ISM Exam, January 26, 2024 (OpenSSL in C/C++) (4,5p)

Implement a C/C++ application for the following requirements:

1. Create a file named as ***name.txt*** to store your full name in text format. Compute and print out a **SHA-256** hash value into the running application console. The **SHA-256** value will be displayed in hex format. **(0,5p)**

2. Encrypt the file ***name.txt*** using **AES-256** in **CBC** mode **(2p)**:

- **IV** provided by the text file ***iv.txt*** and having the hex format to be imported into an internal buffer as binary format.
- AES-256 bit key provided by the binary file named as ***aes.key***.

The output encrypted file will be named as ***enc_name.aes***. No other data will be encrypted (e.g. IV, plaintext length and so forth) besides the content of ***name.txt***.

3. To ensure the destination that no one is tampering with that value, digitally sign (computed for the above SHA-256) the previous encrypted binary file with a **RSA-1024** bit private key generated by your application. Store the signature in another binary file named ***digital.sign***. **(2p)**

Use the RSA-1024 bit private key to sign the file ***name.txt***. Upload your binary signature file (***digital.sign***) together with the RSA-1024 bit public key file.

To get the points, the digital signature must be validated during the assessment.

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.