Sichere Programmierung — Praktikum 4

Thema: Kryptographie mit Java — Wintersemester 2019/2020

Prof. Dr. Christoph Karg — Hochschule Aalen

In diesem Praktikum werden die in der Vorlesung vermittelten Kenntnisse in der Programmierung mit der Kryptographie-API von Java angewendet.

Aufgabe 1 (Kryptographische Hashfunktion).

a) Erstellen Sie anhand des Code Fragments der Vorlesung ein komplettes Beispiel der Nutzung von SHA-256. Das Beispiel soll die Erzeugung einer Prüfsumme und die Verifikation der Prüfsumme enthalten.

b) Dokumentieren Sie die Funktionsweise Ihrer Implementierung.

Aufgabe 2 (Symmetrische Verschlüsselung).

a) Erstellen Sie anhand des Code Fragments der Vorlesung ein komplettes Beispiel der Nutzung von AES-256 im CBC-Mode. Das Beispiel soll die Ver- und Entschlüsselung eines Klartexts sowie die Generierung eines zufälligen Schlüssels enthalten.

b) Dokumentieren Sie die Funktionsweise Ihrer Implementierung.

Aufgabe 3 (Asymmetrische Verschlüsselung).

a) Erstellen Sie anhand des Code Fragments der Vorlesung ein komplettes Beispiel der Nutzung von RSA. Das Beispiel soll die Ver- und Entschlüsselung eines Klartexts sowie die Generierung eines zufälligen Schlüssels enthalten.

b) Dokumentieren Sie die Funktionsweise Ihrer Implementierung.

Aufgabe 4 (Digitale Signatur).

a) Erstellen Sie anhand des Code Fragments der Vorlesung ein komplettes Beispiel der Nutzung des RSA-SHA256-Signaturverfahrens. Das Beispiel soll die die Signierung eines Textes und die entsprechende Überprüfung der Signatur beinhalten.

b) Dokumentieren Sie die Funktionsweise Ihrer Implementierung.