**Readme File for DH project.**

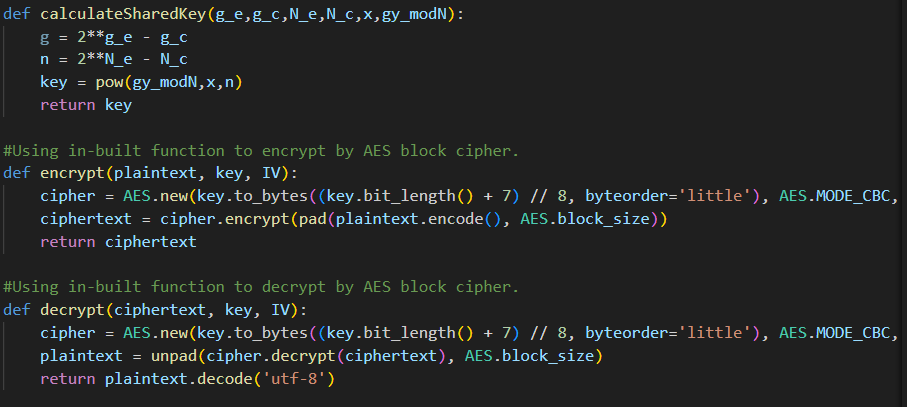
***Setup Steps:***

Please ensure python is installed on the Operating System running the program. Please also ensure that the “pycryptodome” version 3.19.0 python module installed. Please install it using the following command:

**pip install pycryptodome**

***Diffie Hellman program:***

Script written in python for the DH challenge.



Screenshot showing DH.py python script for required functions.



***Input parameters***

Following input parameters are supplied to the program (according to example provided in the question prompt):

IV: "A2 2D 93 61 7F DC 0D 8E C6 3E A7 74 51 1B 24 B2"

g\_e: 251

g\_c: 465

N\_e: 255

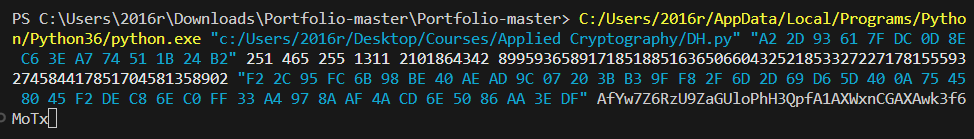
N\_c: 1311

X: 2101864342

g^ymodN: : 8995936589171851885163650660432521853327227178155593274584417851704581358902

ciphertext : "F2 2C 95 FC 6B 98 BE 40 AE AD 9C 07 20 3B B3 9F F8 2F 6D 2D 69 D6 5D 40 0A 75 45 80 45 F2 DE C8 6E C0 FF 33 A4 97 8A AF 4A CD 6E 50 86 AA 3E DF"

plaintext: AfYw7Z6RzU9ZaGUloPhH3QpfA1AXWxnCGAXAwk3f6MoTx



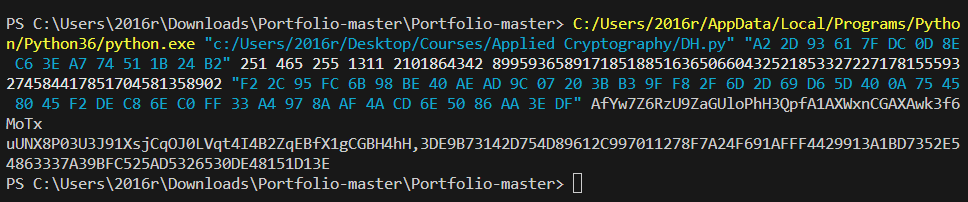
Screenshot showing input values.

***Running the program***

The program can be run with the help of the following command:

**python DH.py "A2 2D 93 61 7F DC 0D 8E C6 3E A7 74 51 1B 24 B2" 251 465 255 1311 2101864342 8995936589171851885163650660432521853327227178155593274584417851704581358902 "F2 2C 95 FC 6B 98 BE 40 AE AD 9C 07 20 3B B3 9F F8 2F 6D 2D 69 D6 5D 40 0A 75 45 80 45 F2 DE C8 6E C0 FF 33 A4 97 8A AF 4A CD 6E 50 86 AA 3E DF" AfYw7Z6RzU9ZaGUloPhH3QpfA1AXWxnCGAXAwk3f6MoTx**

(Note: Please ensure that you are in the same directory as the DH.py file.)



Screenshot showing running the program.

Please note I am using powershell as the CLI a windows machine and have provided the full path to the python executable as well as the DH.py file. It can be replaced by “python” and “DH.py” if you are in the same directory as the DH.py file and python is installed on your OS.

***Output***

Following is the output received after running the program:

uUNX8P03U3J91XsjCqOJ0LVqt4I4B2ZqEBfX1gCGBH4hH, 3D E9 B7 31 42 D7 54 D8 96 12 C9 97 01 12 78 F7 A2 4F 69 1A FF F4 42 99 13 A1 BD 73 52 E5 48 63 33 7A 39 BF C5 25 AD 53 26 53 0D E4 81 51 D1 3E

Here uUNX8P03U3J91XsjCqOJ0LVqt4I4B2ZqEBfX1gCGBH4hH is the decrypted plaintext.

Here 3D E9 B7 31 42 D7 54 D8 96 12 C9 97 01 12 78 F7 A2 4F 69 1A FF F4 42 99 13 A1 BD 73 52 E5 48 63 33 7A 39 BF C5 25 AD 53 26 53 0D E4 81 51 D1 3E is the encrypted ciphertext.

 Screenshot showing the output.