FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
29.11.2023

8. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Aus $p = 31$ und $q = 17$ soll ein RSA-Schlüssel mit kleinst-möglichem e gebildet werden. Wie lautet der öffentliche und wie der private Teil des Schlüssels?

Übung 2

Alice hat einen RSA-Schlüssel zu $n = 29 \cdot 31$ und veröffentlicht $e = 23$.

a) Welchen geheimen Schlüssel hat Alice?

b) Wie lautet die verschlüsselte Nachricht c zum Klartext $m = 6$?

c) Verifizieren Sie, dass die Entschlüsselung von c (aus b)) wieder m ergibt.

d) Verifizieren Sie, dass auch zu $m = 58$ (nicht teilerfremd zu n) die Ver- und Entschlüsselung wieder m ergibt.

e) Was ergibt sich bei der Ver- und Entschlüsselung von $m = 1000$?

Übung 3

Wie sieht das RSA-Verfahren aus, wenn man als zugrunde liegende Gruppe $\mathbb{Z}_{100}$ mit „+“ wählt? (Vgl. Skript S. 29.)

Wie sieht die Ver- und Entschlüsselung zu $e = 11$ und $m = 31$ aus? Was ist dann konkret das Entschlüsselungs-d?

Übung 4

Es soll ein RSA-ähnliches Verfahren RSA^3 entwickelt werden, basierend auf drei Primzahlen p, q und r. Der RSA^3-Modul wird dann $n = p \cdot q \cdot r$.

a) Wie muss zu einem Verschlüsselungs-Exponenten e das zugehörige (private) d bestimmt werden, damit man eine Verschlüsselung $c = m^e \bmod n$ wieder durch $m = c^d \bmod n$ ($m \in \mathbb{Z}_n^\times$) entschlüsseln kann?

b) Ist Ihrer Meinung nach RSA^3 sicherer als das übliche RSA mit ähnlich großem Modul n?