Creating a Functional, Distributable RSA App

LT Mitchell Irmer
October 30, 2023

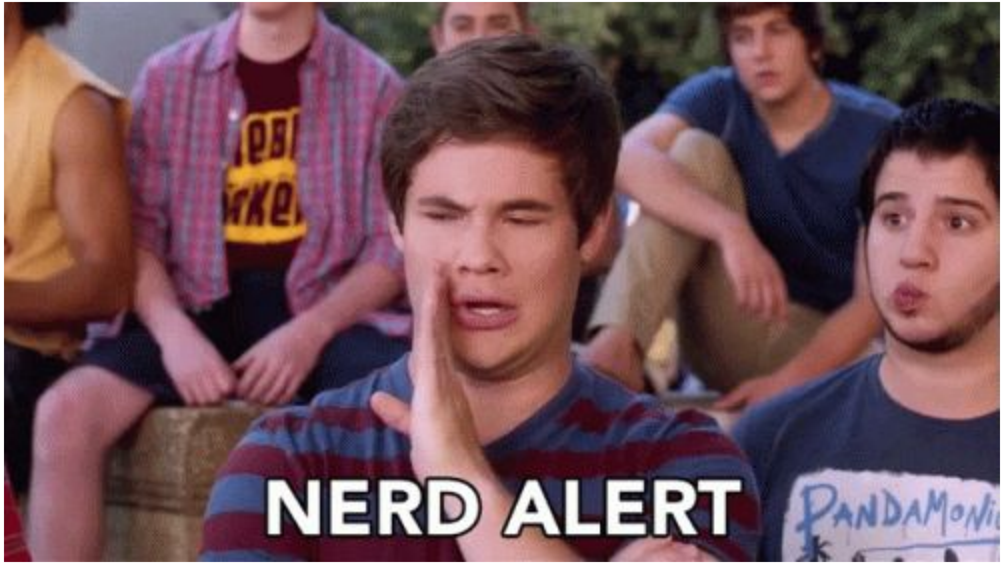
Overview

- Motivation
- Design Criteria
- Julia
- RSA Review
- Program Schematic
- Encoding Methods
- Demo

Overview

- Motivation
- Design Criteria
- Julia
- RSA Review
- Program Schematic
- Encoding Methods
- Demo

