

Network Security Homework3

109064518 高聖哲(Kao Sheng-Che)

- **Develop Environment**

Operation System	Ubuntu 16.04
Compiler	GNU C/C++
Extra Import Library	gmp

- **Set up on Linux Debian System-Step Description**

Enter the following command to install gmp library in Linux 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 the Program**

```
$ g++ 109064518_hw3.cpp -o hw3.out -lgmp -lgmpxx
$ ./hw3.out
```

- **Function of Miller-Rabin:**

- **mpz_class:GenerateRandomPrimeNum**
 - ◆ 首先會先產生隨機的 seed,並使用 Miller-Rabin Method 來決定 larger number 是否為 prime number, 並印出處理後的 256-bit prime number 結果
- **mpz_class:RabinEncryption**
 - ◆ 輸入所需要的明文, 並進行加密動作
- **mpz_class: sortAnswer**
 - ◆ 排序 m1~m4 的順序
- **GCDstruct eGCD:Euclidean algorithm**
 - ◆ 透過 Euclidean algorithm 計算 gcd
- **mpz_class:RabinDecryption**
 - ◆ 輸入所需要的密文, 以及使用 Euclidean algorithm 所產生的值進行解密動作

- The compile result of the Ubuntu terminal

```

jerry86064@jerry86064-VirtualBox: ~/Desktop/109064518_hw3
File Edit View Search Terminal Help
jerry86064@jerry86064-VirtualBox:~/Desktop/109064518_hw3$ make
g++ 109064518_hw3.cpp -o hw3.out -lgmp -lgmp
jerry86064@jerry86064-VirtualBox:~/Desktop/109064518_hw3$ ./hw3.out
[109064518 Sheng-Che Kao Assignment#3]

<Miller-Rabin>
ab4306e9 944e8798 c610d092 3980cbad 654864a9 6dcdb69b bab62867 cfa21d83

<Rabin Encryption>
p = daafe65 2cad1614 f17e87f2 cd80973f
q = f9998862 6723eef2 a54ed484 dfa735c7
n = pq = d5375c87 792a4ac9 135966b6 d1689939 c249ed22 452f77d6 3fa82d67 e95e9cf9

Plaintext = be00bad bebadbad bad00deb deadface deafbeef add00add bed00bed
Ciphertext = 205651dd a3fced3e 74e9c50a 61342e29 b6b8e14e 85ce5666 7b341c78 cc2965cb

```

Fig.1 Miller Rabin Encryption

```

<Rabin Decryption>
Ciphertext = 5452361a db4c34be 04a5903a e00793bc 1086e887 ebed06e2 3ffba0b4 a434
8cc0
Private Key:
p = d5e68b2b 5855059a d1a80dd6 c5dc03eb
q = c96c6afc 57ce0f53 396d3b32 049fe2d3
Plaintext = 00000000 12345678 87654321 12345678 87654321 12345678 87654321

```

Fig.2 Miller Rabin Decryption