Aufgaben zu Kapitel 4: RSA-Verschlüsselung

Aufgabe 4.1 (Asymmetrische Verschlüsselung)

a) *Vorzüge:* Kein vorheriger Austausch geheimer Schlüssel notwendig, deutlich geringere Schlüsselanzahl, Möglichkeit einer digitalen Signatur.

b) *Symmetrisch:* Ein Schlüssel pro Kommunikationskanal $= n \cdot (n-1)/2 = 10 \cdot 9/2 = 45$.
Asymmetrisch: Zwei pro Kommunikationsteilnehmer $= 2 \cdot n = 2 \cdot 10 = 20$.

c) *Symmetrisch:* $100 \cdot 99/2 = 4950$.
Asymmetrisch: $2 \cdot 100 = 200$.

Aufgabe 4.2 (Square-and-Multiply)

Wir berechnen:

$37^1 \mod 143 = 37$
$37^2 \mod 143 = 82$
$37^4 \mod 143 = 3$
$37^8 \mod 143 = 9$
$37^{16} \mod 143 = 81$
$37^{32} \mod 143 = 126$

Es gilt $58 = 32 + 16 + 8 + 2$, wir berechnen daher

$$37^{58} = 37^{32} \cdot 37^{16} \cdot 37^8 \cdot 37^2 \equiv_{143} 126 \cdot 81 \cdot 9 \cdot 82 \equiv_{143} 75,$$

also $37^{58} \mod 143 = 75$.

Aufgabe 4.3 (RSA 1)

a) *Öffentlicher Schlüssel*: $(323, 35)$ mit $n = 323 = 17 \cdot 19$.
Privater Schlüssel: (323,107) mit $\varphi(323) = 16 \cdot 18 = 288$ und $107 \cdot e - 13 \cdot \varphi(n) = 1$ (Berechnung über erweiterten euklidischen Algorithmus, Rechenschritte hier ausgelassen.)

b) *Verschlüsselte Nachricht:* $c = m^e \mod n = 250^{35} \mod 323 = 317$.

Aufgabe 4.4 (RSA 2)

a) $p = 67$, $q = 53$, $n = 3551$, $\varphi(n) = 3432$, $e = 35$, $d = 1667$, da $35 \cdot 1667 - 17 \cdot 3432 = 1$.
Privater Schlüssel ist also (3551, 1667).

b) $n = 1643$, $\varphi(n) = 30 \cdot 52 = 1560$.
Kleinstmögliches e muss teilerfremd zu $\varphi(n) = 1560 = 2^3 \cdot 3 \cdot 5 \cdot 13$ sein. Somit $e = 7$.
Geheimtext: $c = 24^7 \mod 1643 = 778$.

Aufgabe 4.5 (RSA 3)

a) Siehe Folie 47, 48 „Warum funktioniert RSA?“

b) Ja, es würde ebenfalls funktionieren, denn Potenzieren ist kommutativ.

c) Siehe Folie 49 „Warum ist RSA (bisher) sicher?“