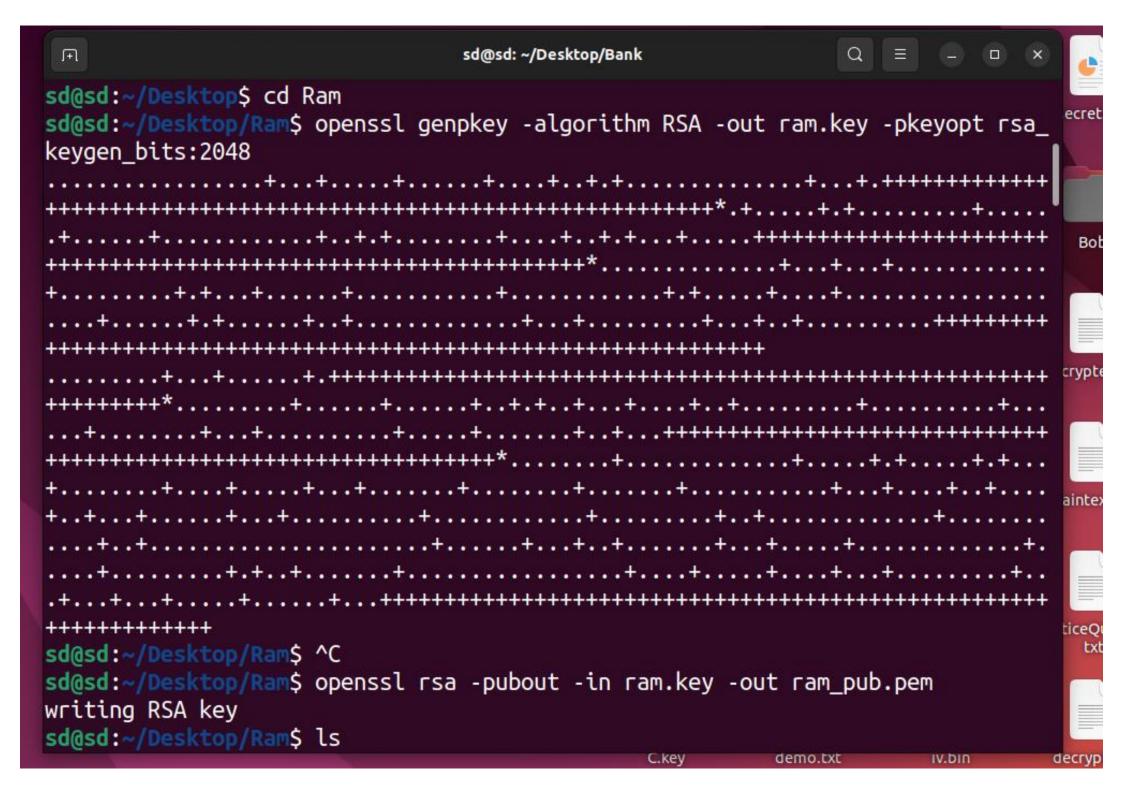
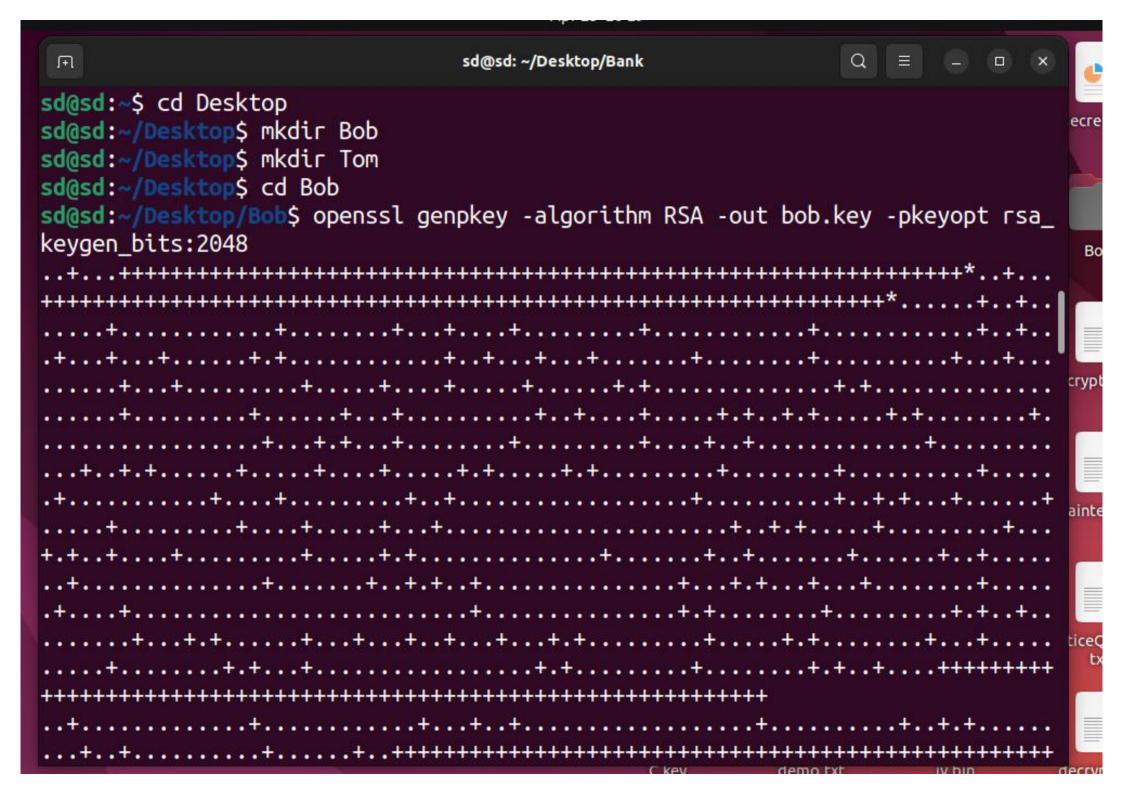
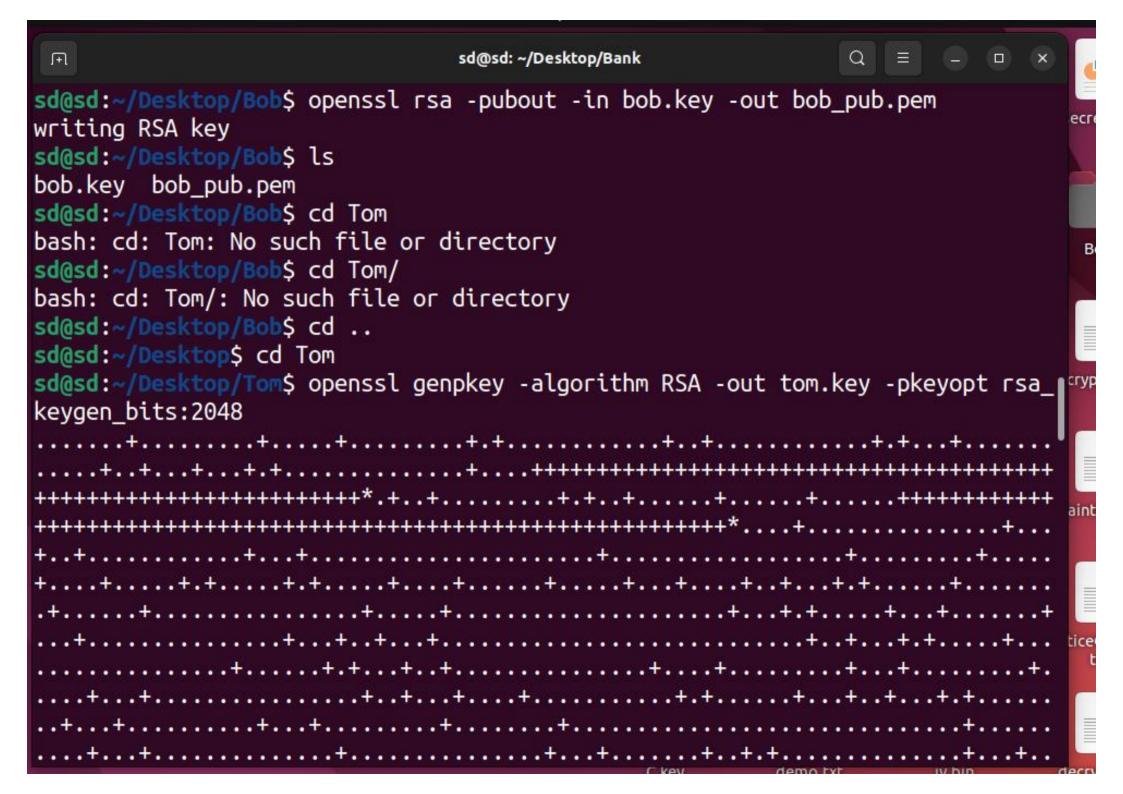
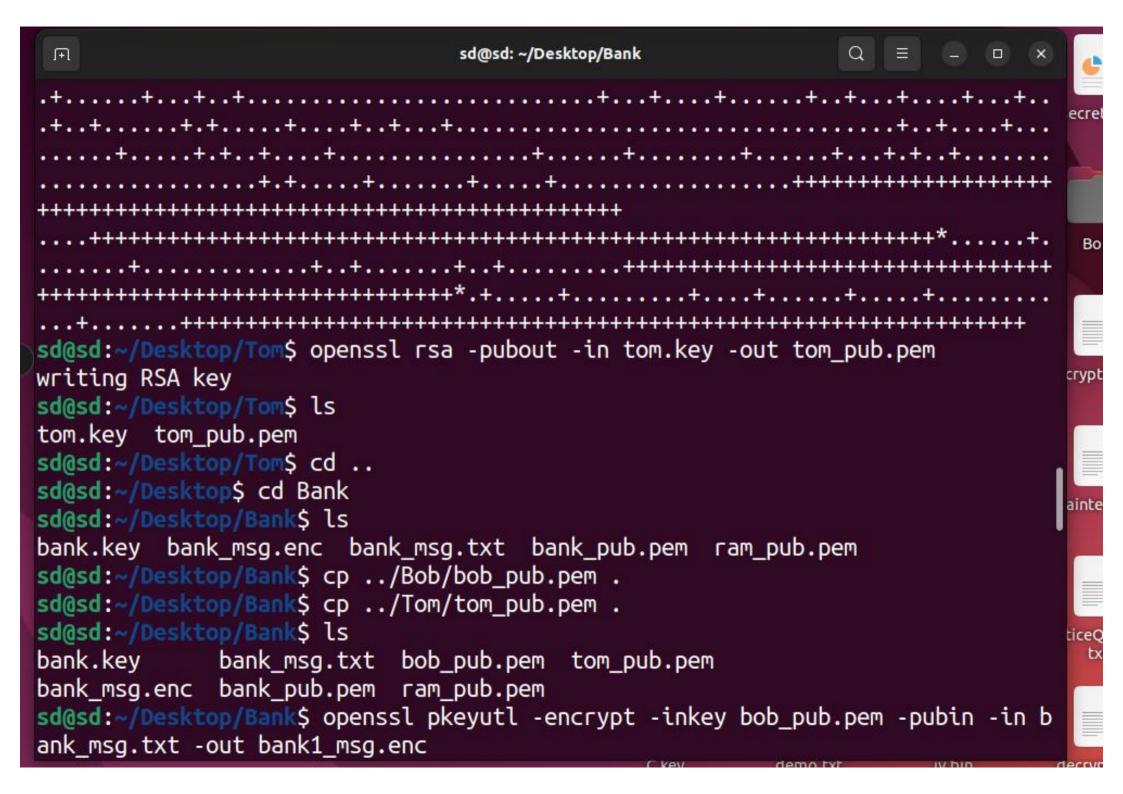
sd@sd: ~/Desktop/Bank +sd@sd:~/Desktop\$ cd Bank sd@sd:~/Desktop/Bank\$ ls sd@sd:~/Desktop/Bank\$ openssl genpkey -algorithm RSA -out bank.key -pkeyopt rs a\_keygen\_bits:2048 sd@sd:~/Desktop/Bank\$ openssl rsa -pubout -in bank.key -out bank\_pub.pem writing RSA key sd@sd:~/Desktop/Bank\$ ls bank.key bank pub.pem sd@sd:~/Desktop/Bank\$ cd ... sd@sd:~/Desktop\$ cd Ram sd@sd:~/Desktop/Ram\$ openssl genpkey -algorithm RSA -out ram.key -pkeyopt rsa\_ keygen bits:2048 IV.bin C.key demo.txt



```
Q = - - ×
 (F)
                                 sd@sd: ~/Desktop/Bank
