FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
25.10.2023

4. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Berechnen Sie mit dem euklidischen Algorithmus

a) $\gcd(282, 252)$,

b) $\gcd(87, 20)$,

c) $\gcd(122354, 267371)$.

Übung 2

a) Bestimmen Sie ein multiplikatives Inverses zu $a = 25$ in $\mathbb{Z}_{61}$.

b) Gibt es ein multiplikatives Inverses zu $a_1 = 14$ bzw. zu $a_2 = 20$ in $\mathbb{Z}_{45}$?

c) Für welche $a \in \mathbb{Z}_m$ gibt es multiplikative Inverse?

d) Folgern Sie aus c): m ist eine Primzahl. $\Rightarrow$ $\mathbb{Z}_m \setminus \{0\}$ ist bzgl. $\odot$ eine Gruppe.

Übung 3

Welche der folgenden Gleichungen sind lösbar? Geben Sie im Falle der Lösbarkeit mit Hilfe des euklidischen Algorithmus eine Lösung (zwischen 0 und dem entsprechenden Modul) an.

a) $25 \cdot x = 13 \bmod 61$,

b) $252 \cdot x = 48 \bmod 282$,

c) $9 \cdot x = 13 \bmod 25$.

d) $24 \cdot x = 9 \bmod 42$.

An zwei Stellen oben berechnet man im Prinzip zunächst das multiplikative Inverse. Wo?

Übung 4

Die (affine) Tauschchiffre ist eine monoalphabetische Chiffrierung, bei der ein Klartextbuchstabe k (interpretiert als Zahl $\in \{0, \ldots, 25\}$) ersetzt wird durch $c := a \cdot k + b \bmod 26$, wobei die konkret gewählten a und b den Schlüssel darstellen.

Welche a, b sind geeignet, d.h. für welche a, b ist die Zuordnung Klartextbuchtstabe $\leftrightarrow$ Geheimtextbuchstabe eineindeutig?