Lab 06: Secret-key encryption

1. Goal of the Lab

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

2. Lab Environment

2.1. OpenSSL

**Secure Sockets Layer (SSL)** is an application-level protocol which was developed by the Netscape Corporation for the purpose of transmitting sensitive information, such as Credit Card details, via the Internet

**OpenSSL** is a robust, commercial-grade implementation of SSL tools, and related general-purpose library based upon SSL, developed by Eric A. Young and Tim J. Hudson

OpenSSL is already installed on SEEDUbuntu.

2.1. xxd and dd

xxd makes a hexdump of a given file.

dd is powerful binary copy command

3. Encryption using different ciphers and modes

The algorithm seems to follow the pattern:  
**(Algorithm name)-(key size)-(encryption mode)**  
Noted: If the key size is omitted or excluded then it means there is only one key-size for that algorithm.

* **Algorithm name:** Sometimes there is number included in the algorithm name whose usage is to distinguish the version of the algorithm; for instance, RC2 and RC4.
* **Key size:** key size is in bit. The longer the key the stronger your encryption is, but the slower operation it takes.
* **Encryption mode:** there are five main encryption mode that widely use in block cipher mode operation, Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR)  
  There are several encryption algorithm in OpenSSL, use openssl enc –help to see.

**4. Tasks**

**4.1. Encrypt and Decrypt Text file**

* Create a sub directory named “crypto\_lab” in your home dir
* Create text file named plain.txt with whatever content that you like. For example “My name is ….”
* Encrypt plain.txt, view the encrypted file with xxd then decrypt it with different aes cipher, in different modes.

For example:

openssl enc -aes-128-cbc -e -in plain.txt -out cipher-aes-128-cbc.bin \ -K 00112233445566778889aabbccddeeff \ -iv 0102030405060708

to encrypt file plain.txt in aes-128 bit with cbc cipher with key –K and initialization vector -iv

Try at least 3 different cipher modes and compare the results.

**4.2 Encryption Mode – ECB vs. CBC**

Download a bitmap file from [here](http://bit.ly/2Abqets) to the crypto\_lab directory, save the file name as origin.bmp

Encrypt the file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes, and then do the following:

* 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 linux dd command to directly modify binary files.
* 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.

**4.3 Encryption Mode – Corrupted Cipher Text**

To understand the properties of various encryption modes, we would like to do the following exercise:

1. Create a text file that is at least 64 bytes long.

2. Encrypt the file using the AES-128 cipher.

3. Unfortunately, a single bit of the 30th byte in the encrypted file got corrupted. You can achieve this corruption using dd command

4. Decrypt the corrupted file (encrypted) using the correct key and IV. Please answer the following questions:

(1) How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after you finish this task.

(2) Please explain why.

(3) What are the implication of these differences?