ISM Exam January 31, 2025 (OpenSSL in C/C++)

Consider you have:

- Digital signature file ***signature.sig***.
- A RSA key file named ***RSAKey.pem*** as the 1024-bit RSA key in PEM format.
- A list of password candidates in ***wordlist.txt***.

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

- Decrypt ***signature.sig*** to get the **SHA-256** message digest. The **RSA_PKCS1_PADDING** padding has been used to generate the RSA signature. Print out the hex format of **SHA-256 (1 p)**
- Compute the message digest according to **SHA-256** for each word candidate after adding the salt called **ISMsalt** at the end of the word candidate. Therefore, the input of hashing operation is the word candidate concatenated with the salt. **(1 p)**
- Compare each **SHA-256** message digest against the decrypted one. Print out the word candidate (without salt) together with the line number where it is stored in the file ***wordlist.txt*** when the comparison is true. **(1 p)**
- Encrypt the word candidate (without salt) found out at previous bullet. The result will be saved into ***word.enc***. The encryption algorithm is **AES-CBC 256 bits**, where the AES key is the **SHA-256** obtained/calculated above. The **IV** content is { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08 }. **(1,5 p)**

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