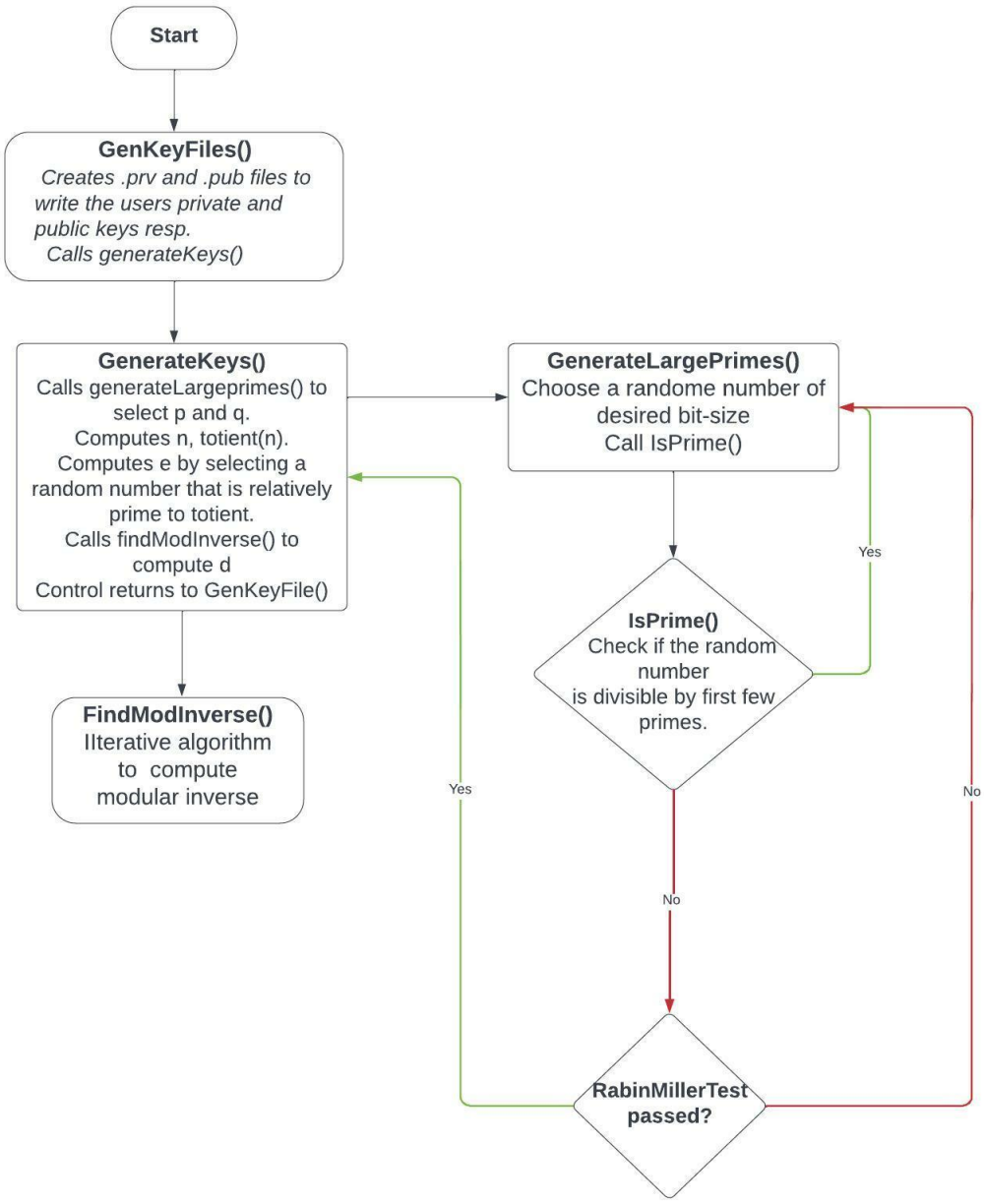
CSCI 531 Applied Cryptography
Programming Assignment 2

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:

