**Mini Project 1: Secret-Key Encryption**

**Project Topic:** Experiements on Symmetric-Key Cryptography Principles

**Project Collaboration Model:** This project component can be developed in a team of 2 members.

**Due Date/Time:** 09/22/2023 11:59:59 PM.

Deliver the .ZIP file (other formats won’t be accepted) containing all your submission files (see the submission requirements in the last section) by the above due date/time. Your ZIP file should contain a Readme.txt file containing the names and the GIDs of the group members. **Each member should submit the same copy of the ZIP file on Blackboard to secure an entry in the Grade Center.** Your .zip file should be named as follows:

P1\_[Your Last Name]\_[Your GMUID].zip. For instance, if John Smith with GMUID: G12345678 were to submit this file, John would name it: P1\_Smith\_G12345678.zip.

Check the validity of your ZIP file before uploading. Any corrupted ZIP file will result in a grade of ZERO.

**Project Objectives**

The learning objective of this lab is for students to get familiar with the concepts in the secret-key (Symmetric-Key) encryption. After finishing the lab, students should be able to 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.

**Lab Setup Intructions**

* This lab has been tested on a pre-configured Ubuntu 20.04 VM, which can be downloaded from the [SEED-Ubuntu20.04.zip](https://drive.google.com/file/d/138fqx0F8bThLm9ka8cnuxmrD6irtz_4m/view) link. When you unzip the file you will get a .vdi file representing the pre-configured Ubuntu image.
* Install the free [VirtualBox](https://www.virtualbox.org/) software to be able to run the Ubuntu image on your computer. The VM image has been tested on Version 6.1.16. You can check the following [VM Manual](https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md) to stand on the detailed steps to import the VM to VirtualBox.
* Start the VM and login into the account with the username **seed**, the password is **dees**. Once you are logged in to the VM, download the lab setup files from the following link: [Lab Setup files](https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_Encryption/Labsetup.zip).

**Tasks**

Check the following PDF file containing the [lab description](https://www.dropbox.com/s/v38rumjjy7i322r/Crypto_Encryption.pdf?dl=0) and complete the following tasks:

Task 1: Frequency Analysis

Task 2: Encryption using Different Ciphers and Modes

Task 3: Encryption Mode – ECB vs. CBC

Task 4: Padding

Task 5: Error Propagation – Corrupted Cipher Text

**Submission**

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. The contribution of both members should be included in the report. You also need to provide explanation to the observations that are interesting or surprising. **Both group members need to submit the same report on Blackboard to secure a slot in the Blackboard Grade Center.**