Vorlesung Netzwerksicherheit – Sommersemester 2023

4. Übungszettel

Abgabe bis Dienstag, 16. Mai 2023 – 16:00 Uhr
Besprechung: Dienstag, 16. Mai 2023

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

Handschriftliche Abgaben werden nicht bewertet

Abgabe via Artemis: https://alpro.besec.uni-bonn.de

Aufgabe 1 (6 Punkte)

Geben Sie die ASN1-Struktur an für:

a) RSA Public Key (PKCS#1)
b) Public Key (PKCS#8)
c) 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).

a) Geben Sie die ASN1-Darstellung des öffentlichen Schlüssels an.
b) 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.