Motivation

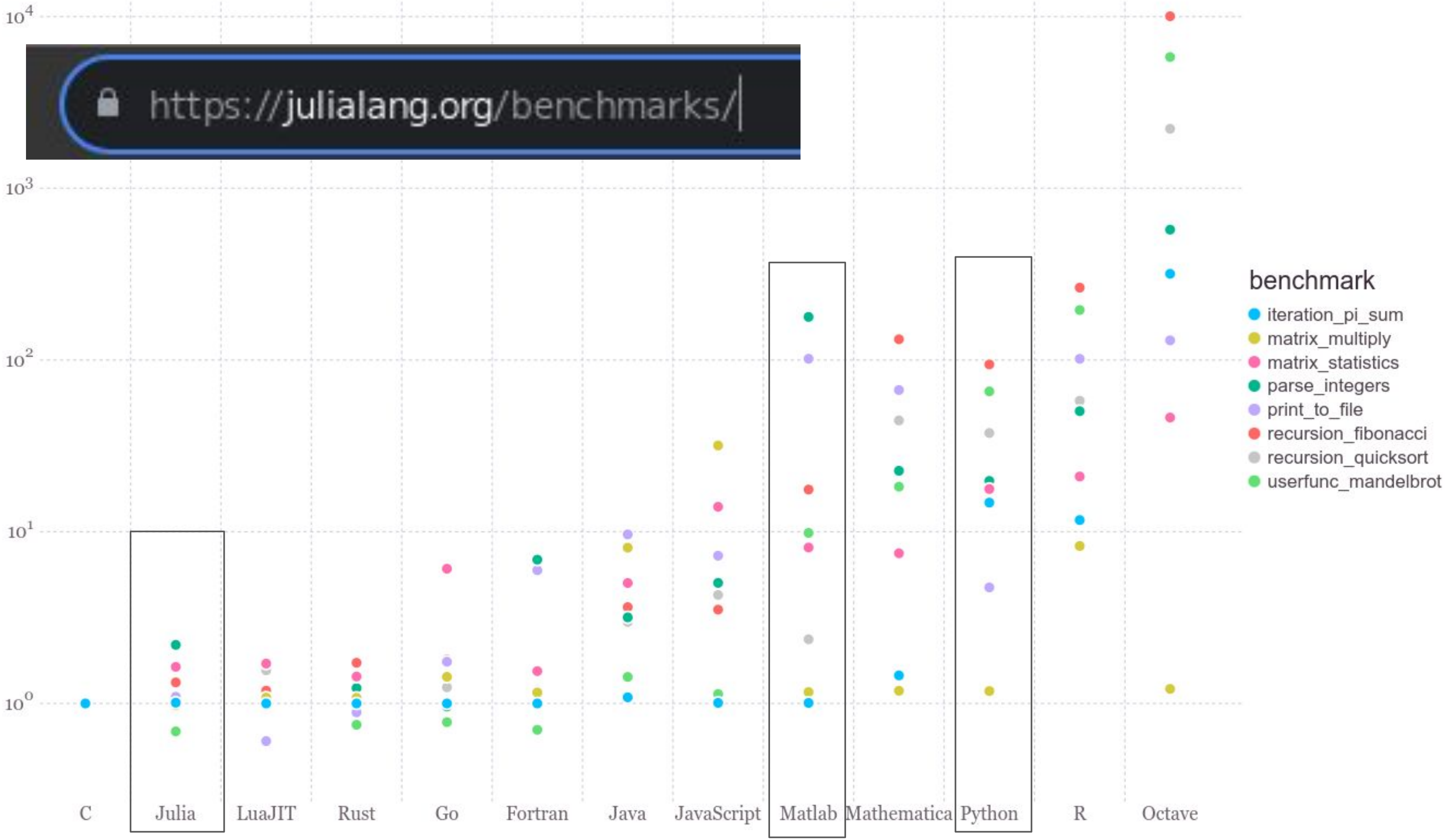


Design Criteria

- Polished enough to share a GitLab repository with other users and implement for fun with just a readme file.
- Keys saved as files for repeated use and distribution.
- Messages loaded and retrieved as files so the program can be run from command line and encoded/encrypted messages emailed as attachments or shared from public cloud storage.

Julia (https://julialang.org/)

- Open-source (MIT license) language – freely distributable.
- Nearly “machine speed” for many operations.
- Handles integers of arbitrary size (“BigInt”).
- Matlab style REPL for debugging.



https://julialang.org/benchmarks/

Overview

- Motivation
- Design Criteria
- Julia
- RSA Review
- Program Schematic
- Encoding Methods
- Demo

RSA Review

- m = plaintext message
- c = ciphertext
- n, e = public key
- d = private key
- p, q = large primes

$$n = pq$$

$$\phi(n) = (p-1)(q-1)$$

$$d = e^{-1}(mod\, \phi_n)$$

$$c = m^e(mod\, n)$$

$$m = c^d(mod\, n)$$

Program Schematic

- Key generation function
  - Generate public and private keys
  - Save as output files
- Encryption function
  - Read in a file
  - Read in encryption keys
  - Encode the message
  - Encrypt the message
- Decryption function
  - Read in a ciphertext file
  - Read in decryption key
  - Decrypt the message
  - Decode the message

Overview

- Motivation
- Design Criteria
- Julia
- RSA Review
- Program Schematic
- Encoding Methods
- Demo

