Secure Applications Programming

Please, provide the source cod files (C++ and Java) and the output resulted from each requirement for the following operations:

1. Decrypt ***key.sec*** file using the public key extracted from provided ***pubISM.pem*** file using OpenSSL in C++.

2. Decrypt ***Msg.enc*** file using the decrypted key.sec file content as AES key (CBC), using OpenSSL in C++.

3. Generate the message digest according to MD5 algorithm for the decrypted ***Msg.enc*** content, using a Java implementation. The first 16 bytes from ***Msg.enc*** are the IV used for MD5 algorithm.

4. Generate a ***X509*** digital certificate by using the public key stored by ***pubISM.pem*** file (Java implementation).

Aplication outputs (console window or output files):

C++: decrypted ***key.sec*** content (AES key), decrypted ***Msg.enc***.
Java: MD5 content, digital certificate storage file.