ISM Exam, February 3, 2023 (OpenSSL in C/C++)

Consider you have a list of pre-defined passwords stored by your database available in ***wordlist.txt***. Develop a C/C++ application using OpenSSL as 3rd party crypto library for the below requirements.

1. In order to secure the users' credentials, you have to apply ***SHA-256*** for all the passwords stored by the text file.

The hashed content must meet the following requirements **(10p)**:

- To be saved into a separate text file named as ***hashes.txt***.
- Each line of the output file ***hashes.txt*** represents the hexadecimal format of the hashed content for the password stored on the same line within the input password file.

2. In ***hashes.txt*** each line is encrypted by using the AES-CBC-256 scheme. The ***IV*** and ***AES-256*** key are stored by the binary file named ***aes-cbc.bin***, where IV is first and it is followed by AES-256 key.

The encrypted content must meet the following requirements **(10p)**:

- To be saved into a separate text file named as ***enc-sha256.txt***.
- Each line of the output file ***enc-sha256.txt*** represents the hexadecimal format of the encrypted SHA-256 stored on the same line in ***hashes.txt***.

3. Generate the digital signature for the file ***enc-sha256.txt*** and save that signature into a file called ***esign.sig***. The message digest algorithm is ***SHA-256***, and the 1024-bit RSA key for signature generation is stored in a PEM file named as ***rsa-key.pem***. **(5p)**

Write a C/C++ application to implement the above requirements (one single C/C++ source code file).

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