CODES, COMPUTER, PRIMZAHLEN

WINFRIED BRUNS

Unter einem Code versteht man gewöhnlich ein Verfahren zur Verschlüsselung von Information. Eine Verschlüsselung kann verschiedenen Aufgaben dienen, zum Beispiel der Absicherung der Information gegen Übertragungsfehler auf störanfälligen Kanälen. Zumindest in der Umgangssprache meint man aber mit dem Begriff Code ein *Kryptosystem*, eine Verschlüsselung zum Zwecke der Geheimhaltung. Ein Kryptosystem wird immer dann benötigt, wenn Nachrichten auf *unsicheren* Kanälen übermittelt werden. Ein unsicherer Kanal ermöglicht es unbefugten Dritten, die übermittelten Nachrichten ebenfalls zu empfangen, vielleicht sogar abzufangen und verfälscht weiterzuleiten. Ein Kanal ist zum Beispiel auch dann unsicher, wenn er es dem Absender gestattet, dem Empfänger eine falsche Identität vorzuspiegeln.
Mathematiker haben seit etwa zwanzig Jahren revolutionär neue Kryptosysteme entwickelt. Eines dieses Verfahren beruht auf der Kenntnis von Primzahlen und ihren Eigenschaften und allen diesen Verfahren ist gemeinsam, daß sie nur mit Hilfe von Computern konstruiert und dann verwendet werden können.
Die klassischen Anwendungsbereiche von Kryptosystemen sind Militär, Diplomatie und – nicht weit davon entfernt – die Geheimdienste. Die neuen Verschlüsselungsverfahren werden natürlich auch von diesen Institutionen mit Freuden eingesetzt, entwickelt worden sind sie aber für eine andere Aufgabe: die Geheimhaltung von Daten in öffentlich zugänglichen Datenbanken und bei der Übertragung von Nachrichten in den riesigen elektronischen Kommunikationsnetzen, die, wenn sie nicht schon heute existieren, in naher Zukunft uns alle einbeziehen werden. Solche Datenbanken und Kommunikationsnetze sind höchst unsicher: Unbefugte können leicht "mithören" oder sich unter dem Deckmantel einer falschen Identität in fremde Datenbestände einschleichen. Daher ist die Verwendung von Kryptosystemen zu ihrem Schutz unentbehrlich.

1. Kryptosysteme und Falltürfunktionen

Wir wollen die Ausgangssituation bei der Verwendung eines Kryptosystems in der Sprache der Mathematik beschreiben. Der Absender B möchte eine Nachricht N, genannt *Klartext* an den Empfänger A senden; um sie schützen, verschlüsselt er sie und sendet das so erhaltene *Chiffrat* C an A. Der Empfänger A entschlüsselt C, um den Klartext N zurückzugewinnen. Das verwendete Kryptosystem besteht also im wesentlichen aus zwei Funktionen, der Verschlüsselung f, $f(N) = C$, und der Entschlüsselung f^{-1}, $f^{-1}(C) = N$. Wenn wir die Menge der Klartexte mit $\mathcal{N}$ bezeichnen,

$$\mathcal{N} = \{\ N\ N \text{ Klartext } \},$$

und diejenige der Chiffrate mit $\mathcal{C}$,

$$\mathcal{C} = \big\{\, C \; C \text{ Chiffrat} \,\big\},$$

können wir dies auch so angeben:

$$f\ \mathcal{N} \to \mathcal{C}, \qquad f^{-1}\ \mathcal{C} \to \mathcal{N}, \qquad f^{-1}(f(N)) = N \quad \text{für alle } N \in \mathcal{N}\,.$$

Natürlich spielen auch die "Alphabete", in denen Klartexte und ihre Chiffrate notiert werden, und die technische Realisation der Übermittlung eine wichtige Rolle. In unserer Diskussion können wir sie aber vernachlässigen.

Bevor ein Kryptosystem benutzt werden kann, muß der Empfänger A dem Absender B den Schlüssel f, mit dem B Nachrichten an A verschlüsseln soll, mitteilen. Alle klassischen Kryptosysteme, die wir aus Zeitgründen leider nicht diskutieren können, haben die Eigenschaft, daß mit der Verschlüsselung f auch die Entschlüsselung f^{-1} bekannt ist oder zumindest sehr schnell ermittelt werden kann. Daher muß A den Schlüssel f auf einem sicheren Kanal mitteilen, und f muß gegenüber Dritten geheimgehalten werden. Der Zwang zur Geheimhaltung von f ist nur deshalb gegeben, weil, wie schon gesagt, die zum unbefugten Mithören notwendige Entschlüsselung f^{-1} sofort aus f gewonnen werden kann.

