# SEEDLAB – CRYPTO LAB

## SECRET KEY ENCRYPTION

* Miral Shah (2014A7PS0200U)



## Contents:

Overview

Initial Steps for setup

Task 1: Encryption using different ciphers and modes

Task 2: Encryption mode- ECB vs. CBC

Overview

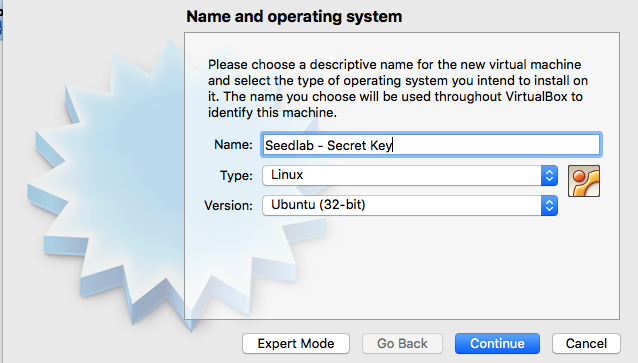
The learning objective of this lab is to get familiar with the concepts in the secret-key encryption. After finishing the lab, you should be able to gain a first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). Moreover, you will be able to use tools and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

Initial steps for setup

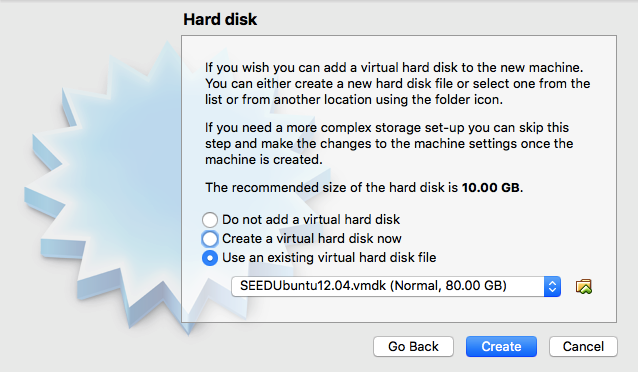
* Install virtual box and download SEEDUbuntu12.04
* Start virtual box and follow the steps below



Click on new to start a new virtual machine



Select the above options and click continue



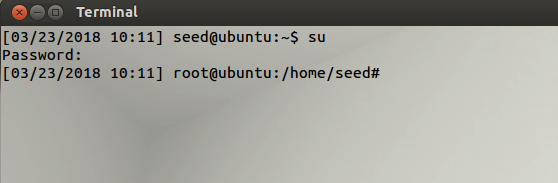
Click on 'Use an existing virtual hard disk file' and select the file where you downloaded SEEDUbuntu12.04

* Start your virtual machine now



Enter the password 'dees' for Seed username

* Start the terminal and type the following commands



For the password, type 'seedubuntu'

Starting the tasks now-

TASK 1: Encryption using different ciphers and modes

Using AES-128-CBC:

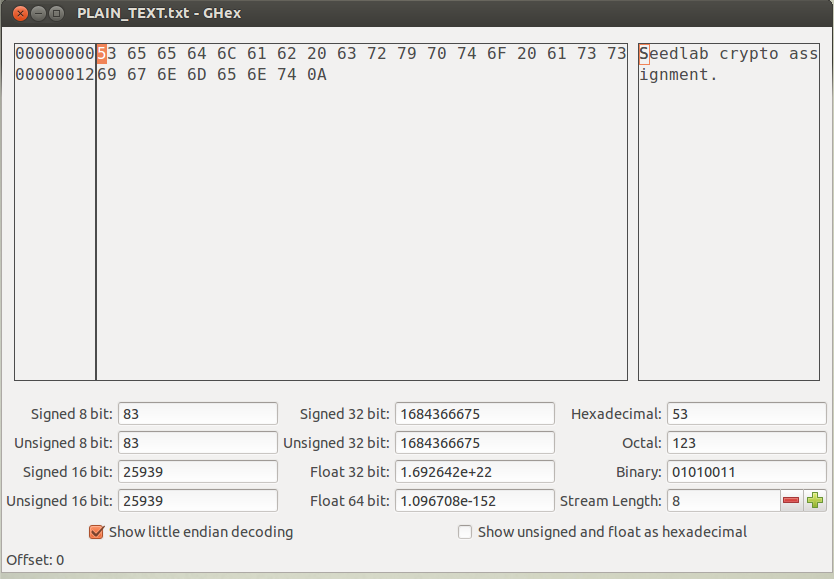
This mode requires a plain text, initialization vector and a key to begin encryption. Even if there is no text entered in the plain text a 128-bit cipher text is generated.