ram.key ram_pub.pem
sd@sd:~/Desktop/Ram$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ echo "Your bank account balance is low" > bank_msg.txt
sd@sd:~/Desktop/Bank$ cp ../ram/ram_pub.pem .
cp: cannot stat '../ram/ram_pub.pem': No such file or directory
sd@sd:~/Desktop/Bank$ cp ../Ram/ram_pub.pem .
sd@sd:~/Desktop/Bank$ ls
bank.key bank_msg.txt bank_pub.pem ram_pub.pem
sd@sd:~/Desktop/Bank$ openssl pkeyutl -encrypt -inkey ram_pub.pem -pubin -in b
ank msg.txt -out bank msg.enc
sd@sd:~/Desktop/Bank$ cat bank_msg.enc
o[?oojoZodoo%ooooooŐ~/oooV|rooxo<o}HoioooooE`xoWooo)soYÆ4odoopo_
oo\ROoo&Aoo`&oEH1هاoo*ooooooooooo o=|ooIooLoooooovooodo+oo^ooZto@Â
                                                   1k-1%d?LOP
.bee6ensd@sd:~/Desktop/Bank$ cp bank_msg.enc ../Ram/
sd@sd:~/Desktop/Bank$ cd ../Ram/
sd@sd:~/Desktop/Ram$ ls
bank_msg.enc ram.key ram_pub.pem
sd@sd:~/Desktop/Ram$ openssl pkeyutl -decrypt -inkey ram.key -in bank_msg.enc
-out decrypted_bank_msg.txt
sd@sd:~/Desktop/Ram$ cat decrypted_bank_msg.txt
Your bank account balance is low
sd@sd:~/Desktop/Ram$ cd
                                               C.key
                                                         demo.txt
```







```
sd@sd: ~/Desktop/Bank
                                                                          F
sd@sd:~/Desktop/Bank$ cat bank1_msg.enc
Da! eoo+Vo yoBToH+ologooEooooIoP#OWo
Г:
o-or6#>odoooc\ooooCoxoJoooWo@eoo.*oooJoQIb"ooos@
                                                   Voo=eoooojC+D>oo"oojooNooooU
'ooi/ARoo6"Ioo
            0?0~0E0000
                      1c) 000Poi\>Ft1E000+0Pq00Vsd@sd:~/Desktop/Bank$
sd@sd:~/Desktop/Bank$ openssl pkeyutl -encrypt -inkey tom_pub.pem -pubin -in b
ank msg.txt -out bank2 msg.enc
sd@sd:~/Desktop/Bank$ cat bank2 msg.enc
Zooo<u>o</u>xoyo3oooyioouooo{Koooog!o3oo>8oooo9@qo~oyoi:oooo"Rooooo2'o
                                                                  eleccoelecles
                                          veeeeHeGTeeeeReeeo뇔eDQu_ee>eee<ge~k
~/ee1weGpcvüe#eZeNeeeQe|:eeF^eeeeX
booloolwoCovJ@Aooo:oOooRoooloGoouooo+<oGoIoo<ooo*#oooooSr.osd@sd:~/Desktop/Ba
sd@sd:~/Desktop/Bank$
sd@sd:~/Desktop/Bank$
sd@sd:~/Desktop/Bank$ cd ...
