Datenkommunikation und Informationssysteme, Übung 8

Domenic Quirl 354437 | Julian Schakib 353889 | Daniel Schleiz 356092

Übungsgruppe 14

A1	A2	A3	Σ
/6	/4	/5	/ 15

Aufgabe 1

(a)

(b) i)

ii)

(c)

A1: / 6

Aufgabe 2

(a) i)

ii)

(b)

A2: / 4

Aufgabe 3

(a) Da $p = 13$ und $q = 23$, ist $n = p \cdot q = 299$. Der public key ist also $\langle 61, 299 \rangle$. Zudem ist $\Phi(299) = (13-1)\cdot(23-1) = 264$. Finde nun d so, dass $d \cdot e = d \cdot 61 \equiv_{264} 1$. Verwende den erweiterten Algorithmus von Euklid:

$$\begin{aligned} 264 &= 4 \cdot 61 + 20 \\ 61 &= 3 \cdot 20 + 1 \\ 20 &= 20 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 61 - 3 \cdot 20 \\ &= 61 - 3 \cdot (264 - 4 \cdot 61) \\ &= -3 \cdot 264 + 13 \cdot 61 \\ &\equiv_{264} 13 \cdot 61 \end{aligned}$$

Nun folgt also, dass der private key $\langle 13, 299 \rangle$ ist.

- Verschlüssele $m_1 = 21$: $c_1 = 21^{61} \equiv_{299} 281$.
- Entschlüssele $c_2 = 291$: $m_2 = 291^{13} \equiv_{299} 5$.

(b) Es ist bekannt, dass $n = 91$. Finde durch geschicktes Ausprobieren heraus, dass die Primfaktorzerlegung von n gegeben ist durch $p = 7$, $q = 13$, da $91 = 7 \cdot 13$. Außerdem ist $\Phi(n) = 6 \cdot 12 = 72$. Suche nun d, sodass $d \cdot e = d \cdot 29 \equiv_{72} 1$. Verwende erneut den erweiterten Algorithmus von EUKLID:

$$\begin{aligned} 72 &= 2 \cdot 29 + 14 \\ 29 &= 2 \cdot 14 + 1 \\ 14 &= 14 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 29 - 2 \cdot 14 \\ &= 29 - 2 \cdot (72 - 2 \cdot 29) \\ &= -2 \cdot 72 + 5 \cdot 29 \\ &\equiv_{72} 5 \cdot 29 \end{aligned}$$

Es folgt, dass der private key gegeben ist durch $\langle 5, 91 \rangle$.

- Dekodiere $c = 3$ zu $m = 3^5 \equiv_{91} 61$.

A3: / 5