23. Streng geheim!

Primzahlen tauchten in dieser Kolumne schon mehrfach auf. In diesem Beitrag soll davon die Rede sein, wie große Primzahlen die Kryptographie, die Wissenschaft vom Verschlüsseln, revolutioniert haben.

Angenommen, Sie haben sich zwei sehr große Primzahlen verschafft – sie sollen p und q heißen –, die nur Sie selber kennen; „groß" bedeutet hier, dass sie einige hundert Stellen haben. Dann wird das Produkt $p \cdot q$ berechnet, es soll n genannt werden.

Bemerkenswerterweise sind dann p und q in der Zahl n auf praktisch unauffindbare Weise versteckt. Heute ist nämlich kein Verfahren bekannt, die Faktoren p und q in realistischer Zeit aus n zu rekonstruieren. Auch nicht, wenn die besten Computer mehrere Jahrtausende rechnen dürften.

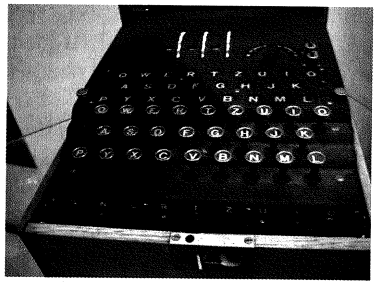

Abbildung 20: Klassische Kryptographie: Die „Enigma"

Diese Tatsache macht sich die Kryptographie zunutze. Sie verwendet einen Satz der Zahlentheorie, der schon vor mehreren hundert Jahren bekannt war: Man kann eine gegebene Zahl unter Verwendung von n so manipulieren, dass diese Veränderung nur dann rückgängig zu machen ist, wenn man p und q kennt. Wenn Ihnen also jemand eine sehr vertrauliche Nachricht schicken soll, so müssen Sie ihm oder ihr nur die Zahl n mitteilen und ein Verfahren vorschreiben, wie die Nachricht mit Hilfe von n zu verändern ist; dazu muss die Nachricht vorher in eine Zahl umgewandelt werden. Das Ergebnis soll Ihnen geschickt werden. Niemand außer Ihnen kann dann mit der verschlüsselten Nachricht etwas anfangen, nur wegen Ihrer Kenntnis von p und q macht das Decodieren keine Schwierigkeiten.

Revolutionär an diesem Verfahren ist, dass es praktisch unter den Augen der Öffentlichkeit stattfinden kann, jeder darf sich das zum Verschlüsseln wichtige n und die verschlüsselte Nachricht ansehen; man spricht auch von der „Kryptographie der öffentlichen Schlüssel", der „public key cryptography".

Der mathematische Anteil – eben wurde etwas vage von der „Manipulation einer Zahl unter Verwendung von n" gesprochen – beruht auf dem im vorigen

Beitrag angesprochenen Rechnen modulo einer Zahl. Es ist auch für Mathematiker sehr erstaunlich, dass diese Rechenmethode aus der Zahlentheorie heute täglich millionenfach bei der Übermittlung vertraulicher Informationen z.B. im Internet eine Rolle spielt.

Verschlüsseln mit dem RSA-Verfahren

Um etwas genauer zu verstehen, was es mit der „Kryptographie der öffentlichen Schlüssel" (also der *public key cryptography*) auf sich hat, muss man einige Begriffe und Ergebnisse kennen. In Grundzügen funktioniert das so genannte RSA-Verfahren[23] wie folgt.

Grundlagen

Da geht es eigentlich nur um das „modulo"-Rechnen, das im Beitrag 22 erläutert wurde. Man sollte also wissen, warum die Gleichung $211 \bmod 100 = 11$ richtig ist[24]. Und wenn man einen Rechner hat, kann man sich auch davon überzeugen, dass

$$26525285981219105863630848047902 3 \bmod 1459001 = 897362$$

stimmt.

Fakten

In Beitrag 22 wurde schon auf eine überraschende Tatsache hingewiesen: Ist n eine Primzahl und k eine weitere Zahl, die zwischen 1 und n liegt, so gilt immer

$$k^{n-1} \bmod n = 1.$$

Mathematiker nennen diese Formel den „kleinen Satz von Fermat[25]". Nimmt man beide Seiten der Gleichung noch einmal mit k mal, so erhält man

$$k^n \bmod n = k.$$

Den Beweis wollen wir hier nicht angeben, wir wollen das Ergebnis einfach als Baustein weiter verwenden.

