Fachhochschule Rosenheim
Fachbereich Informatik
Prof. Dr. R. Hüttl

IT-Security

Übung 2

In dieser Übung schreiben wir ein Java Programm zur Verschlüsselung einer Datei. Wir verwenden dabei die Basistechnologien, die im JDK enthalten sind

Aufgabe 1: Verschlüsseln der Daten

Erweitern sie die gegebene Java Klasse **Encryption** an den markierten Stellen. Die Klasse soll eine Datei verschlüsseln. Die einzelnen Verarbeitungsschritte sind in folgenden Methoden implementiert:

- Einlesen einer Datei in ein Byte-Array.
- Generierung eines Schlüssel für den symmetrischen Algorithmus **AES**
- Verschlüsseln sie der eingelesenen Datei mit dem Algorithmus **AES**, dem Verschlüsselungs-Modus **ECB** und dem Padding **PKCS5Padding**
- Speicherung des Schlüssel Base64 kodiert in einer Datei
- Speicherung der verschlüsselten Daten Base64 kodiert in einer Datei

Aufgabe 2: Entschlüsseln der Daten

Erweitern sie die gegebene Klasse Decryption an den markierten Stellen. Die Klasse soll eine verschlüsselte Datei aus Aufgabe 1 wieder entschlüsseln. Die einzelnen Verarbeitungsschritte sind in folgenden Methoden implementiert:

- Einlesen des Base64 kodierten Schlüssel
- Einlesen der Base64 kodierten Daten
- Initialisierung der notwendigen Klassen zur Entschlüsselung und Entschlüsselung der Daten

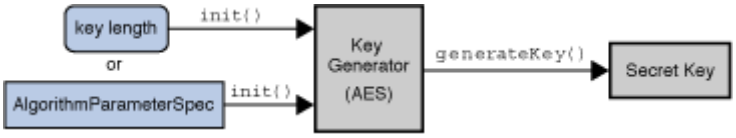
Aufgabe 3: Schreiben sie einen Testtreiber mit JUnit zum Test der Verschlüsselung

- Lesen sie eine Datei ein, verschlüsseln sie diese Datei mit einem generierten Schlüssel und speichern sie die Ergebnisse ab.
- Lesen sie die verschlüsselte Datei und den Schlüssel wieder ein und entschlüsseln die Datei.
- Überprüfen sie das Ergebnis

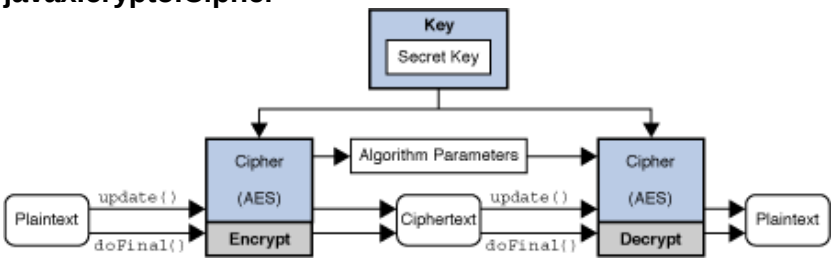
Hinweise:

- Unter folgenden URLs finden sie Hilfen:
  https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html
  http://download.oracle.com/javase/8/docs/technotes/guides/security/

- Folgende Interfaces und Klassen sind notwendig:
  javax.crypto.SecretKey
  javax.crypto. KeyGenerator



javax.crypto.Cipher



- Zur Base64 Kodierung / Dekodierung verwenden sie die Klassen aus dem Paket **java.util.Base64.**

- Wenn die Schlüssellänge für AES länger als 128 Bit sein soll (z.B. 256) dann muss man
  - einen JDK 9 oder höher verwenden oder
  - die JCE Unlimited Strength Jurisdiction Policy Files installieren (siehe http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html). Die Dateien sind in der Vorgabe und müssen in das JRE oder JDK Verzeichnis (unter lib/security) kopiert werden (im Labor bereits installiert).