Encoding Methods - Down the Rabbit Hole

- Text
  - ASCII (English letters only) -> UTF-8
  - “The Absolute Minimum Every Programmer Should Know About Unicode and Character Sets (No Excuses!)”
- Images
  - Pixels: RGB -> 3D matrix -> color planes
  - “Wingdings”:
    - JPEGs are Huffman coded
    - PNGs use libpng
- Office files
  - Combine text and images with some formatting wrappers

```
\ED\C2\FE\22\BC\C6\D6\C3\C4\37\3A\4F\8C\AE\AD\2C\D6\77\69\E6\46
\B3\49\E1\2B\95\5D\A4\F5\CE\01\3E\83\2A\1B\1C\E4\0A\EB\E1\F2\2D
\26\E0\B9\95\71\B6\E0\C8\FB\4A\F0\38\50\D9\1D\7A\0A\4D\5D\8A\2E
\B5\C4\37\D9\A3\B0\BF\0A\F2\99\6E\35\D8\DE\66\76\C9\62\70\33\F8
\01\5E\06\B2\7F\29\D4\3F\98\1B\70\04\80\18\A9\1C\ED\27\86\19\AE
\43\4A\85\73\0B\46\D9\2B\F2\B0\6E\3D\3D\6B\1A\49\EE\25\B1\11\97
\03\B6\32\A0\FA\6E\3C\0E\3A\D4\46\CD\1A\B6\D4\8F\A3\AF\A5\D3\2F
\8D\D5\95\D6\87\75\1B\5E\69\50\CF\0C\C4\EE\0A\15\8A\B2\1C\80\09
\94\B6\D3\C3\12\FC\ED\75\2E\E2\C7\81\CF\04\0C\7B\7B\0A\EA\5E\58
\7A\31\E0\76\3C\0E\BF\C4\9A\8E\93\73\FB\3A\E8\29\71\73\75\34\A7
\0F\30\4C\51\98\38\8D\B0\37\30\CE\CF\EF\0E\07\99\6B\5E\35\F3\6E
\64\86\C0\50\47\23\24\F0\38\7D\55\51\6C\A6\6B\6F\0B\EA\D3\40\93
\C1\0B\FA\0E\E7\9A\EF\7C\44\FA\A5\BF\8A\7C\09\3A\26\9F\00\B4\F1
```

Encoding Methods - Escaping the Rabbit Hole

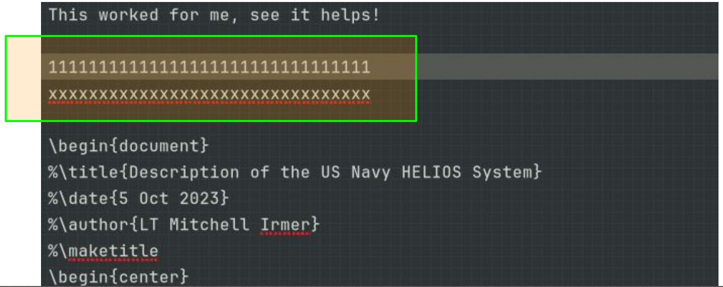
- 8-bit Unsigned Integers (UInt8)
  - 0-255, written as 0x00 to 0xff.
  - Makes data accessible as a vector of arbitrary length at the cost of making the data much larger.
  - Most important: this is the default “read” method in Julia.
- Method:
  - Convert vector of UInt8 to vector of BigInt and raise to encryption. exponent modulo public n.
  - Combine 7 consecutive BigInt into one block (compression).
  - Store blocks in new vector, save as a ciphertext file.

