Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 13

Aufgabe 1 Zeigen Sie, dass man bei dem RSA-Verfahren aus der Kenntnis der öffentlichen Schlüssel n, k und einer der beiden Primzahlen aus $n = p \cdot q$, die geheimen Schlüssel $\varphi(n)$ und l berechnen kann.

Aufgabe 2 Gegeben sind die öffentlichen Schlüssel $n = 26$ und $k = 7$. Zusätzlich ist bekannt, dass das Alphabet beginnend bei A=0 durchnummeriert wird ($A = 0$, $B = 1$, $C = 2$, $\ldots$, $Z = 25$).

(a) Kodieren Sie das Wort „TOLL“, indem Sie die Buchstaben einzeln mittels RSA verschlüsseln!

(b) Bestimmen Sie für dieses einfache Beispiel einen privaten Schlüssel l und dekodieren Sie mit Hilfe von l die Nachricht „REHHA“.

Aufgabe 3 Beweisen oder widerlegen Sie: Für einen Ring $(R, +, \cdot)$ gilt:

(a) $\forall a \in R. a \cdot 0 = 0 \cdot a = 0$

(b) $\forall a, b \in R. a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$

(c) $\forall a \in R : -a = (-1) \cdot a$

Aufgabe 4 Berechnen Sie für die folgenden Polynome $p(x)$ div $q(x)$, $p(x)$ mod $q(x)$ und den ggT der beiden Polynome:

(a)
$$\begin{aligned} p(x) &= -3x^3 - 13x^2 + 15x + 25 \\ q(x) &= 9x^3 - 21x^2 - 5x + 25 \end{aligned}$$

(b)
$$\begin{aligned} p(x) &= -20x^6 + x^5 - 42x^4 + 10x^3 - 49x^2 - 6x - 24 \\ q(x) &= -20x^3 - 15x^2 - 30x \end{aligned}$$

(c)
$$\begin{aligned} p(x) &= x^3 - 3x^2 + 5x - 3 \\ q(x) &= x^3 - 1 \end{aligned}$$