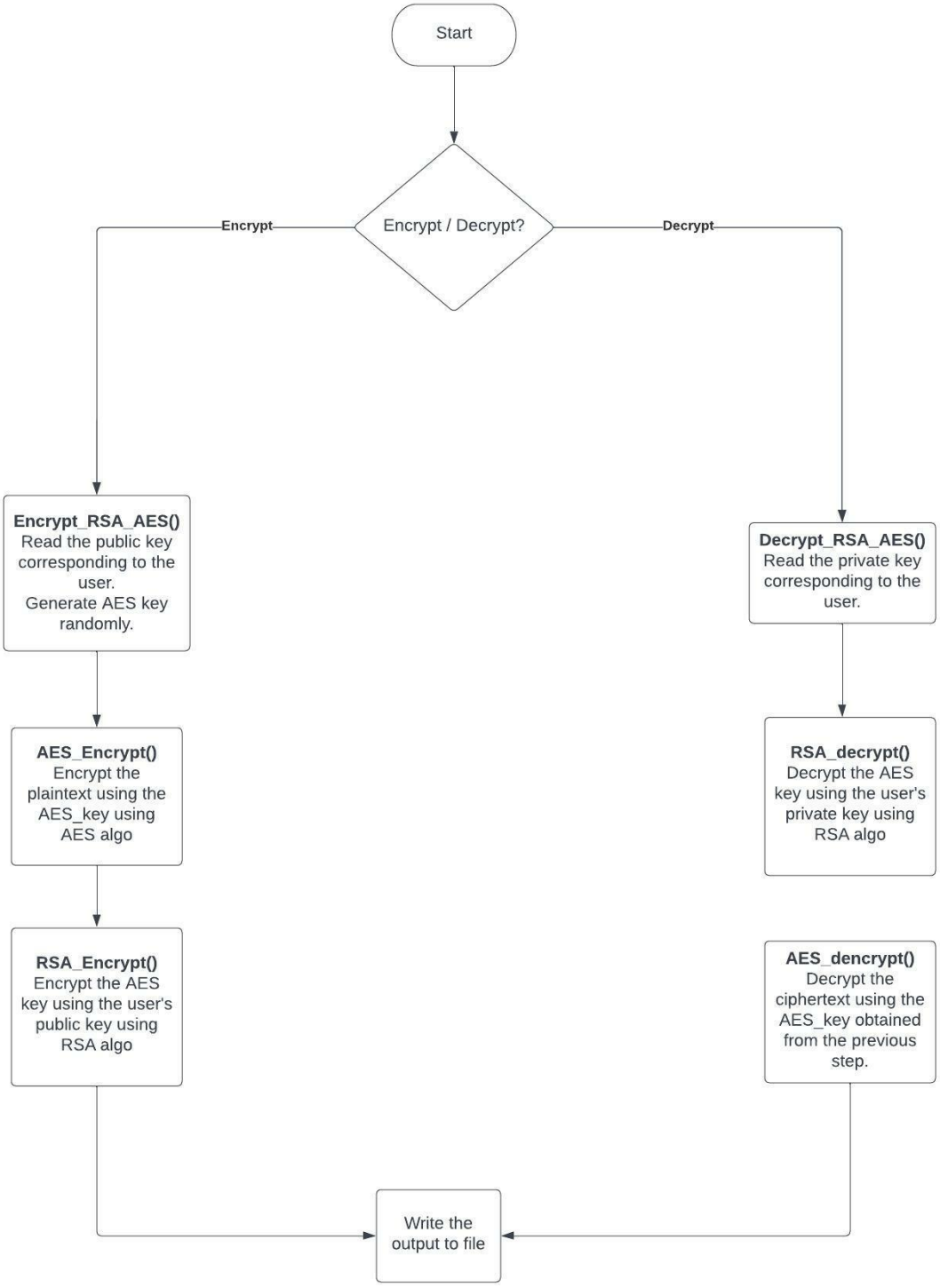
A 16 bytes random number is chosen as the AES key. This key is used to encrypt the plain text using the AES-128 algorithm. It imports pyaes module for this purpose.

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.

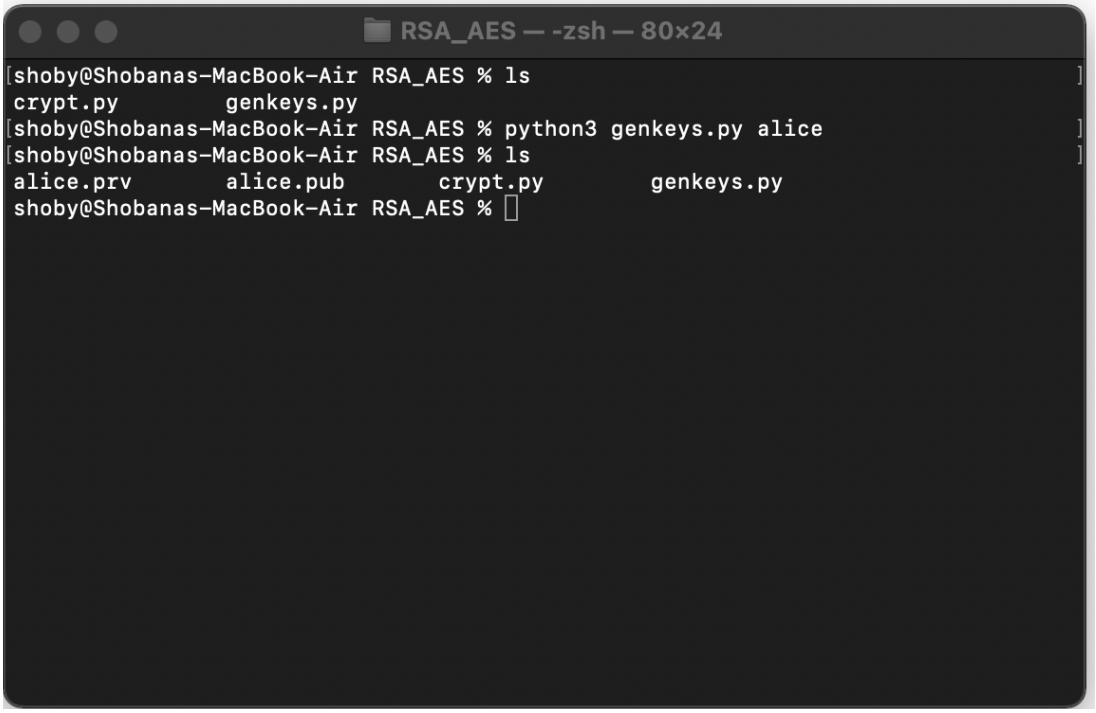
Decryption:

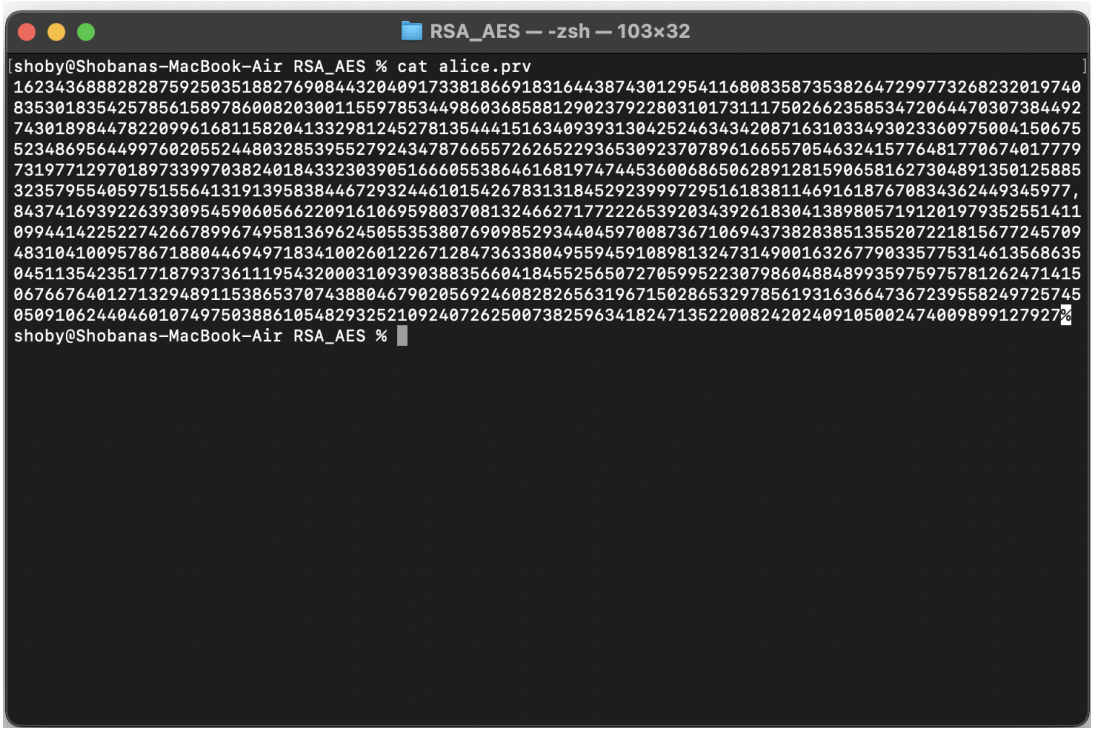
The ciphertext and the encrypted AES key are read from the .cip file along with the user's private key from the .prv file. RSA is first run with the private key to decrypt the encrypted AES key. This gives us the AES key to decrypt the ciphertext. The resulting plaintext is written to a file.

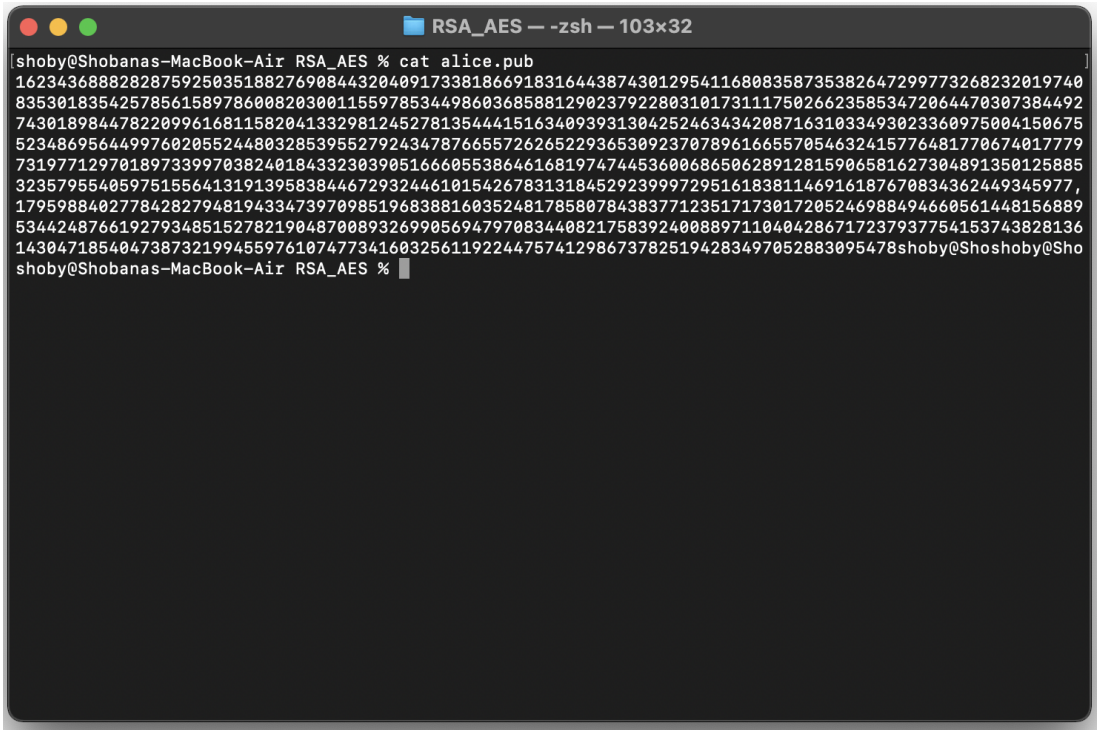
The flowchart of the program is shown below:

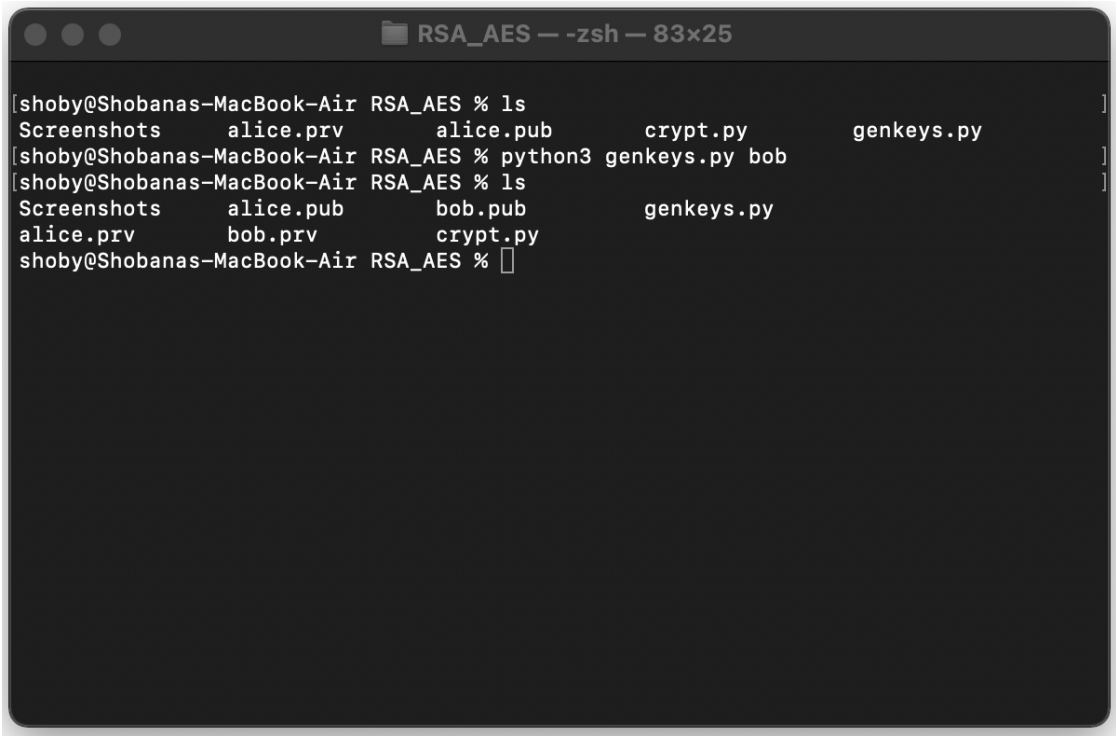

Start
Encrypt / Decrypt?
Encrypt
Decrypt
Encrypt_RSA_AES()
Read the public key corresponding to the user.
Generate AES key randomly.
AES_Encrypt()
Encrypt the plaintext using the AES_key using AES algo
RSA_Encrypt()
Encrypt the AES key using the user's public key using RSA algo
Decrypt_RSA_AES()
Read the private key corresponding to the user.
RSA_decrypt()
Decrypt the AES key using the user's private key using RSA algo
AES_dencrypt()
Decrypt the ciphertext using the AES_key obtained from the previous step.
Write the output to file

