vhb - Kurs: Grundlagen der elementaren Zahlentheorie

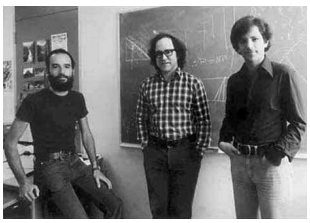
III.4. - Exkurs: Kryptographie mit RSA

Das Übersenden geheimer Nachrichten ist nicht mehr allein das Geschäft von Spionen. Wir leben in einem Zeitalter, in dem wir tagtäglich *online-banking* betreiben oder *smart cards* benutzen. Ein entscheidender Aspekt ist dabei die sichere Datenübermittlung. Viele in der Praxis verwendete Methoden basieren auf dem Gedanken der Benutzung von *Falltürfunktionen*. Eine solche Falltürfunktion ist eine Operation, die in einer Richtung *leicht* zu berechnen ist, dessen Inverses jedoch nahezu *unberechenbar* ist (d.h. in annehmbarer Zeit). *Aber wie findet man eine geeignete Falltürfunktion?* Wir holen etwas aus: Bereits 1801 schrieb Gauß in seinen 'Disquisitiones Arithmeticae' in Artikel 329:

> *'Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört ... ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren (...). trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr specielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie (...) auf grössere Zahlen aber meistenteils kaum angewendet werden können.'*

Es ist ratsam, hier zwei Probleme zu unterscheiden: Sei N eine natürliche Zahl;

- ein **Primzahltest** entscheidet, ob N prim oder zusammengesetzt ist, und
- ein **Faktorisierungsalgorithmus** liefert die Primfaktorzerlegung von N.



Es scheint, dass diese zwei Probleme *unterschiedlich schwierig* sind: Die Primfaktorzerlegung von N benötigt a priori mehr Informationen als die Frage nach der Anzahl der Primfaktoren. Diese vermutliche Asymetrie der Schwierigkeiten bildet das Fundament vieler moderner Kryptosysteme.
Genauer: Die Tatsache, dass es zwar leicht ist, zwei große Primzahlen miteinander zu multiplizieren, aber - jedenfalls nach heutigen Kenntnisstand- sehr aufwendig, aus dem Produkt auf die Faktoren zu schließen, wird in der Kryptographie seit der bahnbrechenden Arbeit von Rivest, Shamir und Adleman Mitte der siebziger Jahre des vergangenen

Jahrhunderts verwendet. Bei dem nach den Initialen seiner Erfinder benannten **RSA-Verfahren** wird als öffentlicher Schlüssel das Produkt zweier großer Primzahlen eingesetzt. Die Sicherheit dieses Systems basiert auf der Unkenntnis einer *schnellen* Faktorisierungsmethode. Zur Erzeugung des öffentlichen Schlüssels hingegen benötigt man Algorithmen zur Generierung von *großen* Primzahlen, also effiziente Primzahltests, die auch die Primalität *großer* Zahlen *schnell* erkennen können.

Doch wie funktioniert RSA? Ein Benutzer, nennen wir ihn Bob, wählt zwei *große* (verschiedene) Primzahlen p und q und berechnet $N = pq$ sowie

$$\varphi(N) = (p-1)(q-1) = N + 1 - p - q;$$

hierbei haben wir die Multiplikativität der Eulerschen φ-Funktion benutzt. Dann wählt Bob *zufällig* eine ganze Zahl e, so dass $1 < e < \varphi(N)$ gilt und e teilerfremd zu $\varphi(N)$ erfüllt ist; hierbei kann die Teilerfremdheit leicht mit dem Euklidischen Algorithmus nachgeprüft werden. Dann bestimmt Bob das multiplikativ Inverse d zu e mod $\varphi(N)$, also

$$d \equiv e^{-1} \; mod \; \varphi(N)$$

(wiederum mit dem Euklidischen Algorithmus). Dies ist gleichbedeutend mit der Existenz einer ganzen Zahl f mit

$$de = 1 + f\varphi(N).$$

Nun ist Bobs *öffentlicher Schlüssel* das Paar (N, e); die Zahl d, die Faktorisierung von N, und ebenso $\varphi(N)$ sind jedoch *geheim*: der öffentliche Schlüssel mag nun beispielsweise in etwas wie einer Art Telefonbuch bekannt gemacht werden. Damit muss ein Schlüssel nicht gesendet werden- ein großer Vorteil gegenüber klassischer Verfahren, und außerdem erleichtert dies die Nutzung kryptographischer Methoden für eine breite Öffentlichkeit. Nun stellen wir uns vor, dass Alice eine geheime Botschaft an Bob schicken möchte. Dazu muss Alice diese in eine Folge von Zahlen umwandeln; dies mag für alle Benutzte (insbesondere Bob) auf ein und dieselbe Art geregelt sein. Stellen wir uns der Einfachheit halber also vor, dass die folgende Zuordnung besteht:

$$\_ \to 99, \; A \to 10, \; B \to 11, \; ..., \; Z \to 35.$$

Eine Textnachricht wird dann einfach in eine Zahlenfolge übersetzt, indem Buchstaben in die entsprechenden Zahlen kodiert werden, wobei wir Päckchen von einer Größe $< N$ bilden (in der Praxis muss man allerdings etwas vorsichtiger zu Werke gehen). Die geheime Nachricht ist also gegeben als eine große ganze Zahl M. Alice kennt Bobs öffentlichen Schlüssel (N, e) und bildet dementsprechend M^e und reduziert dieses modulo N. Nennen wir das Ergebnis C, so gilt also

$$C = M^e \text{ mod } N$$

wobei hier und im folgenden $c = a \; mod \; N$ für den kleinsten positiver Rest c in der Restklasse a mod N steht. Jetzt wird diese Zahl C Bob

zugesendet. Bob dekodiert C nun durch Berechnung der d-ten Potenz von C mod N. Mit dem Satz von Euler gilt nämlich

$$C^d = (M^e)^d = M^{de} = M^{1+f\varphi(N)} = M \cdot (M^f)^{\varphi(N)} \equiv M \bmod N.$$

Nun kann Bob Alices Nachricht lesen. Tatsächlich benötigt man hier für die Anwendung des Eulerschen Satzes, dass M und N teilerfremd sind, was nur in seltenen Fällen verletzt ist; dieses Problem kann man leicht mit einigen technischen Voraussetzungen beheben, worauf wir der Einfachheit halber hier verzichten.