Assignment 1

Due: 11:55 pm 22 July 2023
Total Mark: 100 (16% of Final Mark)

General Instructions: Please read the following instructions carefully.

Implementing Hybrid Encryption/Decryption

In this assignment, your task is to implement a program encrypting/decrypting multiple files using hybrid encryption. You must implement the program using the **pycryptodome** package as a Python script.

The requirements for the program are as follows:

1) Use **Python 3.5 or above** and **pycryptodome** package.
2) The program must have a function encrypting all ".txt" files in the folder where the program is located in. Those files must be encrypted using AES_CBC with a randomly generated 128 bits key. The list of the text file names in the folder must be collected automatically and encrypted in a single execution. The assessor will not type file names to test your program. Try to put at least three files in the folder when you test your program.
3) The randomly generated key used for file encryption in 2) must be encrypted by RSA 2048 public-key encryption algorithm.
4) The program must decrypt the encrypted files in 2) using the decryption mechanism of hybrid encryption. In other words, it takes the encrypted key and the encrypted files as inputs and decrypts them. This can be implemented as a separate program if you want.
5) AES_CBC mode needs an initial vector (IV) for encryption and decryption. You can fix (i.e., hard-code) this parameter in your program .

Submission

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

- An encryption/decryption program satisfying the above requirements. [12 marks]
- Two pairs of a public key and a private key to test your program. [2 marks]
- A `report` that explains 1) all necessary information to run your programs (e.g., additional python packages for your code) and 2) expected outcomes (with screenshots) for the program(s). [2 marks]

Use the Subject Moodle site to upload your assignment. Compress the `Assignment1` folder using a zip program to create `yourStudentID_Assignment1.zip`.