < k$. Für $1 \leq \ell_2 \leq \ell_1 < k$ ist

$$a^{\ell_1}(a^{\ell_2})^{-1} = a^{\ell_1}a^{k-\ell_2} = a^k a^{\ell_1-\ell_2} = a^{\ell_1-\ell_2} \pmod p \in U$$

und für $0 \leq \ell_1 < \ell_2 < k$ ist

$$a^{\ell_1}(a^{\ell_2})^{-1} = a^{\ell_1}a^{k-\ell_2} = a^{k-(\ell_2-\ell_1)} \in U\ .$$

Für $\ell_2 = 0$ ist die Aussage trivial. Da $k = \operatorname{ord} U$ ein Teiler von $\operatorname{ord} G = p - 1$ ist, gibt es ein s, so dass $ks = p - 1$. Also haben wir $a^{p-1} = a^{ks} = (a^k)^s = 1^s = 1$. □

1.4. Zwei Primfaktoren

Betrachten wir nun den Fall $m = pq$, wobei $p \neq q$ Primzahlen sind. Betrachten wir nun die Menge G der Zahlen, die nicht durch p oder q teilbar sind.

Proposition 1.8. *G ist bezüglich der Multiplikation modulo m eine Gruppe. Weiter gilt, dass $a^{(p-1)(q-1)} = 1$ (mod m) für alle $a \in G$.*

Beweis. Nehmen wir an, dass $ab \pmod m$ durch p teilbar ist. Dann ist ab durch p teilbar, was aber nicht möglich ist, da a und b nicht durch p teilbar sind. Analog folgt, dass $ab \pmod m$ nicht durch q teilbar ist. Also ist $ab \pmod m$ in G. Sei $a \in G$. Da G endlich ist, gibt es $0 \leq \ell < k$, so dass $a^\ell = a^k \pmod m$. Nehmen wir an, dass wir das minimale k gewählt haben. Dann ist $a^\ell(a^{k-\ell} - 1) = 0 \pmod m$. Da a^ℓ nicht durch p oder q teilbar ist, muss $a^{k-l} = 1 \pmod m$ gelten. Wir schliessen, dass $\ell = 0$. Also ist $a^k = 1 \pmod m$. Insbesondere ist a^{k-1} das inverse Element von a. Analog zum Primzahlfall folgt, dass $U = \{1, a, a^2, \ldots, a^{k-1}\}$ eine Untergruppe mit k Elementen ist. Wir müssen nun dir Ordnung von G bestimmen. Die Menge $\{1, 2, \ldots, m-1\}$ hat $m-1$ Elemente. Davon sind $p, 2p, \ldots, (q-1)p\}$ durch p teilbar, und $\{q, 2q, \ldots, (p-1)q\}$ durch q teilbar. Ist b sowohl durch p als auch durch q teilbar, so muss b mindestens $pq = m$ sein. Somit hat G $(pq-1)-(q-1)-(p-1) = (p-1)(q-1)$ Elemente. Also muss k ein Teiler von $p - q$ sein. Da $a^k = 1 \pmod m$, folgt $a^{(p-1)(q-1)} = 1$. □

Beispiel 1.9. Nehmen wir $p = 3$ und $q = 5$. Dann ist $m = 15$. Wir haben dann $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Weiter ist $(p-1)(q-1) = 8$. In der Tat haben wir

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^8	1	1	6	1	10	6	1	1	6	10	1	6	1	1

■

1.5. Das RSA-Verfahren

Wir zeigen zuerst, dass es unendlich viele Primzahlen gibt. Daraus folgt, dass man beliebig grosse Primzahlen finden kann.

Hilfssatz 1.10. *Jede natürliche Zahl $a \in \mathbb{N} \setminus \{0,1\}$ hat eine Primfaktorzerlegung. Das heisst, es gibt Primzahlen $p_1, p_2, \ldots, p_n$, die nicht notwendigerweise verschieden sind, so dass $a = p_1 p_2 \cdots p_n$.*