> Zur Illustration nur ein Zahlenbeispiel: Ist $n = 7$ und $k = 3$, so ist $k^n = 3^7 = 2187$. Und es gilt wirklich $2187 \bmod 7 = 3$.

---

[23] Benannt ist es nach den Mathematikern Rivest, Shamir und Adleman, die es im Jahr 1977 vorschlugen.

[24] Dabei ist $211 \bmod 10 = 11$ die Abkürzung dafür, dass 211 modulo 100 gleich 11 ist. Diese etwas kompaktere Schreibweise wird im Folgenden meist verwendet.

[25] Unter dem „großen Satz von Fermat" versteht man das weit schwierigere Problem zu entscheiden, ob es ganzzahlige Lösungen der Gleichung $a^n + b^n = c^n$ im Fall $n > 2$ geben kann; siehe Beitrag 89.

Gebraucht wird aber eine Verallgemeinerung für Zahlen, die eventuell keine Primzahlen sind, sie wurde erstmals von dem Mathematiker Leonhard Euler (1707 bis 1783) bewiesen. Um sie formulieren zu können, muss man wissen, was der Begriff „teilerfremd" besagt: Zwei Zahlen m und n heißen teilerfremd, wenn es außer der 1 keine Zahl gibt, die sowohl Teiler von m als auch von n ist. So sind zum Beispiel 15 und 32 teilerfremd, die Zahlen 15 und 12 sind es aber nicht (denn beide haben den Teiler 3).

Ist dann n eine Zahl, so bezeichnet man mit $\phi(n)$ (gesprochen „fi von n") die Anzahl derjenigen Zahlen zwischen 1 und n, die zu n teilerfremd sind. Ist etwa $n = 22$, so sind die Zahlen $1, 3, 5, 7, 9, 13, 15, 17, 19, 21$ teilerfremd zu n, und deswegen ist $\phi(22) = 10$. Eulers Ergebnis besagt dann: Ist k zu n teilerfremd, so ist

$$k^{\phi(n)} \bmod n = 1.$$

Als „Test" betrachten wir $n = 22$ und $k = 13$. Es ist

$$k^{\phi(n)} = 13^{10} = 137858491849,$$

und 137858491849 modulo 22 ist wirklich gleich 1.

(Wer lieber ein Beispiel hätte, bei dem man auch im Kopf noch mitrechen kann, könnte $n = 6$ und $k = 5$ wählen. Es ist $\phi(6) = 2$, und $5^2 \bmod 6$ ergibt wirklich 1.)

Man sollte noch bemerken, dass der kleine Satz von Fermat als Spezialfall aufgefasst werden kann. Ist nämlich p eine Primzahl, so kann es keine gemeinsamen Teiler von p mit irgendeiner kleineren Zahl geben (da p ja keine echten Teiler hat). Deswegen sind *alle* Zahlen $1, 2, \ldots, p-1$ zu p teilerfremd, d.h. es gilt $\phi(p) = p - 1$. Damit geht der Satz von Euler in diesem Fall in den „kleinen Satz von Fermat" über.

Das RSA-Verfahren

Zu Beginn sucht man sich zwei verschiedene große Primzahlen p und q und rechnet das Produkt $n = p \cdot q$ aus. („Groß" bedeutet hier, dass p und q einige hundert Stellen haben sollten.) Zwischen 1 und n sind nur die Vielfachen von p und q *nicht* zu n teilerfremd, da p und q Primzahlen sind, und deswegen ist $\phi(n) = (p-1) \cdot (q-1)$.

Ein Beispiel: Im Fall $p = 3$ und $q = 5$ ist $n = 15$. Teilerfremd zu n sind die Zahlen

$$1, 2, 4, 7, 8, 11, 13, 14,$$

also genau $8 = (3-1) \cdot (5-1)$ Zahlen.

Dann braucht man noch zwei Zahlen k und l, so dass $k \cdot l$ genau gleich 1 modulo $\phi(n)$ ist.

Damit ist die Vorbereitungsphase abgeschlossen. p, q und l kommen in den Panzerschrank, und n und k werden im Branchenfernsprechbuch abgedruckt. Wer