Technische Hochschule Rosenheim
Fakultät für Informatik
Prof. Dr. Reiner Hüttl

IT-Security

Exercise 2

In this exercise, we will write a Java program to encrypt a file. We use the basic technologies contained in the JDK

Task 1: Encrypt the data

Extend the given Java class ***Encryption*** at the marked places. The class provides methods to encrypt a file. The individual processing steps are implemented in the following methods:

- Read a file into a byte array.
- Generate a key for the symmetric **algorithm AES**
- Encrypt the scanned file with the **AES** algorithm, the **ECB** encryption mode and the **PKCS5Padding**
- Store the Base64 encoded key in a file
- Store the encrypted data Base64 encoded in a file

Task 2: Decrypt the data

Expand the given class ***Decryption*** at the marked places. The class provides methods to decrypt an encrypted file from task 1. The individual processing steps are implemented in the following methods:

- Read the Base64 encoded key
- Read the Base64 encoded data
- Initialize the necessary classes to decrypt and decrypt the data

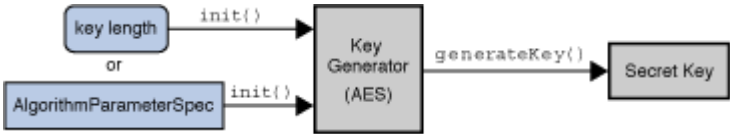
Task 3: Write a test driver with JUnit to test the encryption

- Read a file, encrypt the file with a generated key and save the results.
- Read the encrypted file and the generated key and decrypt the file.
- Verify the result

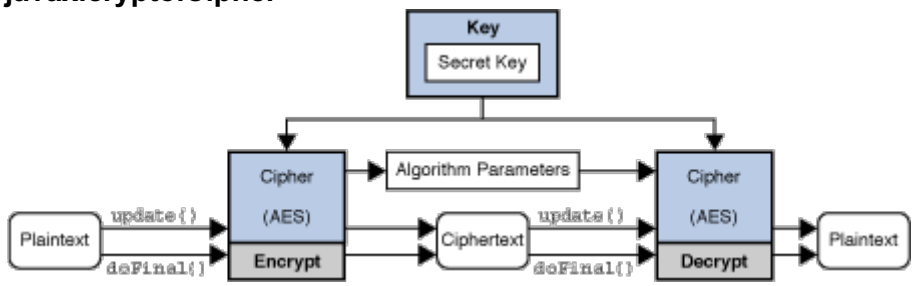
Hints:

- You can find help atthe following URLs:
  https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html
  http://download.oracle.com/javase/8/docs/technotes/guides/security/

- The following interfaces and classes are necessary:
  javax.crypto.SecretKey
  javax.crypto. KeyGenerator



javax.crypto.Cipher



- For Base64 encoding / decoding use the classes from the **package java.util.Base64.**
- If the key length for AES should be longer than 128 bits (e.g. 256) then you have to
  - use a JDK 9 or higher, or
  - install the JCE Unlimited Strength Jurisdiction Policy Files (see http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html).
    The files must be copied to the JRE or JDK directory (under lib/security).