Bemerkung. Es gilt sogar, dass die Primfaktorzerlegung eindeutig ist. ■

Beweis. Nehmen wir an, dass die Aussage nicht gilt. Dann gibt es eine kleinste Zahl a, die nicht in Primfaktoren zerlegbar ist. Wäre a prim, so hätte a eine Primfaktorzerlegung. Also gibt es Zahlen $b, c \in \mathbb{N} \setminus \{0,1\}$, so dass $a = bc$. Da $b, c < a$ haben b und c eine Primfaktorzerlegung $b = p_1 p_2 \cdots p_m$ und $c = q_1 q_2 \cdots q_k$. Dann ist aber $a = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_k$, und a hat eine Primfaktorzerlegung. Dies ist ein Widerspruch, und die Aussage ist bewiesen. □

Hilfssatz 1.11. (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis. Nehmen wir an, die Aussage sei falsch. Gibt es genau n Primzahlen, so können wir diese $p_1, p_2, \ldots, p_n$ nennen. Nun bilden wir die Zahl $a = p_1 p_2 \ldots p_n + 1$. Es folgt, dass a geteilt durch p_k den Rest 1 hat. Somit ist a durch keine der Primzahlen teilbar. Da aber a in Primfaktoren zerlegbar ist, muss es mindestend eine weiter Primzahl geben. Dies widerspricht aber unserer Annahmen, dass es genau n Primzahlen gibt. Somit muss es unendlich viele Primzahlen geben. □

Die folgende Methode der Verschlüsselung heisst RSA-Verschlüsselung, und geht zurück auf Rivest, Shamir und Adleman (1977). Der Empfänger wählt zwei sehr grosse Primzahlen p und q. Gross heisst hier oft $p, q > 10^{100}$. Nun setzt man $m = pq$. Man wählt eine Zahl $c < (p-1)(q-1)$, so dass c und $(p-1)(q-1)$ keine gemeinsamen Primfaktoren besitzen. Dann kann man ein d berechnen, so dass $cd = 1 \pmod{(p-1)(q-1)}$. Dass dies möglich ist, sieht man wie im vorhergehenden Abschnitt, wenn man aus $1, 2, \ldots, pq - p - q$ alle Zahlen enfernt, die einen gemeinsamen Primfaktor mit $(p-1)(q-1)$ haben. Der Empfänger gibt die Zahlen m und c öffentlich bekannt. Will jemand eine Mitteilung $1 \leq t < m$ an den Empfänger schicken, so sendet der

Sender die Nachricht $K = t^c \pmod m$ an den Empfänger. Es gibt eine Zahl s, so dass $cd = s(p-1)(q-1)+1$. Der Empfänger berechnet nun

$$K^d = t^{cd} = t^{s(p-1)(q-1)+1} = (t^{(p-1)(q-1)})^s t = 1^s t = t \ ,$$

und erhält somit die zu sendende Mitteilung.

Um grosse Primzahlen zu finden, macht man sich zunutze, dass in den ersten N Zahlen sich ungefähr $N/\ln N$ Primzahlen befinden (Primzahlentheorem). Das bedeutet, dass in der Nähe von N etwa jede $\ln N$-te Zahl prim ist. Für hundetstellige Zahlen ist also etwa jede 230. Zahl eine Primzahl. Da eine Primzahl ungerade ist, ist somit etwa jede 115. ungerade Zahl Prim. Erzeugt man Zufallszahlen, muss man also nicht besonders lange suchen, bis man auf eine Primzahl trifft. Da es natürlich zu lange dauert, um festzustellen, ob eine Zahl wirklich prim ist, verwendet man Pseudo-Primzahlentests, die einem mit hoher Wahrscheinlichkeit sagen können, ob eine Zahl prim ist (z.B. ist für eine Primzahl p, $b^{p-1} = 1 \bmod p$ für alle $1 \le b \le p-1$).

Das Verfahren funktioniert nur für Mitteilungen t, die keine Vielfachen von p und q sind. Es gibt $p+q-2$ verbotene Mitteilungen unter den $m-1$ möglichen Mitteilungen. Nehmen wir an, dass alle Mitteilungen gleich wahrscheinlich sind, so ist die Wahrscheinlichkeit, eine nicht dekryptierbare Mitteilung zu senden $\frac{p+q-2}{pq-1}$. Leiten wir den Ausdruck nach p ab, erhalten wir

$$\Big(\frac{p+q-2}{pq-1}\Big)' = \frac{(pq-1)-(p+q-2)q}{(pq-1)^2} = -\frac{q^2-2q+1}{(pq-1)^2} = -\Big(\frac{q-1}{pq-1}\Big)^2 < 0 \ .$$

Somit ist der Ausdruck fallend in p und auch fallend in q. Nehmen wir $p < q$ an. Dann ist

$$\frac{p+q-2}{pq-1} < \frac{2p-2}{p^2-1} = \frac{2}{p+1} \ .$$

Ist also $p > 10^{100}$, so ist $\frac{p+q-2}{pq-1} < 2 \cdot 10^{-100}$. Es ist also sehr unwahrscheinlich, dass eine nicht dekryptierbare Mitteilung auftritt.