Die Notwendigkeit eines zweiten, sicheren Kanals zum Austausch der Schlüssel macht die Verwendung eines klassischen Kryptosystems in Kommunikationsnetzen mit mehreren hundert oder gar zehntausend Teilnehmern unmöglich. Den Ausweg bieten die vor cażwanzig Jahren erfundenen

Kryptosysteme mit öffentlichem Schlüssel,

in der englischsprachigen Literatur *public key cryptosystems* genannt. Sie beruhen auf der Verwendung von *Falltürfunktionen* für die Verschlüsselung. Falltüren zeichnen sich ja dadurch aus, daß man sie in einer Richtung sehr leicht, in der Gegenrichtung aber nur sehr schwer durchschreiten kann. Wir wollen also eine Funktion

$$f\ \mathcal{N} \to \mathcal{C}$$

eine Falltürfunktion nennen, wenn sich für jedes $N \in \mathcal{N}$ das Chiffrat $f(N)$ und für jedes $C \in \mathcal{C}$ der Klartext $f^{-1}(\mathcal{C})$ sehr leicht berechnen lassen, es hingegen praktisch nicht möglich ist, trotz der Kenntnis von f die Entschlüsselung f^{-1} zu bestimmen. Wir können hier die vagen Begriffe "leicht" und "praktisch nicht möglich" nicht präzisieren. (Das dafür zuständige mathematische Gebiet ist die *Komplexitätstheorie*.)

Ein Kryptosystem mit öffentlichem Schlüssel funktioniert nun so:

(1) Jeder Teilnehmer A konstruiert eine Falltürfunktion f_A; die in die Konstruktion einfließende, nur ihm bekannte Zusatzinformation liefert gleichzeitig f_A^{-1}.

(2) Er gibt f_A bekannt, hält aber die Entschlüsselung f_A^{-1} natürlich geheim.

(3) Will nun ein anderer Teilnehmer B eine Nachricht N an A senden, so verschlüsselt er sie mittels f_A und sendet das Chiffrat $C = f_A(N)$ an A.

(4) Wenn A das Chiffrat C empfängt, wendet er die nur ihm bekannte Entschlüsselung f_A^{-1} an und erhält $N = f_A^{-1}(f_A(N))$ zurück.

Da es nicht möglich ist, f_A^{-1} aus f_A zu bestimmen, kann f_A öffentlich bekannt sein und die Notwendigkeit eines sicheren Kanals zum Austausch der Schlüssel entfällt. Man kann natürlich einwenden, daß es prinzipiell immer möglich ist, zu einer bekannten Funktion die Umkehrfunktion zu bestimmen. Wenn wir auch nicht mathematisch präzisiert haben, was "praktisch nicht möglich" heißt: Die Ermittlung von f_A^{-1} muß einen Aufwand erfordern, der den durch das Brechen des Kryptosystems zu erzielenden Gewinn bei weitem überwiegt, oder eine so lange Zeit benötigen, daß nach ihrem Ablauf jegliches Interesse an der zu erlangenden Information erloschen ist.
Bei der Verwendung von Kryptosystemen mit öffentlichem Schlüssel muß indes einer Gefahr vorgebeugt werden: der Vorspiegelung einer falschen Identität. Niemand hindert ja einen dritten Teilnehmer C daran, sich für B auszugeben und unter Verwendung von f_A verschlüsselte Nachrichten an A zu senden, die A nicht von Mitteilungen unterscheiden kann, die wirklich von B stammen. Jedes Chiffrat muß also mit einer "Unterschrift" versehen sein, die den Absender eindeutig identifiziert. Glücklicherweise lassen sich solche Unterschriften gerade in diesen Systemen exzellent realisieren; wir kommen darauf später zurück.

2. Das Rechnen mit Restklassen

Im folgenden verstehen wir unter einer *Zahl* stets eine ganze Zahl beliebigen Vorzeichens. Jede Zahl $n > 1$ läßt sich im wesentlichen eindeutig als Produkt von Primzahlen schreiben:

$$n = p_1 \dots p_r, \qquad p_i \text{ Primzahl.}$$

Diese Aussage ist der *Hauptsatz der elementaren Zahlentheorie. Im wesentlichen eindeutig* heißt: die Primfaktoren $p_1 \dots p_r$ sind bis auf ihre Reihenfolge eindeutig bestimmt. Zur Erinnerung: Eine positive Zahl p heißt Primzahl, wenn $p > 1$ ist und sich nur durch 1 und p teilen läßt. Daß jede Zahl $n > 1$ eine Darstellung als Produkt von Primzahlen besitzt, ist leicht zu sehen; daß diese im wesentlichen eindeutig ist, ist schon schwieriger zu beweisen. Die Zerlegung in Primfaktoren für sehr große Zahlen zu finden, ist aber (bisher) praktisch unmöglich, und darauf beruht das RSA-*Kryptosystem*, das von Rivest, Shamir und Adleman vor etwa 1978 vorgeschlagen wurde.
Um es zu verstehen, müssen wir mit Restklassen rechnen können. Sei m eine *positive* Zahl. Wir sagen, a sei *kongruent zu b modulo m*, wenn a und b bei Division durch m den gleichen Rest lassen:

$$a \equiv b \ (m) \iff \begin{cases} a = q_1 m + r, \\ b = q_2 m + r, \end{cases} \qquad 0 \le r \le m-1.$$

