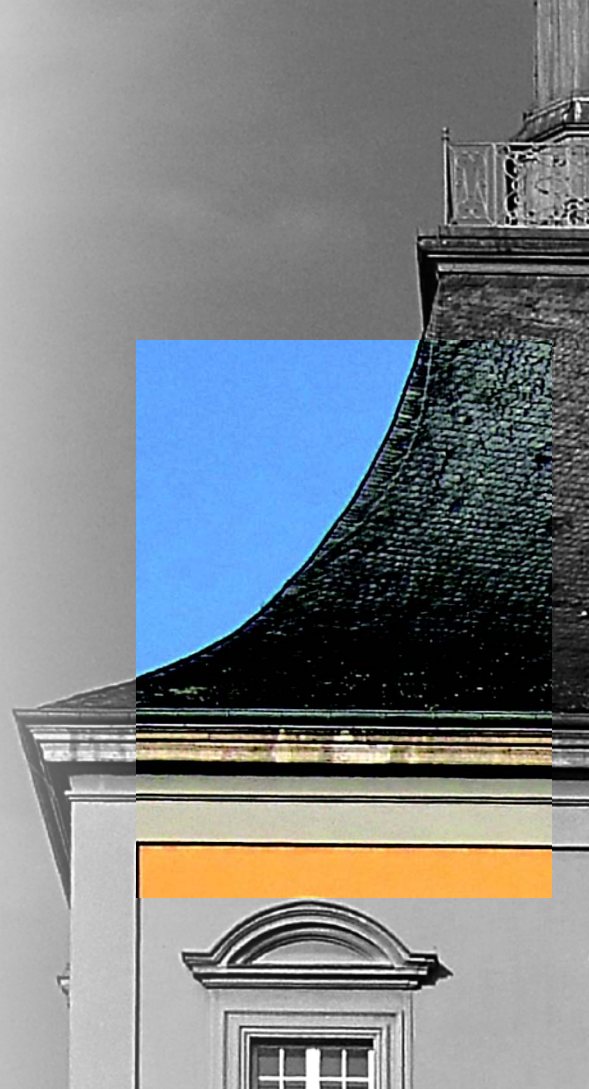
UNIVERSITÄT BONN

ÜBUNG
NETZWERKSICHERHEIT

SOMMERSEMESTER 2020

DI. 16-18 UHR



UNIVERSITÄT BONN

4. ÜBUNGSBLATT – AUFGABE 1

- Geben Sie die ASN1-Struktur an für

  a) RSA Public Key (PKCS#1)

  b) Public Key (PKCS#8)

  c) Private Key (PKCS#8)

UNIVERSITÄT BONN

4. ÜBUNGSBLATT – AUFGABE 2

- 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.

UNIVERSITÄT BONN

4. ÜBUNGSBLATT – AUFGABE 3

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

  a) Geben Sie in Ihrer Abgabe die ASN1-Darstellung des öffentlichen Schlüssels an.

  b) Übermitteln Sie Ihren Public-Key in einer separaten Datei mit der Abgabe und signieren Sie mit Ihrem privaten Schlüssel Ihre Abgabedatei vor dem Versand. Die Signaturdateien senden Sie bitte ebenfalls separat.

  (Hinweis: Diese Aufgabe muss von jedem Übungs-Partner durchgeführt werden. Es muss also jeder Übungspartner Ihre Abgabe signieren und per E-Mail den Public-Key und die erstellte Signatur senden.)