

## RSA-Algorithmus

*Schlüsselerzeugung:*

- Man wählt für jeden Teilnehmer zwei verschiedene, große Primzahlen  $p$  und  $q$  und bildet das Produkt

$$n := pq$$

sowie

$$\varphi(n) = (p - 1)(q - 1).$$

- Man wählt eine natürliche Zahl  $e$ , die teilerfremd zu  $\varphi(n)$  ist, d.h.

$$\text{ggT}(e, \varphi(n)) = 1.$$

- Man bestimmt eine natürliche Zahl  $d$  mit

$$ed \bmod \varphi(n) = 1.$$

Öffentlicher Schlüssel:  $(n, e)$ .

Privater Schlüssel:  $(n, d)$ .

Es sei  $m < n$  eine Nachricht.

*RSA-Verschlüsselung* mit öffentlichem Schlüssel  $(n, e)$ :

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

*RSA-Entschlüsselung* mit privatem Schlüssel  $(n, d)$ :

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

**Behauptung** Es gilt  $m' = m$ .

*Beweis.* Nach Konstruktion von  $d$  gilt  $ed = k\varphi(n) + 1$  für eine natürliche Zahl  $k$ . Nach dem Satz von Euler gilt:

$$m' = c^d \bmod n = m^{ed} \bmod n = m^{k\varphi(n)+1} \bmod n = m.$$

□

**Beispiel 10.2** • Wähle  $p = 61$  und  $q = 53$ . Dann ist

$$n = pq = 61 \cdot 53 = 3233$$

sowie

$$\varphi(n) = (p - 1)(q - 1) = 60 \cdot 52 = 3120.$$

- Wähle  $e = 17$ . Die Zahlen 17 und 3120 sind teilerfremd.
- Bestimme die Zahl  $d$  mit der Eigenschaft

$$17 \cdot d \bmod 3120 = 1.$$

Es gilt  $d = 2753$ , denn

$$17 \cdot 2753 = 46801 = 1 + 15 \cdot 3120.$$

Öffentlicher Schlüssel:  $(n = 3233, e = 17)$ .

Privater Schlüssel:  $(n = 3233, d = 2753)$ .

Wähle als Nachricht  $m = 123 < 3233$ . Um  $m$  zu verschlüsseln, berechnen wir

$$c = 123^{17} \bmod 3233 = 855.$$

Um 855 zu entschlüsseln, berechnen wir

$$m' = 855^{2753} \bmod 3233 = 123.$$

### Zur Sicherheit des RSA-Algorithmus

Es darf nicht möglich sein, aus dem öffentlichen Schlüssel eines Teilnehmers seinen privaten Schlüssel zu ermitteln. Um den privaten Schlüssel  $(n, d)$  aus dem öffentlichen Schlüssel  $(n, e)$  zu berechnen, muss man  $\varphi(n)$  kennen.

**Satz 10.3** *Es sei  $n$  das Produkt zweier Primzahlen  $p$  und  $q$ . Dann ist es genauso schwierig,  $\varphi(n)$  zu bestimmen, wie  $n$  zu faktorisieren.*

*Beweis.* a) Angenommen,  $\varphi(n)$  ist bekannt. Dann kann man aus den beiden Gleichungen

$$\begin{aligned} \varphi(n) &= (p-1)(q-1) \\ n &= pq \end{aligned}$$

die Zahlen  $p$  und  $q$  bestimmen, also  $n$  faktorisieren.

b) Kennt man  $p$  und  $q$ , so bestimmt man  $\varphi(n)$  nach der Formel

$$\varphi(n) = (p-1)(q-1).$$

□

Damit es schwierig ist,  $\varphi(n)$  zu bestimmen, muss also die Faktorisierung von  $n$  schwierig sein. Der Weltrekord im Faktorisieren einer Zahl lag im Jahre 2005 bei einer Zahl mit 663 Bits. In der Praxis werden beim RSA-Algorithmus Zahlen  $n$  mit mehr als 1024 Bits verwendet, das sind über 300 Dezimalstellen. Gegenwärtig wird empfohlen, dass  $n$  mindestens 2048 Bits lang sein soll.



**Beispiel 11.2** In dem vollständigen Graphen  $K_n$  hat jede Ecke den Grad  $n - 1$ , da sie mit jeder der  $n - 1$  anderen Ecken durch genau eine Kante verbunden ist.

**Definition** Ein *Baum* ist ein zusammenhängender Graph, der keinen Kreis (einer Länge  $> 0$ ) enthält.

**Bemerkung 11.1** In einem Baum sind je zwei Ecken durch höchstens eine Kante verbunden.

Wir machen nun die Generalvoraussetzung, dass wir nur Bäume mit endlich vielen Ecken betrachten. Ein solcher Baum hat dann auch nur endlich viele Kanten.

**Definition** Eine *Endecke* ist eine Ecke vom Grad 1.

**Lemma 11.1** *Jeder Baum mit mindestens zwei Ecken hat mindestens eine Endecke.*

*Beweis.* Es sei  $G$  ein Baum mit mindestens zwei Ecken. Es sei  $e_0$  eine Ecke von  $G$ . Da  $G$  zusammenhängend ist, gilt  $d(e_0) \geq 1$ . Also ist  $e_0$  mit einer Ecke  $e_1$  durch eine Kante verbunden. Ist  $e_1$  eine Endecke, so sind wir fertig. Andernfalls ist  $e_1$  mit einer weiteren, von  $e_0$  verschiedenen, Kante  $e_2$  verbunden. Ist  $e_2$  eine Endecke, so sind wir fertig. Ansonsten gibt es eine neue Kante zu einer Ecke  $e_3$ , usw. Alle diese Ecken sind verschieden, da es keinen Kreis gibt. Da  $G$  nur endlich viele Ecken besitzt, muss die Konstruktion abbrechen. Sie bricht an einer Endecke ab.  $\square$

**Satz 11.1** *Es sei  $G$  ein Baum mit  $n$  Ecken und  $m$  Kanten. Dann gilt  $m = n - 1$ .*

*Beweis.* (durch Induktion über  $n$ )

Induktionsanfang  $n = 1$ : Dann besteht  $G$  nur aus einer Ecke und keiner Kante. Also gilt  $m = 1 - 1 = 0$ .

Induktionsschritt  $n \rightarrow n + 1$ : Die Behauptung sei richtig für alle Bäume mit  $n \geq 1$  Ecken. Es sei  $G$  ein Baum mit  $n + 1$  Ecken. Nach Lemma 11.1 hat  $G$  eine Endecke  $e'$ . Wir entfernen die Ecke  $e'$  und die einzige mit ihr verbundene Kante  $k'$ . Dadurch erhalten wir einen Baum  $G'$  mit  $n$  Ecken. Nach Induktionsannahme hat  $G'$  genau  $n - 1$  Kanten. Also hat  $G$  genau  $n$  Kanten, was zu zeigen war.  $\square$

**Satz 11.2** *Es sei  $G$  ein Graph mit  $n$  Ecken und  $m$  Kanten. Wenn  $G$  zusammenhängend ist, gilt  $m \geq n - 1$  und es gilt  $m = n - 1$  genau dann, wenn  $G$  ein Baum ist.*