

Network Security Assignment#1
108064535 陳文遠(Wen-Yuan Chen)

- **ENVIRONMENT**

Operation System	Ubuntu 18.04
Compiler	GNU C/C++
Extra Library	GMP

- **INSTALL GMP ON LINUX DEBIAN SYSTEM**

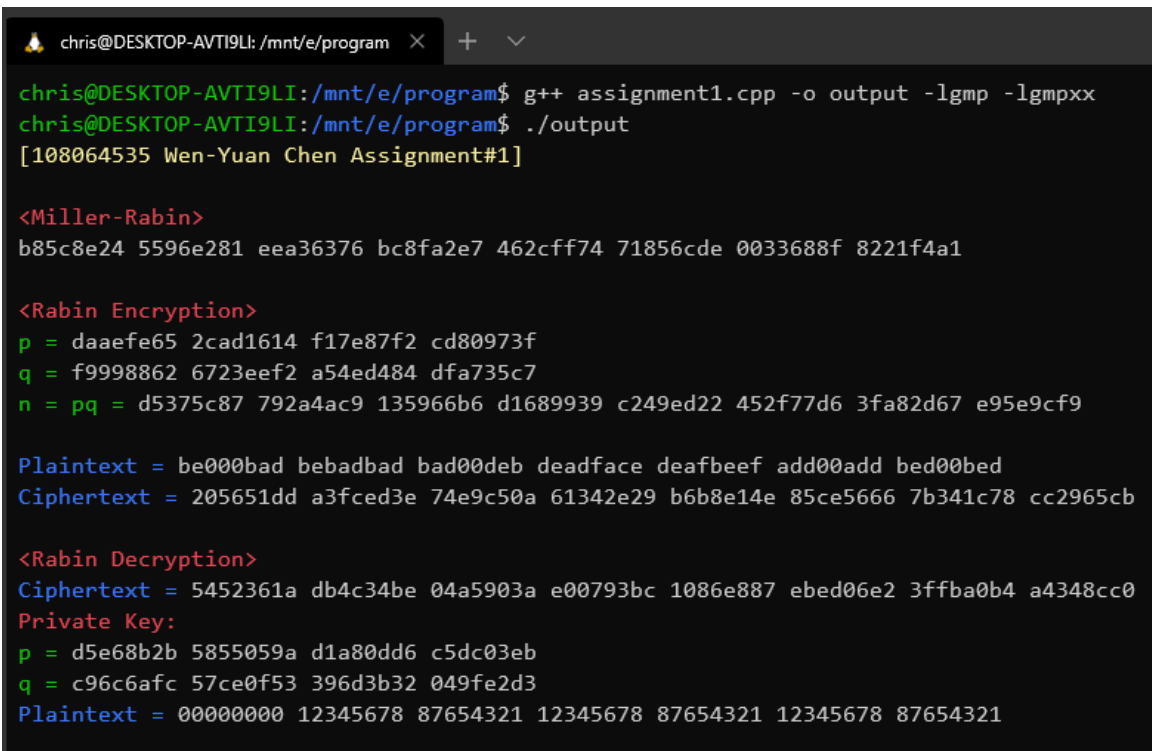
Please enter the following command to install gmp library in your linux computer terminal.

```
$ sudo apt-get install m4
$ wget https://gmplib.org/download/gmp/gmp-6.1.2.tar.bz2
$ tar -jvxf gmp-6.1.2.tar.bz2
$ cd gmp-6.1.2
$ ./configure --enable-cxx
$ make
$ make check
$ make install
```

- **COMPILE AND RUN MY PROGRAM**

```
$ g++ assignment1.cpp -o output -lgmp -lgmpxx
$ ./output
```

After compiling ,executing and typing input, the result will show on your terminal as following figure.



```
chris@DESKTOP-AVTI9LI: /mnt/e/program
chris@DESKTOP-AVTI9LI:/mnt/e/program$ g++ assignment1.cpp -o output -lgmp -lgmpxx
chris@DESKTOP-AVTI9LI:/mnt/e/program$ ./output
[108064535 Wen-Yuan Chen Assignment#1]

<Miller-Rabin>
b85c8e24 5596e281 eea36376 bc8fa2e7 462cff74 71856cde 0033688f 8221f4a1

<Rabin Encryption>
p = daaefe65 2cad1614 f17e87f2 cd80973f
q = f9998862 6723eef2 a54ed484 dfa735c7
n = pq = d5375c87 792a4ac9 135966b6 d1689939 c249ed22 452f77d6 3fa82d67 e95e9cf9

Plaintext = be000bad bebadbad bad00deb deadface deafbeef add00add bed00bed
Ciphertext = 205651dd a3fced3e 74e9c50a 61342e29 b6b8e14e 85ce5666 7b341c78 cc2965cb

<Rabin Decryption>
Ciphertext = 5452361a db4c34be 04a5903a e00793bc 1086e887 ebed06e2 3ffba0b4 a4348cc0
Private Key:
p = d5e68b2b 5855059a d1a80dd6 c5dc03eb
q = c96c6afc 57ce0f53 396d3b32 049fe2d3
Plaintext = 00000000 12345678 87654321 12345678 87654321 12345678 87654321
```

If you don't understand my instructions or cannot execute, please let me know, I will try my best to figure out the problem.