

Übung 1

IT-Sicherheit

10.3.2026

Elektronische Abgabe bis 30.4.26 an gerrit.kalkbrenner@hwr-berlin.de.
Verfassen Sie bitte eine Email mit allen nachfolgend beschriebenen Inhalten.

Aufgabe 1: Installieren Sie OpenSSL auf Ihrem Notebook, PC oder Smartphone. Machen Sie sich mit den Funktionen und ihrer Benutzung vertraut.

Aufgabe 2: Erstellen Sie eine Datei, in der Ihr Name und in der zweiten Zeile Ihre HWR-Email-Adresse gespeichert sind. Erstellen Sie von dieser Datei einen kryptographischen Fingerabdruck mit den Verfahren MD5 und SHA3-256. Speichern Sie die Datei selbst und die beiden Fingerabdrücke in der oben genannten Email.

Aufgabe 3: Chiffrieren Sie die in Aufgabe 2 erstellte Datei mit AES256. Als Schlüssel verwenden Sie bitte Ihre email-Adresse. Speichern Sie die Chiffre in der oben genannten Email.

Aufgabe 4: Recherchieren Sie, welche Krypto-Software es aktuell weiterhin für SHA, AES, RSA und TLS für die Betriebssysteme Windows, MacOS und Linux gibt. Fassen Sie das Ergebnis in einer Tabelle zusammen. Speicherung in der oben genannten Email.

Aufgabe 5: Generieren Sie einen öffentlichen und einen privaten RSA1024 Schlüssel. Speichern Sie Ihren öffentlichen Schlüssel in der oben genannten Email.

Aufgabe 6: Signieren Sie die Datei aus Aufgabe 2. Speichern Sie die Signatur in der oben genannten Email.

Aufgabe 7: Recherchieren Sie, welche Anbieter derzeit kostenlos Ihren öffentlichen Schlüssel hosten.

(10 Punkte)