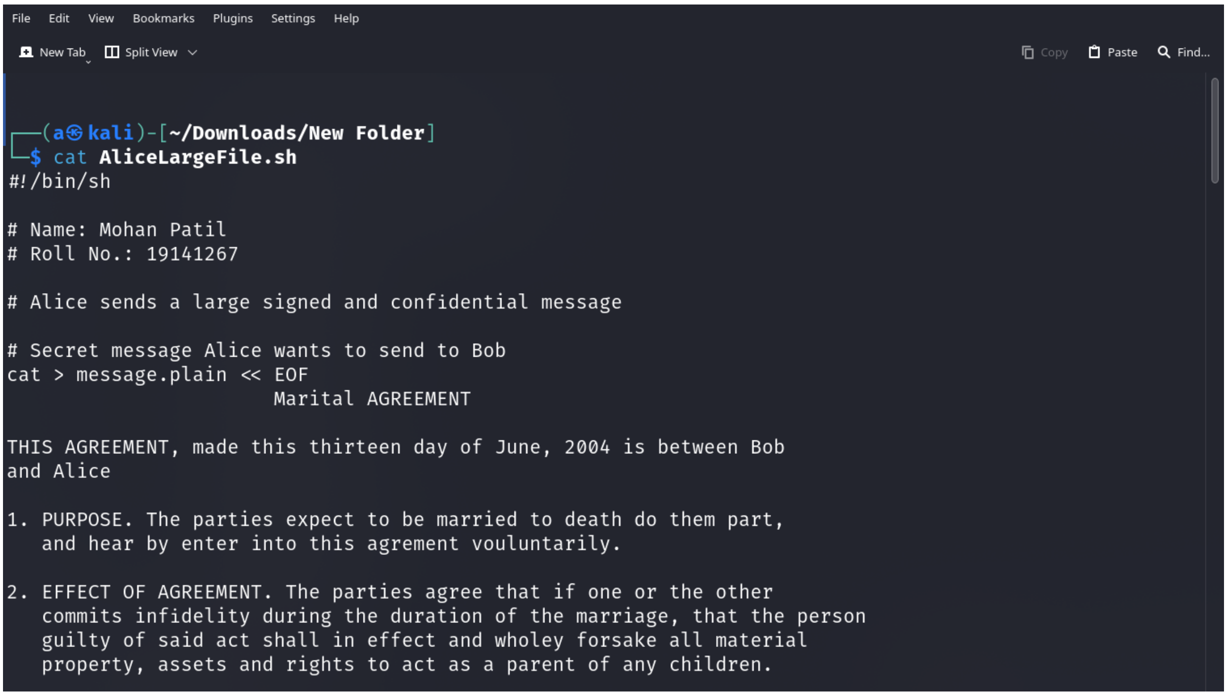
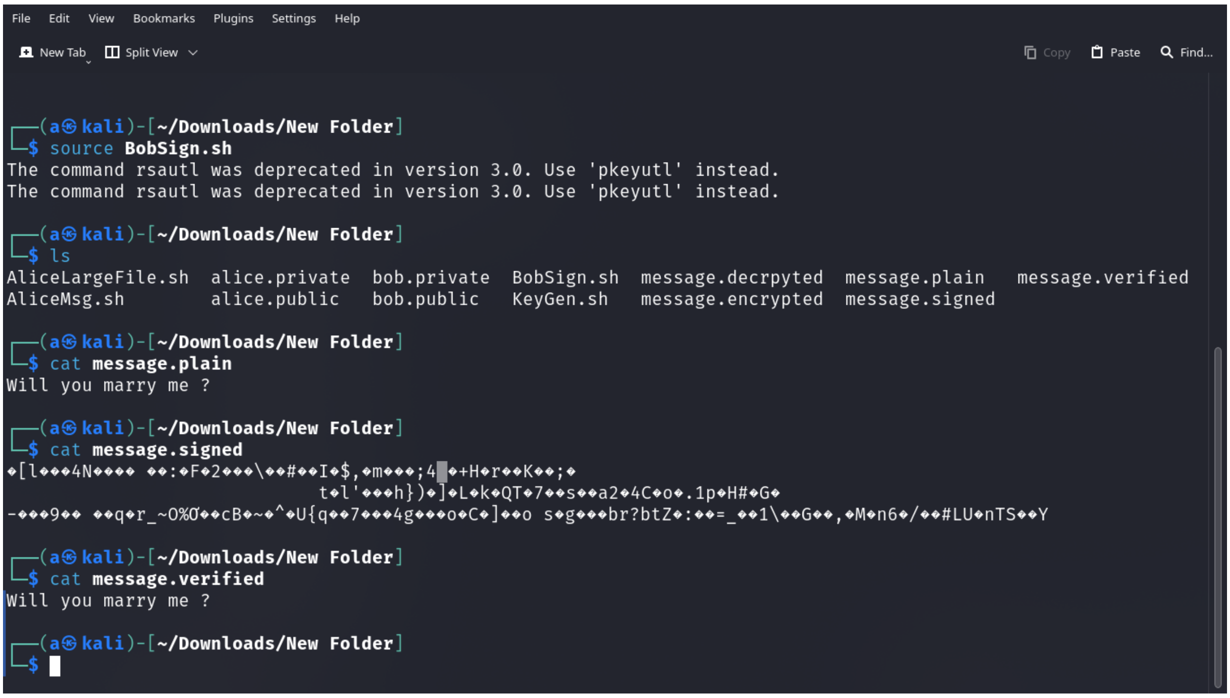
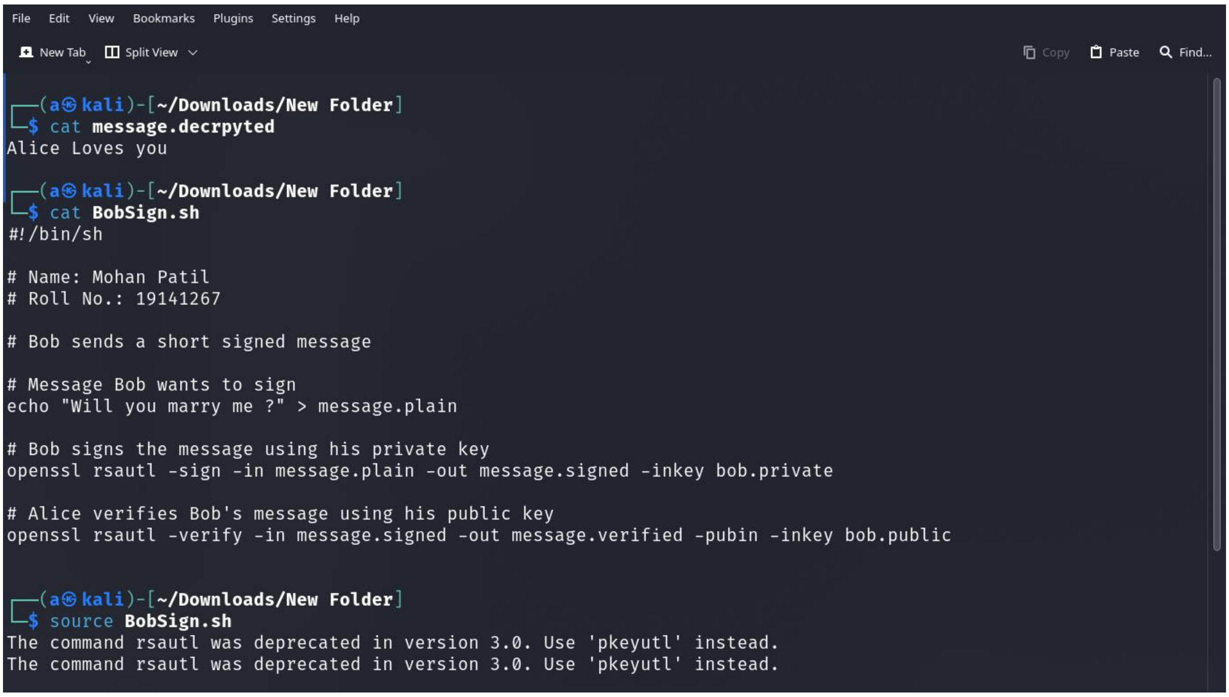
Experiment No. 11 Name: Mohan Patil Roll No. 19141267



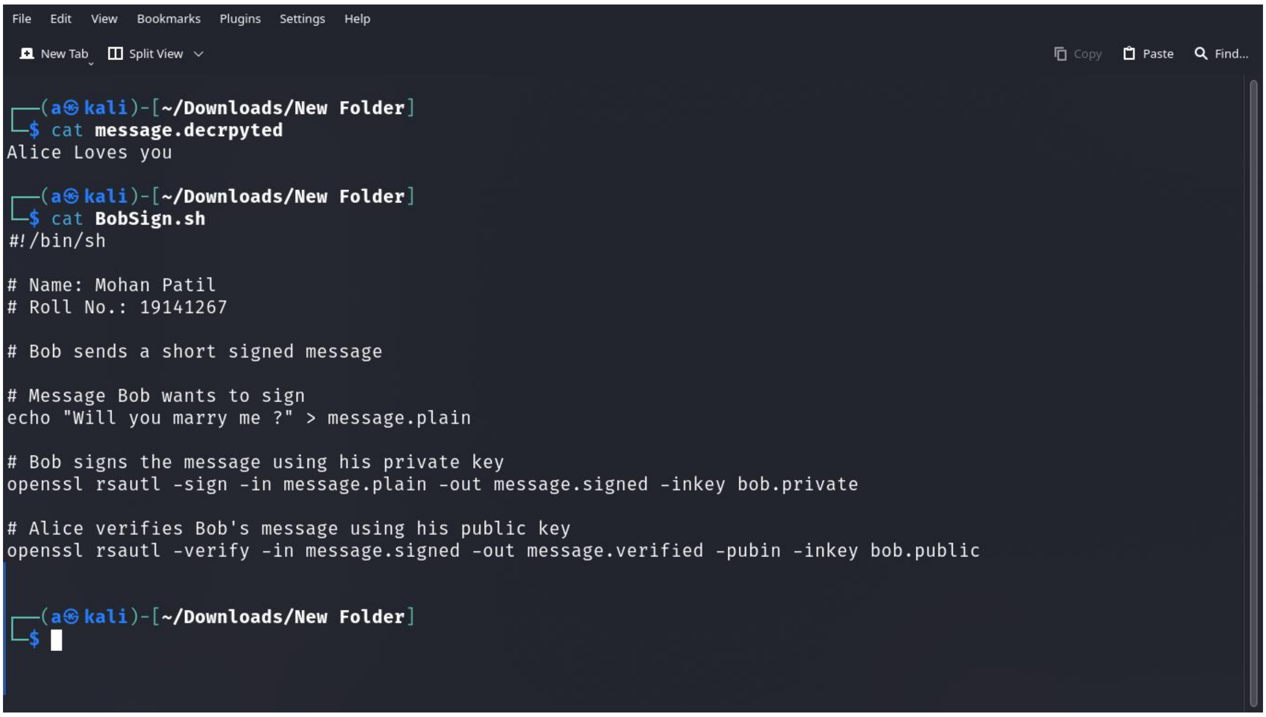
```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat AliceLargeFile.sh
#!/bin/sh

# Name: Mohan Patil
# Roll No.: 19141267

# Alice sends a large signed and confidential message

# Secret message Alice wants to send to Bob
cat > message.plain << EOF
