CS-4331-Special Topics in Security

Fall 2016

LAB #1: Modes of Operation

This lab is meant to give you hands-on experience with some of the concepts of symmetric ciphers. You will use OpenSSL, a program and library that supports a wide range of cryptographic operations.

1. You will first create random keys and initialization vectors that you will use throughout the lab.

   For example, to create an 8 byte random number (hex), you can use the command:

   ```
   openssl rand 8 —hex
   ```

   Create a random 8-byte key and 8-byte IV that you will use for DES operations and a random 16-byte key and 16-byte IV that you will use for AES operations.

2. To encrypt the file MyFile and produce the output in the file ciphertext.bin, you use the command:

   ```
   openssl enc nameofcipher -e -in MyFile -out cipher.bin -K key -iv intializationvector
   ```

   The –e stands for encryption. To decrypt you would use –d and specify the cipher text as input. An example of the nameofcipher is: -aes-128-cbc for 128-bit aes being used in cbc mode or –des-ecb for DES being used in cbc mode.

   Remember that you will not need the iv for all schemes.

   In this exercise you will compare the behavior of the CBC and ECB modes of operation. You have been provided with an image file, CS4331.bmp. The file is for a logo of an upcoming movie and you don't want bootleggers to see it before the movie's official release date. So you have decided to encrypt the file before sending it to your colleagues in Winterfell.

   (a) Before doing anything with the image file, view it using an image viewer of your choice.

   (b) Encrypt the image file using: (i) –des-ecb, (ii) –aes-128-ecb. You now have two different encrypted files (Lets say you name them CS4331desecb.bmp and CS4331aes128ecb.bmp). Try to view these two encrypted files using the image editor you used previously.

What do you see and why?

(c) To correct the issues you should have met above, you will use the help of a hex editor. Install bless (a hex editor) and use it to open the original unencrypted image file. Now that you can directly view the bytes in the file, copy the first 54 bytes of CS4331.bmp and paste them to replace the first 54 bytes of CS4331desecb.bmp and the first 54 bytes of CS4331aes128ecb.bmp.

Use the image viewer to view each of the two new files you have created.

(i) Why is it that you are able to view the images now when you were unable to do so previously in (b)?

(ii) Are you impressed by the encryption? Explain why (why not).

(d) Repeat steps (b) through (c) using the schemes: (i) –des-cbc, (ii) –aes-128-cbc

Explain the difference in observations between the case when you used the ecb options and when you used the cbc options.

3. In this exercise, you will compare the effects of data corruption on ecb, cbc, ofb and cfb. You will create a small text file that is several blocks long, encrypt the file using DES or an AES configuration of your choice, flip a single bit in the cipher text and then decrypt the corrupted cipher text to observe the impact of the corruption on each of the above 4 modes of operation. Discuss your observations and how they relate to the operation mechanisms of the different cipher options.

NOTE: The project report will comprise descriptions of your observations at each stage, supported by screen shots showing what you observed.