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

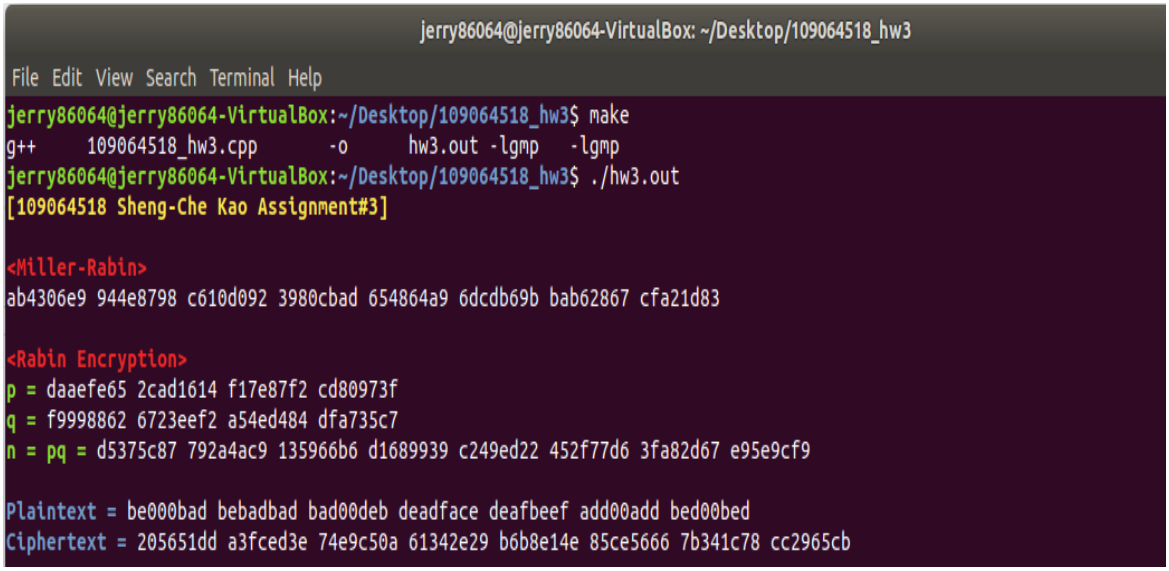

Fig.1 Miller Rabin Encryption

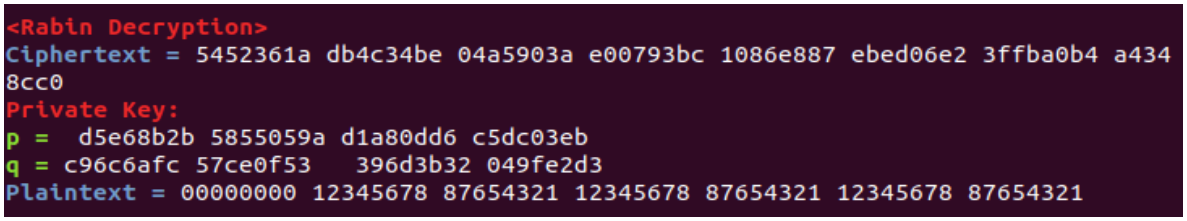

Fig.2 Miller Rabin Decryption