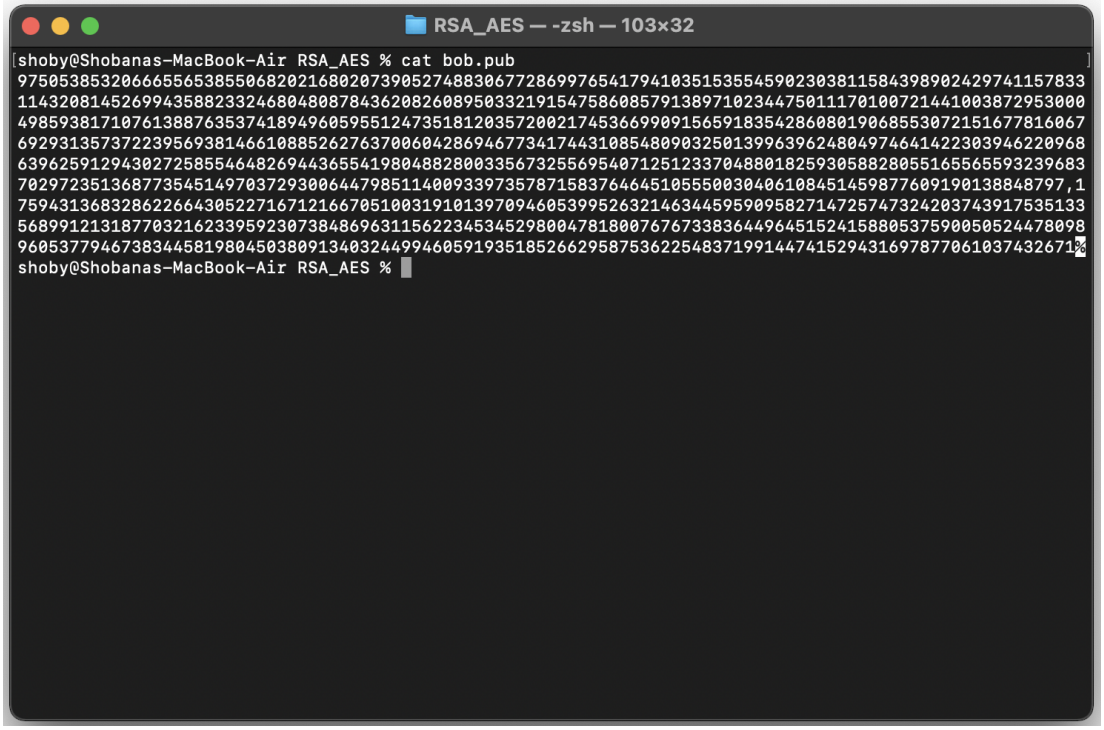
Screenshots

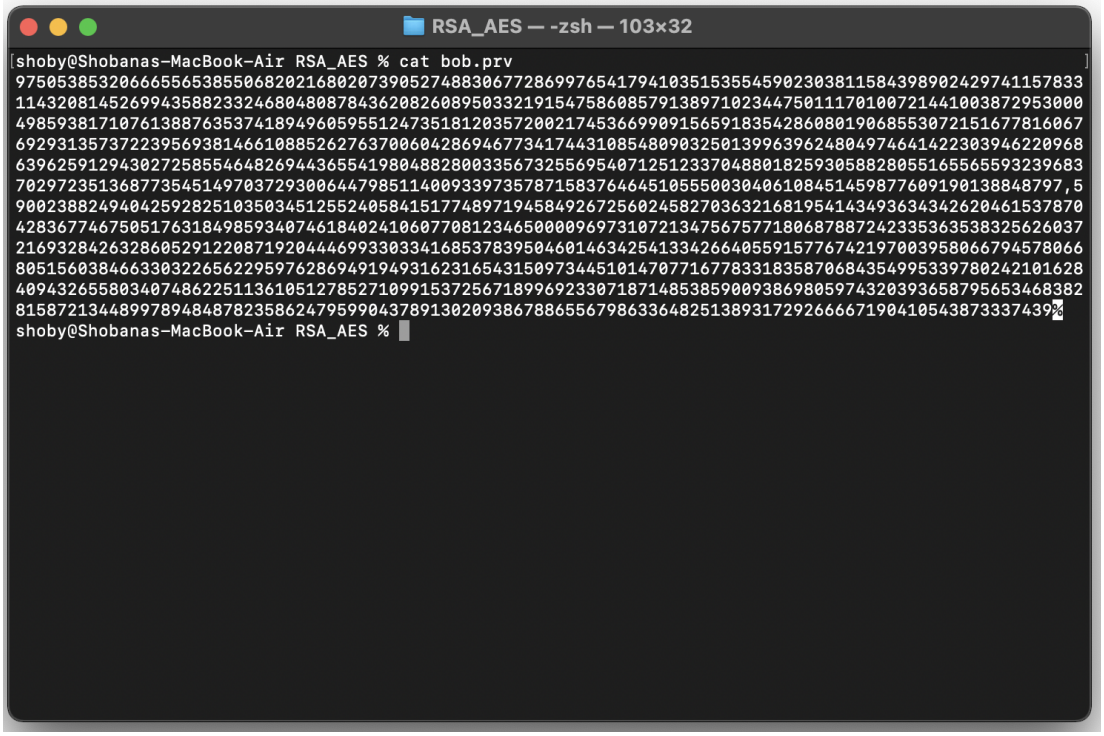




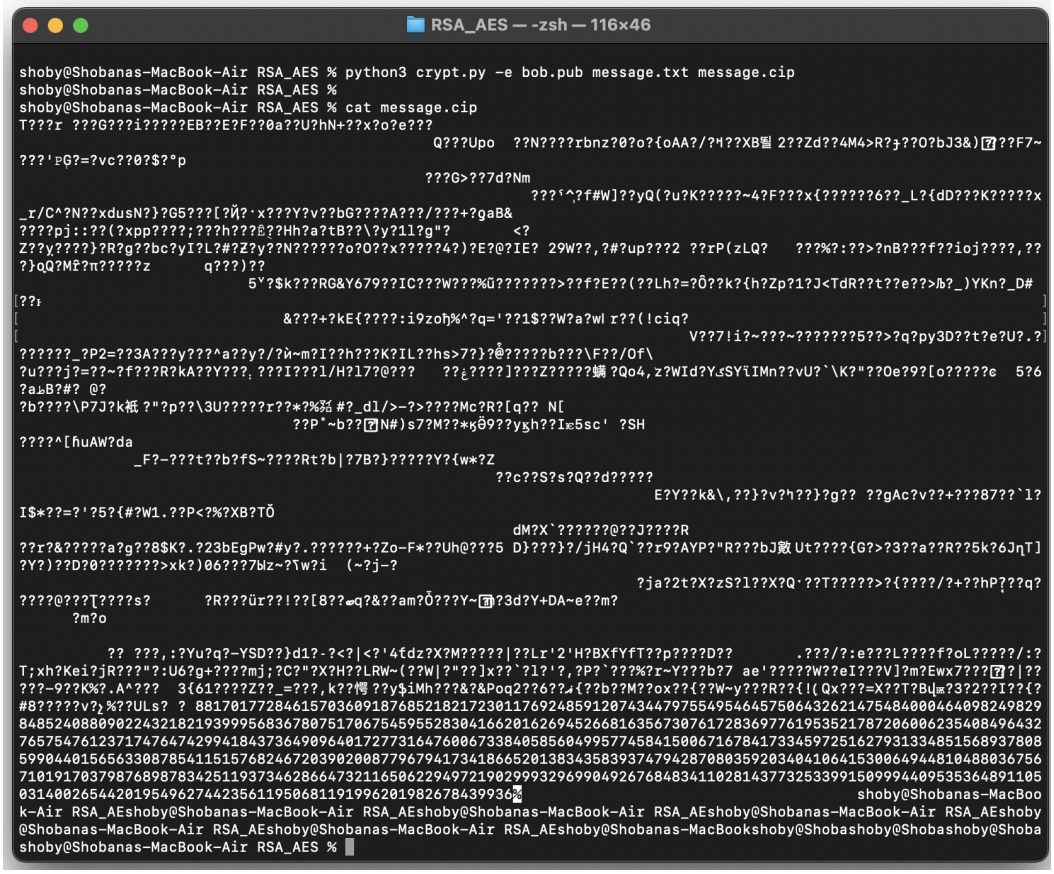

RSA_AES — -zsh — 103×32
[shoby@Shobanas-MacBook-Air RSA_AES % cat alice.pub
16234368882828759250351882769084432040917338186691831644387430129541168083587353826472997732682320197408353018354257856158978600820300115597853449860368588129023792280310173111750266235853472064470307384492743018984478220996168115820413329812452781354441516340939313042524634342087163103349302336097500415067552348695644997602055244803285395527924347876655726265229365309237078961665570546324157764817706740177797319771297018973399703824018433230390516660553864616819747445360068650628912815906581627304891350125885323579554059751556413191395838446729324461