Encoding Methods - Data Compression

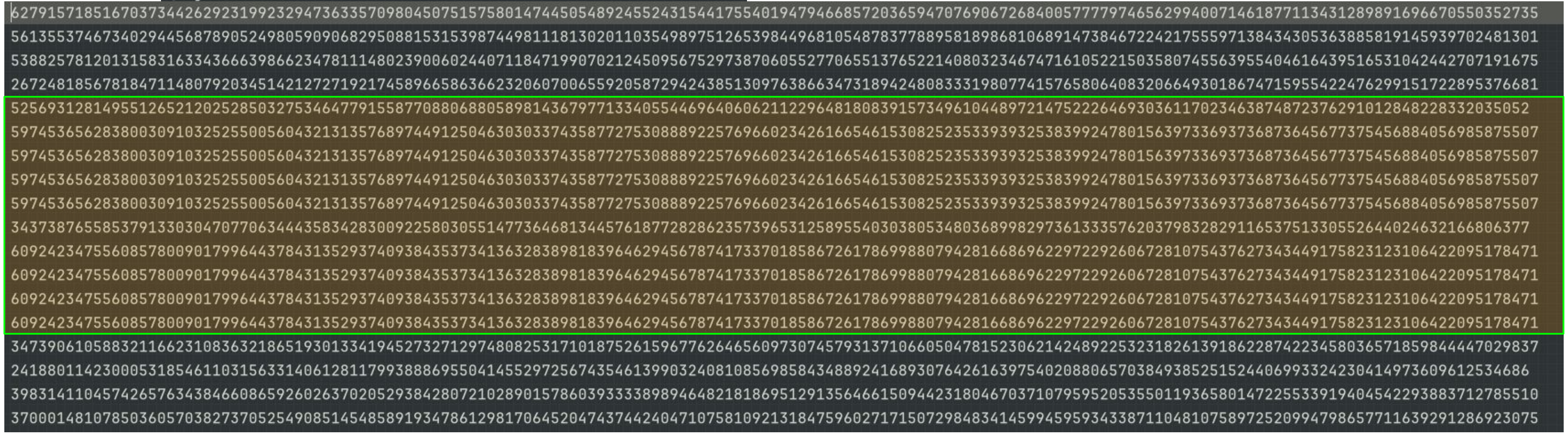
- Combining 7 UInt8 into a single BigInt block before encryption

Extension	Plain	Cipher (No Compression)	Cipher (Blocksize = 7)
.txt	5.0 kB	846.8 kB	121 kB
.odt	55 kB	7.6 MB	1.1 MB
.pdf	1.1 MB	188.2 MB	27.3 MB
.jpg	4.6 MB	Didn’t attempt, probably ~790 MB	111 MB

Cryptanalyzing the Ciphertext (.txt codewords)

