Crypto Lab I – Symmetric-Key Encryption

IMPORTANT NOTES: Study lecture materials at least 1 hour and attempt the tasks in Section 2 prior to the lab session. Prepared questions will be discussed in the lab session.

1 Overview

The learning objective of this lab is for students to get familiar with the concepts in the secret-key (symmetric key) encryption. After finishing the lab, students should be able to gain a first-hand experience on encryption algorithms, avalanche effect, and modes of operation.

2 Lab Environment

Create the plaintext file. Run the command `echo "Say the year is the year of the phoenix" > plain.txt` will create a file in current directory or use a text editor such as nano to create the text file.

OpenSSL. In this lab, we will play with various encryption algorithms and modes. You can use the following `openssl enc` command to encrypt/decrypt a file. To see the manuals, you can type `man openssl` and `man enc`.

```
 %  openssl enc ciphertype -e  -in plain.txt -out cipher.bin \
                -K  00112233445566778889aabbccddeeff \
                -iv 0102030405060708
```

Please replace the `ciphertype` with a specific cipher type, such as `-aes-128-cbc`, or `-aes-128-ecb`. You can find the meaning of the command-line options and all the supported cipher types by typing "`man enc`". We include some common options for the `openssl enc` command in the following:

```
 -in <file>      input file
 -out <file>     output file
 -e              encrypt
 -d              decrypt
 -K/-iv          key/iv in hex is the next argument
 -[pP]           print the iv/key (then exit if -P)
```

3 Lab Task: Encryption Mode – ECB vs. CBC

The file `art.bmp` in the `/srv/fit2093files/fit2093lab` folder contains a simple picture. We would like to encrypt this picture, so people without the encryption keys cannot know what is in the picture.

1. Copy the `art.bmp` file to the home directory and encrypt the `art.bmp` file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes.

2. Let us treat the encrypted picture as a picture, and use a picture viewing software to display it. However, for the `.bmp` file, the first 54 bytes contain the header information about the picture, we have to set it correctly, so the encrypted file can be treated as a legitimate `.bmp` file. We will replace the header of the encrypted picture

with that of the original picture. You can use a hex editor tool (e.g. `bless`) to directly modify binary files. Your tutor will demonstrate how to do this.

3. Display the encrypted picture using any picture viewing software. Can you derive any useful information about the original picture from the encrypted picture? Please explain your observations.

4 Optional Exercises for Further Exploration

4.1 Avalanche effect

1. Encrypt the plaintext file using `-aes128` algorithm using a key provided in command line with `-K` and IV using `-iv`.
2. Change a single bit of the key and encrypt the file again (choose a different name for the output file), and compare the content of the two files. You can do this by changing the provided key with the option `-K`.
3. Change a single bit of the plaintext and encrypt the file with the key and IV used in the first step and compare the two encrypted files. You can do this using the `bless` hex editor, or a text editor and change for instance the first letter from `S` to `R` (hex 52).
4. Change a single bit in the first encrypted file and decrypt it and compare the recovered file with the plaintext file.

4.2 Encryption Modes – Error Propagation

To understand the properties of various modes of operation, we would like to do the following exercises:

1. Encrypt `plain.txt` file using the AES-128 cipher in ECB, CBC, CFB, OFB, CTR modes.
2. Unfortunately, the 4th byte in the received encrypted file was corrupted. You can simulate this corruption (which would in practice happen due to communication reception errors) using a hex editor. Decrypt the corrupted file using the correct key and IV and determine how many plaintext blocks are recovered correctly and how many are corrupted in each of the above modes of operation.