ISM Exam, July 2, 2024 (OpenSSL in C/C++)

Consider the following requirements to sign a plaintext and identify the right RSA private key for that signature **(2p)**:

1. Decrypt the files ***privateKey_1.enc, privateKey_2.enc*** and ***privateKey_3.enc*** to restore 3 RSA private keys by considering:

- AES-ECB as crypto algorithm for decryption.
- AES-ECB key in hex format:
  0xff, 0xff, 0xff, 0xff, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x10, 0x11, 0x12
- RSA private key size is 1024 bits.
- RSA private keys are in PEM format.
- The actual size of each PEM RSA restored key file is 887 bytes.

2. Use each PEM RSA restored private key to sign the plaintext ***in.txt*** by considering: **(2p)**:

- Message digest algorithm is SHA-256.
- Padding type is ***RSA_PKCS1_PADDING***.

3. Use the signature stored by ***eSign.sig*** to identify the right RSA private key used to generate it. Print out the information regarding the RSA private key used to generate ***eSign.sig***. **(0,5p)**

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.