Übungen zur Kryptologie

Blatt 2 SoS 2024 — H. Kiechle

Präsenzaufgaben

4. Wir betrachten die Restklassen mod 9, also die Menge $\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \ldots, \overline{8}\}$.

(a) Erstellen Sie eine Verknüpfungstafel für die Multiplikation in $\mathbb{Z}_9$.

(b) Bestimmen Sie

i. das neutrales Element e;

ii. alle invertierbaren Elemente.

Was ist also $\mathbb{Z}_9^\times$?

Hausaufgaben

5. *Fortsetzung von Aufgabe 4*

(a) Erstellen Sie eine Verknüpfungstafel für die Multiplikation $\cdot_9$ auf $\mathbb{Z}_9^\times$.

(b) Geben Sie zu jedem Element aus $\mathbb{Z}_9^\times$ das Inverse an.

(c) Zeigen Sie, dass $\left(\mathbb{Z}_9^\times, \cdot_9\right)$ eine Gruppe bildet.

(d) Berechnen Sie alle Potenzen von $\overline{2}$ und $\overline{3}$. Was fällt auf?

6. Wählen Sie einen Text in deutscher Sprache mit ca. 200 Buchstaben (Umlaute und „ß“ wie üblich ersetzt; keine Leerzeichen; alles klein geschrieben). Der Text aus Aufgabe 3 ist so gesetzt und hat ungefähr diese Länge.

Verschlüsseln Sie ihren Text mit der Vigenère-Chiffre unter Verwendung eines selbst gewählten Schlüssels der Länge höchstens 10.

Bitte geben Sie neben dem verschlüsselten Text auch den Klartext und das Schlüsselwort mit ab.

Hinweis: Wir werden den verschlüsselten Text für die kommenden Übungen brauchen! Deshalb wäre es hilfreich, wenn Sie ihn in elektronischer Form vorliegen haben.