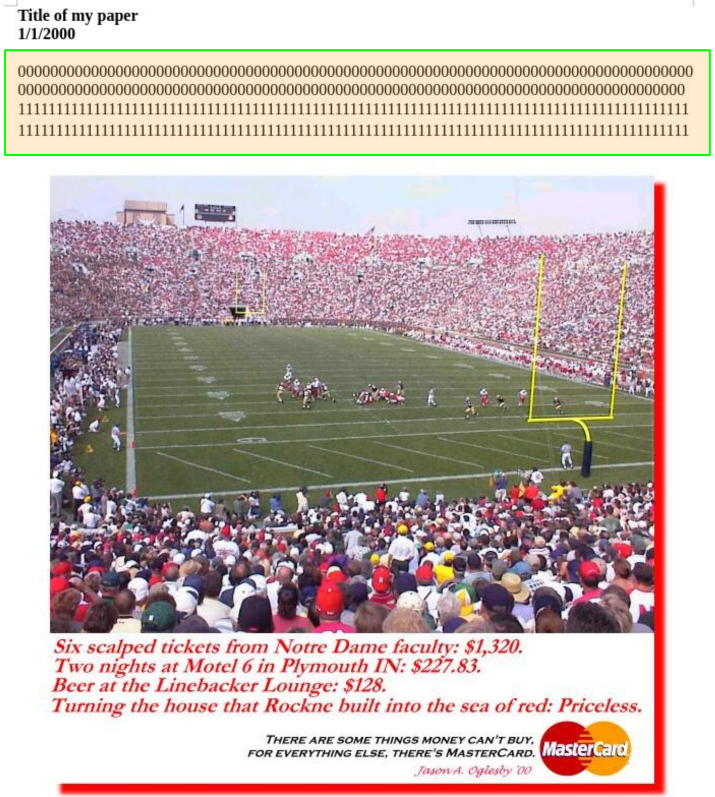


```
This worked for me, see it helps!

11111111111111111111111111111111
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

\begin{document}
%\title{Description of the US Navy HELIOS System}
%\date{5 Oct 2023}
%\author{LT Mitchell Irmer}
%\maketitle
\begin{center}
```



```
62791571851670373442629231992329473633570980450751575801474450548924552431544175540194794668572036594707690672684005777797465629940071461877113431289891696670550352735
56135537467340294456878905249805909068295088153153987449811181302011035498975126539844968105487837788958189868106891473846722421755597138434305363885819145939702481301
53882578120131583163343666398662347811148023900602440711847199070212450956752973870605527706551376522140803234674716105221503580745563955404616439516531042442707191675
26724818567818471148079203451421272719217458966586366232060700655920587294243851309763866347318942480833319807741576580640832066493018674715955422476299151722895376681
5256931281495512652120252850327534647791558770880688058981436797713340554469640606211229648180839157349610448972147522264693036117023463874872376291012848228332035052
59745365628380030910325255005604321313576897449125046303033743587727530888922576966023426166546153082523533939325383992478015639733693736873645677375456884056985875507
59745365628380030910325255005604321313576897449125046303033743587727530888922576966023426166546153082523533939325383992478015639733693736873645677375456884056985875507
59745365628380030910325255005604321313576897449125046303033743587727530888922576966023426166546153082523533939325383992478015639733693736873645677375456884056985875507
59745365628380030910325255005604321313576897449125046303033743587727530888922576966023426166546153082523533939325383992478015639733693736873645677375456884056985875507
3437387655853791330304707706344435834283009225803055147736468134457618772828623573965312589554030380534803689982973613335762037983282911653751330552644024632166806377
60924234755608578009017996443784313529374093843537341363283898183964629456787417337018586726178699880794281668696229722926067281075437627343449175823123106422095178471
60924234755608578009017996443784313529374093843537341363283898183964629456787417337018586726178699880794281668696229722926067281075437627343449175823123106422095178471
60924234755608578009017996443784313529374093843537341363283898183964629456787417337018586726178699880794281668696229722926067281075437627343449175823123106422095178471
60924234755608578009017996443784313529374093843537341363283898183964629456787417337018586726178699880794281668696229722926067281075437627343449175823123106422095178471
34739061058832116623108363218651930133419452732712974808253171018752615967762646560973074579313710660504781523062142489225323182613918622874223458036571859844447029837
2418801142300053185461103156331406128117993888695504145529725674354613990324081085698584348892416893076426163975402088065703849385251524406993324230414973609612534686
39831411045742657634384660865926026370205293842807210289015786039333389894648218186951291356466150944231804670371079595205355011936580147225533919404542293883712785510
37000148107850360570382737052549085145485891934786129817064520474374424047107581092131847596027171507298483414599459593433871104810758972520994798657711639291286923075
```