sd@sd:~/Desktop$ cd Bob
sd@sd:~/Desktop/Bob$ openssl pkeyutl -decrypt -inkey bob.key -in bank1_msg.enc
 -out decrypted_bank1_msg.txt
Can't open "bank1_msg.enc" for reading, No such file or directory
405776E4BB7D0000:error:80000002:system library:BIO_new_file:No such file or di
```

```
Q = - -
 (<del>+</del>)
                                 sd@sd: ~/Desktop/Bank
sd@sd:~/Desktop/Bob$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ cp bank1_msg.enc ../Bob/
sd@sd:~/Desktop/Bank$ cd ...
sd@sd:~/Desktop$ cd Bob
sd@sd:~/Desktop/Bob$ ls
bank1 msg.enc bob.key bob_pub.pem
sd@sd:~/Desktop/Bob$ openssl pkeyutl -decrypt -inkey bob.key -in bank1_msg.enc
 -out decrypted bank1 msg.txt
sd@sd:~/Desktop/Bob$ cat decrypted_bank1_msg.txt
Your bank account balance is low
sd@sd:~/Desktop/Bob$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ cp bank2_msg.enc ../Tom/
sd@sd:~/Desktop/Bank$ cd ...
sd@sd:~/Desktop$ cd Tom
sd@sd:~/Desktop/Tom$ openssl pkeyutl -decrypt -inkey tom.key -in bank2_msg.enc
 -out decrypted_bank2_msg.txt
sd@sd:~/Desktop/Tom$ cat decrypted_bank2_msg.txt
Your bank account balance is low
sd@sd:~/Desktop/Tom$ echo "Please verify my bank account balance." > my_msg.tx
sd@sd:~/Desktop/Tom$ ls
bank2 msg.enc decrypted bank2 msg.txt my msg.txt tom.key tom pub.pem
```

```
Ħ.
                                sd@sd: ~/Desktop/Bank
                                                               Q = - -
sd@sd:~/Desktop/Tom$ cp ../Bank/bank_pub.pem .
sd@sd:~/Desktop/Tom$ ls
bank2_msg.enc decrypted_bank2_msg.txt tom.key
bank pub.pem my msg.txt
                                        tom pub.pem
sd@sd:~/Desktop/Tom$ openssl pkeyutl -encrypt -inkey bank_pub.pem -pubin -in m
y msg.txt -out bank3 msg.enc
sd@sd:~/Desktop/Tom$ cat bank3_msg.enc
ooZXMoooolo4^o7oooEoo ooNr}oooOouoowoool
8000 | 0000000CJ0000p000/00]00
                            oo5onoo/cAoooDooojoooHo#4'ooY{Qo[oo+A`Nooov2ZaKo #
•``eld"ee:eZeX7Qee0ee]eXBteeeee.keeeK)e$eee'ewee*lsd@sd:~/Desktop/Tom$
sd@sd:~/Desktop/Tom$ cd ..
