**Assignment 2: Report**

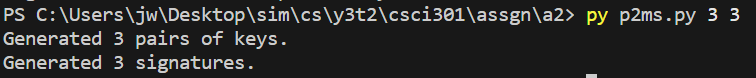
This assignment is written on Python 3.10.12 and uses the pycryptodome package.

As the program takes in command-line arguments, each program should be executed with the relevant values. For p2ms.py, two arguments are taken to generate the number of signatures (M) and public/private key pairs (N).

Command-line script for generating 3 signatures and 3 pairs of keys

For verify.py, two arguments are taken as well, and they are used to obtain the files of public keys and signatures to read.

Command-line script for reading files ‘scriptPubKey.txt’ and ‘scriptSig.txt’

Upon running p2ms.py, the command-line arguments would be saved as variables M and N in the program, then generates the keys N times and the signatures M times. The generated public keys are written into scriptPubKey.txt, while the private keys are saved in an array and used for generating the signatures. These signatures would then be written into scriptSig.txt. The terminal would print a statement after all public keys are written in, and another statement after all signatures are written in.

scriptPubKey.txt will contain the value of N on the first line and the generated public keys (parameter y), while scriptSig.txt will contain the value of M on the first line and the generated signatures. Each line break represents a new entry, and all contents of the file are written in hexadecimal numbers.

A screen shot of a computer

Description automatically generatedAfter running verify.py, the command-line arguments would be set as the file names to open for reading. These files would be the same files that were written into in p2ms.py, which are scriptPubKey.txt and scriptSig.txt. The retrieved values are first merged into an array which would serve as a stack, then the stack values are categorized into two arrays containing the public key and signature values. A statement would be printed in the terminal to indicate the completed construction of the stack, and another statement is printed when the stack has all its values gone through and categorized. The program then iterates through the array of signatures to find its matching public key (which will be identified through iteration of the public key array), and prints out the verification result accordingly.

Verification of signatures with each public key, which will indicate signatures in numerical order (1, 2, 3, …) and public keys by their array index (0, 1, 2, …)