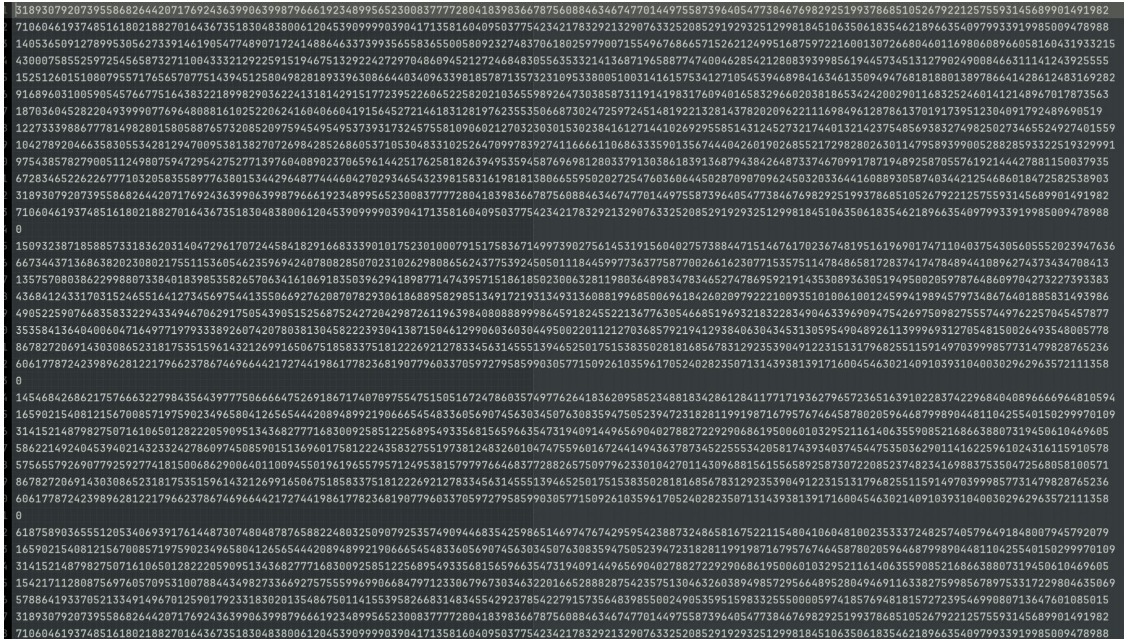
Cryptanalyzing the Ciphertext (.odt)



