ISM Exam, June 25, 2024 (OpenSSL in C/C++)

Consider the following requirements to verify a RSA signature **(1,75p)**:

1. Decrypt the file ***encrypted.aes*** to get the clear message by considering the following inputs:

- AES-CBC crypto algorithm.
- AES-CBC-128 bit key (hex format):
  0xff, 0xff, 0xff, 0xff, 0x00, 0x00, 0x00, 0x00, 0x08, 0x07, 0x06, 0x05, 0x00, 0x00, 0x00, 0x00
- IV (hex format):
  0xff, 0xff, 0xff, 0xff, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x10, 0x11, 0x12

2. Decrypt the file ***esign.sig*** contains a RSA signature by considering the following information **(1,75p)**:

- RSA-1024-bit key.
- File ***public.pem*** stores the RSA public key as PEM format.

3. Validate the signature against the clear message. Message digest algorithm is SHA-256. **(1p)**

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.