Wählen wir etwa $m = 15$:

$$\begin{aligned} 36 &\equiv 6 (15), & 22 &\equiv 7 \ (15), & 105 &\equiv 0 \ (15), \\ -7 &\equiv 8 \ (15), & -1 &\equiv 14 \ (15), & -23 &\equiv 7 \ (15). \end{aligned}$$

Man sieht leicht:

$$a \equiv b \ (m) \qquad \iff \qquad a - b \text{ wird von } m \text{ geteilt.}$$

Alle Zahlen, die zu einer gegebenen Zahl a kongruent sind, faßt man zur Restklasse $\overline{a}$ zusammen:

$$\overline{a} = \{b \, b \equiv a \ (m)\},$$

etwa modulo 15:

$$\overline{3} = \{\dots, -27, -12, 3, 18, 33, 48, \dots\},$$
$$\overline{-5} = \{\dots, -35, -20, -5, 10, 25, 40, \dots\}.$$

Jede Restklasse enthält natürlich genau eine Zahl a zwischen 0 und $m-1$, und man verwendet üblicherweise diese, um die Restklasse zu bezeichnen. Diese Bemerkung ist besonders wichtig für das Rechnen mit Restklassen auf dem Computer: Wenn man die Zahl m darstellen kann, so kann man *alle* Restklassen modulo m darstellen – im Gegensatz zu *allen* Zahlen!
Restklassen (modulo derselben Zahl!) lassen sich addieren und multiplizieren: Wir setzen "einfach"

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Hierbei muß man sich folgendes klarmachen: Diese Definition von Addition und Multiplikation von Restklassen ist nur dann gerechtfertigt, wenn $\overline{a+b}$ und $\overline{ab}$ schon vollständig durch $\overline{a}$ und $\overline{b}$ bestimmt sind, *nicht* aber von den zur Darstellung dieser Restklassen gewählten Zahlen a und b abhängen.
Beispiel: $m = 15$,

$$\overline{2} + \overline{4} = \overline{6}, \quad \overline{3} + \overline{14} = \overline{17} = \overline{2}, \quad \overline{6} + \overline{9} = \overline{15} = \overline{0},$$
$$\overline{2} \cdot \overline{3} = \overline{6}, \quad \overline{7} \cdot \overline{13} = \overline{91} = \overline{1}, \quad \overline{6} \cdot \overline{10} = \overline{60} = \overline{0}.$$

Addition und Multiplikation erfüllen die uns geläufigen Kommutativ-, Assoziativ- und Distributivgesetze. Ferner ist

$$\overline{a} + \overline{0} = \overline{a}, \quad \overline{0} \ \overline{a} = \overline{0}, \quad \overline{1} \ \overline{a} = \overline{a}$$

für alle Restklassen $\overline{a}$ modulo m. Wie wir an den Beispielen gerade gesehen haben, treten aber zwei Eigenschaften auf, die uns beim Rechnen mit ganzen Zahlen nicht begegnen:

(i) Die Multiplikation ist im allgemeinen *nicht nullteilerfrei*, etwa $\overline{6} \cdot \overline{10} = \overline{0}$ modulo 15.
(ii) Es gibt im allgemeinen Restklassen $\overline{a} \neq \pm\overline{1}$, $\overline{b} \neq \pm\overline{1}$ mit $\overline{a} \ \overline{b} = \overline{1}$, etwa $\overline{7} \cdot \overline{13} = \overline{1}$ modulo 15.

Über das Phänomen (ii) gibt uns der folgende Satz genau Auskunft:

Satz 1. *Genau dann gibt es modulo m zu $\overline{a}$ ein $\overline{b}$ mit $\overline{a} \ \overline{b} = \overline{1}$, wenn a und m teilerfremd sind.*

Dabei heißen a und m *teilerfremd*, wenn a und m keinen Primteiler gemeinsam haben. Wir können dies auch so ausdrücken: Der größte Teiler von a und m – das ist die größte a und m teilende positive ganze Zahl – ist 1.

