# Die RSA – Verschlüsselung

## 1. Das RSA - Verfahren

In der modernen Kryptologie hat sich die RSA – Verschlüsslung als eine der sichersten Methoden durchgesetzt. Sie wird heute in wichtigen Bereichen wie im Bankenwesen (z.B. bei der Verschlüsslung von Geheimzahlen), bei der Verschleierung von Pay – TV - Programmen, bei der Verschlüsselung von Mobilfunknetzen oder bei Geheimdiensten verwendet. Daher ist es interessant zu wissen, wie diese Verschlüsslung funktioniert. Dies werden wir in den nächsten Abschnitten klären.

## 2. Der Eulersche Satz

Leonard Euler entdeckte eine mathematische Regel, die für die RSA – Verschlüsselung grundlegend ist. Wählt man zwei positive Primzahlen p und q mit $p \neq q$, dann gilt:

$$m^{s(p-1)(q-1)} \bmod n = m,$$

$m, n, s \in \mathbb{N}$ mit $m \leq n$.

Das heißt also, wenn man die Potenz $m^{s(p-1)(q-1)}$ durch n teilt, so erhält man als Rest dieser Division wieder die Basis m. Diese Gültigkeit ist grundlegend für die Verschlüsselung mit dem RSA – Verfahren (siehe Abschnitt 3).

## 3. Festlegen und Generieren der Schlüssel

Wollen zwei Teilnehmer sich gegenseitig eine Nachricht senden, die für die Öffentlichkeit geheim bleiben soll, die also nur von den beiden entschlüsselt werden können soll, so müssen diese zuerst einige Schlüssel festlegen. Zunächst erhält jeder Teilnehmer zwei große, voneinander verschiedene Primzahlen p und q. Je größer p und q sind, desto schwieriger ist die verschlüsselte Nachricht zu knacken. Das Produkt n der beiden Primzahlen ($n = pq$) kann als öffentlicher Schlüssel verwendet werden. Das heißt, dieser kann unverschlüsselt und in aller Öffentlichkeit ausgetauscht werden, ohne dass eine Entschlüsselung einfacher wird.

Die Teilnehmer suchen nun nach einer Zahl $e \in \mathbb{N}$, die teilerfremd von der Zahl $(p-1)*(q-1)$ ist, das heißt $(p-1)*(q-1)$ und e haben außer 1 keine gemeinsamen Teiler. Dies ist durch einfaches Probieren schnell herauszufinden. Auch die Zahl e kann im Endeffekt als öffentlicher Schlüssel verwendet werden.

Ebenfalls einfach ist es, eine Zahl $d \in \mathbb{N}$ zu finden, für die gilt:

$$ed = s\,(p-1)\,(q-1) + 1,\ s \in \mathbb{N}.$$

Dabei kann die Zahl s so gewählt werden, wie es für d am besten passt, s ist also eine beliebige natürliche Zahl. Nun kann d als geheimer Schlüssel verwendet werden. Entscheidend an dieser Formel ist, dass es einfach für einen Spion ist d zu bestimmen, wenn er e, p und q kennt. **Es ist aber, vor allem bei großen p und q, nahezu unmöglich nur durch Kenntnis der öffentlichen Schlüssel n und e den geheimen Schlüssel d herauszufinden.**

Das Ganze wirkt mit einem Beispiel sicherlich einleuchtender (Wir wählen hier der Einfachheit halber nur relativ kleine p und q).

Nehmen wir an, zwei Teilnehmer einigen sich auf $p = 43$ und $q = 71$.

Wir erhalten zunächst als öffentlichen Schlüssel $n = pq = 43 * 71 = 3053$.

Den zweiten öffentlichen Schlüssel e erhalten wir einfach. Wir suchen eine Zahl, die teilerfremd zu $(p-1)*(q-1) = (43-1)*(71-1) = 42 * 70 = 2940$ ist. Durch Probieren

erhalten wir als teilerfremde Zahlen für e zum Beispiel 11, 13, 17,... . Wir wollen hier e = 11 wählen.
Nun müssen wir ein passendes d suchen. Es muss ja die Gleichung

$$ed = s\,(p-1)\,(q-1) + 1,$$

also $11d = 2940s + 1$

(denn e=11 und (p-1)*(q-1) = 2940)

erfüllen.
Durch Probieren erhalten wir schnell für d = 1871. Dies ist der Fall für s=7, denn 2940 * 7 + 1 = 20581 = 11 * 1871.
So erhalten wir als geheimen Schlüssel d = 1871.
Auch wenn sich die Suche nach d besonders langwierig anhört, so ist sie doch recht einfach. Stellt man in unserem Beispiel die Gleichung
11d = 2940s + 1 nach d um, so erhalten wir: d = (2940s + 1)/11. Wir können nun einfach verschiedene s (s = 1, 2, 3, 4,...) einsetzen und schauen, für welches es ein glattes Ergebnis für d gibt.

