[illegible]

```
sd@sd:~/Desktop/Ram$ openssl genpkey -algorithm RSA -out ram.key -pkeyopt rsa_keygen_bits:2048
```



```
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 bank_msg.txt -out bank_msg.enc
sd@sd:~/Desktop/Bank$ cat bank_msg.enc
[?jZed%???"0~/??V|r??x<?}H?i????E`x?W???)s?YÃ4?d?p?_
??\R0??&A??`&?EH1?J??*?????0??_?=|??I??L?????v????d?+??^??Zt?@Ä
lk-|?d?LQP????
.b??6?n
sd@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
```


sd@sd: ~/Desktop/Bank

```
sd@sd:~$ cd Desktop
```


```
sd@sd:~/Desktop$ mkdir Bob
```

```
sd@sd:~/Desktop$ mkdir Tom
```

```
sd@sd:~/Desktop$ cd Bob
```

```
sd@sd:~/Desktop/Bob$ openssl genpkey -algorithm RSA -out bob.key -pkeyopt rsa_
keygen_bits:2048
```

A large grid of 20 rows and 100 columns of dots. The dots are arranged in a pattern that resembles a stylized 'X' or a cross, with the highest density of dots in the center and tapering off towards the edges. The dots are small and black, set against a white background.



ecre

B

сгур

aint

rice

t

если

если

если

если

C key	demo.txt	iv bin	decry
-------	----------	--------	-------

sd@sd: ~/Desktop/Bank

[illegible]

```
. . . ++++++* . . . +.  
. . . . + . . . . + . + . . . . + . . . . ++++++  
+++++++* . + . . . + . . . + . . . + . . . + . . . .  
. . . + . . . . ++++++
```

```
sd@sd:~/Desktop/Tom$ openssl rsa -pubout -in tom.key -out tom_pub.pem
```

writing RSA key

```
sd@sd:~/Desktop/Tom$ ls
```

```
tom.key  tom_pub.pem
```

```
sd@sd:~/Desktop/Tom$ cd ..
```

```
sd@sd:~/Desktop$ cd Bank
```

```
sd@sd:~/Desktop/Bank$ ls
```

```
bank.key  bank_msg.enc  bank_msg.txt  bank_pub.pem  ram_pub.pem
```

```
sd@sd:~/Desktop/Bank$ cp ../Bob/bob_pub.pem .
```

```
sd@sd:~/Desktop/Bank$ cp ../Tom/tom_pub.pem .
```

```
sd@sd:~/Desktop/Bank$ ls
```

```
bank.key      bank_msg.txt  bob_pub.pem  tom_pub.pem
```

bank_msg.enc bank_pub.pem ram_pub.pem

```
sd@sd:~/Desktop/Bank$ openssl pkeyutl -encrypt -inkey bob_pub.pem -pubin -in bank_msg.txt -out bank1_msg.enc
```



```
sd@sd:~/Desktop/Bank$ cat bank1_msg.enc
```

```
Da!|e+V yBT H+l عEoI P#OW
```

```
r:
```

```
-r6#>dC\ CxJ W@ê.*JQIb" s
```

```
V=e jC+D>" jN U
```

```
'i/AR6"I
```

```
?~E
```

```
1c)P i\>Ft1E+PqVsd@sd:~/Desktop/Bank$
```

```
sd@sd:~/Desktop/Bank$ openssl pkeyutl -encrypt -inkey tom_pub.pem -pubin -in bank_msg.txt -out bank2_msg.enc
```

```
sd@sd:~/Desktop/Bank$ cat bank2_msg.enc
```

```
Z xÿ3Yiu{K g!3>89@q~y i:"R2'
```

```
Qe@ @
```

```
~/1wGpcvÜ#Z NQ |:eF^X
```

```
vHGT R o ñ DQu_><g~k
```

```
bL1wCvJ :oR1Gu+<GI< *#Sr.sd@sd:~/Desktop/Bank$
```

```
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:BI0_new_file:No such file or di
```



```
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
t
sd@sd:~/Desktop/Tom$ ls
bank2_msg.enc  decrypted_bank2_msg.txt  my_msg.txt  tom.key  tom_pub.pem
```



```
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
??ZXM??l?4^?7??E?? ??nr}????o?u??w???l
8???|????0??cJ????pō?/??]??
                                ??5?n??/cA???D???j???H?#4'???Y{Q?[??+A`N???v2ZaK? #
?`'?ld"??Z?X7Q??0??]??XB??.k???K)?$???'w??*l
sd@sd:~/Desktop/Tom$
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
```



```
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
??ZXM??l?4^?7??E?? ??nr}???o?u??w???l
8???|???0??cJ???pō??/??]??
                                ??5?n??/cA???D???j???H?#4'??Y{Q?[??+A`N???v2ZaK? #
?` `?ld"?? ?Z?X7Q??0??]??XB†???.k???K)?$???'??w??*l
sd@sd:~/Desktop/Tom$
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$
```


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 bank_msg.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 signature.bin bank_msg.txt
```

Verified OK

```
sd@sd:~/Desktop/Bank$
```