

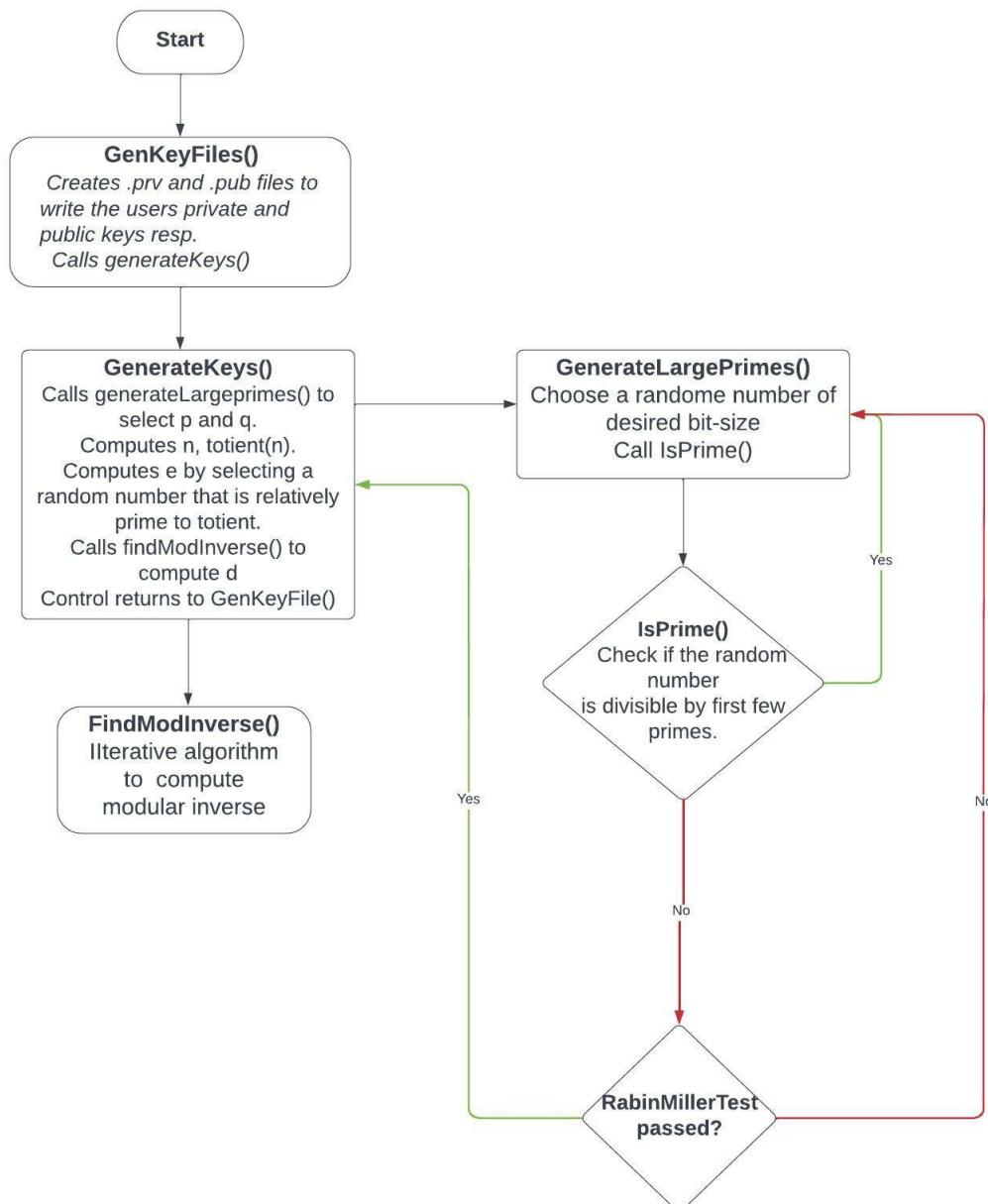
# CSCI 531 Applied Cryptography

## Programming Assignment 2

Submitted by Shobana Chandrasekaran

- **Genkeys.py:**

This python program is used to generate the public and private keys of the user. It takes as input the name of the user from the common line. The output of the program is two files .prv and .pub containing the private and public keys respectively. RSA system is implemented and the program's flow is shown below:



The RSA key generation implementation starts with the generation of large prime numbers p and q. To generate such large numbers, we first pick a random number of desired bit size. We then check if any of the first few primes divide the chosen random number. If yes, we pick a new random number. If not, we pass that number to the Rabin-Miller primality test. If the number passes the Rabin-Miller test then it is our large prime else we choose a different random number and follow these steps again.

