HW4

建置環境

- Python 3.6.5 :: Anaconda, Inc. on windows 10

使用方式

- 命令列輸入 `python main.py -init <NumOfBit>` 建立 RSA key 相關資訊，無輸入 `<NumOfBit>` 預設為 1024 bit
- 命令列輸入 `python main.py -init <prime1> <prime2>` 用質數建立 RSA key 相關資訊
- 命令列輸入 `python main.py -e <text> <N> <key>` 使用加密
- 命令列輸入 `python main.py -d <text> <N> <key>` 使用解密
- 命令列輸入 `python main.py -d <text> <N> <key> <p> <q>` 快速解密
- 其實加解密都一樣，所以 `-d` or `-e` 都沒關係
- 明文、密文、N、key、p、q 輸入 16 進制，ex `0x1234567890abcdef` or `1234567890abcdef`

實作部分

1. 小數字 RSA 加解密
    - ./RSA.py
2. 1024 bit RSA
    - ./RSA.py
3. 產生大質數
    - ./RandPrime.py
4. Square & multiply
    - ./SquareAndMultiply.py
5. Chinese Remainder Theorem
    - ./RSA.py

實作過程困難與心得

- 在實作大質數時，發現時產生出來的數字竟然有偶數，於是在 Miller–Rabin 前面加上了已知小質數的判斷
- 有一次不小心隨機出兩個相同的質數，導致計算結果不一樣，後來讓他們大小差 1 bit 就永遠不會不一樣了
- 實作中國餘式定理時，因取 mod 自己筆記的方式有點不樣，導致公式有點錯亂，算出錯誤的值

截圖

```
D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -init 0x47 0x53

p =  0x47    71
q =  0x53    83
N =  0x1705
Public  Key =  0x3
Private Key =  0xef3

D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -e 0x7e2 0x1705 0x3

0x8ad   2221

D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -d 0x8ad 0x1705 0xef3

0x7e2   2018
```

```
D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -init

p =  0xcaaa7e968efb9d61d9167e442fea0ef160684eacafd9c5883a88e706c1278c4cf58453c5d06840c13f1c269fd2b675392a25b1b9eb6a724ac46c941e37013f13
q =  0x142eb0d1ed3e4c200dbd34865bc6928e226c6e07089b9919860365b5adbe3e4d94565286876d474a32762a1221889d750611f0fae8c1c353cb916484c42c80943
N =  0xffa4881ea435d79acc40ed4160af85964a9334908299cad49369359778ffde3ccc6d14628c34589464a190e202868d7eb0da2671e447c8091c9d0415ab7186b243f408350a253e14c358cbb1742afc9b62d2f2de89f0cb46d932f50cf62a2229e5f699238d6c3ec22769c44d4064eaac5a845e62c698ce11902730b79d632cf9
Public  Key =  0x3
Private Key =  0xaa6db0146d793a6732d5f380eb1fae6431b77860571131e30cf0ce64fb553ed332f362ec5d783b0d986bb5ec01af08ff20916ef6982fdab0bdbe02b91cf659cacee9a8551a2de9cc099f58afafe52dda926d2d2b8ae8f8197ef7cc723b69cb57c75e134e2eca5b93d5f1fdb238c3141734d513518a0c19b161c2e2de17bbedc3

D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -e 0x123456789eeefff 0xffa4881ea435d79acc40ed4160af85964a9334908299cad49369359778ffde3ccc6d14628c34589464a190e202868d7eb0da2671e447c8091c9d0415ab7186b243f408350a253e14c358cbb1742afc9b62d2f2de89f0cb46d932f50cf62a2229e5f699238d6c3ec22769c44d4064eaac5a845e62c698ce11902730b79d632cf9 0x3

0x1790fc5120b2d1354b9a81e857bb27c397d3acccfff

D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -d 0x1790fc5120b2d1354b9a81e857bb27c397d3acccfff 0xffa4881ea435d79acc40ed4160af85964a9334908299cad49369359778ffde3ccc6d14628c34589464a190e202868d7eb0da2671e447c8091c9d0415ab7186b243f408350a253e14c358cbb1742afc9b62d2f2de89f0cb46d932f50cf62a2229e5f699238d6c3ec22769c44d4064eaac5a845e62c698ce11902730b79d632cf9 0xaa6db0146d793a6732d5f380eb1fae6431b77860571131e30cf0ce64fb553ed332f362ec5d783b0d986bb5ec01af08ff20916ef6982fdab0bdbe02b91cf659cacee9a8551a2de9cc099f58afafe52dda926d2d2b8ae8f8197ef7cc723b69cb57c75e134e2eca5b93d5f1fdb238c3141734d513518a0c19b161c2e2de17bbedc3

0x123456789eeefff

D:\AllProjects\python\Information-Security-Homework\HW4\YoYo>python main.py -d 0x1790fc5120b2d1354b9a81e857bb27c397d3acccfff 0xffa4881ea435d79acc40ed4160af85964a9334908299cad49369359778ffde3ccc6d14628c34589464a190e202868d7eb0da2671e447c8091c9d0415ab7186b243f408350a253e14c358cbb1742afc9b62d2f2de89f0cb46d932f50cf62a2229e5f699238d6c3ec22769c44d4064eaac5a845e62c698ce11902730b79d632cf9 0xaa6db0146d793a6732d5f380eb1fae6431b77860571131e30cf0ce64fb553ed332f362ec5d783b0d986bb5ec01af08ff20916ef6982fdab0bdbe02b91cf659cacee9a8551a2de9cc099f58afafe52dda926d2d2b8ae8f8197ef7cc723b69cb57c75e134e2eca5b93d5f1fdb238c3141734d513518a0c19b161c2e2de17bbedc3 0xcaaa7e968efb9d61d9167e442fea0ef160684eacafd9c5883a88e706c1278c4cf58453c5d06840c13f1c269fd2b675392a25b1b9eb6a724ac46c941e37013f13 0x142eb0d1ed3e4c200dbd34865bc6928e226c6e07089b9919860365b5adbe3e4d94565286876d474a32762a1221889d750611f0fae8c1c353cb916484c42c80943

0x123456789eeefff
```