

RSA实验报告

姓名：周泽龙
学号：2020213990
课程：应用密码学
日期：2020年11月15日

1 完成内容

软件实现RSA：

- 1024位以上公私钥的生成
- 768位以下公私钥在 **1s内生成**
- 明文加密、密文解密
- 图形界面**GUI**
- 语言：C++
- IDE：Visual Studio 2019

2 程序使用说明

2.1 非图形界面

```
Microsoft Visual Studio 调试控制台
请输入模N位数（十进制位数）：78
RSA init...
Total time:171ms
素数p: 870052406392997634143074650531411155567
素数q: 776787004535730300442426832916160147463
公钥N (e=65537): 675845402551120515882664136204939336075618177864504329618041809341745953376521
密钥d: 198039811260688136274328731429263698520904917583387488818973937411092392531537

请输入明文（10进制数字串）：1234567890112233445566778899
密文：462190910874701679556154446206912230557646444011776059699040188363530820720207
解密：1234567890112233445566778899
```

- 首先输入想要的模N的位数
 - **10进制表示**
- 程序自动生成公私钥
- 其次输入想要加密的明文
 - **10进制数字串**
- 程序自动生成密文，并自动对密文解密
- 2进制，10进制位数对照与公私钥生成时间表如下：

2进制位	10进制位	时间 (ms)
256	78	171
768	232	968
1024	309	7598
2048	617	205170

```
C:\Users\Administrator\Desktop\20201213990_周泽龙_RSA\bin\RSAin\RSA.exe
请输入模N位数（十进制位数）：232
RSA init...
Total time:968ms
素数p: 45528544538452017030194842856593331623302722744222974924236673170139046363225184873533504979796587427113696287874
767
素数q: 72384967491668591120048630238758522416311438477431027953131205443168908969882268409448124827586025009308058681370
603
公钥N (e=65537): 3295582216358834832781179646694071871718071576709933243668080781355091240866324423238479793459913689225
521009844307581500554917146654480943753158976099034606255730286154546779909998092122466438882921787790769527775817200577
579274501
密钥d: 16658185770071733754297898615443874283901392666992684828874149265903246644823340886616891239749540074000005263150
94882985915890542927457727820584825066206098892454452557919230547075449671248697228583010081239498036640600882808221845
请输入明文（10进制数字串）：4353453453464564565756756754675674567567567567
密文：499346620801806347194266308332426431272684083950927181488665389894312626266616659363723780735375067392631115724409
925628701348392558235197215173857899878245621174018042723638435446192394720674477852293423777984863128148340442370516
解密：4353453453464564565756756754675674567567567567
```

```

Microsoft Visual Studio 调试控制台
请输入模N位数（十进制位数）：310
RSA init...
Total time:7598ms
素数p: 56078018706589679275440974736785701551319081995394195775678226730567508098162929352191713015016738899613863478719
355130708744023848370290174003838919964183
素数q: 59388276267503574739067807706007893654926554232044840422186973582673049983582918245406714890509556112984015555291
568561614350413154861987501202834383200559
公钥(n, e=(65537)): 3330376867481181359858423533047182343031708639809690611757998647610693063560366662239250926414860270989
416225363812932667134322290701563003683106812223958056797841351395088273500454482041127778163523413608897552494304569748
692461319005081360115586671928197348703849701504494855249069975447647040370853185578297
密钥(d): 31004311066841911763993185009731096802272091724074773578982714113862948440414588827157358060702115576484468733981
865915114698456078289174356579293044754584725654257529630515862734012002162207192555981049269203803749165951763781492365
76047107253746769876129026615860581255106643450546514195097665553762652941329
请输入明文（10进制数字串）：1234567890112233445566778899
加密: 325941439075032197714882982734774199747738408949748462931399628787426317556984216869987882423180141309374488174798
871355776683474561206392434429166137588602324230099301809580690003095535283641788748384973065329813666883269137403010461
2411888998510298497970667663696432002404445561822958508851695430643198241972
解密: 1234567890112233445566778899

