FIT 3173 Software Security
Week 2 Tutorial and Lab Sheet
Password Storage

I. Lab Discussion and Question

1. How to secure passwords in general application systems?
2. What are the suggested authentication guidelines in OWASP "Authentication Cheat Sheet" page? (accessible here: https://www.owasp.org/index.php/Authentication_Cheat_Sheet)
3. What are the guidelines provided in OWASP "Password Storage Cheat Sheet" page? (accessible here: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)
4. What are the possible uses of password-based cryptography?
5. What is the purpose of using salt? Should the value of the salt be kept secret? Why or why not?
6. Configure openssl library in your Ubuntu VM by running following commands:

```
cd openssl-1.0.1/
sudo ./config
sudo make
sudo make test
sudo make install
```

7. Copy the **pass_hash.c** into Home folder
   Open a new terminal and run following commands to obtain results:

```
gcc -I /usr/local/ssl/include/ -L /usr/local/ssl/lib/ -o
pass_hash pass_hash.c -lcrypto -ldl
./pass_hash
```

8. Change the password and iteration count in the **pass_hash.c** file and recompile the program
   Change the hash function from SHA256 and SHA512 (you need to change other variables in the program accordingly otherwise you may encounter errors).
9. What is the purpose of the iteration count?

II. Extension Questions:

1. Check the openssl library document on symmetric encryption functions: https://www.openssl.org/docs/crypto/EVP_EncryptInit.html#
2. List a few other cryptographic libraries.

III. More advanced articles for your interest

For more advanced look at password-based key derivation look at "STRONGER KEY DERIVATION VIA SEQUENTIAL MEMORY-HARD FUNCTIONS" by COLIN PERCIVAL, accessible here: http://www.tarsnap.com/scrypt/scrypt.pdf

An attack on AES: "Efficient Cache Attacks on AES, and Countermeasures" Tromer, Osvik, Shamir.