ISM Assignment 1 for C/C++ Secure Application Development

You have breached the adversary database and got both an encrypted password hash value and the AES ECB key. The encrypted hash value is given in the attached binary file (***pass.enc***) and the AES key is provided by the binary file ***aes.key***.

You know that your adversary is using one of the most 10 million used passwords available here https://weakpass.com/wordlist/1935 (download file ***ignis-10M.txt***).

You also know that they are using a technique that will make your rainbow tables useless because they add "***ismsap***" as a prefix to all user passwords and after that they hash them using SHA-256. The output from the SHA-256 step is encrypted using the key stored by the binary file ***aes.key***.

Write a simple C/C++ application that will brute force the adversary password by using the 3rd party development library OpenSSL. The C/C++ implementation should contain one single **.c** or **.cpp** file. **The source code file name must contain your name**. The C/C++ implementation must print out the corresponding password at the console without the prefix "***ismsap***".

The C development library OpenSSL can be downloaded from your ISM accounts (x86 Win version: https://portal.ism.ase.ro/mod/folder/view.php?id=450) as binary bundle.

All the solutions will be cross-checked with MOSS from Stanford. Solutions with a similarity of more than 50% will be canceled.