                       Marital AGREEMENT

THIS AGREEMENT, made this thirteen day of June, 2004 is between Bob
and Alice

1. PURPOSE. The parties expect to be married to death do them part,
   and hear by enter into this agrement vouluntarily.

2. EFFECT OF AGREEMENT. The parties agree that if one or the other
   commits infidelity during the duration of the marriage, that the person
   guilty of said act shall in effect and wholey forsake all material
   property, assets and rights to act as a parent of any children.
```



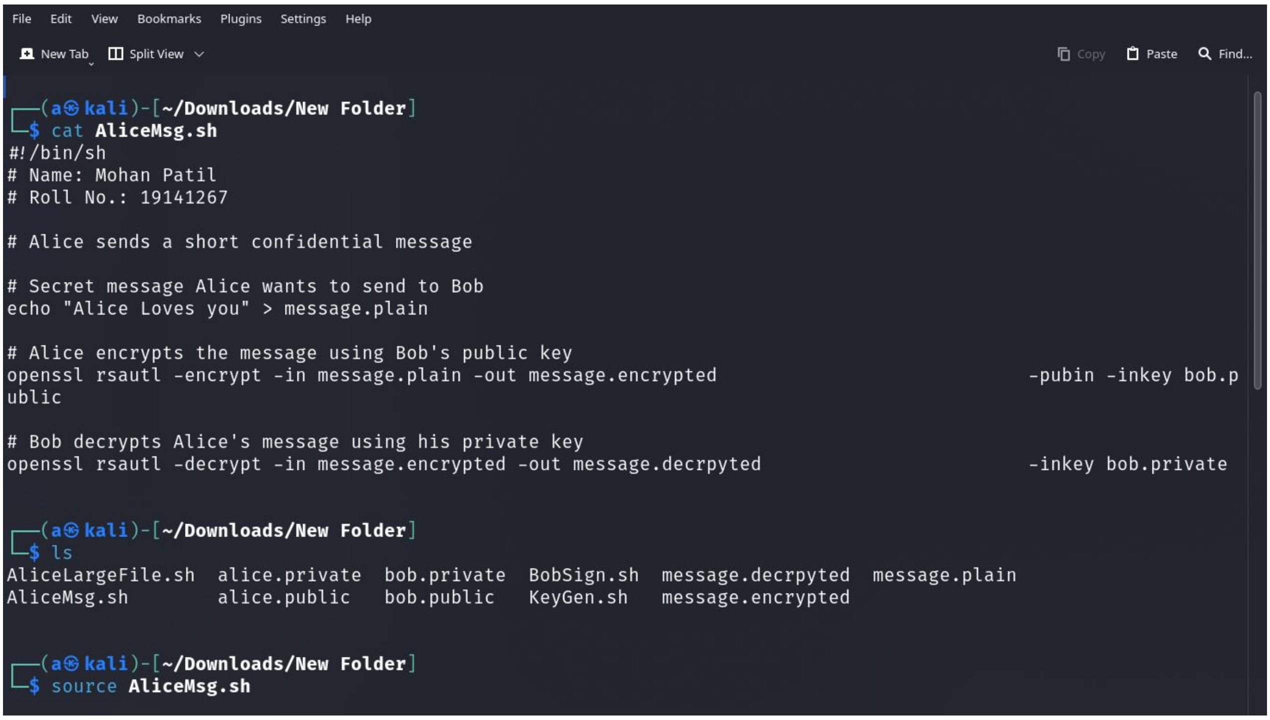
```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ source BobSign.sh
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ ls
AliceLargeFile.sh  alice.private  bob.private  BobSign.sh  message.decrpyted  message.plain   message.verified
AliceMsg.sh        alice.public   bob.public   KeyGen.sh   message.encrypted  message.signed

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat message.plain
Will you marry me ?

