FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2025/26
17.12.2025

11. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Bestimmen Sie alle Primitivwurzeln modulo 13.

Übung 2

Bestimmen Sie die folgenden diskreten Logarithmen in $\mathbb{Z}_{13}^{\times}$:

a) $\log_2 6$ b) $\log_6 7$ c) $\log_2 7$.

Übung 3

In den reellen Zahlen gilt $\log_a b \cdot \log_b c = \log_a c$.

Eine ähnliche Gleichung gilt auch für diskrete Logarithmen. Welche?

Übung 4

Alice und Bob vereinbaren einen gemeinsamen geheimen Schlüssel mittels des Diffie-Hellman-Schlüsselaustauschs. Sie einigen sich auf $p = 37$ und $g = 5$.

Alice wählt $\alpha = 12$, Bob $\beta = 23$. Welche Zahlen werden öffentlich ausgetauscht? Wie lautet die gemeinsame geheime Zahl?

Übung 5

Ist der Diffie-Hellman-Schlüsselaustausch in der Gruppe $(\mathbb{Z}_m, +)$ sicher?

Übung 6

Sei p eine (große) Primzahl und g eine Primitivwurzel.

Ist $f : \mathbb{N} \to \mathbb{Z}_p,\ n \mapsto g^n \bmod p$

a) eine Einwegfunktion,

b) kollisionsresistent,

c) eine kryptografische Hashfunktion?