Die Anzahl der Restklassen $\overline{a}$ modulo m, für die a teilerfremd zu m ist (auch dies hängt nur von $\overline{a}$ ab!), bezeichnet man traditionell mit $\varphi(m)$, und nennt die Funktion φ die *Eulersche* φ-Funktion nach Leonard Euler (1707-1783), einem der größten Mathematiker des 18. Jahrhunderts.
Zum Beispiel $m = 15$: Von den Zahlen zwischen 0 und 14 sind

$$1, 2, 4, 7, 8, 11, 13, 14 \text{ teilerfremd zu } 15, \text{ also } \varphi(15) = 8.$$

Ähnlich kann man etwa

$$\varphi(24) = 8, \quad \varphi(49) = 42, \quad \varphi(210) = 48$$

bestimmen. Für sehr große Zahlen m kann man $\varphi(m)$ natürlich nicht durch Abzählen der zu m teilerfremden Zahlen zwischen 0 und $m - 1$ ermitteln. Dazu benutzt man den folgenden

Satz 2. (a) *Die Zahlen m und n seien teilerfremd. Dann gilt*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(b) *Sei $m = p_1^{e_1} \dots p_r^{e_r}$ mit paarweise verschiedenen Primzahlen p_i. Dann gilt*

$$\varphi(m) = (p_1 - 1)p_1^{e_1 - 1} \dots (p_r - 1)p_r^{e_r - 1}.$$

Man kann also $\varphi(m)$ leicht ermitteln, wenn man die Primfaktorzerlegung von m kennt.

Es ist äußerst wichtig, daß man für teilerfremdes a und m die Restklasse $\overline{b}$ mit $\overline{a}\ \overline{b} = \overline{1}$, deren Existenz in Satz 1 behauptet wird, leichter bestimmen kann. Dazu dient der *Algorithmus von Euklid* (um 300 vChr). Wir formulieren ihn zunächst so, daß er nur den größten gemeinsamen Teiler von a und m berrechnet:

(1) Setze $c := a$ und $d := m$.
(2) Dividiere d mit Rest durch c:

$$d = qc + r, \quad 0 \le r \le c - 1.$$

(3) Wenn $r = 0$ ist, ist c der größte gemeinsame Teiler von a und m.
(4) Andernfalls setze man $d := c$ und $c := r$ und geht wieder zu Schritt 2.

Der Algorithmus endet nach endlich vielen Schritten, weil die in Schritt (2) sukzessiv gebildeten Reste r_i immer kleiner werden: $r_1 > r_2 > r_3 > \dots$, sodaß schließlich $r = 0$ erreicht werden muß.
Wenn man den Algorithmus so ablaufen läßt, ermittelt er lediglich den größten gemeinsamen Teiler von a und m. Immerhin sieht man dann, ob a und m teilerfremd sind.
Beispiel: $a = 92$, $m = 3485$

Duchlauf	d	c	r	q
1	3485	92	81	37
2	92	81	11	1
3	81	11	4	7
4	11	4	3	2
5	4	3	1	1
6	3	1	0	3

Mit einer kleinen Erweiterung können wir aber wesentlich mehr erreichen. Hinter Schritt (1) fügen wir ein:
(1′) Setze $u := 0$, $v := 1$, $b := 1$, $e := 0$.
Schritt (3) erweitern wir durch die Feststellung: (3) ... und es gilt $c = b \cdot a + em$.
Schritt (4) erweitern wir so:
(4) Andernfalls setzt man

$$\begin{aligned} d &:= c & \qquad c &:= r \\ b_1 &:= b & \qquad e_1 &:= e \\ b &:= u - qb & \qquad e &:= v - qe \\ u &:= b_1 & \qquad v &:= e_1 \end{aligned}$$

und geht zu Schritt (2).
(Die Hilfsvariablen b_1 und e_1 dienen nur dazu, die "alten" Werte von b und e zu "retten".)
Wenn man den Algorithmus bei (3) abgebrochen hat, gilt

$$c = ba + em,$$

und nach Übergang zu den Restklassen:

$$\overline{c} = \overline{b}\,\overline{a} + \overline{e}\,\overline{m} = \overline{b}\,\overline{a} + \overline{e} \cdot \overline{0} = \overline{b}\,\overline{a}.$$

Wenn a und m teilerfremd sind, also $c = 1$ ist, hat man damit

$$\overline{1} = \overline{b}\,\overline{a}.$$

(Wenn man nur an der Bestimmung von $\overline{b}$ interessiert ist, ist es überflüssig, die Zahlen e und v mitzuführen; überdies genügt es natürlich, die Restklassen $\overline{b}$ und $\overline{u}$ jeweils zu kennen.)
Wir erweitern das obige Beispiel $a = 92$, $m = 3485$.

