**Public key generation**

**A screenshot of a computer

Description automatically generated**

Running the pubkeygen.py script to generate the public key and domain parameters to be used. The file dsa\_public\_key.pem will be generated. (Privacy enhanced mail)

**Generating scriptPubKey and scriptSig**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Enter the number of public keys to be generated and the number of signatures to be signed. 3 pairs of scriptPubKeys and scriptSigs will be generated and saved as .txt files. scriptPubKey1 will be paired with scripSig1 and so on.

**Number of PubKey > Number of Sigs**

**A screenshot of a computer program

Description automatically generated**

No errors encountered if number of pubkeys > sigs.

**Number of Sigs > Number of PubKeys**

A computer code with white text

Description automatically generated

Program displays an error message and prompts the user to reenter the number of public key and sigs

**Hexadecimal formatted and operators for scriptSig.txt**

**A screenshot of a computer

Description automatically generated**

4 signatures signed = OP\_M where M = 4

4 different signed signatures in hexadecimal format.

**Hexadecimal formatted and operators for scriptPubKey.txt**

**A screenshot of a computer

Description automatically generated**

6 pub keys generated = OP\_N where N = 6

6 different pubkeys generated and in hexadecimal format.

OP\_CHECKMULTISIG operator at the end.

**Simulation of P2MS verification (6pubkeys, 4sigs)**

**A computer screen shot of a program

Description automatically generated**

scriptPubKey1.txt and scriptSig1.txt (correct pair)

The program finds the correct pubkey match for the first signature. Once that is found the index of the pubkey is flagged and then the subsequent key-sig pairs can be found as they are in order. If the number of correct key-sig pairs and M tallies, 1 is pushed into the stack.

**Simulation of P2MS verification (6pubkeys, 4sigs) (Wrong pubkey – sig pair)**

A computer screen shot of white text

Description automatically generated

scriptPubKey2.txt and scriptSig3.txt (wrong pair)

The program is unable to find any matching public keys for the first signature. It displays that no key-sig pairs are found and 0 is pushed into the stack.

**Simulation of P2MS verification (4pubkeys, 4sigs)**

**A computer screen shot of a program

Description automatically generated**

scriptPubKey3.txt and scriptSig3.txt (correct pair)

The program finds all the key pairs and pushes a 1 into the stack.

**Simulation of P2MS verification (4pubkeys, 4sigs) (Wrong pubkey – sig pair)**

**A computer screen shot of white text

Description automatically generated**

scriptPubKey1.txt and scriptSig2.txt (wrong pair)

The program checks through the key-sig pairs. Since all of them are wrong matches, it returns an error message and pushes a 0 into the stack.