015426783131845292399972951618381146916187670834362449345977,179598402778428279481943347397098519683881603524817858078438377123517173017205246988494660561448156889534424876619279348515278219048700893269905694797083440821758392400889711040428671723793775415374382813614304718540473873219945597610747734160325611922447574129867378251942834970528830954 78shoby@Shoshoby@Shoshoby@Shobanas-MacBook-Air RSA_AES %

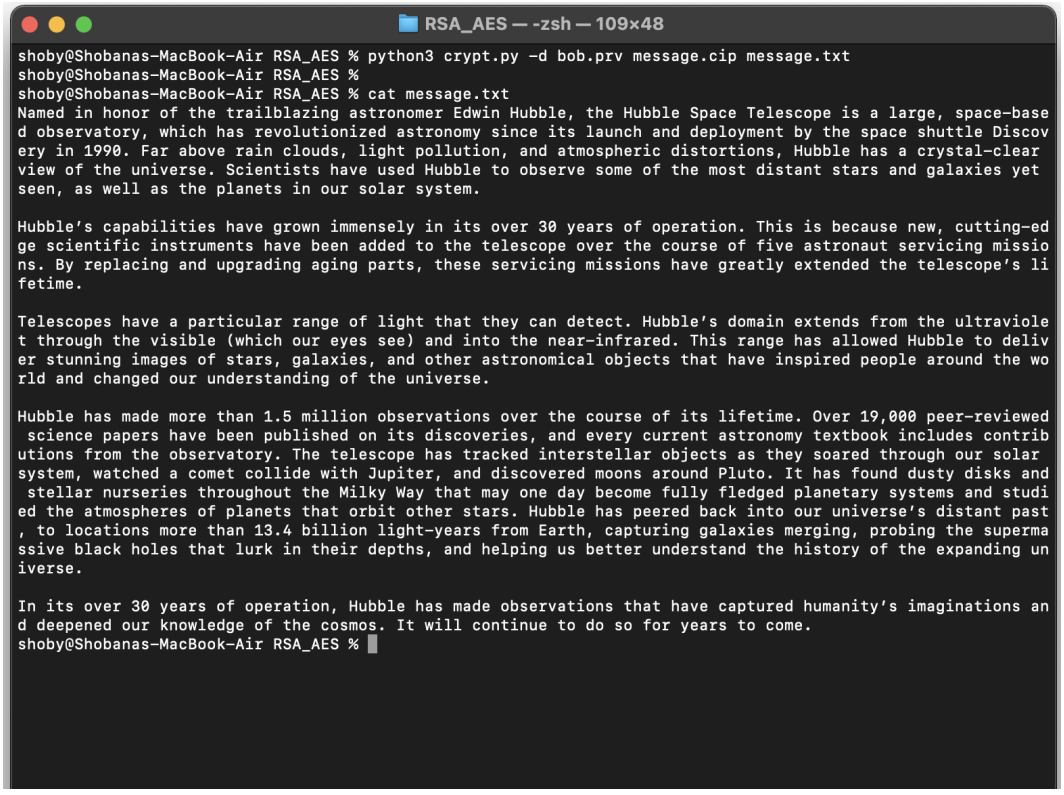

RSA_AES — -zsh — 83×25
[shoby@Shobanas-MacBook-Air RSA_AES % ls
Screenshots alice.prv alice.pub crypt.py genkeys.py
[shoby@Shobanas-MacBook-Air RSA_AES % python3 genkeys.py bob
[shoby@Shobanas-MacBook-Air RSA_AES % ls
Screenshots alice.pub bob.pub genkeys.py
alice.prv bob.prv crypt.py
shoby@Shobanas-MacBook-Air RSA_AES %

