Secret Key Encryption

CS 334: Information Security (Summer 1444 - Summer 2023)
Due: Saturday 18/01/1445 - 0508/2023

Introduction

So far in this course, you've seen many cryptosystems, learned how they work, and how they may be broken. We discussed symmetric and asymmetric cryptography and how the keys are generated and used to encrypt and decrypt messages.

For this course's project, we'll take a closer look at Secret-Key Encryption. This project will help you gain You'll gain 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. This lab was created by Seed Labs, which is a project led by Professor Wenliang Du, with many of his students working on these labs and environments.

This lab covers the following topics:

- Secret-key encryption
- Substitution cipher and frequency analysis
- Encryption modes, IV, and paddings
- Common mistakes in using encryption
- Programming using the crypto library

Background

In this lab you'll be performing the following 3 Tasks:

- Task 2: Encryption using Different Ciphers and Modes
- Task 3: Encryption Mode – ECB vs. CBC
- Task 7: Programming using the Crypto Library

You'll find the full lab details and detailed steps on how to execute the tasks above, on the lab's webpage https://seedsecuritylabs.org/Labs_16.04/Crypto/Crypto_Encryption/ . You will also find a link to an Ubuntu VM which has all the tools you'll need pre-installed, such as openssl and its libraries.

Submission

As mentioned in the lab description. You need to submit a detailed lab report 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. In your report, you need to answer all the questions listed in this lab.

If you have any questions or need assistance, kindly send me an email at mmtezeghdanti@imamu.edu.sa

Note: *We take plagiarism very seriously. The project's level of difficulty is very reasonable, so make sure you do this project yourself. For that reason, please change the VM's wallpaper to a unique picture of your choosing and make sure your terminal or browser window doesn't cover the entire screen when you take a screenshot (do not use any of the wallpapers already included in Ubuntu).*