Open text editor and type any plaintext sentence. This will be saved as PLAINTEXT.txt

On the desktop, open an empty text editor file and name it as Cipher.txt. This will save our ciphertext after encrypting the plaintext

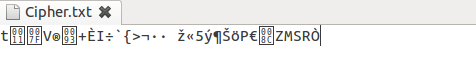


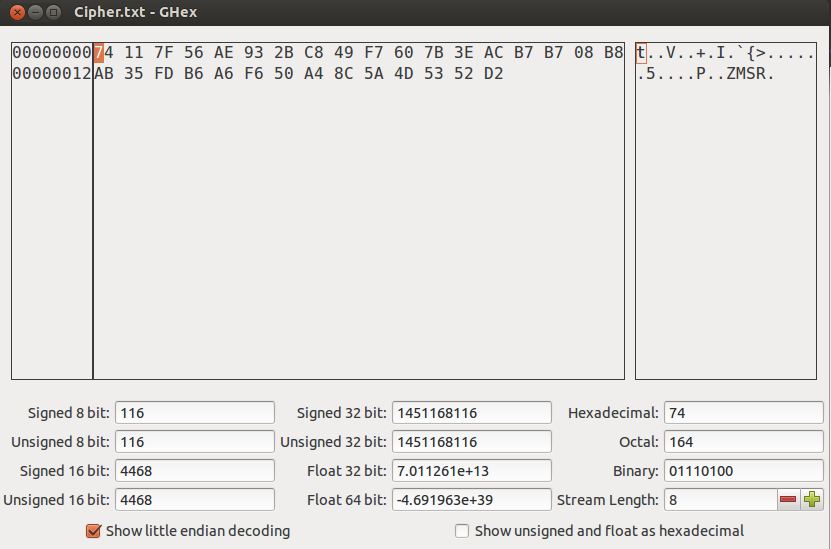
Open Ghex and load the plaintext file to see its hex conversion



In terminal, type the command to encrypt plaintext using AES-28-CBC



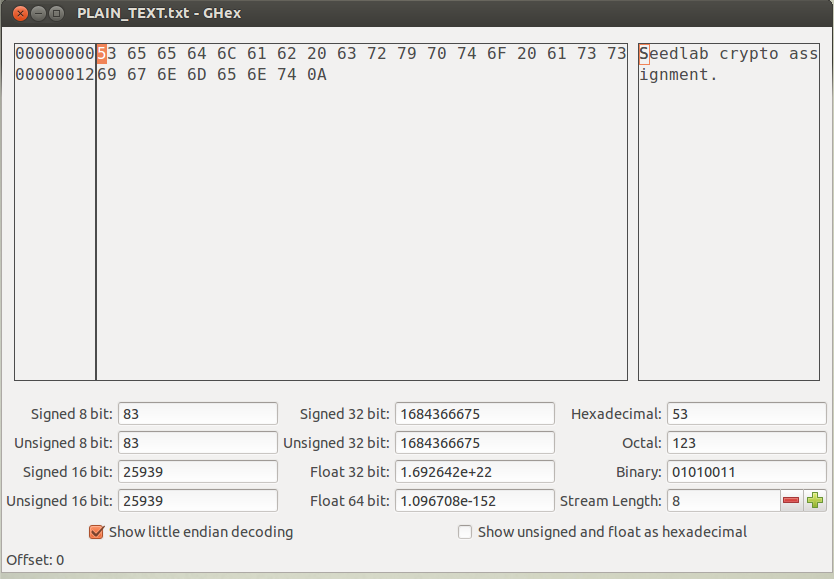




Using AES-128-CFB:

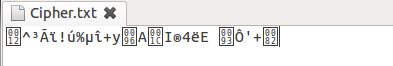
This mode requires an initialization vector and a key to begin encryption. Since CFB is a stream cipher, if there is no text entered in the plain text, cipher text will not be generated.

