CS 4351: Computer Security **Instructor: Dr. Deepak Tosh**
Fall 2022 **Due Date:** 11/6/2022, Midnight

ASSIGNMENT# 3: Secret Key Crypto

INTRODUCTION:

The learning objective of this lab is for students to get familiar with the concepts in the secret-key encryption and some common attacks on encryption. From this lab, students will gain a first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). Moreover, students will be able to use tools and write programs to encrypt/decrypt messages.

Suggested Environment:
The suggested environment to conduct this attack is SEED Virtual Machine.

Task# 1: Encryption using Different Ciphers and Modes [30 Pts]

In this task, 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, -bf-cbc, -aes-128-cfb, etc. In this task, you should try at least 3 different ciphers. 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)
```

Task# 2: Encryption Mode – ECB vs. CBC [35 Pts]

We would like to encrypt a picture (pic_original.bmp), so people without the encryption keys cannot know what is in the picture. Please encrypt the file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes, and then do the following:

1. Let us treat the encrypted picture as a picture and use a picture viewing software to display it. How-ever, 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. We can use the bless hex editor tool (already installed on our VM) to directly modify binary files. We can also use the following commands to get the header from p1.bmp, the data from p2.bmp (from offset 55 to the end of the file), and then combine the header and data together into a new file.

```
$ head -c 54 p1.bmp > header
$ tail -c +55 p2.bmp > body
$ cat header body > new.bmp
```

2. Display the encrypted picture using a picture viewing program. Can you derive any useful information about the original picture from the encrypted picture? Please explain your observations.
3. Select a picture of your choice, repeat the experiment above, and report your observations.

Task# 3: Error Propagation – Corrupted Cipher Text [35 pts]

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

1. Create a text file that is at least 1000 bytes long.
2. Encrypt the file using the AES-128 cipher.
3. Unfortunately, a single bit of the 55th byte in the encrypted file got corrupted. You can achieve this corruption using the bless hex editor.
4. Decrypt the corrupted ciphertext file using the correct key and IV.

Please answer the following question: How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, and CFB respectively? Please provide justification as well as evidences.

Notes on Report Submission:
You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

Grading:

The assignment will be graded based on
(1) Clarity of the report,
(2) Correctness of each answer, and
(3) Demonstration of evidence

Note: When requested, the student would have to demonstrate and answer additional questions to the instructor.

Submission:

Please submit your reports in PDF format (lastname_firstname.pdf) on **BLACKBOARD only**. Make sure to answer the questions in order and CLEARLY STATE YOUR ASSUMPTIONS, if you are unsure about something.

If you have any questions, comments, concerns, doubts, or confusions, please stop by my office to clarify. You can also email me on dktosh@utep.edu. I will be very happy to help.