With p and q, we compute N and totient. We then select a random number that is relatively prime to the totient. N along with this result will be our user's public key. We then find the modular inverse of the result. This will constitute the user's private key along with N. The output is written to files.

Note: Because the Rabin Miller test iterations are set to 10, it may take a while for the output files to appear.

- **Crypt.py:**

This python program will encrypt or decrypt according to the input command. It uses an argument parser to choose between encryption and decryption.

Encryption:

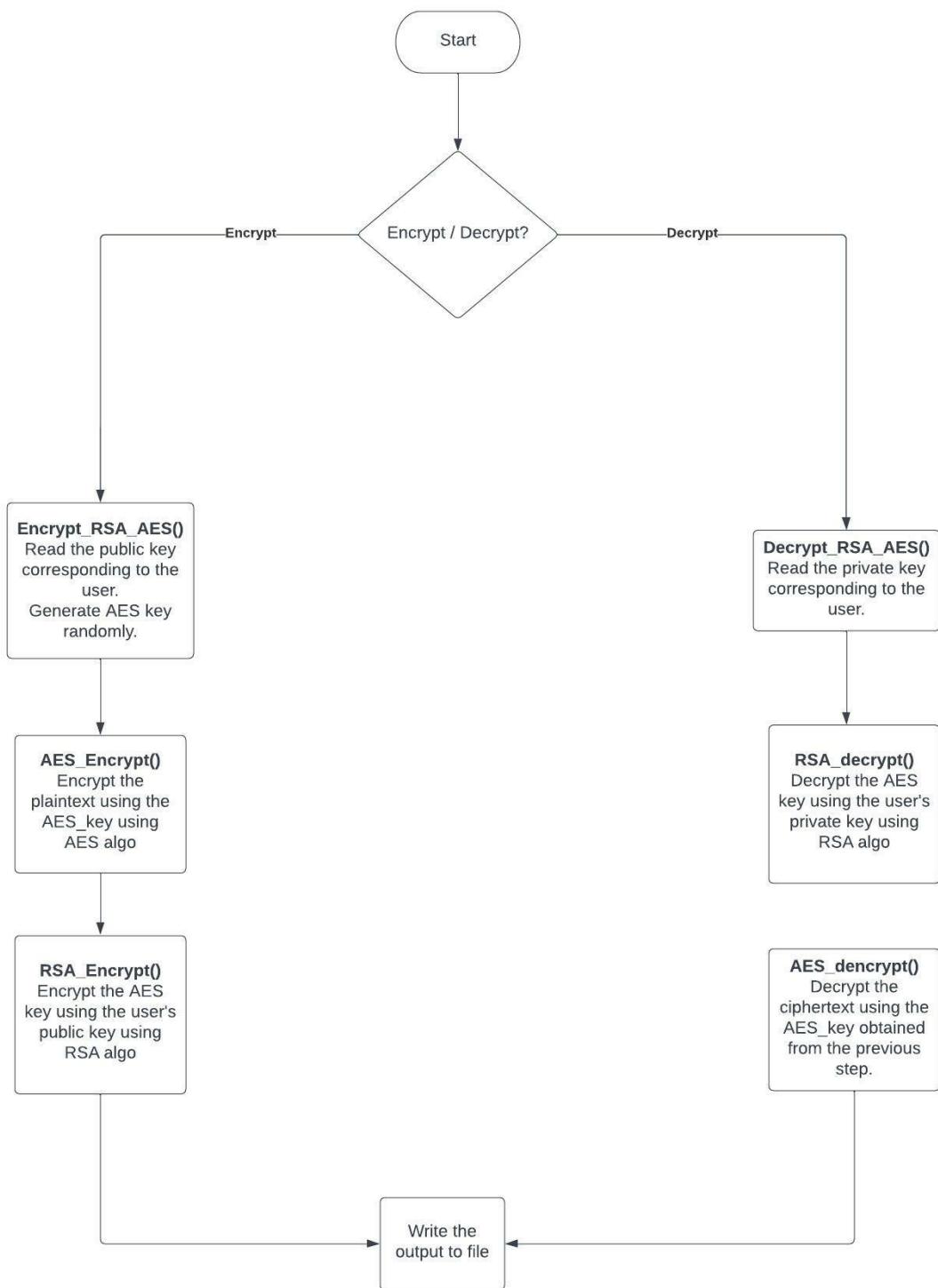
A 16 bytes random number is chosen as the AES key. This key is used to encrypt the plain text using the AES-128 algorithm. It imports pyaes module for this purpose.

