Vorlesung Netzwerksicherheit – Sommersemester 2021

**4. Übungszettel**

Abgabe: Bis Dienstag, 18. Mai 2021 – 16:00 Uhr  
Besprechung: Dienstag, 18. Mai 2021

Abgabe via Artemis

**Aufgabe 1 ( 3 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 (5 Punkte)**

Stellen Sie den folgenden Text entsprechend der IA5-Zeichentabelle dar und geben diesen in Hexadezimaler Darstellung in Ihrer Abgabe 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)**

1. 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. Der fertige Code kann auf Artemis hochgeladen werden.

**Aufgabe 4 (6 Punkte)**

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

1. Geben Sie in Ihrer Textabgabe die ASN1-Darstellung des öffentlichen Schlüssels an.
2. Übermitteln Sie Ihren Public-Key in einer separaten Datei mit der Abgabe und signieren Sie mit Ihrem privaten Schlüssel Ihren Abgabetext. Laden Sie die Signaturdatei bitte ebenfalls separat hoch. (Hinweis: Diese Aufgabe muss von jedem Übungs-Partner durchgeführt werden. Es muss also jeder Übungspartner Ihre Abgabe signieren und Public-Key und die erstellte Signatur auf Artemis hochladen.)