Assignment 2

Due: 11:55 pm 15 Aug 2022
Total Mark: 100 (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 programs creating/executing P2MS script using the **Pycryptodome** package.

The requirements for the programs are as follows:

1. Use **Python 3.5 or above** and **Pycryptodome** package.
2. To simulate 2-of-4 P2MS script, the program (randomly) is needed to generate 4 pairs of DSA 2048 bits public keys/private keys under the same public parameters (g, p, q).
   a) The public keys are written in the scriptPubKey (i.e., scriptPubKey.txt) in the following format:

      OP_2 [PubKey1] [PubKey2] … [PubKey4] OP_4 OP_CHECKMULTISIG

   b) The program generates 2 DSA signatures using the private keys generated. The text – "Contemporary topic in security" is signed in each signature and they must be signed by the different private keys. The signature is stored in the scriptSig (i.e., scriptSig.txt) in the following format:

      OP_1 [Sig1] [Sig2]

3. You need to implement **a separate program** to execute a P2MS script by taking scriptPubKey and scriptSig from the above task. In particular, the program 1) takes scriptPubKey and scriptSig from files 2) constructs a script and 3) executes the script. You **must** implement this in a separate program if you want. Show how the script is executed in your program by printing out the stack information for each processing step.

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 2048 bits as a signature algorithm.
3) It should be noted that the message signed in the signatures is fixed as "Contemporary topic in security".
4) scriptPubKey and scriptSig must be properly formatted as described above.
5) For the detail on how P2MS script is processed, please check the following websites:

- https://learnmeabitcoin.com/technical/p2ms
- https://wiki.bitcoinsv.io/index.php/Bitcoin_Transactions

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. [80 marks]
- **Three different pairs of scriptSig and scriptPubKey** which are generated by your program. [10 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). [10 marks]

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