The AES key is encrypted using the RSA algorithm using the user's public key. Both the ciphertext and the encrypted AES key are written to the .cip output file.

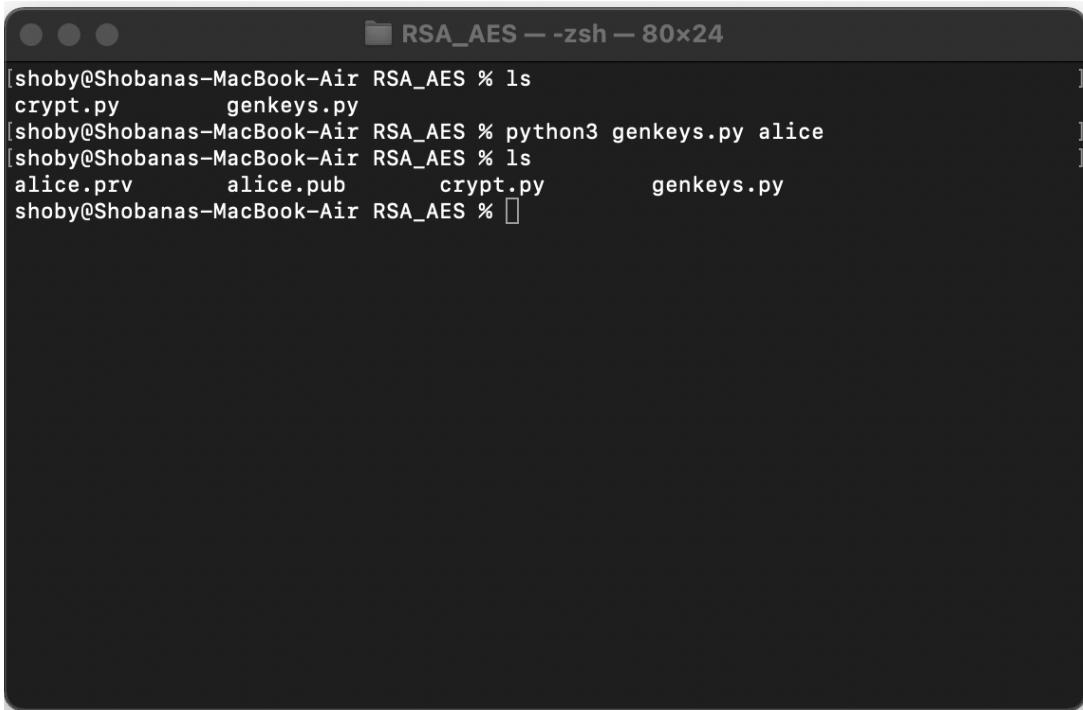
Decryption:

The ciphertext and the encrypted AES key are read from the .cip file along with the user's private key from the .prv file. RSA is first run with the private key to decrypt the encrypted AES key. This gives us the AES key to decrypt the ciphertext. The resulting plaintext is written to a file.

