cs3235:4: - Laboratory #4 for September 18, 2019

The first part of this laboratory can be done in groups of two. The learning objective of this lab is for students to get familiar with the concepts in the secret-key encryption. After finishing lab3 and lab4, students should have gained first-hand experiences on encryption algorithms, encryption modes, paddings, and initial vector (IV). Moreover, students will be able to use tools and write programs to encrypt/decrypt messages. Parts 2 and 3 are homework questions, to be done individually - they can be submitted any time up to midnght on September 21st.

1 Lab 4, part 1: Programming using the Crypto Library

So far, we have learned how to use the tools provided by `openssl` to encrypt and decrypt messages. In this task, we will learn how to use `openssl`'s crypto library to encrypt/descrypt messages in programs.

OpenSSL provides an API called EVP, which is a high-level interface to cryptographic functions. Although OpenSSL also has direct interfaces for each individual encryption algorithm, the EVP library provides a common interface for various encryption algorithms. To ask EVP to use a specific algorithm, we simply need to pass our choice to the EVP interface. A sample code is given in `https://www.openssl.org/docs/man1.1.0/crypto/EVP_EncryptInit.html`. Please get yourself familiar with this program, and then do the following exercise.

You are given a plaintext and a ciphertext, and you know that `aes-128-cbc` is used to generate the ciphertext from the plaintext, and you also know that the numbers in the IV are all zeros (not the ASCII character '0'). Another clue that you have learned is that the key used to encrypt this plaintext is an English word shorter than 16 characters; the word that can be found from a typical English dictionary. Since the word has less than 16 characters (i.e. 128 bits), space characters (hexadecimal value 0x20) are appended to the end of the word to form a key of 128 bits. Your goal is to write a program to find out this key. A word list is here: `https://hugh.comp.nus.edu.sg/cs3235/lab4/words.txt`. The plaintext and ciphertext is in the following:

```
Plaintext (total 21 characters): This is a top secret.
Ciphertext (in hex format): 8d20e5056a8d24d0462ce74e4904c1b5
                            13e10d1df4a2ef2ad4540fae1ca0aaf9
```

1. If you choose to store the plaintextmessage in a file, and feed the file to your program, you need to check whether the file length is 21. Some editors may add a special character to the end of the file. If that happens, you can use a hex editor tool to remove the special character.

2. In this task, you are supposed to write your own program to invoke the crypto library. No credit will be given if you simply use the `openssl` commands to do this task.

3. Use the Ubuntu vm and run these commands as an administrative user:

```
su root
apt-get update
apt-get install openssl libssl-dev
```

After running these commands you should be able to compile:

```
gcc -o enc yourcode.c -lcrypto -ldl
```

Your task: write a short (less than 8000 characters) lab report to describe what you have done and what you have observed. Please also upload your code to the IVLE before midnight, 21st September 2019. Your file should be a single "C" file, with the name `<yourid>.c` (for example `e0012345.c`).

Once you have your plan ready, both you and your lab partner should access the cs3235 grading website to enter in your plan - each copy should identify you and your partner:

`https://hugh.comp.nus.edu.sg/cs3235/lab4/gradeslab4-1.php`

You will only see your own plan, not everyone else's.

2 Lab 4, part 2: (individual) Crypto homework question (a)

An essential component of the RSA cryptographic scheme is raising a large number x to a large power y (modulo some other number n). We could do this by just multiplying x by itself $y-1$ times (we will call this method A), but this is not fast. Find a faster method (method B) for calculating x^y. Estimate the time complexity of method A and method B using big O notation, and given that a multiplication takes 1mS, and assuming that all other operations are instantaneous, estimate the time to calculate x^y using each method, where y is about 2^{300}.

Once you have your answer, access the cs3235 grading website, giving a brief explanation of your method (B), and your time estimates with working:

`https://hugh.comp.nus.edu.sg/cs3235/lab4/gradeslab4-2.php`

You will only see your answer, not everyone else's.

3 Lab 4, part 3: (individual) Crypto homework question (b)

Consider the following ciphertext, which was enciphered using a rotation cipher:
TEBKFKQEBZLROPBLCERJXKBSBKQP.

Decipher it, explaining a technique for deciphering it, that does not use computers.

Once you have your answer, access the cs3235 grading website to give the likely deciphered text, and your explanation of a deciphering method:

`https://hugh.comp.nus.edu.sg/cs3235/lab4/gradeslab4-3.php`

You will only see your answer, not everyone else's.