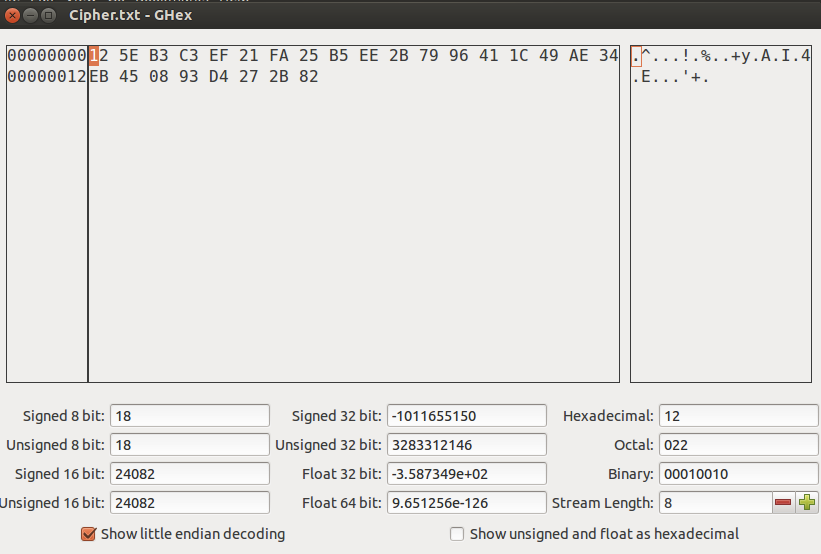




In terminal, type the command to encrypt plaintext using AES-28-CFB



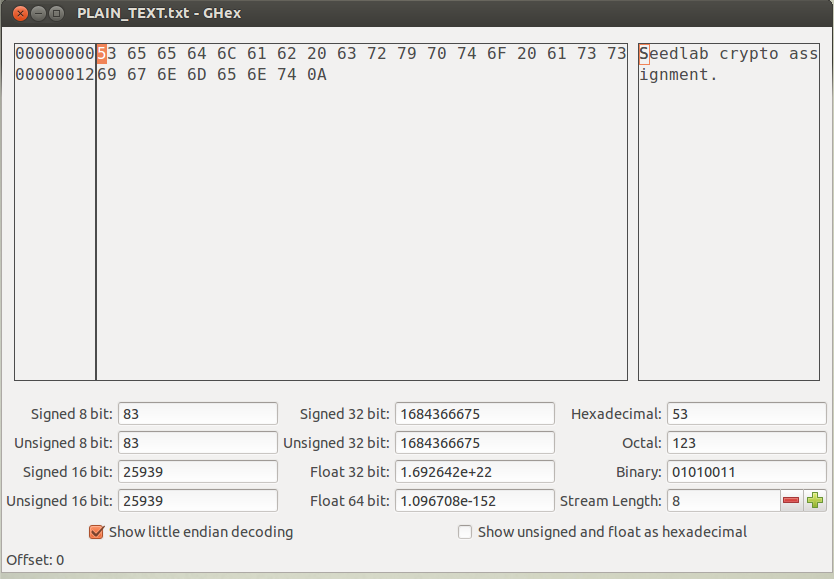




Using AES-128-OFB:

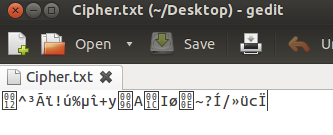
This mode requires an initialization vector and a key to begin encryption. If there is no text entered in the plain text, cipher text will not be generated. This cipher mode supports parallel encryption to form cipher text.