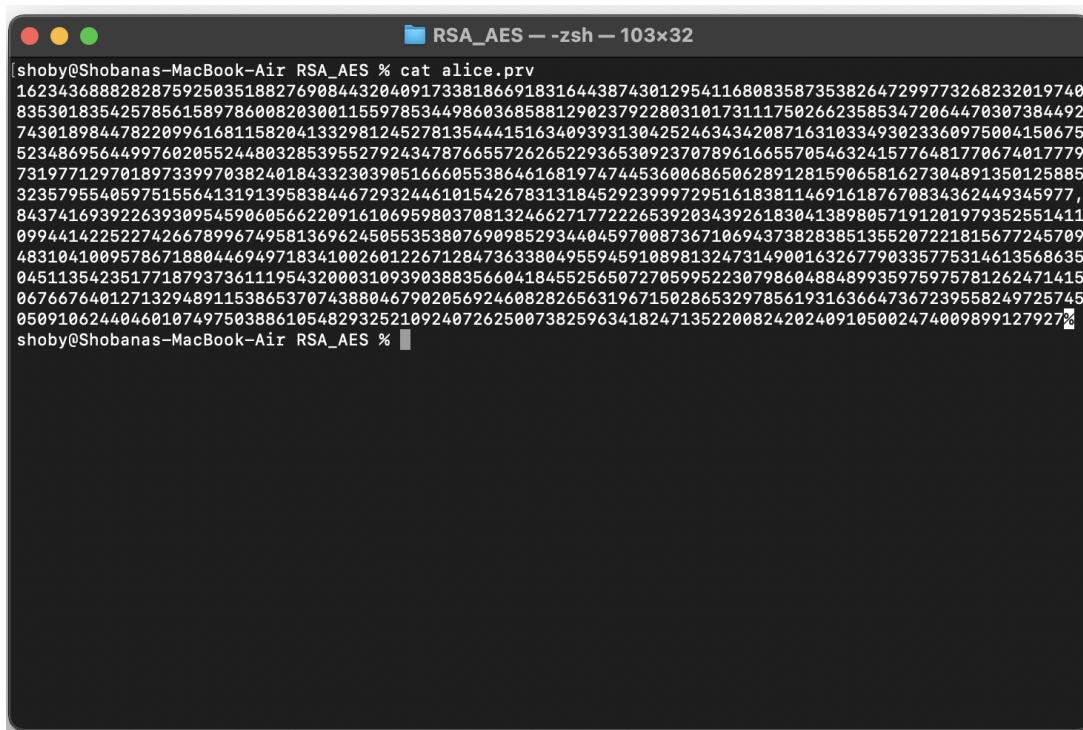
The flowchart of the program is shown below:



## Screenshots



```
[shobya@Shobanas-MacBook-Air RSA_AES % ls
crypt.py      genkeys.py
[shobya@Shobanas-MacBook-Air RSA_AES % python3 genkeys.py alice
[shobya@Shobanas-MacBook-Air RSA_AES % ls
alice.prv      alice.pub      crypt.py      genkeys.py
shobya@Shobanas-MacBook-Air RSA_AES % ]
```



```
[shobya@Shobanas-MacBook-Air RSA_AES % cat alice.prv
16234368882828759250351882769884432040917338186691831644387430129541168808358735382647299773268232019740
8353018354257856158978600820300115597853449860368588129023792280310173111750266235853472064470307384492
7430189844782209961681158204133298124527813544415163409393130425246343420871631033493023360975004150675
5234869564499760285524480328539552792434787665572626522936530923707896166557054632415776481778674817779
731977129701897339970382401843323039051666055386461681974744536006865028912815906581627304891350125885
323579554059751556413191395838446729324461015426783131845292399972951618381146916187670834362449345977,
8437416939226393095459060566220916106959803708132466271772226539203439261830413898057191201979352551411
09944142252274267899674958136962450535380769098529344845970087367106943738283851355207221815677245709
4831041009578671880446949718341002601226712847363380495594591089813247314900163267790335775314613568635
0451135423517718793736111954320003109390388356604184552565072705995223079860488489935975975781262471415
0676676401271329489115386537074388046790205692460828265631967150286532978561931636647367239558249725745
050910624404601074975038861054829325210924072625007382596341824713522008242024091050024740098991279278
shobya@Shobanas-MacBook-Air RSA_AES % ]
```

RSA\_AES -- zsh -- 103x32

```
[shoby@Shobanas-MacBook-Air RSA_AES % cat alice.pub
162343688828287592503518827698443204091733818669183164438743012954116808358735382647299773268232019740
835301835425785615897860082030011559785349860368588129023792280310173111750266235853472064470307384492
743018984478220961681158204133298124527813544415163409393130425246343420871631033493023360975004150675
5234869564499760205524480328539552792434787665572626522936530923707896166557054632415776481770674017779
7319771297018973399703824018433230398516660553864616819747445360068650628912815906581627304891350125885
323579554059751556413191395838446729324461015426783131845292399972951618381146916187670834362449345977,
179598840277842827948194334739709851968388160352481785807843837712351717301729524698849460561448156889
5344248766192793485152782190487008932699856947970834408217583924008897110404286717237937754153743828136
1430471854047387321994559761074773416032561192244757412986737825194283497052883095478shoby@Sho
shoby@Shobanas-MacBook-Air RSA_AES % ]
```