Eine Nachricht ist ohne Kontrollbits ungefähr $10^{200} \approx 2^{665}$. Ein sehr gutes Glasfaserkabel kann pro Sekunde etwa $10^{16}/665 = 1.5 \cdot 10^{13}$ Nachrichten übermitteln. Somit muss man im Schnitt

$$\frac{1}{2 \cdot 10^{-100}} \cdot \frac{1.5 \cdot 10^{13}}{\mathrm{s}} \approx 3 \cdot 10^{86}\mathrm{s} \approx 9.5 \cdot 10^{78} Jahre \ .$$

Zum Vergleich, der Urknall ereignete sich vor etwa $1.37 \cdot 10^{10}$ Jahren.

Beispiel 1.12. Sei $p = 5$ und $q = 11$, also $m = 55$. Wir haben $(p-1)(q-1) = 40$. Somit darf der Schlüssel c nicht durch 2 oder 5 teilbar sein. Wählen wir $c = 7$. Der Wert d ist durch die Gleichung $cd = 1 \mod 40$ bestimmt. Wir suchen den Wert $40s + 1$, der durch 7 teilbar ist. Dies ist 161, also $d = 23$. Um eine Nachricht, sagen wir 32 zu übermitteln, berechnen wir

$$32^7 = 34\,359\,738\,368 = 43 \mod 55.$$

Es wird der Code 43 übermittelt. Um zu dechiffrieren, berechnet man

$$43^{23} = 37\,134\,234\,731\,477\,575\,983\,465\,092\,780\,473\,537\,507 = 32 \mod 55.$$

Somit wurde die ursprüngliche Nachricht wieder ermittelt. ■

Bei diesem Verfahren mit öffentlichem Schlüssel kennt jeder den Schlüssel. Wieso aber funktioniert das Verfahren? Man kennt also m, c und die übermittelte Nachricht K. Wenn p und q sehr gross sind, so kann man nicht alle $m-1$ möglichen Nachrichten durchprobieren, um die Zahl zu finden, für die $t^c = K \pmod m$ gilt. Man braucht daher d, um $K^d = t$ zu finden. Alle bisherigen Versuche, den Code zu knacken, basieren darauf, m zu faktorisieren, also p und q zu finden. Für p, q gross, gibt es bisher keine numerische Methode, die dies in nützlicher Zeit schafft.

Der Vorteil der öffentlichen Schlüssel ist ferner, dass der Schlüssel nur im Besitz des Ausstellers ist. Zum Beispiel auf dem Internet muss man ja den Schlüssel den andern Teilnehmern der Kommunikation übermitteln. Will man dies übers Internet machen, ist der Schlüsselaustausch nicht sicher. Kann man aber eine Nachricht nur ver- aber nicht entschlüsseln, so ist es nutzlos für emandem, der die Verbindung abhört.

Man kann den Schlüssel auch verwenden, um sich selber zu identifizieren. Nehmen wir an, ein Sender mit Schlüssel m_1, c_1 will eine Nachricht an einen Empfänger mit Schlüssel m_2, c_2 senden. Der Sender kennt die Zahl d_1, der Empfänger die Zahl d_2. Der Sender erstellt zuerst die Nachricht $K_1 = t^{d_1} \pmod{m_1}$. Diese Nachricht verschlüsselt er mit dem Schlüssel des zweiten Teilnehmers, $K_2 = K_1^{c_2} \pmod{m_2}$, und übermittelt K_2. Der Empfänger erstellt die erste Nachricht $K_1 = K_2^{d_2} \pmod{m_2}$. Danach verschlüsselt er die Nachricht mit dem Schlüssel des Senders, $K_1^{c_1} \pmod{m_1}$. Der Empfänger ist der einzige, der K_1 aus K_2 erhalten kann. Der Sender ist der einzige, der die Nachricht K_1 erstellen kann. Somit kann der Empfänger sicher sein, dass die Nachricht vom Sender stammt.