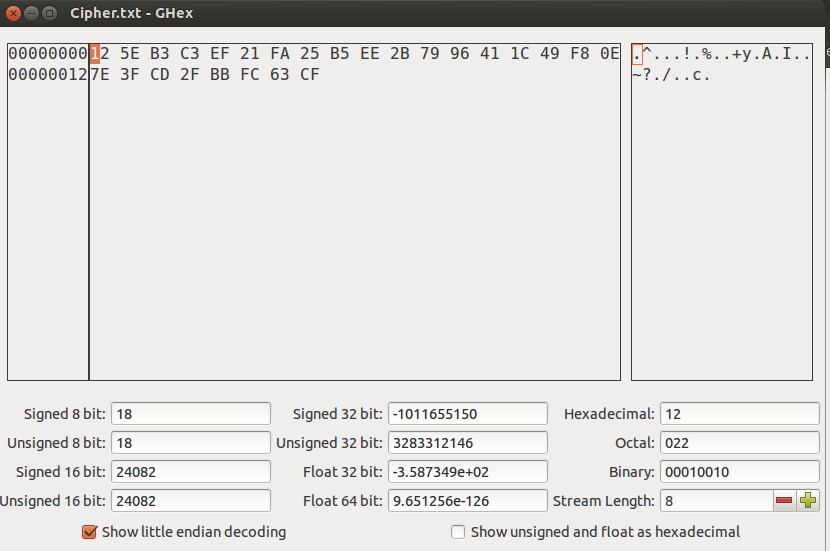




In terminal, type the command to encrypt plaintext using AES-28-OFB







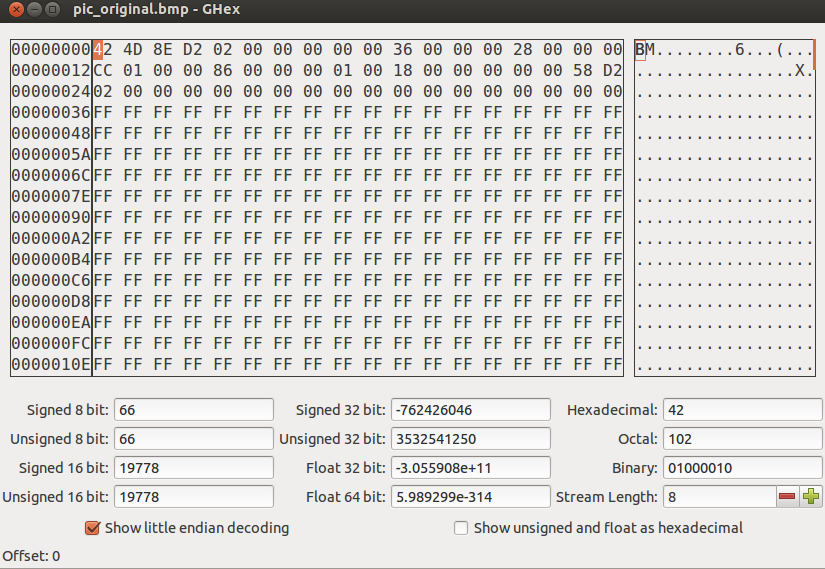
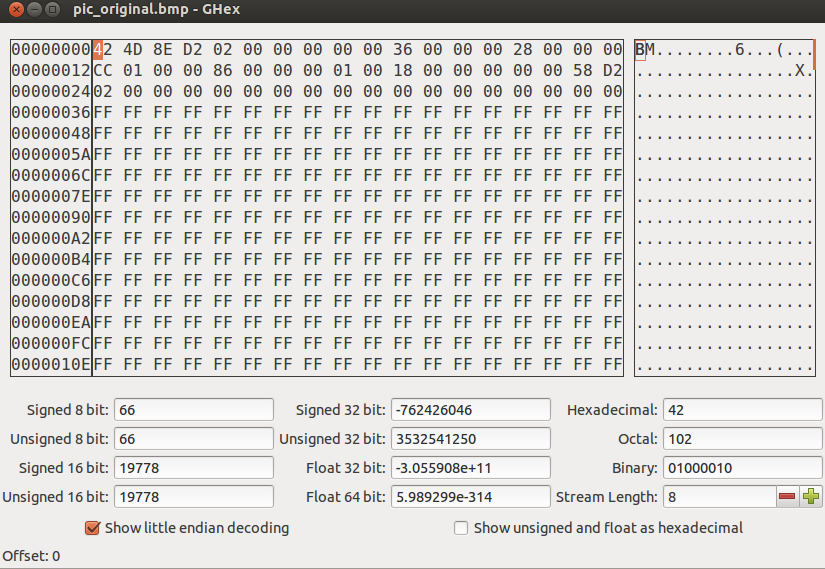
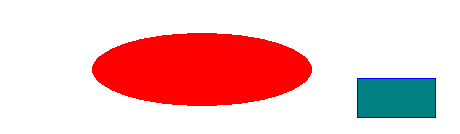
TASK 2: Encryption mode – CBC vs. ECB