RSA\_AES -- zsh -- 83x25

```
[shoby@Shobanas-MacBook-Air RSA_AES % ls
Screenshots    alice.prv      alice.pub      crypt.py      genkeys.py
[shoby@Shobanas-MacBook-Air RSA_AES % python3 genkeys.py bob
[shoby@Shobanas-MacBook-Air RSA_AES % ls
Screenshots    alice.pub      bob.pub       genkeys.py
alice.prv      bob.prv      crypt.py
shoby@Shobanas-MacBook-Air RSA_AES % ]
```

```
shoby@Shobanas-MacBook-Air RSA_AES % cat bob.pub
9750538532066655653855068202168020739052748830677286997654179410351535545902303811584398902429741157833
1143208145269943588233246804808784362082608950332191547586085791389710234475011170100721441003872953000
4985938171076138876353741894960595512473518120357200217453669909156591835428608019868553072151677816067
6929313573722395693814661088526276370060428694677341744310854809032501399639624804974641422303946220968
639625912943027258554648269443655419804882800335673255695407125123370488018259305882805516556593239683
70297235136877354514970372930064479851140093397357871583764645105550030406108451459877609190138848797,1
7594313683286226643052271671216670510031910139789468539952632146344595909582714725747324203743917535133
5689912131877032162339592307384869631156223453452980047818007676733836449645152415880537590050524478098
96053779467383445819804503809134032449460591935185266295875362254837199144741529431697877061037432671%
shoby@Shobanas-MacBook-Air RSA_AES %
```

```
shoby@Shobanas-MacBook-Air RSA_AES % cat bob.prv
9750538532066655653855068202168020739052748830677286997654179410351535545902303811584398902429741157833
1143208145269943588233246804808784362082608950332191547586085791389710234475011170100721441003872953000
4985938171076138876353741894960595512473518120357200217453669909156591835428608019068553072151677816067
6929313573722395693814661088526276370060428694677341744310854809032501399639624804974641422303946220968
639625912943027258554648269443655419804882800335673255695407125123370488018259305882805516556593239683
70297235136877354514970372930064479851140093397357871583764645105550030406108451459877609190138848797,5
9002388249404259282510350345125524058415177489719458492672560245827036321681954143493634342620461537870
4283677467505176318498593407461840241060770812346500009697310721347567577180687887242335363538325626037
2169328426328605291220871920444699330334168537839504601463425413342664055915776742197003958066794578066
805156038466330322656229597628694919493162316543150973445101470771677833183587068435499539780242101628
4094326558034074862251136105127852710991537256718996923307187148538590093869805974320393658795653468382
8158721344899789484878235862479599043789130209386788655679863364825138931729266667190410543873337439%
shoby@Shobanas-MacBook-Air RSA_AES %
```

```
RSA_AES — zsh — 80x40
[shoby@Shobanas-MacBook-Air RSA_AES % cat message.txt
Named in honor of the trailblazing astronomer Edwin Hubble, the Hubble Space Telescope is a large, space-based observatory, which has revolutionized astronomy since its launch and deployment by the space shuttle Discovery in 1990. Far above rain clouds, light pollution, and atmospheric distortions, Hubble has a crystal-clear view of the universe. Scientists have used Hubble to observe some of the most distant stars and galaxies yet seen, as well as the planets in our solar system.

Hubble's capabilities have grown immensely in its over 30 years of operation. This is because new, cutting-edge scientific instruments have been added to the telescope over the course of five astronaut servicing missions. By replacing and upgrading aging parts, these servicing missions have greatly extended the telescope's lifetime.

Telescopes have a particular range of light that they can detect. Hubble's domain extends from the ultraviolet through the visible (which our eyes see) and into the near-infrared. This range has allowed Hubble to deliver stunning images of stars, galaxies, and other astronomical objects that have inspired people around the world and changed our understanding of the universe.

