Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 13

Aufgabe 1. Es sei n das Produkt zweier Primzahlen p und q mit $p \geq q \geq 5$. Zeige Sie, dass dann $|\mathbb{Z}_n^*| \geq \frac{1}{2}n$.

Aufgabe 2. Finden Sie $x \in \mathbb{Z}_{210}$ mit den Bedingungen:

$1 = x \bmod 3$

$3 = x \bmod 7$

$5 = x \bmod 10$

Aufgabe 3. 17 chinesische Piraten erbeuten eine Truhe mit Goldstücken. Beim Versuch, diese gleichmäßig zu verteilen, bleiben 7 Goldstücke übrig. Um diese entbrennt ein heftiger Streit, bei dem einer der Piraten das Leben lässt. Die verbleibenden 16 Piraten versuchen erneut, die Goldstücke gerecht zu verteilen, behalten jedoch 11 Stücke übrig. Bei der folgenden Auseinandersetzung geht wieder einer der Streitenden über Bord. Den 15 Überlebenden gelingt dann die Teilung. Wie viele Goldstücke müssen es mindestens gewesen sein?

Aufgabe 4. 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 5. 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, ... , 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 6. Gegeben sind die öffentlichen Schlüssel $n = 667$ und $k = 43$. Sie fangen eine Nachricht mit dem Inhalt 288 ab. Versuchen Sie, den RSA zu knacken und die Nachricht zu dekodieren!

Aufgabe 7. Zeigen Sie, dass zwei aufeinanderfolgende Fibonacci-Zahlen F_n und F_{n+1} teilerfremd sind ($ggT(F_n, F_{n+1}) = 1$).