ISM Exam February 5, 2021 (OpenSSL in C/C++)

Consider you have:

- Digital signature file ***hfile.sign***.
- A public key ***pExam.pem*** as the RSA 1024 paired key for that used to get ***hfile.sign***.
- A list of password candidates in ***wordlist.txt***.

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

- Decrypt ***hfile.sign*** to get the plaintext content as an **SHA-256**. The used padding is **PKCS1**. **(5 p)**
- Encrypt each password candidate from ***wordlist.txt***. Each encrypted password candidate will be saved as hex representation into ***enclist.txt*** for each corresponding line. The encryption algorithm is **AES-CBC 128 bits**, where the key is the first half of the SHA-256 obtained at previous bullet. The **IV** content is { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08 }. **(10 p)**
- Encrypt the file ***enclist.txt*** according to **RSA** scheme with **PKCS1**. **(5 p)**
- Compute SHA-1 for ***enclist.txt***. **(5 p)**

The application will print into the runtime output console:

- SHA-256 obtained from ***hfile.sign*** as hex representation.
- SHA-1 computed for ***enclist.txt*** as hex representation.

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