Cipher Block chaining (CBC):

This is a block cipher encryption in which each block of the plain text is XORed with the previously generated cipher text and then it is encrypted. So each cipher clock depends upon all plain texts that were processed.

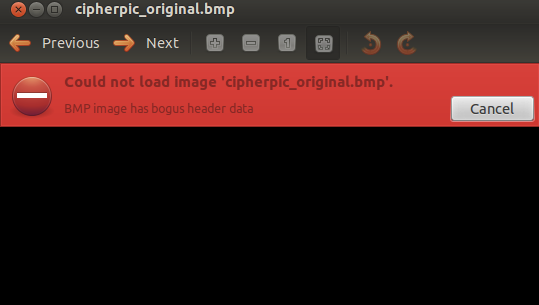
Save 'pic\_original.bmp' from the seedlabs website onto the desktop.

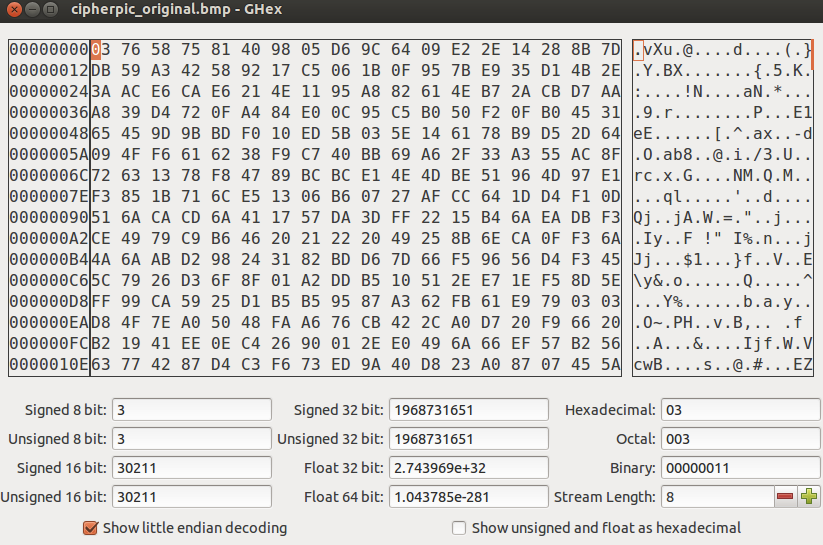
Save another bmp file 'cipherpic\_original.bmp'



