EN650.601 Lab Assignment 2 - Secret-Key Encryption

In this lab, you will apply your knowledge of block cipher modes of operation to find out some interesting facts. You have to complete five tasks in this lab and submit a report describing your works and observations. The lab is one of the exercises in SEED Project. It provides Virtual Machine (VM) image in order to simplify setups of experimental environment. We are using the Ubuntu 16.04 image for this lab. Load the VM image with your Virtualbox or VMware, and read the User Manual carefully before you start working on the labs.

Lab Notices:

- You can **skip Task 1** and **Task 7**– frequency analysis against monoalphabetic substitution cipher and programming using the crypto library.
- You can use any bmp file you found for Task 3 as long as you can see the differences between it is ECB and CBC encrypted. Though lena is the standard testing image, it is not a good choice in this lab due to its complexity. Use some simple image that has large areas of same colors instead. The header of pictures encrypted by ECB and CBC should be the same.
- For Task 5, you should consider the decryption processes for ECB, CBC, CFB and OFB.
- Include screenshots, codes, IVs, keys you use in your report.
- Take screenshots periodically and include it in your report. They not only serve as evidences of completion but also help the grader understand what you're trying to achieve.

Points Breakdown

This lab has 50 points in total. The five tasks are worth 5, 10, 10, 10, 15 points respectively.