Vorlesung Netzwerksicherheit – Sommersemester 2022

**4. Übungszettel**

Abgabe bis Dienstag, 10. Mai 2022 – 16:00 Uhr  
Besprechung: Dienstag, 10. Mai 2022

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

Abgabe via Artemis: [https://alpro.besec.uni-bonn.de](https://alpro.besec.uni-bonn.de/)

**Aufgabe 1 (6 Punkte)**

Geben Sie die ASN1-Struktur an für:

1. RSA Public Key (PKCS#1)
2. Public Key (PKCS#8)
3. Private Key (PKCS#8)

**Aufgabe 2 (3 Punkte)**

Stellen Sie den folgenden Text entsprechend der IA5-Zeichentabelle dar und geben diesen in Hexadezimal-Darstellung an:

Max und Moritz machten beide,

Als sie lebten, keinem Freude:

Bildlich siehst du jetzt die Possen,

Die in Wirklichkeit verdrossen,

Mit behaglichem Gekicher,

Weil du selbst vor ihnen sicher.

Aber das bedenke stets:

Wie man's treibt, mein Kind, so geht's.

**Aufgabe 3 (6 Punkte)**

*Hinweis: Diese Aufgabe soll auf Artemis bearbeitet werden. Dort finden sie auch die Python-Datei.*

Ergänzen Sie das Entschlüsselungsverfahren für RSA in RSA\_decrypt.py und entschlüsseln Sie den in CIPHER enthaltenen Text mit dem gegebenen Schlüssel.

Tipp: In Python lässt sich die Potenzierung modulo z effizient mit pow(x,y,z) implementieren.

**Aufgabe 4 (5 Punkte)**

Erzeugen Sie ein RSA-Schlüsselpaar mit OpenSSL (oder einem alternativen Werkzeug Ihrer Wahl).

1. Geben Sie die ASN1-Darstellung des öffentlichen Schlüssels an.
2. Signieren Sie die Abgabe-PDF mit ihrem privaten Schlüssel. Laden Sie auf Artemis eine ZIP-Datei hoch, welche die Abgabe-PDF sowie den Public-Key und die Signatur jedes Gruppenmitglieds enthält. Es muss also jedes Gruppenmitglied die Abgabe-PDF signieren.