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ ls
bank1 msg.enc bank.key
                             bank_msg.txt bob_pub.pem tom_pub.pem
bank2_msg.enc bank_msg.enc
                             bank_pub.pem ram_pub.pem
sd@sd:~/Desktop/Bank$ cd ...
sd@sd:~/Desktop$ cd Tom
sd@sd:~/Desktop/Tom$ cp bank3_msg.enc ../Bank/
sd@sd:~/Desktop/Tom$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ openssl pkeyutl -decrypt -inkey bank.key -in bank3_msg.e
nc -out decrypted_bank3_msg.txt
sd@sd:~/Desktop/Bank$ cat decrypted_bank3_msg.txt
                                                         demo.txt
                                                                     IV.bin
```

```
Q = - - ×
 (F)
                                sd@sd: ~/Desktop/Bank
bank2_msg.enc decrypted_bank2_msg.txt tom.key
bank pub.pem my msg.txt
                                       tom pub.pem
sd@sd:~/Desktop/Tom$ openssl pkeyutl -encrypt -inkey bank_pub.pem -pubin -in m
y msg.txt -out bank3 msg.enc
sd@sd:~/Desktop/Tom$ cat bank3_msg.enc
ooZXMoooolo4^o7oooEoo ooNr}ooooouoowoool
8000 00000000 J0000 DO00 /00 00
                           oo5onoo/cAoooDooojoooHo#4'ooY{Qo[oo+A`Nooov2ZaKo #
e``old"ee @eZeX7QeeOee]eXBteeeee.keeeK)e$eee'ewee*lsd@sd:~/Desktop/Tom$
sd@sd:~/Desktop/Tom$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ ls
bank1 msg.enc bank.key bank_msg.txt bob_pub.pem tom_pub.pem
bank2 msg.enc bank_msg.enc
                            bank_pub.pem ram_pub.pem
sd@sd:~/Desktop/Bank$ cd ...
sd@sd:~/Desktop$ cd Tom
sd@sd:~/Desktop/Tom$ cp bank3_msg.enc ../Bank/
sd@sd:~/Desktop/Tom$ cd ...
sd@sd:~/Desktop$ cd Bank
sd@sd:~/Desktop/Bank$ openssl pkeyutl -decrypt -inkey bank.key -in bank3_msg.e
nc -out decrypted_bank3_msg.txt
sd@sd:~/Desktop/Bank$ cat decrypted_bank3_msg.txt
Please verify my bank account balance.
sd@sd:~/Desktop/Bank$
```

```
sd@sd: ~/Desktop/Bank
 F
Please verify my bank account balance.
sd@sd:~/Desktop/Bank$ ls
bank1_msg.enc bank.key bank_pub.pem
                                                    ram_pub.pem
bank2 msg.enc bank msg.enc bob pub.pem
                                                    tom_pub.pem
bank3_msg.enc bank_msg.txt decrypted_bank3_msg.txt
sd@sd:~/Desktop/Bank$ cp bank_msg.txt ../Ram/
sd@sd:~/Desktop/Bank$ cd ../Ram/
sd@sd:~/Desktop/Ram$ ls
bank_msg.enc bank_msg.txt decrypted_bank_msg.txt ram.key ram_pub.pem
sd@sd:~/Desktop/Ram$ openssl dgst -sha256 -sign ram.key -out signature.bin ban
k msq.txt
sd@sd:~/Desktop/Ram$ ls
bank_msg.enc decrypted_bank_msg.txt ram_pub.pem
bank_msg.txt ram.key
                                     signature.bin
sd@sd:~/Desktop/Ram$ cp signature.bin ../Bank/
sd@sd:~/Desktop/Ram$ cd ../Bank/
sd@sd:~/Desktop/Bank$ ls
bank1_msg.enc bank.key bank_pub.pem
                                                    ram_pub.pem
bank2_msg.enc bank_msg.enc bob_pub.pem
                                                    signature.bin
bank3_msg.enc bank_msg.txt decrypted_bank3_msg.txt tom_pub.pem
sd@sd:~/Desktop/Bank$ openssl dgst -sha256 -verify ram_pub.pem -signature sign
ature.bin bank_msg.txt
Verified OK
sd@sd:~/Desktop/Bank$
                                              C.kev
                                                       demo.txt
                                                                   IV.bin
```