#3 ISM Challenge (OpenSSL in C/C++)

Consider you have:

- Encrypted files ***Session.key***, ***message1.enc***, ***message2.enc***, and ***message3.enc***.
- A private key ***sStudent.pem*** as the paired key for that used to get ***Session.key***.
- Digital signature files ***sfile.sign*** and ***mfile.sign***.
- A public key ***pISM.pem*** as the paired key for that used to get ***sfile.sign*** and ***mfile.sign***.

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

- Decrypt ***Session.key*** to get the plaintext content as an AES-CBC key. Print the key content in hexa into the Console Application.
- Validate the AES-CBC key is the intended one by using ***sfile.sign***. Print the validation information into the Console Application. Message digest algorithm used was SHA-256, and the encryption used was RSA, PKCS1 padding.
- Decrypt the all three messages by using AES-CBC with the restored validated key. Pick up the right one by checking ***mfile.sign***. Print the file name into the Console Application. Message digest algorithm used was SHA-256, and the encryption used was RSA, PKCS1 padding. The IV has value 0x01 for each byte.
- Encrypt a file contains: your name, the name of the right plaintext file (e.g. message1). The encrypted output will be saved in a separate file. Encrypt algorithm is AES-CBC by using the key obtained above and the IV specified above.

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