Assignment 1

Due: 11:55 pm 30 Jan 2021
Total Mark: 100 (16% of Final Mark)

General Instructions: Please read the following instructions carefully.

Creating Ransomware

In this assignment, your task is to write a simple ransomware using Python script with the **pycryptodome** package.

The assumptions on the ransomware are as follows: 1) An attacker has already broken into a victim's Linux/Unix machine on which **Python 3.5 or above** and **pycryptodome** package are installed; 2) the attacker put its ransomware program, which is not necessary to be a single file, in the victim's machine; 3) the victim has three to four text files and a python file in the directory where ransomware locates. Note that the text files have extension "`.txt`" and the python file has extension "`.pye`".

The ransomware should perform the following:

1) It generates a 256 bits random key for symmetric encryption using AES_CBC.
2) It encrypts **all `.txt` files** to **`.enc` files** in the current directory using the key that the attacker generated in step 1). The files in the other folders or the files in the same folder but having different file extensions must not be impacted by the ransomware.
3) It comments out all the content of the existing **`.pye`** file in the target folder (do not delete the content) and replicates itself to the **`.pye` file** for the further propagation.
4) The key in step 1) is encrypted to `key.bin` using public key encryption.
5) It will finally display a message for asking ransom "Your text files are encrypted. To decrypt them, you need to pay me $5,000 and send `key.bin` in your folder to [me]." "[me]" should be your student email address.

Other requirements:

- In step 1), the key used to encrypt files must not appear in the source code of the ransomware program and must not be stored in the plaintext format in the victim's system.
- All **`.txt`** files locating in the folder where ransomware program is located must be deleted after they are encrypted to the **`.enc`** files.
- AES_CBC mode needs an initial vector (IV) for encryption and decryption. You can fix (i.e., hard-code) this parameter in your ransomware .
- You must use ***pycryptodome*** for AES and public key encryption.
- The infected **`.pye` file** in step 3) shares the public key of your original ransomware.

Your next task is to write programs, key-recovery and file-recovery programs that recover (decrypt) all the encrypted files if the victim pays the ransom.

6) The key-recovery program decrypt the encrypted key (`key.bin`) and encode the decrypted key to base64 and store it in `key.txt`.
7) The file-recovery program must allow a user to decrypt the encrypted files created in step 2) using the key file created in 6). You do not need to recover the infected **.pye file** in step 3).

Submission

Write programs that satisfy the above requirements. Make a folder named `Assignment1` and include

- a ransomware program [50 marks]
- recovery programs [30 marks]
- The private key file associated with the public key used in a ransomware program (named `ransomprvkey.pem`) [10 marks]
- `A short report` that 1) gives all necessary information to run your programs (e.g., the other python pacakages for your code) and 2) explain expected outcomes (with screenshots) of each programs. [10 marks]

Compress the `Assignment1` folder using a zip program to create `yourStudentID_Assignment1.zip`.

Use Subject Moodle site to upload your zip file.