SAP Exam – July 2019

Student name: _____ Year:_____

C++ (20p)

(10 pts) 1. Write the source code to compute the message digest of the text saved by Message.txt. Message Digest scheme is SHA-256. Print the computed SHA-256 message digest as hexa-decimal letters into the application running console.

(10 pts) 2. Write the source code to encrypt the message digest SHA-256 computed before. The encryption scheme is a DES family one. DES keys are set by yourself. Print the encrypted SHA-256 message digest as hexa-decimal letters into the application running console.

Java (20p)

A company is trying to implement a secure solution for online communication. For that, the IT admin chooses to encrypt the data using AES with a 128 bit key using ECB mode.

In order to send the symmetric key to the client, the company is using a PKI based solution. The AES key is stored encrypted in the **ClientISM.key** binary file. The key is encrypted using the client RSA public key available in the **SAPCertificateX509.cer.**

In order to assure the client that the key will not be tempered, the admin is sending a separate message the SHA-1 message digest of the **ClientISM.key file.**

(5 p) 1. Please generate and display in Hex format, the SHA-1 value of the **ClientISM.key** file.

(10 p) 2. Using the client private key, stored in the Java keystore **sapkeystore.ks**, decrypt the key file and extract the key plaintext value (and display it as String).

(5p) 3. Once the client receives the symmetric password, decrypt the **Comm.enc** file (encrypted with the AES key in ECB mode with PKCS5 padding)

The keystore has been generated using these commands:

keytool.exe -genkey -keyalg RSA -alias sapkey1 -keypass sapex2016 -storepass passks -keystore sapkeystore.ks -dname "cn=Catalin Boja, ou=ISM, o=IT&C Security Master, c=RO"

keytool.exe -export -alias sapkey1 -file SAPCertificateX509.cer -keystore sapkeystore.ks -storepass passks