RSA-Verschlüsselung

Schlüsselerzeugung

1) Man wählt (in der Praxis sehr große) Primzahlen p und q.

2) $\boxed{n := p \cdot q}$, $\boxed{m := \varphi(n) = (p-1)\cdot(q-1)}$

3) e wird so gewählt, dass $\boxed{ggT(e\,,\,m) = 1}$ **ist.**

4) d sei die modulare Inverse von e zum Modul m: $\boxed{d := e^{-1} \pmod m}$

5) (n , e) … öffentlicher Schlüssel,

(n , d) … geheimer Schlüssel (geheim ist nur d),

p, q und m werden nicht mehr benötigt, bleiben aber unbedingt geheim!

Verschlüsselung

Zu verschlüsseln ist eine (vorher in geeigneter Weise als Zahl codierte) zu n teilerfremde Nachricht a. Die Verschlüsselung erfolgt durch Potenzieren mit e: $\boxed{b :\equiv a^e \pmod n}$ **. b ist der Geheimtext, der gesendet wird.**

Entschlüsselung

Der Empfänger und Besitzer des geheimen Schlüssels bildet $b^d \pmod n$ **und erhält** $\boxed{b^d \equiv a \pmod n}$ **, denn es gilt nach dem Satz von EULER:**

$$b^d \equiv (a^e)^d \equiv a^{e\cdot d} \equiv a^{1+k\cdot m} \equiv a^{1+k\cdot\varphi(n)} \equiv a\cdot(a^{\varphi(n)})^k \equiv a \pmod n$$

Beispiel: Übungsaufgabe A 2.4 (Lösung)

a) $n = p\cdot q = 13\cdot 19 = \underline{\underline{247}}$, $m = \varphi(n) = (p-1)\cdot(q-1) = 12\cdot 18 = \underline{\underline{216}}$

Bestimmung der Inversen von e = 11 zum Modul m = 216:

		11 = 0·216 + 1·11
216 : 11 = 19 Rest 7	7 = 216 – 19·11	7 = 1·216 – 19·11
11 : 7 = 1 Rest 4	4 = 11 – 7	4 = –1·216 + 20·11
7 : 4 = 1 Rest 3	3 = 7 – 4	3 = 2·216 – 39·11
4 : 3 = 1 Rest 1	1 = 4 – 3	1 = –3·216 + 59·11

$\Rightarrow$ $\underline{d = 59}$ **ist die modulare Inverse von e zum Modul m = 216.**

b) $a^e \equiv 5^{11} \equiv 177 \pmod{247}$ **, d.h. Geheimtext b = 177 .**

Entschlüsselung (zur Kontrolle): $b^d \equiv 177^{59} \equiv 5 \pmod{247}$ **.**

c) $b^d \equiv 2^{59} \equiv 241 \pmod{247}$ **, d.h. Entschlüsselung a = 241 .**

Bemerkung: Die Restberechnungen in b) und c) können entweder mit einem Rechner mit mod-Funktion erfolgen oder durch Aufspaltung in kleinere Potenzen, z.B. $2^{59} \equiv (2^8)^7 \cdot 2^3 \equiv 256^7 \cdot 8 \equiv 9^7 \cdot 8 \equiv 38263752 \equiv 241 \pmod{247}$.