#1116 ISM Challenge (OpenSSL in C/C++ implementations), January 20, 2022

Consider you have:

- Encrypted files ***Session_key.enc*** and ***message.enc***.
- A private key ***sStudent.pem*** as the paired key for that used to get ***Session_key.enc***.
- Digital signature file ***file.sign***.
- A public key ***pISM.pem*** as the paired key for that used to get ***file.sign***.

Write a C/C++ application (one single source code file) by using the OpenSSL library to:

- Decrypt ***Session_key.enc*** to get the plaintext content as an AES-CBC key. Print the key content in hexa into the Console Application. **(5 points)**

- Validate the AES-CBC key is the intended one by using ***file.sign***. Print the validation statement into the Console Application. Message digest algorithm used was SHA-256, and the encryption used was RSA, PKCS1 padding. **(5 points)**

- Decrypt ***message.enc*** by using AES-CBC with the restored and validated AES key. The IV has value 0x01 for each byte. Print out to Console Application the plaintext after decryption. **(5 points)**

All the solutions will be cross-checked with MOSS from Stanford and the very similar source code files (over 50%) will not be evaluated.