FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2024/25
09.10.2024

2. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Ist die Menge aller Vigenère-Verschlüsselungen eine (ggf. kommutative) Gruppe, wenn man als Verknüpfung die Hintereinanderausführung der Verschlüsselung nimmt?

Übung 2

a) Bestimmen Sie das inverse Element zu 15 in $\mathbb{Z}_{20}$ mit „$\oplus$“, und lösen Sie damit die Gleichung $15 \oplus x = 2 \bmod 20$.

b) Bestimmen Sie das inverse Element zu 3 in $\mathbb{Z}_5 \setminus \{0\}$ mit „$\odot$“, und lösen Sie damit die Gleichung $3 \odot x = 4 \bmod 5$.

c) Bestimmen Sie das inverse Element zu $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$ in der Gruppe der invertierbaren 2×2-Matrizen mit „$\cdot$“, und lösen Sie damit die Gleichung $A \cdot X = \begin{pmatrix} 2 & -1 \\ 4 & 0 \end{pmatrix}$.

Übung 3

a) Was besagt Satz 1.3 angewendet
   - auf die Gruppe $\mathbb{Z}_5 \setminus \{0\}$ mit „$\odot$“,
   - auf die Gruppe $\mathbb{Z}_7 \setminus \{0\}$ mit „$\odot$“?

   Geben Sie Beispiele an!

b) Was besagt Satz 1.3 angewendet auf die Gruppe aller Caesar-Verschiebungen bzw. aller monoalphabetischen Verschlüsselungen?

Zusatzaufgabe (für Knobler)

Sei $M = \{\blacksquare, \bigstar, \blacktriangle\}$.

Konstruieren Sie eine Verknüpfungstabelle für M, so dass man eine Gruppe erhält.

Wieviel Möglichkeiten haben Sie?