Title of my paper
1/1/2000

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

Six scalped tickets from Notre Dame faculty: $1,320.
Two nights at Motel 6 in Plymouth IN: $227.83.
Beer at the Linebacker Lounge: $128.
Turning the house that Rockne built into the sea of red: Priceless.
THERE ARE SOME THINGS MONEY CAN'T BUY,
FOR EVERYTHING ELSE, THERE'S MASTERCARD.
MasterCard
Jason A. Oglesby '00



```
3189307920739558682644207176924363990639987966619234899565230083777728041839836678756088463467477014497558739640547738467698292519937868510526792212575593145689901491982
7106046193748516180218827016436735183048380061204539099990390417135816040950377542342178329213290763325208529192932512998184510635061835462189663540979933919985009478988
1405365091278995305627339146190547748907172414886463373993565583655005809232748370618025979007155496768665715262124995168759722160013072668046011698060896605816043193 3215
4300075855259725456587327110043332129225915194675132922427297048609452127246848305563533214136871965887747400462854212808393998561944573451312790249008466311141243925555
1525126015108079557176565707751439451258049828189339630866440340963398185787135732310953380051003141615753412710545394689841634613509494768181880138978664142861248316928 2
9168960310059054576677516438322189982903622413181429151772395226065225820210365598926473038587311914198317609401658329660203818653424200290116832524601412148967017873563
1870360452822049399907769648088161025220624160406604191564527214618312819762355350668730247259724514819221328143782020962211169849612878613701917395123040917924896905 19
1227333988677781498280158058876573208520975945495495373931732457558109060212703230301530238416127144102692955851431245273217440132142375485693832749825027346552492740 1559
1042789204663583055342812947009538138270726984285268605371053048331025264709978392741166661106863335901356744404260190268552172982802630114795893990052882859332251932999 1
9754385782790051124980759472954275277139760408902370659614425176258182639495359458769698128033791303861839136879438426487337467099178719489258705576192144427881150037935
6728346522622677710320583558977638015344296487744460427029346543239815831619818138066559502027254760360644502870907096245032033644160889305874034421254686018472582538903
3189307920739558682644207176924363990639987966619234899565230083777728041839836678756088463467477014497558739640547738467698292519937868510526792212575593145689901491982
7106046193748516180218827016436735183048380061204539099990390417135816040950377542342178329213290763325208529192932512998184510635061835462189663540979933919985009478988
0
1509323871858857331836203140472961707244584182916683339010175230100079151758367149973902756145319156040275738844715146761702367481951619690174711040375430560555202394763 6
6673443713686382023080217551153605462359694240780828507023102629808656243775392450501118445997736377587700266162307715357511478486581728374174784894410896274373434708413
1357570803862299880733840183985358265706341610691835039629418987714743957151861850230063281198036489834783465274786959219143530893630519495002059787648609704273227393383
4368412433170315246551641273456975441355066927620870782930618688958298513491721931349313608819968500696184260209792221009351010061001245994198945797348676401885831493986
4905225907668358332294334946706291750543905152568752427204298726119639840808889998645918245522136776305466851969321832283490463396909475426975098275557449762257045457877
3535841364040060471649771979333892607420780381304582223930413871504612990603603044950022011212703685792194129384063043453130595490489261139996931270548150026493548005778
8678272069143030865231817535159614321269916506751858337518122269212783345631455513946525017515383502818168567831292353904912231513179682551159149703999857731479828765236
6061778724239896281221796623786746966442172744198617782368190779603370597279585990305771509261035961705240282350713143938139171600454630214091039310400302962963572111358
0
1454684268621757666322798435643977750666647526918671740709755475150516724786035749776264183620958523488183428612841177171936279657236516391022837422968404089666696481059 4
1659021540812156700857197590234965804126565444208948992190666545483360569074563034507630835947505239472318281199198716795767464587802059646879989044811042554015029997010 9
3141521487982750716106501282220590951343682777168300925851225689549335681565966354731940914496569040278827229290686195006010329521161406355908521686638807319450610469605
5862214924045394021432332427860974508590151369601758122243583275519738124832601047475596016724414943637873452255534205817439340374544753503629011416225961024316115910578
5756557926907792592774181500686290064011009455019619655795712495381579797664683772882657509796233010427011430968815615565892587307220852374823416988375350472568058100571
8678272069143030865231817535159614321269916506751858337518122269212783345631455513946525017515383502818168567831292353904912231513179682551159149703999857731479828765236
6061778724239896281221796623786746966442172744198617782368190779603370597279585990305771509261035961705240282350713143938139171600454630214091039310400302962963572111358
0
6187589036555120534069391761448730748048787658822480325090792535749094468354259865146974767429595423887324865816752211548041060481002353337248257405796491848007945792079
1659021540812156700857197590234965804126565444208948992190666545483360569074563034507630835947505239472318281199198716795767464587802059646879989044811042554015029997010 9
3141521487982750716106501282220590951343682777168300925851225689549335681565966354731940914496569040278827229290686195006010329521161406355908521686638807319450610469605
1542171128087569760570953100788443498273366927575559969906684797123306796730346322016652888287542357513046326038949857295664895280494691163382759985678975331722980463506 9
5788641933705213349149670125901792331830201354867501141553958266831483455429237854227915735648398550024905359515983325550000597418576948181572723954699080713647601085015
3189307920739558682644207176924363990639987966619234899565230083777728041839836678756088463467477014497558739640547738467698292519937868510526792212575593145689901491982
7106046193748516180218827016436735183048380061204539099990390417135816040950377542342178329213290763325208529192932512998184510635061835462189663540979933919985009478988
```

Overview

- Motivation
- Design Criteria
- Julia
- RSA Review
- Program Schematic
- Encoding Methods
- Demo

Demo

- Alice and Bob exchange keys.
- Alice sends an encrypted file to Bob.
- Bob decrypts and opens the file.

References

- https://julialang.org/benchmarks
- MA4570: class notes and coursework.ipynb
- https://www.joelonsoftware.com/2003/10/08/the-absolute-minimum-every-software-developer-absolutely-positively-must-know-about-unicode-and-character-sets-no-excuses/
- https://web.stanford.edu/class/ee398a/handouts/lectures/08-JPEG.pdf
- Sea of Red photo: huskermax.com