**Updates were rejected because the remote contains work that you doCIS 458 System Security**

**Lab 01 – Encryption with OPENSSL**

**Time Due:** Friday, 9/13/2019 in Blackboard

Please answer all questions in the Answer Sheet; put your answers in a Word or PDF or a text file; submit your work by the due time through Blackboard.

**Educational Objectives**

This lab is designed for students to gain first-hand experience with symmetric encryption algorithms and operation modes of block ciphers using available libraries in OpenSSL.

**Lab Environment**

This lab will be performed on an DC computer.

**Section 1 Introduction**

The cryptographic libraries implemented by OpenSSL project will be used in this lab. Detailed description about OpenSSL and the libraries can be found from the following link:

<https://www.openssl.org/>

By default, OpenSSL is installed in most Linux distributions. Many applications have been using OpenSSL libraries and APIs.

The following command will display the OpensSSL version on a Linux system:

openssl version

**Question 1:** What is the latest stable version of OpenSSL? Which version is installed on the EOS machine? (**Hint:** You can find the latest stable version from the Downloads page in OpenSSL web site.)

OpenSSL 1.1.1 11 Sep 2018

**Section 2 Encryption Using Different Ciphers and Modes**

The following command can be used to encrypt/decrypt a file using OpenSSL libraries.

openssl enc -*cipher\_type* –e|-d -in *file* –out *file* –K *key* –iv *initial\_vector*

where

cipher\_type: the cipher, e.g., –aes-128-cbc, -aes-128-ebc, and etc.

-e|-d: encryption | decryption

-in file: input file

-out file: output file

-K key: the Key in hex, e.g., -K 00112233445566778899aabbccddeeff

-iv initial\_vector: initial vector in hex, e.g., -iv 0102030405060708

Please use man page to learn how to use the command openssl enc. (man openssl, man enc)

The following command will display all available options:

openssl enc –help

**Question 2:** What is the command you would use to display all of the cyphers?

openssl ciphers -v

Please do the following:

* Create a test file of at least 100 bytes of your choice.
* Encrypt this file.
* Decrypt this file.
* Try the above using at least three different cipher types.

You can find the meaning of the command line options and all the supported cipher types by using the man page of enc (man enc).

**Question 3:** What were the ciphers and operations modes that you tried?

**Question 4:** Was the plain text correctly retrieved from the cipher text? If no, explain why.

**Section 3 Operation Mode: ECB *versus* CBC**

The file *pic\_lab01.bmp*, an image in bit map format, is posted in my home directory. Please copy it over to your machine:

cp /home/wangx/Public/teaching/cis458/pic\_lab01.bmp ./

You will study the difference between operation modes of ECB and CBC using this picture as an example. Please perform the following:

* Open the file *pic\_lab01.bmp* using any image viewer (Firefox will work fine for this purpose.) to view the picture. And then close it.
* Encrypt the file using the ECB and CBC modes (*e.g.*: aes-128-ecb and aes-128-cbc), respectively, and save the cipher texts in different files (*e.g.*, picture\_ecb.bmp and picture\_cbc.bmp).

Now, the encrypted pictures cannot be viewed (you can try it) because the header information is “damaged” by the encryption process. The header information resides in the first 56 bytes in a *.bmp* file. In order to view the encrypted picture, the original header information must be recovered.

Assume you stored the encrypted image in the following files:

pic-aes-128-ecb.bmp

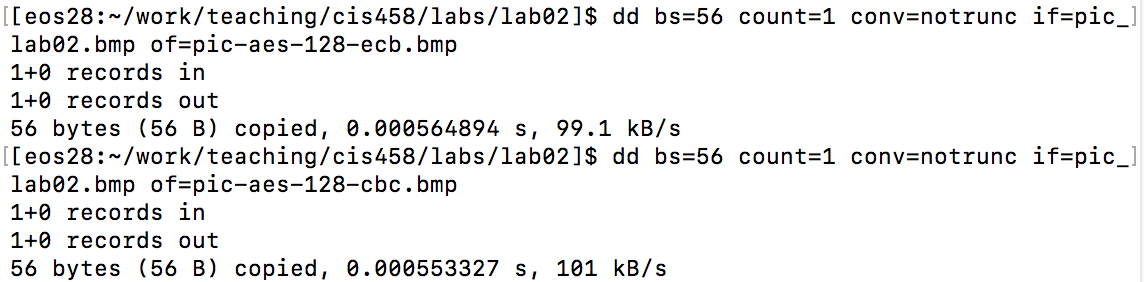
pic-aes-128-cbc.bmp

Then perform the following to recover the header information:

dd bs=56 count=1 conv=notrunc if=pic\_lab01.bmp of=pic-aes-128-ecb.bmp

dd bs=56 count=1 conv=notrunc if=pic\_lab01.bmp of=pic\_aes-128-cbc.bmp

As shown in the screenshot below:



Then, view the encrypted pictures (pic-aes-128-ecb.bmp, pic-aes-128-cbc.bmp).

**Question 5:** Take screenshots that show the encrypted pictures (both ECB and CBC modes) when they are viewed and attach them here. Indicate the operation mode that is used for encrypting them for each.

**Question 6:** Please explain your observations of the results for the previous question. More specifically, please argue the ECB mode against the CBC mode. Which operation mode can more completely hide the original information and is more secure? Explain your arguments.

**Section 4 Performance Test (4% bonus)**

For the bonus part, please write a script to measure the performance of the ciphers implemented in OpenSSL. In this test, you must select at least three different ciphers of your choice. For each cipher, you must choose at least three operation modes of your choice.

**Hint:**

You can perform the test in different ways. For example:

* Generate a large file and measure the time to encrypt it using different ciphers.
* Use **opensll speed** command (use **man speed** to learn the details).
* Write a script.

**Question B01:** Briefly describe what you did and attach your working code.

**Question B02:** Give a diagram or table to show your measured results. Briefly summarize your observations.

**Congratulations!** You have completed this lab for the class. Hope you enjoyed doing this lab. Please let your instructor know if you have any comments.

**Answer Sheet**

========================== **Required Questions** ===========================

**Question 1:** What is the latest stable version of OpenSSL? Which version is installed on the EOS machine? (**Hint:** You can find the latest stable version from the Downloads page in OpenSSL web site.)

The latest stable version is openssl 1.1.1

The version on my pc is openssl 1.1.1 11 September 2018

**Question 2:** What is the command you would use to display all of the cyphers?

Openssl cipher -v

**Question 3:** What were the ciphers and operations modes that you tried?

**Question 4:** Was the plain text retrieved from the cipher text correctly? If no, explain why.

**Question 5:** Take screenshots that show the encrypted pictures (both ECB and CBC modes) when they are viewed and attach them here. Indicate the operation mode that is used for encrypting them for each.

**Question 6:** Please explain your observations of the results for the previous question. More specifically, please argue the ECB mode against the CBC mode. Which operation mode can more completely hide the original information and is more secure? Explain your arguments.

=========================== **Bonus Part (4%)** ============================

**Question B01:** Briefly describe what you did and attach your working code.

**Question B02:** Give a diagram or table to show your measured results. Briefly summarize your observations.