4. Ver- und Entschlüsseln

Das Ver- und Entschlüsseln mit den generierten Schlüsseln ist einfach. Sei m das Originalzeichen, so gilt für ein verschlüsseltes Zeichen c:

$$c = m^e \bmod n.$$

Da zum Verschlüsseln einer Nachricht lediglich die öffentlichen Schlüssel benötigt werden, kann jede beliebige Person eine Nachricht verschlüsseln und an einen der beiden Teilnehmer schicken. Das Entschlüsseln ist allerdings nur solchen Personen vorbehalten, die auch den geheimen Schlüssel d kennen. Denn um bei einem vorliegenden verschlüsselten Zeichen c wieder auf das Originalzeichen m zu kommen gilt:

$$m = c^d \bmod n.$$

Der Beweis dieser Gültigkeit beruht auf höheren mathematischen Grundlagen. Auf jeden Fall ist der Euklidische Satz aus Punkt 2 entscheidend für den letzten Schritt. Es gilt:

$$\begin{aligned} & c^d \bmod n \\ = & (m^e)^d \bmod n \\ = & m^{s\,(p-1)\,(q-1)\,+\,1} \bmod n \\ = & m \end{aligned}$$

Das RSA – Verfahren gehört daher zu den sogenannten asymmetrischen Verschlüsselungsverfahren. Hier braucht der Sender grundsätzlich nicht den geheimen Schlüssel des Empfängers zu kennen. Prinzipiell kann jeder mit den öffentlichen Schlüsseln eine Nachricht verschlüsseln, aber die Entschlüsselung ist nur dem Empfänger mit dem geheimen Schlüssel möglich.
Im Gegensatz dazu stehen symmetrische Verschlüsselungsverfahren. Hier besitzen sowohl Sender als auch Empfänger geheime Schlüssel. Das heißt, wer eine Nachricht verschlüsseln kann, der kann sie auch wieder entschlüsseln.

5. Ist RSA zu knacken?

Wie man sieht, ist eine nach RSA verschlüsselte Nachricht nur mit Hilfe des Schlüssels d zu knacken. Als öffentliche Schlüssel sind aber für einen Außenstehenden nur e und n bekannt. Die Variable d lässt sich aber nur mit Hilfe der beiden Primzahlen p und q errechnen (siehe Punkt 3). Daher ist das Grundproblem bei der Entzifferung die Zahl n in ein Produkt zweier Primzahlen zu zerlegen. Dies ist

aber – je nach verwendeten Primzahlen – nahezu unmöglich. Bei wichtigen Angelegenheiten werden nämlich nicht nur so kleine Primzahlen wie die aus unserem Beispiel verwendet, sondern oftmals solche mit über einhundert Ziffern. Multipliziert man diese, so entsteht eine noch viel monströsere Zahl. Es gibt aber keinen Algorithmus, der eine Zahl in seine Primfaktoren zerlegen kann. Man kann höchstens durchprobieren, was allerdings bei solch immensen Zahlen ewig dauern kann.
Viele Forscher haben sich daher vorgenommen immer neue und immer größere Primzahlen zu suchen. So gibt es immer wieder „neue unbekannte Zahlen“, die eine RSA - verschlüsselte Nachricht nahezu unknackbar machen.
Kryptologen empfehlen, für n Zahlen mit mindestens 512 Bit (das entspricht 155 Stellen) zu verwenden. Viele Produkte bieten RSA mit 64-Bit-Zahlen (= 20 Stellen). Diese sind allerdings für eine sichere Verschlüsselung völlig ungeeignet, denn viele Computeralgebra – Systeme wie Derive können solche Zahlen in wenigen Sekunden faktorisieren.

## 6. Aufgaben

a) Zwei Teilnehmer legen sich auf die Primzahlen p = 51 und q = 97 fest. Wähle e, d und s möglichst klein und verschlüssele anschließend den Geheimcode 8539.
b) Ein Bote eines Geheimdienstes entdeckt als öffentliche Schlüssel einer geheimen Nachricht für n = 21 und e = 5. Wie lautet der geheime Schlüssel d?
c) Ein verschlüsselter Code lautet 1 11 12 16. Wie lautet der Originalcode, wenn wie in b) verschlüsselt wurde?