Assignment 2

Due: 11:55 pm 12 August 2023
Total Mark: 17 (17% of Final Mark)

General Instructions: Please read the following instructions carefully.

Implementing Pay-to-Multi-Signature (P2MS)

In this assignment, your task is to implement a program creating/executing P2MS script using the **Pycryptodome** package.

The requirements for the program are as follows:

1) Use **Python 3.5 or above** and **Pycryptodome** package.
2) To simulate P2MS script, the program takes two parameters – the number of signatures (M) for scriptSig and the number of public keys (N) for scriptPubKey. N is equal to or greater than M and outputs scriptPubKey (in scriptPubKey.txt) and scriptSig (in scriptSig.txt).
   a) The program is needed to generate N pairs of DSA 1024 bits public keys/private keys randomly.
   b) The program generates M DSA signatures using the private keys generated in a). The text – "CSCI301 Contemporary Topics in Security 2023" is signed in each signature and they must be signed by the different private keys.
   c) scriptPubKey and scriptSig must be generated using the values generated in a) and b)
3) Your program is needed to execute a P2MS script by taking scriptPubKey and scriptSig. In particular, the program 1) takes scriptPubKey and scriptSig from files 2) constructs a script and 3) executes the script. You can implement this in a separate program.

Additional information:

1) The scriptPubKey and scriptSig must be properly formatted and all values written in them must be represented as hexadecimal numbers.
2) It should be noted that the program is using DSA 1024 bits as a signature algorithm.
3) It should be noted that the text signed in the signatures is fixed as "CSCI301 Contemporary Topics in Security 2023".
4) scriptPubKey and scriptSig must include the proper operators to be executed.

Submission

Write a program(or programs) that satisfies the above requirements. Make a folder named `Assignment2` and include

- A creating/executing program for a P2MS script, which satisfies the above requirements. [13 marks]
- Three different pairs of scriptSig and scriptPubKey which are generated by your program. [2 marks]
- A `report` that explains 1) all necessary information to run your programs (e.g., additional python packages for your code) expected outcomes (with screenshots) for the program(s). [2 marks]

Use the Subject Moodle site to upload your assignment. Compress the `Assignment2` folder using a zip program to create `yourStudentID_Assignment2.zip`.