Durchlauf	d	c	r	q	b	u	e	v
1	3485	92	81	37	1	0	0	1
2	92	81	11	1	-37	1	1	0
3	81	11	4	7	38	-37	-1	1
4	11	4	3	2	-303	38	8	-1
5	4	3	1	1	644	-303	-17	8
6	3	1	0	3	-947	644	25	-17

Beachte: Die in einer Zeile stehenden Werte der Variablen beschreiben den Zustand nach Ausführung von Schritt 2.
Also gilt $1 = (-947) \cdot 92 + 25 \cdot 3485$ und modulo 3485

$$\overline{92} \cdot \overline{2538} = \overline{1},$$

weil $\overline{-947} = \overline{2538}$.

3. Potenzen von Restklassen

Als nächstes müssen wir das Potenzieren von Restklassen diskutieren. Wo man nach den üblichen Rechenregeln multipliziert, kann man natürlich auch Potenzen bilden: Man setzt

$$\overline{a}^0 := \overline{1}, \quad \overline{a}^1 = \overline{a}, \quad \overline{a}^2 = \overline{a} \cdot \overline{a}, \quad \overline{a}^3 = \overline{a}^2 \cdot \overline{a}, \text{ usw.}$$

Dann gelten die bekannten Potenzrechenregeln:

$$\overline{a}^{k+l} = \overline{a}^k \cdot \overline{a}^l, \quad (\overline{a}\ \overline{b})^k = \overline{a}^k\ \overline{b}^k, \quad \overline{a}^{kl} = (\overline{a}^k)^l.$$

Dabei sind k und l nichtnegative ganze Zahlen.
Berechnen wir einmal die Potenzen von $\overline{2}$ und $\overline{3}$ modulo 15:

$\overline{2}^0 = \overline{1}$	$\overline{3}^0 = \overline{1}$
$\overline{2}^1 = \overline{2}$	$\overline{3}^1 = \overline{3}$
$\overline{2}^2 = \overline{4}$	$\overline{3}^2 = \overline{9}$
$\overline{2}^3 = \overline{8}$	$\overline{3}^3 = \overline{27} = \overline{12}$
$\overline{2}^4 = \overline{16} = \overline{1}$	$\overline{3}^4 = \overline{36} = \overline{6}$
$\overline{2}^5 = \overline{2}^4 \cdot \overline{2} = \overline{1} \cdot \overline{2} = \overline{2}$	$\overline{3}^5 = \overline{3}$
$\overline{2}^6 = \overline{4}$	$\overline{3}^6 = \overline{9}$
$\overline{2}^7 = \overline{8}$	$\overline{3}^7 = \overline{12}$
$\overline{2}^8 = \overline{1}$	$\overline{3}^8 = \overline{6}$
$\overline{2}^9 = \overline{2}$	$\overline{3}^9 = \overline{3}$
etc.	etc.

In beiden Fällen ist die Folge der Potenzen periodisch. Dies ist kein Zufall, sondern beruht auf wichtigen zahlentheoretischen Sätzen, deren erster von *Pierre de Fermat* (1601-1665) stammt:

Satz 3. *Sei $m = p$ eine Primzahl. Dann gilt:*

(a) *Wenn a nicht von p geteilt wird, z.B. $1 \leq a \leq p-1$ gilt, ist*

$$\overline{a}^{p-1} = \overline{1}.$$

(b) *Für alle Zahlen a ist $\overline{a}^p = \overline{a}$.*

Der wesentliche Teil ist (a); (b) ist eine triviale Folgerung. Der erste Teil des Fermatschen Satzes wurde von Euler verallgemeinert:

Satz 4. *Sei m eine beliebige positive Zahl. Dann gilt für alle zu m teilerfremden Zahlen a:*

$$\overline{a}^{\varphi(m)} = \overline{1}.$$

Der zweite Teil läßt sich nicht in der gleichen Weise verallgemeinern. Wählt man z.B. $m = 12$, so ist

$$\overline{10}^0 = \overline{1}, \quad \overline{10}^1 = \overline{10}, \quad \overline{10}^2 = \overline{4}, \quad \overline{10}^3 = \overline{4}, \quad \overline{10}^5 = \overline{4}, \ldots$$

und $\overline{10}^k = \overline{10}$ gilt nur für $k = 1$. Wenn wir aber wie oben $m = 15$ wählen, so gilt in Analogie zu Satz 4,(b)

$$\overline{a}^{\varphi(15)+1} = \overline{a}^9 = \overline{a}$$

für alle zu 15 teilerfremden a, wie man leicht durch Ausprobieren aller Restklassen herausfindet. Was 12 von 15 in diesem Zusammenhang unterscheidet, ist, daß 12 einen Primfaktor, nämlich 2, mehrfach enthält, während dies bei 15 nicht der Fall ist.