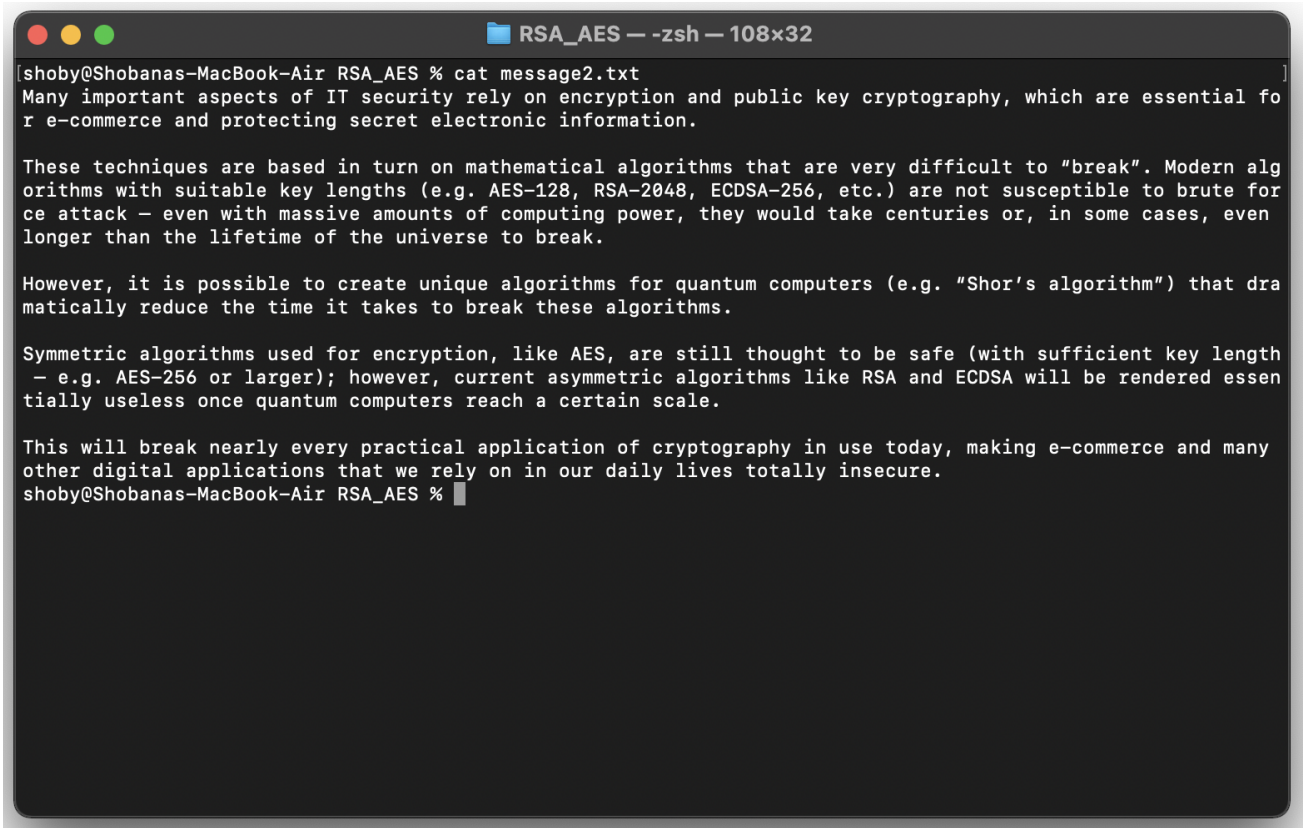

RSA_AES — -zsh — 103×32
[shoby@Shobanas-MacBook-Air RSA_AES % cat bob.pub
97505385320666556538550682021680207390527488306772869976541794103515355459023038115843989024297411578331143208145269943588233246804808784362082608950332191547586085791389710234475011170100721441003872953000498593817107613887635374189496059551247351812035720021745366990915659183542860801906855307215167781606769293135737223956938146610885262763700604286946773417443108548090325013996396248049746414223039462209686396259129430272585546482694436554198048828003356732556954071251233704880182593058828055165565593239683702972351368773545149703729300644798511400933973578715837646451055500304061084514598776091901388487975,1759431368328622664305227167121667051003191013970946053995263214634459590958271472574732420374391753513356899121318770321623395923073848696311562234534529800478180076767338364496451524158805375900505244780989605377946738344581980450380913403244994605919351852662958753622548371991447415294316978770610374326713shoby@Shobanas-MacBook-Air RSA_AES %

