Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 12

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.

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“.

3. Beweisen Sie die folgenden Aussagen:

   a) Zwei aufeinanderfolgende Fibonacci-Zahlen sind teilerfremd.

   b) Jede vierte Fibonacci-Zahl ist durch 3 teilbar.

4. Zeigen Sie die folgende Gleichung mit vollständiger Induktion:

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1$$