Name: Toh Yong Qin

UOW id: 7059073

This report is about P2MS script.

All necessary information to run my programs.

-python 3.8.10

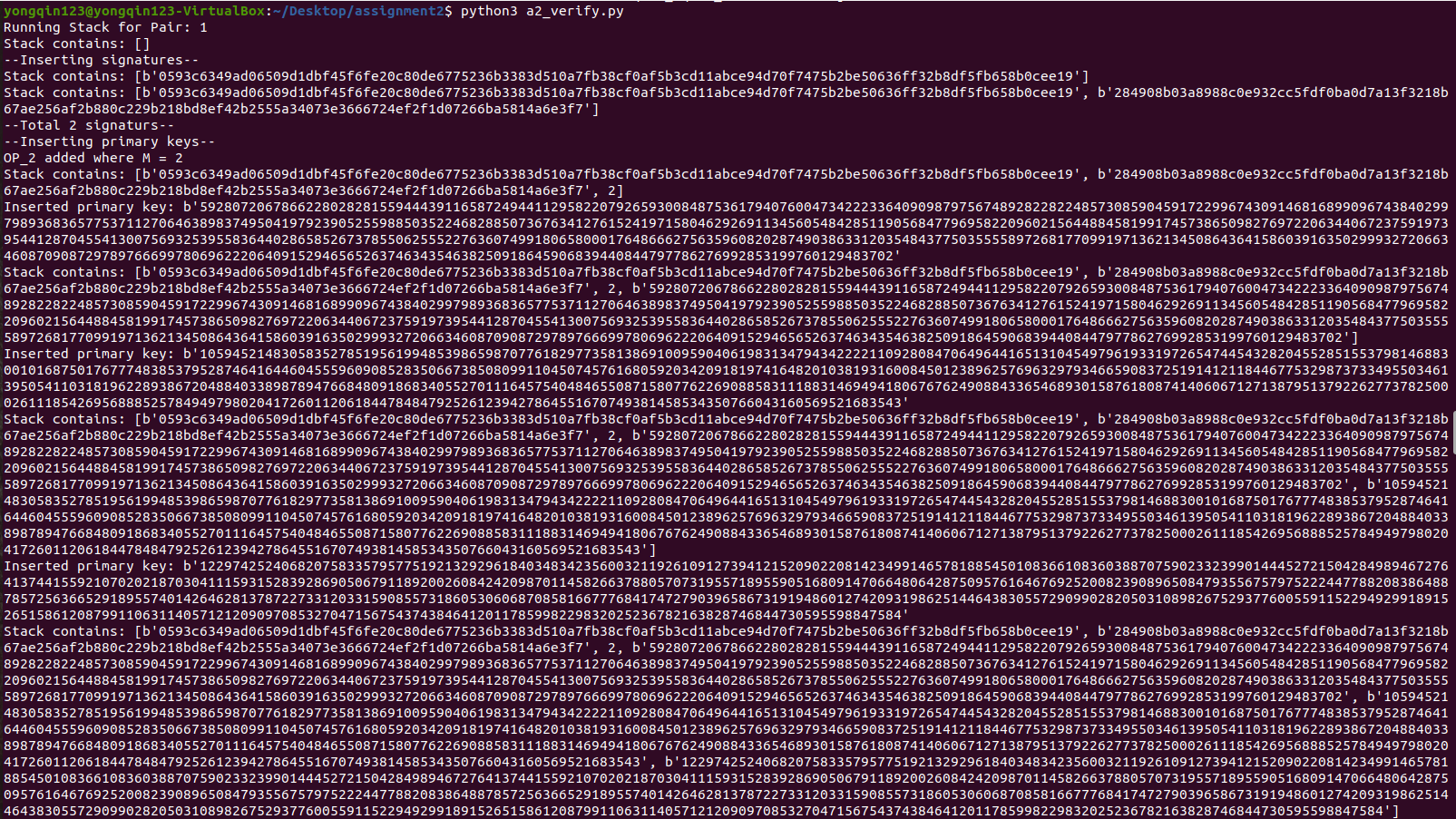
-pycryptodome libnrary

Firstly, running a2\_sign.py will generate 3 pairs of scriptPubKey.txt and scriptSig.txt files.