Satz 5. *Die Zahl m sei Produkt paarweise verschiedener Primzahlen $m = p_1 \dots p_r$, $p_i \neq p_j$ für $i \neq j$. Dann gilt für alle Zahlen a:*

$$\overline{a}^{\varphi(m)+1} = \overline{a}.$$

Dabei ist folgendes zu beachten:

(a) $\varphi(m) = (p_1 - 1) \dots (p_r - 1)$, vglṠatz 2.
(b) Die kleinste Zahl k, für die $\overline{a}^{k+1} = \overline{a}$ für alle a ist, ist das kleinste gemeinsame Vielfache von $p_1 - 1, \dots, p_r - 1$. Für $m = 15$ gilt also $k = 4$.
(c) $\overline{a}^{\varphi(m)} = \overline{1}$ gilt genau dann, wenn a zu m teilerfremd ist. Aus $\overline{a}^{\varphi(m)+1} = \overline{a}$ darf man *nicht* schließen, daß $\overline{a}^{\varphi(m)} = \overline{1}$ ist. Vergleiche dazu, das obige Beispiel $m = 15$, $a = 3$.

Bei dem RSA-Kryptosystem (und vielen verwandten Systemen) muß man Potenzen

$$\overline{a}^k$$

für sehr große Zahlen m, a – und vor allem – k bestimmen. Es wäre unmöglich, diese Potenzen auszurechnen, wenn man etwa $\overline{a}$ k-mal mit sich selbst multiplizieren müßte. Es gibt aber ein Potenzierungsverfahren, das erheblich schneller abläuft und die Bestimmung solcher Potenzen zu einer "leichten" Aufgabe macht.
Betrachten wir als Beispiel 3^{21}. Es gilt

$$3^{21} = 3^{16} \cdot 3^4 \cdot 3, \quad \text{weil } 21 = 16 + 4 + 1.$$

Ausgehend von 3 erhalten wir durch fortgesetztes Quadrieren:

$$3^1 = 3,\ 3^2 = 9,\ 3^4 = 81,\ 3^8 = 6561,\ 3^{16} = 43046721$$

Dann bilden wir das Produkt

$$3^{21} = 3^{16} \cdot 3^4 \cdot 3 = 43046721 \cdot 81 \cdot 3 = 10460353203$$

Wir haben also statt 20 Multiplikationen nur 6 benötigt. Wir führen die gleiche Rechnung noch einmal modulo 11 durch

$$\begin{aligned}
&\overline{3}^{21} = \overline{3}^{16} \cdot \overline{3}^4 \cdot \overline{3},\\
&\overline{3}^1 = \overline{3}, \quad \overline{3}^2 = \overline{9}, \quad \overline{3}^4 = \overline{81} = \overline{4}, \quad \overline{3}^8 = \overline{16} = \overline{5}, \quad \overline{3}^{16} = \overline{25} = \overline{3},\\
&\overline{3}^{21} = \overline{3}^{16} \cdot \overline{3}^4 \cdot \overline{3} = \overline{3} \cdot \overline{4} \cdot \overline{3} = \overline{3}.
\end{aligned}$$

Der Trick bei der Berechnung von a^k oder $\overline{a}^k$ besteht offensichtlich darin, zunächst nur diejenigen Potenzen auszurechnen, für die der Exponent eine Potenz von 2 ist. Dies erreicht man durch fortgesetztes Quadrieren. Aus den so erhaltenen Potenzen

wählt man dann diejenigen aus, deren Exponenten aufaddiert gerade k ergeben. Um letztere zu finden stellt man k im Zweiersystem dar: Am Beispiel demonstriert:

$$\begin{aligned} 21 = (10101)_2 \quad &= 1\cdot 2^4 \quad + 0\cdot 2^3 \quad + 1\cdot 2^2 \quad + 0\cdot 2^1 \quad + 1\cdot 2^0 \\ &= 1\cdot 16 \quad + 0\cdot 8 \quad + 1\cdot 4 \quad + 0\cdot 2 \quad + 1\cdot 1. \end{aligned}$$

Die Exponenten derjenigen Potenzen von a oder $\overline{a}$, die aufzumultiplizieren sind, erscheinen in dieser Darstellung gerade mit dem Koeffizienten 1.