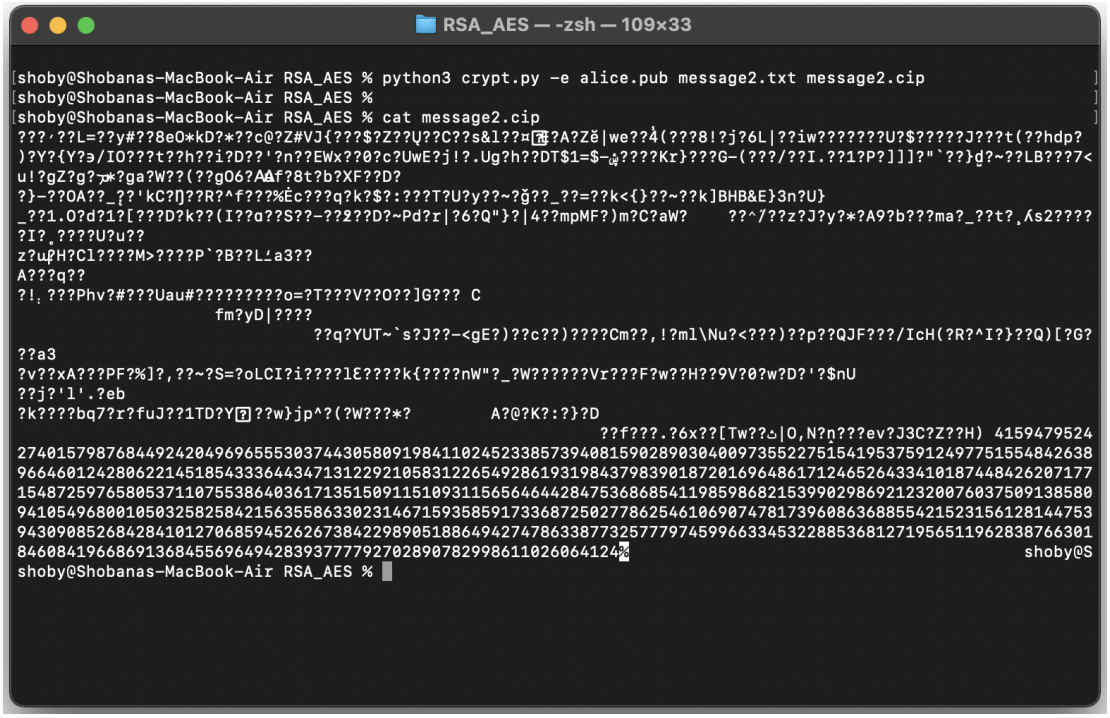

RSA_AES — -zsh — 103×32
[shoby@Shobanas-MacBook-Air RSA_AES % cat bob.prv
97505385320666556538550682021680207390527488306772869976541794103515355459023038115843989024297411578331143208145269943588233246804808784362082608950332191547586085791389710234475011170100721441003872953000498593817107613887635374189496059551247351812035720021745366990915659183542860801906855307215167781606769293135737223956938146610885262763700604286946773417443108548090325013996396248049746414223039462209686396259129430272585546482694436554198048828003356732556954071251233704880182593058828055165565593239683702972351368773545149703729300644798511400933973578715837646451055500304061084514598776091901388487975,5900238824940425928251035034512552405841517748971945849267256024582703632168195414349363434262046153787042836774675051763184985934074618402410607708123465000096973107213475675771806878724233536353832562603721693284263286052912208719204446993303341685378395046014634254133426640559157767421970039580667945780668051560384663303226562295976286949194931623165431509734451014707716778331835870684354995339780242101628409432655803407486225113610512785271099153725671899692330718714853859009386980597432039365879565346838281587213448997894848782358624795990437891302093867886556798633648251389317292666671904105438733374397shoby@Shobanas-MacBook-Air RSA_AES %

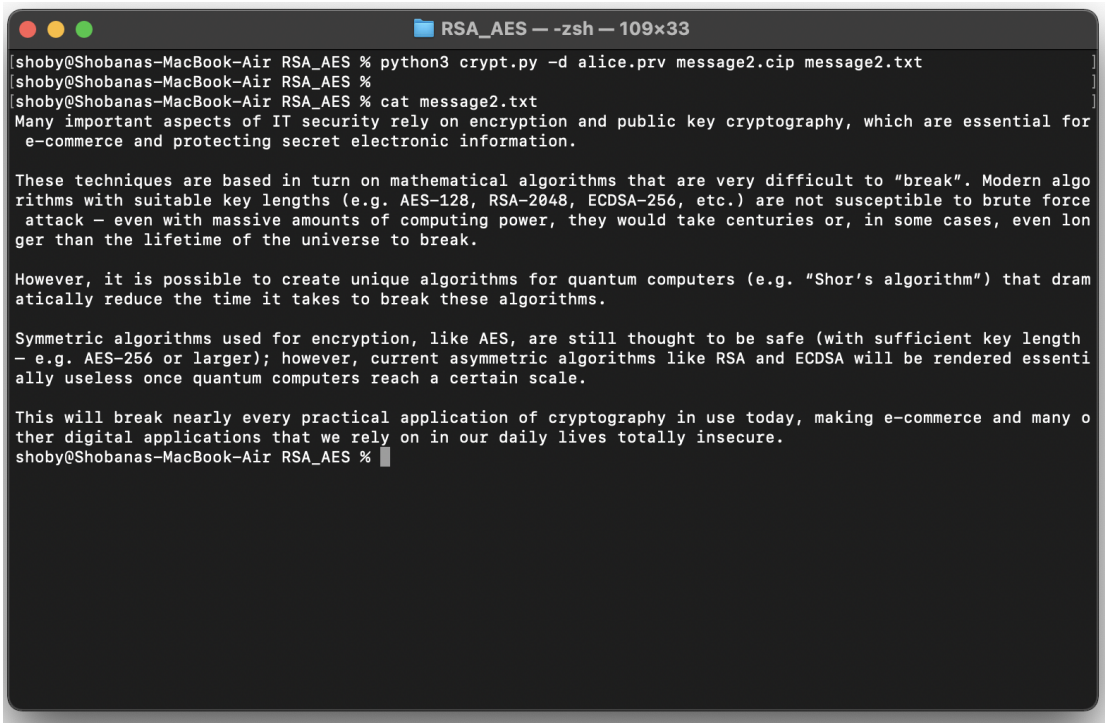

RSA_AES — -zsh — 80×40
shoby@Shobanas-MacBook-Air RSA_AES % cat message.txt
Named in honor of the trailblazing astronomer Edwin Hubble, the Hubble Space Tel
escope is a large, space-based observatory, which has revolutionized astronomy s
ince its launch and deployment by the space shuttle Discovery in 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 sy
stem.
Hubble's capabilities have grown immensely in its over 30 years of operation. Th
is is because new, cutting-edge scientific instruments have been added to the te
lescope over the course of five astronaut servicing missions. By replacing and u
pgrading aging parts, these servicing missions have greatly extended the telesco
pe's lifetime.
Telescopes have a particular range of light that they can detect. Hubble's domai
n 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 lifeti
me. Over 19,000 peer-reviewed science papers have been published on its discover
ies, and every current astronomy textbook includes contributions from the observ
atory. 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 atmosphe
res 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, capt
uring 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 captur
ed humanity's imaginations and deepened our knowledge of the cosmos. It will con
tinue to do so for years to come.
shoby@Shobanas-MacBook-Air RSA_AES %


RSA_AES — -zsh — 116×46
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
shoby@Shobanas-MacBook-Air RSA_AES %


RSA_AES — -zsh — 109×48
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 — 108×32
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 — 109×33
[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
shoby@S
shoby@Shobanas-MacBook-Air RSA_AES %


RSA_AES — -zsh — 109×33
[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 algo
rithms 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 lon
ger 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 dram
atically 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 essenti
ally 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 o
ther digital applications that we rely on in our daily lives totally insecure.
shoby@Shobanas-MacBook-Air RSA_AES %