Hubble has made more than 1.5 million observations over the course of its lifetime. Over 19,000 peer-reviewed science papers have been published on its discoveries, and every current astronomy textbook includes contributions from the observatory. The telescope has tracked interstellar objects as they soared through our solar system, watched a comet collide with Jupiter, and discovered moons around Pluto. It has found dusty disks and stellar nurseries throughout the Milky Way that may one day become fully fledged planetary systems and studied the atmospheres of planets that orbit other stars. Hubble has peered back into our universe's distant past, to locations more than 13.4 billion light-years from Earth, capturing galaxies merging, probing the supermassive black holes that lurk in their depths, and helping us better understand the history of the expanding universe.

In its over 30 years of operation, Hubble has made observations that have captured humanity's imaginations and deepened our knowledge of the cosmos. It will continue to do so for years to come.
shoby@Shobanas-MacBook-Air RSA_AES % ]
```

```

RSA_AES — zsh — 116x46

shoby@Shobanas-MacBook-Air RSA_AES % python3 crypt.py -e bob.pub message.txt message.cip
shoby@Shobanas-MacBook-Air RSA_AES %
shoby@Shobanas-MacBook-Air RSA_AES % cat message.cip
T???r ???G??i????EB??E?F??o?u?hN+??x?o?e???
    Q???Upo ??N????ibnz?0?o?{oAA?/?h??XB? 2??Zd??4M4>R?j?0?bJ38) ??F7~
    ???PG?=?vc??0?$?*p
    ???G>??7d?Nm
    _?/C?N??xdusN?)?G5??#[?d?·x??Y?v??bG??A??/??+?gaB&
    ??pj::?(xpp???:??h??B??Hh?a??TB??\?y?11?g?" <?
    Z??y?????R?g??bc?yI?L?#?z?y?N?????o?0??x?????4)?E?o?IE? 29W?,?#up??2 ?zP(zLQ?  ??%?::?>nB??ff?ioj????,??
    ?}oQ?M?#n?????z q??????
      5`$k??RG&Y679?IC??W?%?U?????>?f?E?((?Lh?=?Ô?k?{h?Zp?1?J<TdR??t??e??>J?_)YKn?_D#
[??:
  &??+?kE{????:i9zoh?^?q='?1$?W?a?wl r?(!ciq?
  [ V??7!i?~??~?????5??>?q?py3D??t?e?U?.?
  ?????_?P2=?3A??y??^a??y?/?m?I??h??K?l?hs?7?)?&?????h??\?F?/Of\?
  ?U??j?=?~?f??R?KA????, ??i????/H?17?Q???? ??é?????Z?????m?Q04, z?WId?YsSYIMn??vU? \K?''?Oe??9?lo?????c 5?6
  ?aB?#? @?
  ?b????P7J?k??"p??\u3u?????r??*?%?#_d.l->->????Mc?R?[q?? N[
  ??P*~b?@N#)s7?M??*g?9??ygh?Ie5sc' ?SH
  ?????^*[huAW?da
  _F?-??t??b?fs~????Rt?b|?7B?)?????Y?{w*?Z
  ??c??S?S?Q??d?????
  E?Y??k&\,??}?v?i??}?g?? ??gAc?v??+??87??`1?
  I$***=?'5?{#?W1.??P<%?XB?TÖ
  dM?X'??????Q?J????R
  ??r?&????a?g??8$K?.?23bEgPw?#y?.?????+?Zo-F?*Uh@???5 D)?/?jH4Q`?x?9AYP?"R??bJ數Ut????{G?>?3??a??R??5k?6JnT]
  ??Y)?D?0?????>xk?)06??7blz~?i?w?i (~?j-?
  ?ja?2t?X?z?S?1?X?Q? ??T?????>?{????/+??hP?qq?
  ??????T????s ?R????ür?!![8?=?q??am?Ö??Y~?3d?Y+DA-e??m?
  ?m?o
  ?? ??,:?Yu?q?~YSD??d1?-?<?4fdz?X?M?????|??Lr'2'H?BXfYfT??p????D?? .??/?:e??L????f?oL????/?:?
  T;xh?Kei?jR?????U6?g+????mj;?C?2'X?h??LRw-?W?!"?x??_?1? ?,?P?'??x?r-Y??b?7 ae'?????W?eI??V?]m?Ewx7???
  ??-9??K?A? ?? 3(61??Z??,?i??,?k?W?y?iMh??&?&Pq2??6?&{??b?M?ox??&?W~y??R??{(|Qx??=X??B?j?m?Z???
  #8??&?V?%?UL? 88170177284615703669187685218217230176792485912074347975549546457506432621475484000464098249829
  848524880890243321821939956836780751786754595528304166201626945266373076172836977619538721787206006235408496432
  76575476123717476474299418437364989640172773164760067338405856049957745841500671678417334597251627931334851568937808
  599044015656330878551157682467203902008779679417341866520138343583937479428708035920340410641530064944810488036756
  710191703798768987834251193734628664732116506229497219029932699049267684834110281437732533991509994409535364891105
  031400265442019549627442356119568119199620198267843936% shoby@Shobanas-MacBoo
k-Air RSA_AEshoby@Shobanas-MacBook-Air RSA_AEshoby@Shobanas-MacBook-Air RSA_AEshoby@Shobanas-MacBook-Air RSA_AEshoby@Shobashoby@Shobashoby@Shoba
shoby@Shobanas-MacBook-Air RSA_AES %