4. Das RSA-Kryptosystem

Das RSA-Kryptosystem arbeitet nach folgendem Schema: (1) Jeder Teilnehmer A wählt zufällig zwei große Primzahlen p und q mit etwa 100 Dezimalstellen.
(2) Er bildet das Produkt $m_A = pq$ und $\varphi(m_A) = (p-1)(q-1)$.
(3) Er wählt eine zu $\varphi(m)$ teilerfremde Zahl e_A zwischen 1 und $\varphi(m)$, etwa die kleinste Zahl $e_A > 1$, die zu $\varphi(m_A)$ teilerfremd ist.
(4) Er bestimmt die Zahl d_A, $1 \le d_A \le \varphi(m_A)$ mit $\overline{e}_A\overline{d}_A = \overline{1}$ modulo $\varphi(m_A)$.
(5) Er gibt m_A und e_A öffentlich bekannt, hält aber d_A, p, q und $\varphi(m_A)$ geheim.
(6) Wenn B eine Nachricht an A senden will, so stellt er diese zunächst als eine Folge von Zahlen $n_1, \dots, n_r$ zwischen 0 und $m_A - 1$ dar. Dann bestimmmt er zu jeder dieser Zahlen n_i

$$\overline{c}_i = \overline{n}_i^{e_A} \text{ modulo } m_A$$

und sendet die Folge $\overline{c}_1, \dots, \overline{c}_r$ an A. (Jede der Restklassen wird dabei natürlich durch c_i mit $0 \le c_i \le m_A - 1$ repräsentiert.)
(7) A empfängt $\overline{c}_1, \dots, \overline{c}_r$ und bildet die Potenzen

$$\overline{c}_i^{d_A} = \overline{n}_i \text{ modulo } m_A$$

und erhält die ursprüngliche Nachricht $n_1, \dots, n_r$ zurück. Nach Wahl von d_A gilt ja

$$\overline{e}_A\overline{d}_A = \overline{1} \text{ modulo } \varphi(m_A)$$

also

$$e_A d_A = t\varphi(m_A) + 1$$

mit einer Zahl $t \ge 0$. Damit ist mit $m = m_A$

$$\begin{aligned} \overline{c}_1^{d_A} = \overline{n}_i^{e_A d_A} = \overline{n}_i^{t\varphi(m)+1} = (\overline{n}_i^{\varphi(m)})^t\overline{n}_i = (\overline{n}_i^{\varphi(m)})^{(t-1)}\overline{n}_i^{\varphi(m)}\overline{n}_i \\ = \overline{n}_i^{\varphi(m)(t-1)}\overline{n}_i = \cdots = \overline{n}_i \end{aligned}$$

nach Satz 5.
Ein Beispiel soll dies veranschaulichen. Um es von Hand durchführen zu können, wählen wir – fern der Realität – in Schritt (1) die Primzahlen $p = 5$ und $q = 7$, also $m_A = 35$, $\varphi(m_A) = 24$. Damit stehen 35 Restklassen für die Darstellung von Nachrichten zur Verfügung und wir können ihnen die Großbuchstaben, den Wortzwischenraum $\sqcup$ und die Satzzeichen zuordnen:

$$A \leftrightarrow 1, \dots, Z \leftrightarrow 26, \quad \sqcup \leftrightarrow 27, \quad . \leftrightarrow 28 \quad \text{, usw.}$$

In Schritt (3) wählen wir $e = 11$ und erhalten $d = 11$: $\overline{e}\overline{d} = \overline{121} = \overline{1}$ modulo 24.
Nun soll die Nachricht "ICH LIEBE DICH." verschlüsselt und das Chiffrat wieder entschlüsselt werden:

	n_i	Verschlüsselung	c_i	Entschlüsselung	n_i
I	9	$\overline{9}^{11} = \overline{4}$	4	$\overline{4}^{11} = \overline{9}$	9
C	3	$\overline{3}^{11} = \overline{12}$	12	$\overline{12}^{11} = \overline{3}$	3
H	8	$\overline{8}^{11} = \overline{22}$	22	$\overline{22}^{11} = \overline{8}$	8
$\sqcup$	27	$\overline{27}^{11} = \overline{13}$	13	$\overline{13}^{11} = \overline{27}$	27
L	12	$\overline{12}^{11} = \overline{3}$	3	$\overline{3}^{11} = \overline{12}$	12
I	9	$\overline{9}^{11} = \overline{4}$	4	$\overline{4}^{11} = \overline{9}$	9
E	5	$\overline{5}^{11} = \overline{10}$	10	$\overline{10}^{11} = \overline{5}$	5
B	2	$\overline{2}^{11} = \overline{18}$	18	$\overline{18}^{11} = \overline{2}$	2
E	5	$\overline{5}^{11} = \overline{10}$	10	$\overline{10}^{11} = \overline{5}$	5
$\sqcup$	27	$\overline{27}^{11} = \overline{13}$	13	$\overline{13}^{11} = \overline{27}$	27
D	4	$\overline{4}^{11} = \overline{9}$	9	$\overline{9}^{11} = \overline{4}$	4
I	9	$\overline{9}^{11} = \overline{4}$	4	$\overline{4}^{11} = \overline{9}$	9
C	3	$\overline{3}^{11} = \overline{12}$	12	$\overline{12}^{11} = \overline{3}$	3
H	8	$\overline{8}^{11} = \overline{22}$	22	$\overline{22}^{11} = \overline{8}$	8
.	28	$\overline{28}^{11} = \overline{7}$	7	$\overline{7}^{11} = \overline{28}$	28

