SAP Exam – February 2021

Java

Evaluation:

- The solution is obtained by writing the source code in the exam template, ***YourNameExam.java***.
- **DO NOT change** the given methods signature
- Each solution must provide a package name in this format ***ism.ase.ro.sap.exam.lastName.firstName***
- ***The solution must generate each result on its own. Using hardcoded values (obtained from other students) is not allowed (the solution will be evaluated with 0)***
- To get each requirement points you need to provide an error free (0 compiler errors) program that generates/displays correct results. Incorrect or partially correct solutions are not evaluated
- All solutions will be cross-checked with MOSS. Solutions that share more than 30% (except the given code) will be evaluated with 0.

To increase the security of your sensitive resources, all your employees are using passphrases to login for different services. Your system admin is using the passphrase stored in the Passphrase.txt file.

(5 p) In order to use this passphrase as a secret password you will compute its **SHA-1** value. That will be your access key. Print it on the screen to check it.

(10 p) The system admin is storing sensitive data in the **EncryptedData.data** file. Knowing that

- the file has been encrypted using AES in CBC mode please decrypt it
- The encryption **didn't use any padding** as the file length is ok.
- The IV value is also known because **it is stored at the beginning of the encrypted file**.
- The encryption key is equal with the first 128 bits of the previous SHA1 hash value

Let's suppose that the obtained plaintext is named ***OriginalData.txt***.

(10 p) In the end you want to digitally sign (using RSA digital signature) the obtained plaintext ***OriginalData.txt***. Your private key, named **sapexamkey**, is stored in the Java Key store file, **sap_exam_keystore.ks.** The key password and the keystore password are stored in the ***OriginalData***.txt file that you decrypted earlier.

The obtained digital signature must be stored in the **DataSignature.ds** file. It will be used by others to check the file.

Upload

- **the .java file with your solution**
- ***OriginalData.txt***
- ***DataSignature.ds***