```

```

Microsoft Visual Studio 调试控制台
请输入明文(10进制数字串)：618
RSA init...
Total time:205170ms
素数p: 27314490840376436293866543202012649148495499719316018944462037847871677073867842737818983285278278011752158963797
417056690274032542941242569010324931054151122379794276340134201975118418343643279663266582693194150598601813271707011196
2763014103513801769015971712605226252295041900421372840134629586013855799811
素数q: 11503720854658909405499864541282355648506493987437277141475520741458554574813079835741460931336609039255405691273
716256824217101316798925967504665361064334410209280896770548313438969894905068455152001088338780748802660874766179440593
98580499242048746215702810186031058874361723283743886851790316994956304171
公钥n (e=65537): 3142182779148281703251189583745827282808649164633313376190102893894689575435139321053704912375983758540
46260617995191736428763619170317433845221812117093443453654888182632514164002843353917144079465756008856723935309569340
942081727139458081203633973531865983196915605559730483807565565418968609856464955786704815551339268254988551938539323632
159429041159751234424854584356760603102970652553019291030453163670021275068817325846791030591933587397845688700229085294
380814162371311246498364135328754194125048279954977318079914727360510270072074045491605487246350606016143268655150336267
5047091288617862148853285800311681
密钥d: 13022388340089793451333683306242338652775914673552427248892993150597931482734000503401083223987075219451309652021
5563769367320014503238014401441433013814930859669750632530925810109893416120410721203341985351626799749374212004344008404686
030001517245510529181838041047259527077504260295297056982255277524367100129947228854246762904802412103384490218928373443
37868339674279460603155518114952371327964621253743905160295922692183092817237061920860546652313420988998268992344269892
334151016729619333657040207394467071523603379179078415851964907076998922826097591884362175451011789768917621518304630846
922014673757091006251573
请输入明文(10进制数字串)：2453246546234235246456651234545234556
密文: 240525283163991126722612647926700607271289157525505538558267906479436450857338193244962532318350765600875919427688
682346954232690288155767048245585302744479973472030608203751369182477446273890172057852789464245781629007441569555644819
7817739840357674194252087796381065451649695583297507658956741631027193363101601191778775043205566119485369340604283943
098963722093350032521237936961701805315248450025308634783126642619583703865334617310762992612854412893085726924023340204
976981413516390656193066372878043292303629149295775653503738788160035305767569494518377696910331645768802350670997882492
06935592465370389877784
解密: 24532465462342352464566512345234556

```

2.2 图形界面

RSA

模n的位数（十进制）：

618

初始化

退出

公钥N:
(e=65537)

425885192773001471135927996801494436478981121290294601231752334979
832364319461950911863290584924011782978216872190939256749794196817
33768306082135060988899169448284760852012981087958222274799371475
845447673929201162516949023545653554588197622340604251248288506309
403106260852985400867411901527965893495069194899770911435441684990
281799024625249445188503600974735476413366059744135357289982998445

私钥d:

414772940462980681114376249322504621773104170599747219323726387914
578944984028837768764182800005262677146507290558479636549874333586
526882474373931449065179560916073581473279604483133108032616987094
142047830750249822237351501073415466510534349163583129292224399838
416040760356188094987019537647824573662355332372078325770318928047
616149396174136853842526030063781191688101806891760572802348513685

素数p:

527549223103286155911632438159308492140952161531102182058852964127
571131542808568159383804198553459900164971996736608042103760037013
138952894032789588114666057799752287257391739297241071243805688481

素数q:

80728996294933344306427267033912110258467660658678387500947320820
444968458601497021501145725248836533612333692472850113987534713521
483664205857968354321642455786622979475457912827700638211339449162

明文:
(十进制
数字串)

243523454986316498475924735098763484242902420432520123429842583465
896349569346534097503947593247593475932745973495073495345991041638
94169234629649016046012374601364

加密

292803114476884458486602173492644733502536521166741914236060957824
283165601375489696754124649902280538005778950686325018271492373003
967465288981524030944633128113720259968613609231739445253874234917

解密

243523454986316498475924735098763484242902420432520123429842583465
896349569346534097503947593247593475932745973495073495345991041638
94169234629649016046012374601364

- 首先输入模n的位数，然后点击“初始化”按钮
 - 初始化过程中，按钮“加密”、“解密”和“初始化”为灰色状态，不可按
 - 初始化结束，即生成公私钥结束后，按钮“加密”变为黑色状态，可按
 - “初始化”按钮可重复点击，**重新初始化**
- 输入明文数字串
- 点击“加密”按钮
 - 按钮“解密”变为黑色状态，可按
- 点击“解密”按钮
 - 输出解密后的信息
 - 按钮“解密”变为灰色状态，不可按
- 可**重复加解密**信息

3 总结

3.1 实验感想与收获

- 太久没写C++，重新拾起后，不是在写C++，而是在写BUG
- 实现自己的高精度类，有点困难，但收获颇丰，想到了很多优化方法，如多线程、移位操作等，但没有实现，有以下两点原因：
 - 时间不足
 - 一开始的架构设计不佳，导致后期不好进行改动和优化

3.2 课程建议

- 期末大作业早点公布（>人<），不想再经历期中这种大作业堆积的困境了。