Text

Description automatically generated

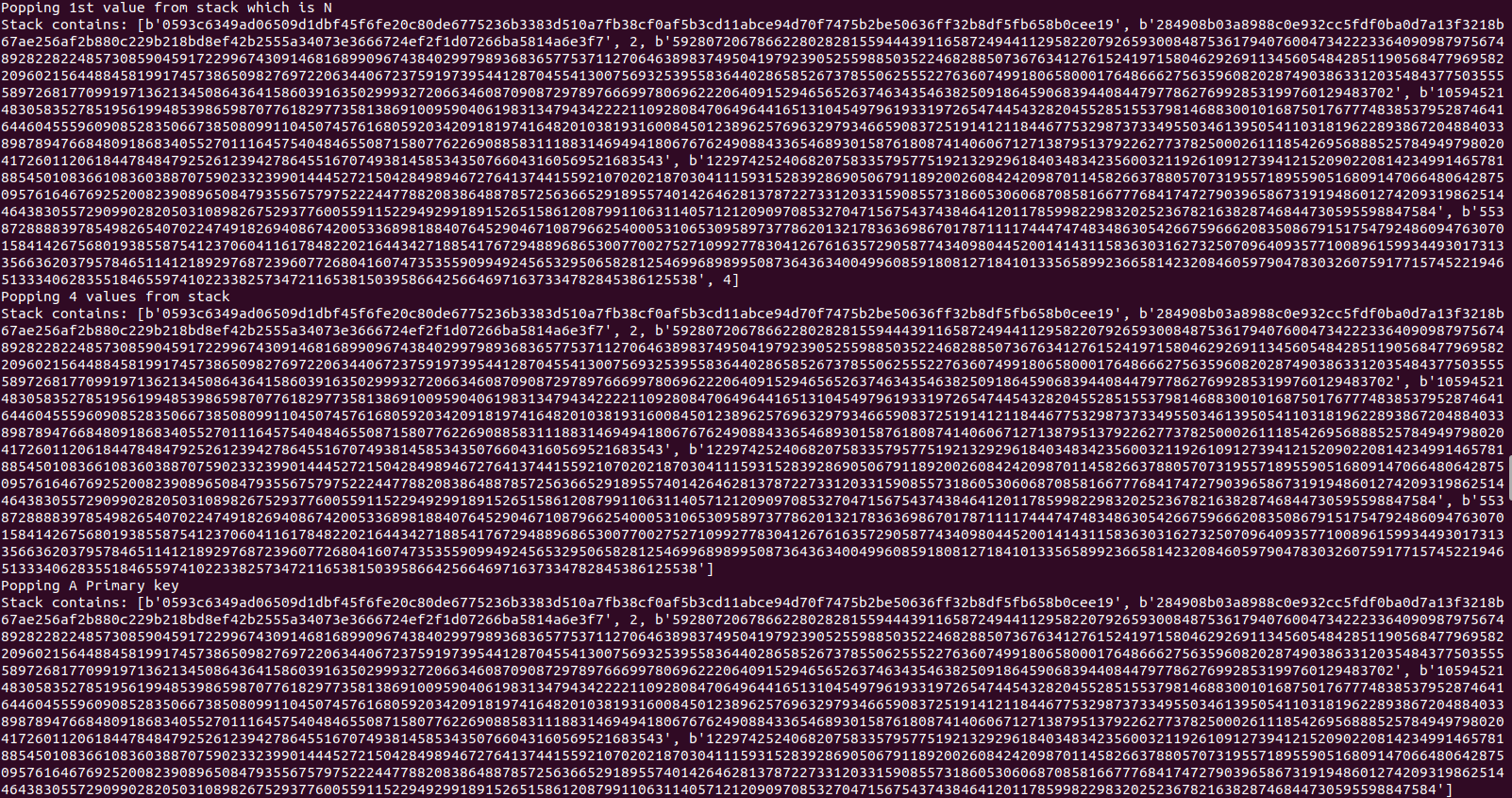
Next, run a2\_verify.py will verify if at least 2 out of 4 keys are authenticated. The two screenshots below shows the output of the script where it appends 2 signatures, then OP\_2, 4 primary keys and OP\_4 into the stack. Once at OP\_CHECKMULTISIG, the script stops appending.



Text

Description automatically generated

The screenshots below shows the output of the script where it pops all value one by one starting from the N value which is OP\_4, 4 primary keys, M value which is OP\_2 and then 2 signatures. The signatures will then be authenticated with each public key. If there are 2 valid keys the program will stop and the value 1 will be appended to the stack which shows that the signatures are authenticated.



A picture containing background pattern

Description automatically generated

Text

Description automatically generated