```

```

RSA_AES — zsh — 109x48

shoby@Shobanas-MacBook-Air RSA_AES % python3 crypt.py -d bob.prv message.cip message.txt
shoby@Shobanas-MacBook-Air RSA_AES %
shoby@Shobanas-MacBook-Air RSA_AES % cat message.txt
Named in honor of the trailblazing astronomer Edwin Hubble, the Hubble Space Telescope is a large, space-base
d observatory, which has revolutionized astronomy since its launch and deployment by the space shuttle Discov
ery in 1990. Far above rain clouds, light pollution, and atmospheric distortions, Hubble has a crystal-clear
view of the universe. Scientists have used Hubble to observe some of the most distant stars and galaxies yet
seen, as well as the planets in our solar system.

Hubble's capabilities have grown immensely in its over 30 years of operation. This is because new, cutting-ed
ge scientific instruments have been added to the telescope over the course of five astronaut servicing missio
ns. By replacing and upgrading aging parts, these servicing missions have greatly extended the telescope's li
fetime.

Telescopes have a particular range of light that they can detect. Hubble's domain extends from the ultraviole
t through the visible (which our eyes see) and into the near-infrared. This range has allowed Hubble to deliv
er stunning images of stars, galaxies, and other astronomical objects that have inspired people around the wo
rld and changed our understanding of the universe.

Hubble has made more than 1.5 million observations over the course of its lifetime. Over 19,000 peer-reviewed
science papers have been published on its discoveries, and every current astronomy textbook includes contrib
utions from the observatory. The telescope has tracked interstellar objects as they soared through our solar
system, watched a comet collide with Jupiter, and discovered moons around Pluto. It has found dusty disks and
stellar nurseries throughout the Milky Way that may one day become fully fledged planetary systems and studi
ed the atmospheres of planets that orbit other stars. Hubble has peered back into our universe's distant past
, to locations more than 13.4 billion light-years from Earth, capturing galaxies merging, probing the superma
ssive black holes that lurk in their depths, and helping us better understand the history of the expanding un
iverse.

In its over 30 years of operation, Hubble has made observations that have captured humanity's imaginations an
d deepened our knowledge of the cosmos. It will continue to do so for years to come.
shoby@Shobanas-MacBook-Air RSA_AES %

