FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik
Prof. Georg Hoever

WS 2025/26
zu bearbeiten bis
17.12.25

Praktikum 4
zur Vorlesung Kryptologie

Ziel ist die Versendung einer signierten und verschlüsselten Datei. Dazu soll die kleine RSA-Schlüsselverwaltung, die auf meiner Internetseite entstanden ist, verwendet werden.

1. Wählen Sie eine Datei, die Sie versenden möchten.
2. Signieren Sie Ihre Datei unter Verwendung von SHA256. Nutzen Sie zur Hashwert-Berechnung das kleine Programm, das auf meiner Internetseite bereit steht.

   Senden Sie mir Ihre Signatur zu.
3. Senden Sie mir Ihre Datei hybrid verschlüsselt zu unter Verwendung der Schlüssel auf der Internetseite und von AES mit (zufälligem) Schlüssel (*session-key*). Nutzen Sie zur AES-Verschlüsselung das kleine Programm, das auf meiner Internetseite bereit steht (mit der Option „verschlüsselt“, damit nicht ein *.exe-File produziert wird, das beim Versenden vom Mailserver geblockt wird).
4. Sie erhalten von mir eine Mail mit einer hybrid verschlüsselten Datei und einer entsprechenden Signatur.

   Überprüfen Sie die Signatur und mailen mir, ob Sie die Signatur erfolgreich verifizieren konnten.

Tipp, falls Sie mit Aribas arbeiten:

In Aribas können Sie Hex-Zahlen einlesen, indem Sie der Hexzahl (ohne Leerzeichen) „0x“ voranstellen.
Mit dem Befehl `set_printbase(16)` erhalten Sie alle folgenden Ausgaben in Hex-Form.
Mit `set_printbase(10)` kann man wieder auf dezimale Ausgabe umstellen.