Um ein RSA-Kryptosystem zu brechen, muß man die Zahl d_A bestimmen, und hierfür ist bisher kein effektiveres Verfahren bekannt als die Bestimmung der Primfaktoren p und q von m_A. Für Zahlen der genannten Größenordnung erfordert dies jedoch mit den besten bekannten Methoden und schnellsten verfügbaren Computern immer noch astronomische Rechenzeiten.
Nach dem, was gerade gesagt wurde, erscheint es paradox, daß man sich die in Schritt (1) genannten Primzahlen überhaupt beschaffen kann. Dies gelingt, weil es schnelle "Primzahltests" gibt, Verfahren mit denen man entscheiden kann, ob eine gegebene Zahl p Primzahl ist – ohne daß bei einem negativen Ergebnis ein Faktor von p bestimmt wird! Eine Andeutung, wie solche Tests funktionieren, gibt Satz 3. Man wählt eine Zahl a, $1 \leq a \leq p-1$, und prüft ob $a^{p-1} \equiv 1 \ (p)$ gilt. Wenn nicht, wissen wir, daß p keine Primzahl ist – obwohl wir keinen Primteiler von p kennen. Wenn ja, können wir allerdings mit diesem Test nicht erkennen, ob p zusammengesetzt ist.
Um Schritt (1) auszuführen, wählt man mittels eines Zufallsgenerators eine Ziffernfolge der genannten Länge und prüft ob die von ihr dargestellte Zahl p eine Primzahl

ist. Wenn nicht, ersetzt man sie, wenn sie gerade ist, durch $p+1$, andernfalls durch $p+2$ und führt den Primzahltest durch. Da Primzahlen relativ "dicht" liegen (dies kann man präzisieren) findet man nach wenigen Schritten so eine Primzahl. Um zu verhindern, daß m mit den bekannten Verfahren relativ schnell in seine Primfaktoren zerlegt werden kann, sollten p und q noch einige Nebenbedingungen erfüllen, zB̈nicht zu nahe benachbart sein und $p-1$ und $q-1$ sollten je einen sehr großen Primfaktor enthalten.
Schließlich wollen wir noch das Problem der "Unterschrift" diskutieren. Es läßt sich zum Beispiel so lösen: Wenn B eine Nachricht an A senden will, so sendet er mit jedem Chiffrat $\overline{e}_i$ zusätzlich $\overline{c}_I^{d_B}$ modulo m_B. Der Empfänger A kennt ja e_B, kann dann $\overline{c}_I^{d_B e_B}$ bilden und erhält so auf einem zweiten Wege $\overline{c}_i$. Da ein dritter Teilnehmer C die nur B bekannte Zahl d_B nicht kennt, kann er die zu $\overline{c}_i$ gehörende Unterschrift $\overline{c}_i^{d_B}$ nicht erzeugen.

5. Literatur

Zunächst zwei Bücher zur Zahlentheorie:

I. Niven, H.S. Zuckerman, Einführung in die Zahlentheorie I,II, Bibliographisches Institut, Mannheim, 1976.
R. Remmert, P. Ullrich, Elementare Zahlentheorie, Birkhäuser, Basel, 1987.

Kryptosysteme mit öffentlichen Schlüsseln werden in einer populärwissenschaftlichen Zeitschrift zum ersten Mal diskutiert in

M.E. Hellman, Die Mathematik neuer Verschlüsselungssysteme, Spektrum der Wissenschaft, 10, 1979, 92-101.

Die Originalarbeit zum RSA-System ist

R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications ACM, 21, 1978, 120-126.

Eine Darstellung der Zahlentheorie unter dem Aspekt ihrer Anwendung in der Kryptologie:

N. Koblitz, A course in number theory and cryptography, Springer-Verlag, 1987.

Deutsche Bücher zum Thema:

P. Horster, Kryptologie, Bibliographisches Institut, 1985.
F. L. Bauer, Entzifferte Geheimnisse, Springer-Verlag, 1997.

Ein exzellenten Überblick über die Geschichte der Kryptologie und den Einfluß der Kryptologie auf politische und militärische Entscheidungen:

D. Kahn, The codebreakers, the story of secret writing, Scribner, New York, 1996.

Fr den Einstieg empfehle ich

S. Singh, Geheime Botschaften, Deutscher Taschenbuchverlag, 2006.

Jede der genannten Quellen enthält natürlich wiederum zahlreiche Literaturhinweise.

Universität Osnabrück, Fachbereich Mathematik/Informatik, D-49069 Osnabrück, Germany
E-mail address: wbruns@uos.de