```

```
RSA_AES -- zsh -- 108x32
[shoby@Shobanas-MacBook-Air RSA_AES % cat message2.txt
Many important aspects of IT security rely on encryption and public key cryptography, which are essential fo
r e-commerce and protecting secret electronic information.

These techniques are based in turn on mathematical algorithms that are very difficult to "break". Modern alg
orithms with suitable key lengths (e.g. AES-128, RSA-2048, ECDSA-256, etc.) are not susceptible to brute for
ce attack – even with massive amounts of computing power, they would take centuries or, in some cases, even
longer than the lifetime of the universe to break.

However, it is possible to create unique algorithms for quantum computers (e.g. "Shor's algorithm") that dra
matically reduce the time it takes to break these algorithms.

Symmetric algorithms used for encryption, like AES, are still thought to be safe (with sufficient key length
– e.g. AES-256 or larger); however, current asymmetric algorithms like RSA and ECDSA will be rendered essen
tially useless once quantum computers reach a certain scale.

This will break nearly every practical application of cryptography in use today, making e-commerce and many
other digital applications that we rely on in our daily lives totally insecure.
shoby@Shobanas-MacBook-Air RSA_AES % ]
```

```
RSA_AES -- zsh -- 109x33

[shoby@Shobanas-MacBook-Air RSA_AES % python3 crypt.py -e alice.pub message2.txt message2.cip
[shoby@Shobanas-MacBook-Air RSA_AES %
[shoby@Shobanas-MacBook-Air RSA_AES % cat message2.cip
?????L=?y#??8e0*kD?*??c@Z#VJ{????$Z??U??C??s&1??=???A?Zë|we??^4(???8!j?6L|??iw??????U$????J???t(?hdP?
)?Y?{Y?_IO?????i?D??'n??EWx??0?c?UwE?j!?.Ug?h??DT$1=$-_d????Kr}???G-(????/I..?1?P?])]??"`??}d?~??LB????<
u!?gZ?g?_?*ga?W?({?g06?Aaf?8t?b?XF??D?
?}-?2oA??_?`'kC2?]??R?f??%É????q?k?$_??T?U?y??~?g??_?=??k<{}?~?k]BHB&E}3n?U}
_??1.0?d?1?[??D?k?({I??o??S??-??D?~Pd?r|?6?Q"?)|4??mpMF?)m?C?aW?      ??^/?z?J?y*?A9?b??ma?_??t?,_s2?????
?I?,?????U??
z?uPH?C1?????M>????P`?B??L_a???
A?????
?!, ???Phv?#???Uau#?????????o=?T???V??O??]G??? C
fm?yD|???
??q?YUT~`s?J??-<gE?)??c??)????Cm??,!?m1\Nu?<???)??p??QJF??-/IcH(?R?^I?)??Q)[?G?
??a3
?V??xA????PF?%],??~?S=?oLCI?i????lE?????k{????nW"?_?W?????Vr???F?w??H??9V?0?w?D?'?nU
??j?'!'.?eb
?k?????bq7?r?fu?j?1TD?Y[?w?]jp^?(?W????*?          A?@?K?:?})?D
                ??f????.?6x??[Tw??_|O,N?n????ev?J3C?Z??H) 4159479524
27401579876844924204969655303743058091984110245233857394081590289030400973552275154195375912497751554842638
966460124280622145185433364434713122921058312265492861931984379839018720169648617124652643341018744826207177
1548725976580537110755386403617135150911510931156564644284753686854119859868215399029869212320076037509138580
941054968001050325825842156358633023146715935859173368725027786254610690747817396086368855421523156128144753
943090852684284101270685945262673842298905188649427478633877325779745996633453228853681271956511962838766301
846084196686913684556964942839377792702890782998611026064124
shoby@Shobanas-MacBook-Air RSA_AES %
```

```
RSA_AES -- zsh -- 109x33

[shoby@Shobanas-MacBook-Air RSA_AES % python3 crypt.py -d alice.prv message2.cip message2.txt
[shoby@Shobanas-MacBook-Air RSA_AES %
[shoby@Shobanas-MacBook-Air RSA_AES % cat message2.txt
Many important aspects of IT security rely on encryption and public key cryptography, which are essential for e-commerce and protecting secret electronic information.

These techniques are based in turn on mathematical algorithms that are very difficult to "break". Modern algorithms with suitable key lengths (e.g. AES-128, RSA-2048, ECDSA-256, etc.) are not susceptible to brute force attack – even with massive amounts of computing power, they would take centuries or, in some cases, even longer than the lifetime of the universe to break.

However, it is possible to create unique algorithms for quantum computers (e.g. "Shor's algorithm") that dramatically reduce the time it takes to break these algorithms.

Symmetric algorithms used for encryption, like AES, are still thought to be safe (with sufficient key length – e.g. AES-256 or larger); however, current asymmetric algorithms like RSA and ECDSA will be rendered essentially useless once quantum computers reach a certain scale.

This will break nearly every practical application of cryptography in use today, making e-commerce and many other digital applications that we rely on in our daily lives totally insecure.
shoby@Shobanas-MacBook-Air RSA_AES %
```