ASSIGNMENT LAB-4

for

CSE 478: Introduction to Computer Security Lab

Submitted to

Dr. Md Sadek Ferdous

Assistant Professor, Dept of CSE, SUST

Prepared by

Masum Ahmed (2016331028)

Shamihul Islam Khan Limon(2016331078)

Department of Computer Science and Engineering

Shahjalal University of Science and Technology

20 April 2020

I’ve used Python as a language and [PyCrypto] as a library for crypto functionalities.

# Requirements to run **lab_manual_4.py** :

1. [PyCrypto] [matplotlib] installation, another libraries ship with python3+ installation
2. I’ve used Spyder [Anaconda] and macOS Mojave to run the CODE
3. Some directories [aes, rsa, rsa-signature, sha256] are needed to present in the root directory for all functionalities

# HELP

I’ve used [PyCrypto] documentation to write code. I also got help from [here] when I got stuck in RSA-Encryption. Crypto can’t encrypt messages because of the lack of argument K in the ‘encrypt’ function. I solved this problem by using PKCS1_OAEP which pads public or private keys.

# OBSERVATION :

N.B. Only Encryption and Decryption Process time is measured. Key generation time is not measured in elapsed time.

- ❏ Encryption/Decryption in AES using ECB mode doesn't vary so much. [Screenshot_1]
- ❏ AES-128 Encryption in CFB mode takes more time than ECB mode. [Screenshot_2]
- ❏ AES-128-CFB encryption and RSA-1024 Encryption takes almost the same time [Screenshot_2]
- ❏ AES-256-CFB encryption takes double time than RSA-1024 encryption [Screenshot_3]
- ❏ RSA-1024, RSA-2048, RSA-4096 encryption times gradually increase. RSA-4096 needs double time than RSA-1024. [Screenshot_4]
- ❏ RSA-1024 Decryption takes more than Encryption. [Screenshot_5]
- ❏ RSA-4096 decryption takes eight times multiple of encryption elapsed time. [Screenshot_5]