Übung zur Vorlesung
Kryptokomplexität IIBearbeitungszeit: 23. April bis 3. Mai
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1 (10 Punkte): Faktorisierungsangriffe auf RSA

- (a) Sei $x^2 + a_1x + a_0 = 0$ eine quadratische Gleichung mit den Koeffizienten a_0 und a_1 , und den Lösungen p und q .
- ▶ Zeigen Sie, dass $p + q = -a_1$ und $p \cdot q = a_0$ gilt.
- (b) Gegeben seien jeweils ein RSA-Modul $n \in \mathbb{N}$ und die zugehörige Zahl $\varphi(n)$, wobei φ die Euler-Funktion ist.
- ▶ Faktorisieren Sie jeweils n .
- (i) $n = 72487$, $\varphi(n) = 71896$,
- (ii) $n = 81061$, $\varphi(n) = 80172$.

Aufgabe 2 (10 Punkte): Fälschung von RSA-SignaturenErich fängt die folgenden RSA-signierten Nachrichten $(m_i, \text{sig}_A(m_i))$ von Alice ab:
$$\langle 576, 102 \rangle, \langle 215, 1595 \rangle, \langle 338, 764 \rangle, \langle 59, 1130 \rangle, \langle 512, 339 \rangle, \langle 26, 988 \rangle, \langle 532, 1392 \rangle.$$
Der öffentliche Schlüssel ist $(n, e) = (1961, 7)$.

- (a) ▶ Führen Sie den *Chosen-Plaintext*-Angriff aus der Vorlesung für alle $r \in \{1, 2, 3\}$ durch und wählen Sie $e_i = 1$ für alle i .
- (b) Nehmen Sie an, alle Nachrichten seien mit Blocklänge 2 über dem kanonischen Alphabet $\Sigma = \{A, B, \dots, Z\}$ kodiert.
- ▶ Ergeben die Nachrichten von Alice und/oder die gefälschte Nachricht von Erich aus Aufgabenteil (a) Sinn?

Aufgabe 3 (10 Punkte): Primitive Elemente I

- (a) ► Bestimmen Sie alle primitiven Elemente in $\mathbb{Z}_{19}^*$ und $\mathbb{Z}_{65}^*$.
- (b) ► Bestimmen Sie das kleinste primitive Element in $\mathbb{Z}_{89}^*$.
- Wie viele primitive Elemente gibt es in $\mathbb{Z}_{89}^*$?

Aufgabe 4 (10 Punkte): Primitive Elemente II

Sei p eine Primzahl mit $p \equiv 1 \pmod{4}$.

► Zeigen Sie:

Wenn γ ein primitives Element in $\mathbb{Z}_p^$ ist,
dann ist auch $p - \gamma$ ein primitives Element in $\mathbb{Z}_p^*$.*