Kryptologie
Übungsblatt 3

Aufgabe 3.1

Sie sind der Wahlleiter bei einer geheimen Wahl in Ihrem Sportverein, bei der Sie selber nicht mitstimmen dürfen. Sie haben die Idee die Wahl elektronisch mittels RSA durchzuführen. Jede wahlberechtigte Person sendet Ihnen dazu in RSA-verschlüsselter Form entweder „Kandidat A“, „Kandidat B“, „Kandidat C“ oder „Enthaltung“ zu. Am Ende wird Kandidat B gewählt und zwar mit 102 zu 154 zu 87 Stimmen, bei 23 Enthaltungen. Können Sie - auch ohne die Nachrichten zu entschlüsseln - feststellen, wer für welchen Kandidaten gestimmt hat?

Aufgabe 3.2

Angenommen Bob verwendet den öffentlichen RSA-Schlüssel $(n, e) = (77, 17)$ und empfängt von Alice die Chiffre 42. Was ist der Klartext von Alice?

Aufgabe 3.3

Seien p und q zwei verschiedene Primzahlen, sei $n = p \cdot q$ und sei (n, e) der öffentliche Schlüssel für das RSA-Verfahren. Die Nachricht m werde zu $c = m^e \mod n$ verschlüsselt. Sei d das multiplikative Inverse von e, also der geheime Schlüssel.
Die Entschlüsselung lässt sich mithilfe des chinesischen Restsatzes beschleunigen. Wie könnte man dies realisieren?

Aufgabe 3.4

Berechnen Sie $2^{51} \mod 11$ mit der modularen Exponentiation.

Aufgabe 3.5

(a) Für alle $a \in \mathbb{Z}_{18}^*$ bestimme man $\langle a \rangle$.

(b) Welche Mächtigkeit haben diese Untergruppen?

(c) Gibt es eine Primitivwurzel von $\mathbb{Z}_{18}^*$? Falls ja, geben Sie alle möglichen Primitivwurzeln an. Falls nein, begründen Sie, warum es keine gibt.

(d) Welche der folgenden Gruppen sind zyklisch:

$$\mathbb{Z}_{30}^*, \mathbb{Z}_{27}^*, \mathbb{Z}_{125}^*, \mathbb{Z}_{101}^*, \mathbb{Z}_{64}^*?$$

Aufgabe 3.6

Wenn man eine Primitivwurzel a modulo 29 sucht, welches Kriterium sollte a erfüllen? Geben Sie ein solches a an.