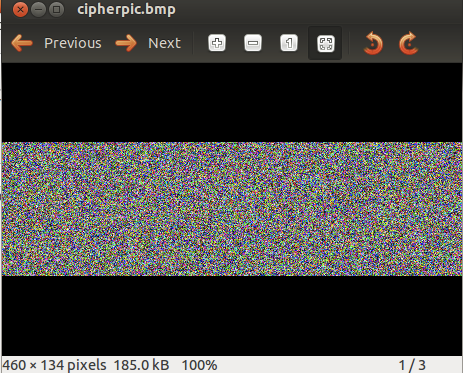
In terminal, type the command





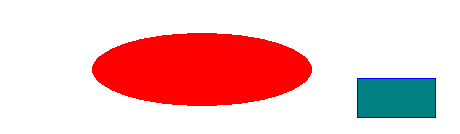


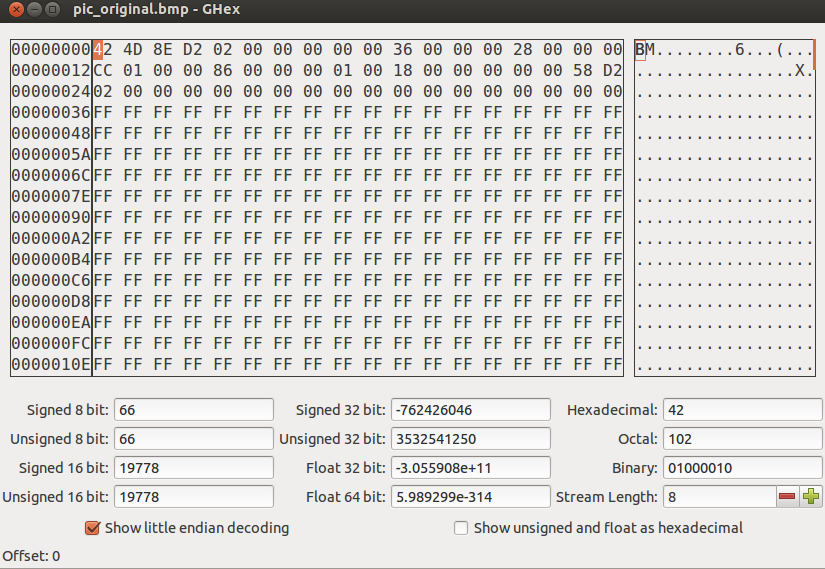
The first 54 bits of the encrypted bmp file is replaced with the first 54 bits of the original bmp file. By doing this the encrypted image can be seen using image viewer. However any information about the original image cannot be observed in this encrypted bmp file. This is because CBC mode generates different cipher text for repeating plain text.



Electronic Code Book (ECB):

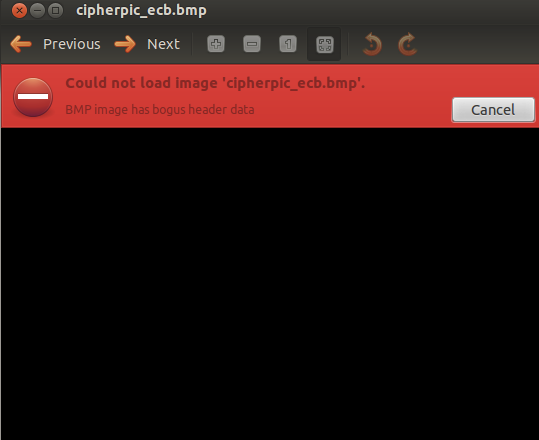
This is the simplest block cipher encryption in which a block of plain text is converted into cipher text by encrypting it with a key.

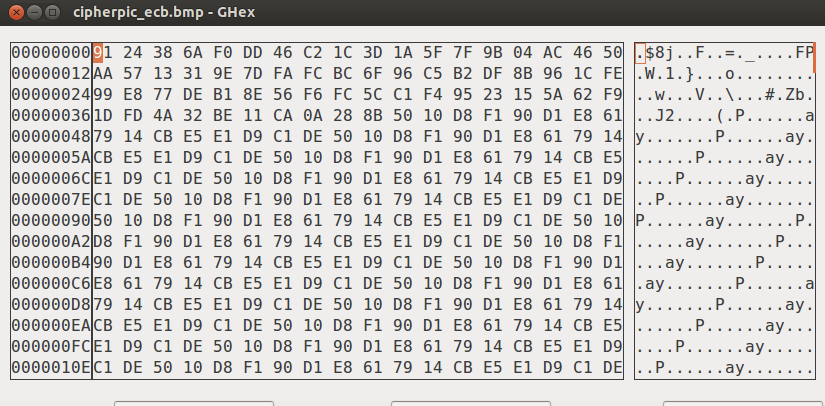




In terminal, type the command







The first 54 bits of the encrypted bmp file is replaced with the first 54 bits of the original bmp file. By doing this the encrypted image can be seen using image viewer. Information about the original image can be observed in this encrypted bmp file. This is because ECB mode generates same cipher text for repeating plain text. Even though the cipher image is different from the original image, most of the original image’s information can be obtained from the cipher image.

