Name: Truc Ho Nguyen

NetID: thv20002

Section: 8

VM IP Address: 172.16.49.54

1. To find the answer for Question 1, I opened the Q1hash.txt file and read its contents. Then I manually used the sha256sum command on every .exe file in the Q1files directory until one returned the correct hash (sob.exe).

2. To find the answer for Question 2, I wrote the program Q2.py which opened every .exe file in the Q2files directory and performed the sha256 hash. If the hash matched the contents of Q2hash.txt, it would print the file (fungicidal.exe).

3. To find the answer for Question 3, I wrote the program Q3.py which opened every .exe file in the Q3files directory and verified its signature with its respective .exe.sign file using the public key given in Q3pk.pem. If the verification was successful, it would print the file (condor.exe). To experiment, I tested the time required for verifying signatures with hashed data compared to the time required for unhashed data.

4. To find the answer for Question 4, I wrote the program D4.py which opened Encrypted4 and used the same variable and encryption key found in R4.py. Then, it printed the decrypted information (perigon36&).

5. To find the answer for Question 5, I wrote the program D5.py which opened Encrypted5 and created the same variable found in R5.py. Then, it used the same key found in R5.py and printed the decrypted information (commutual22$).

6. For Question 6, I followed the directions to write the programs KG6.py, R6.py, AD6.py, and D6.py. I chose the same AES-CBC cryptosystem used in questions 4-5, because it was symmetric and I already had experience using it. I also chose a key size of 2048 bits for a good balance of security and time performance. I showed my code to a TA to receive my approval code (ZQ5F7I).