CS458 Information Security Programming Assignment 1

Instructor: Kevin Jin TA: Xin Liu

Due date: 9/25/2015, 11:59 PM

1. Introduction

In this assignment, you will use the openSSL library (www.openssl.org) to implement two functions for encryption and decryption. The function implementations should be put in the file fscrypt.cc and fscrypt2.cc.

You should use the block cipher method **blowfish** for encryption/decryption, which is provided in the openSSL library. Blowfish uses 64-bit blocks and typically 128-bit keys.

The header file fscrypt.h declares the encryption/decryption functions.

```
#include "openssl/blowfish.h"

const int BLOCKSIZE = 8;           // Block size for blowfish

// encrypt plaintext of length bufsize. Use keystr as the key.

void *fs_encrypt(void *plaintext, int bufsize, char *keystr, int *resultlen);

// decrypt ciphertext of length bufsize. Use keystr as the key.

void *fs_decrypt(void *ciphertext, int bufsize, char *keystr, int *resultlen);
```

Both functions allocate the result buffer of at least the required size (using `new()/malloc()`) and return a pointer to it. Both functions also return the number of valid bytes (including the padding bytes) in the result buffer in `resultlen`. The application code is responsible for deleting the buffer.

Given the blowfish algorithm, you task is to use CBC operation mode for encryption. For padding, pad with the length of the pad in all the padded characters (PKCS5 padding). Assume that the initialization vector contains NULL characters (all 0's).

Description of blowfish functions can be found at
http://www.openssl.org/docs/crypto/blowfish.html

Use the following functions to facilitate your work:

`BF_set_key` use all characters of the keystr, excluding NULL terminator. Valid keystr is assumed to be a string.

`BF_cbc_encrypt` and `BF_ecb_encrypt`

You need to provide two ways to implement the encryption/decryption functions:

1. In fscrypt.cc, utilize BF_set_key and BF_cbc_encrypt
2. In fscrypt2.cc, utilize BF_set_key and BF_ecb_encrypt, and implement the CBC mode on your own.

The cipher text generated by the functions in both files should be the same.

You will need to include "openssl/blowfish.h" (from the openssl package) and link with the "crypto" library.

You can type the following command in your terminal to install the required library

```
sudo pat-get install libssl-dev
```

You will be given a driver program (main.cc) to test your code. You can use the following command to compile:

```
gcc (or g++) main.cc fscrypt.cc –lcrypto

gcc (or g++) main.cc fscrypt2.cc –lcrypto
```

2. Instructions

Download the assignment package from Blackboard or Course website or Piazza, the package includes:

- This assignment sheet
- Four files: fscrypt.h, fscrypt.cc, fscrypt2.cc, main.cc

The only files you need to modify are fscrypt.cc and fscrypt2.cc.

For your convenience, please use C/C++ in Linux environment to develop your code. You can use native Linux or setup a Virtual Machine (e.g., virtual box)

Only a softcopy submission is required. The deliverables include:

- Four files: fscrypt.h, fscrypt.cc, fscrypt2.cc, main.cc. Two of them should be modified.
- A readme file, describing how to run your code.

Please zip all the files and submit it through Blackboard, with the name **"Prog1_Lastname_Firstname_A#.zip"**

3. Grading criteria:

Weight of this programming assignment: 7.5% of the total score of this course

We will grade your work based on:

- On time submission
    - **Late submission policy: half mark deduction if less than one day, and zero mark otherwise**
- Code (e.g., using the required methods, readability)
- Successful compilation and execution
- Correct functionality tested with our testing code

Note that we will use slightly different programs (other than the one in main.cc) to test your code.