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat message.signed
�[l���4N���� ��:�F�2���\��#��I�$,�m���;4 �+H�r��K��;�
                             t�l'���h})�]�L�k�QT�7��s��a2�4C�o�.1p�H#�G�
-���9�� ��q�r_~O%Ơ��cB�~�^�U{q��7���4g����o�C�]��o s�g���br?btZ�:��=_��1\��G��,�M�n6�/��#LU�nTS��Y

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat message.verified
Will you marry me ?

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ █
```



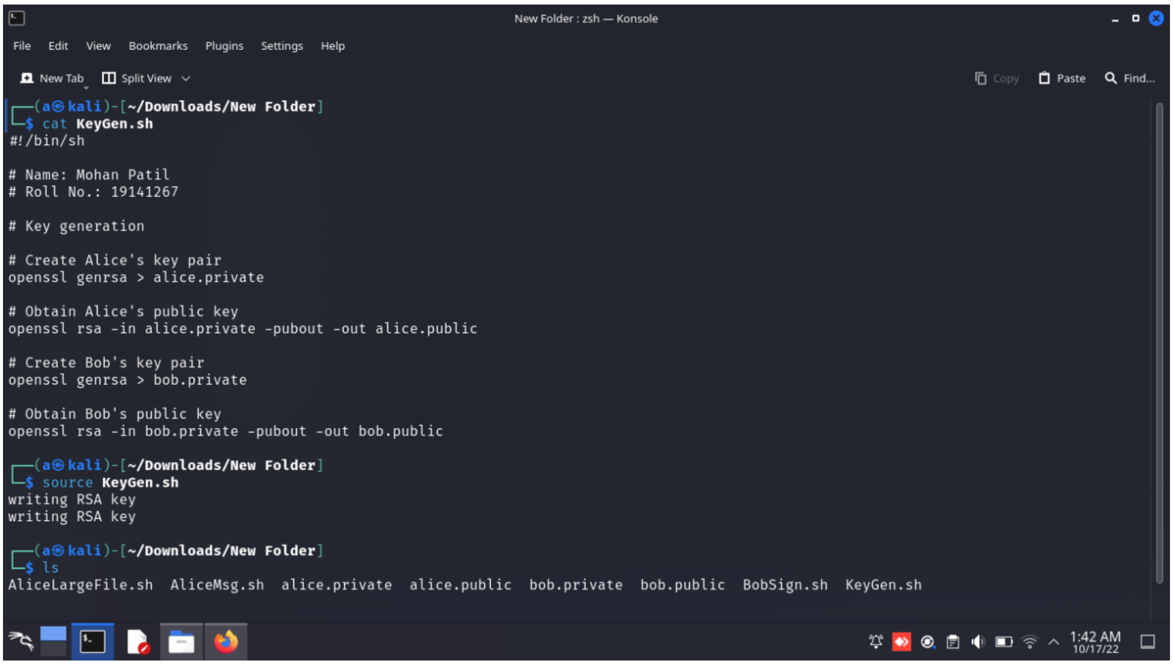
```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat message.decrpyted
Alice Loves you

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat BobSign.sh
#!/bin/sh

# Name: Mohan Patil
# Roll No.: 19141267

# Bob sends a short signed message

# Message Bob wants to sign
echo "Will you marry me ?" > message.plain

# Bob signs the message using his private key
openssl rsautl -sign -in message.plain -out message.signed -inkey bob.private

# Alice verifies Bob's message using his public key
openssl rsautl -verify -in message.signed -out message.verified -pubin -inkey bob.public


┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ source BobSign.sh
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
```



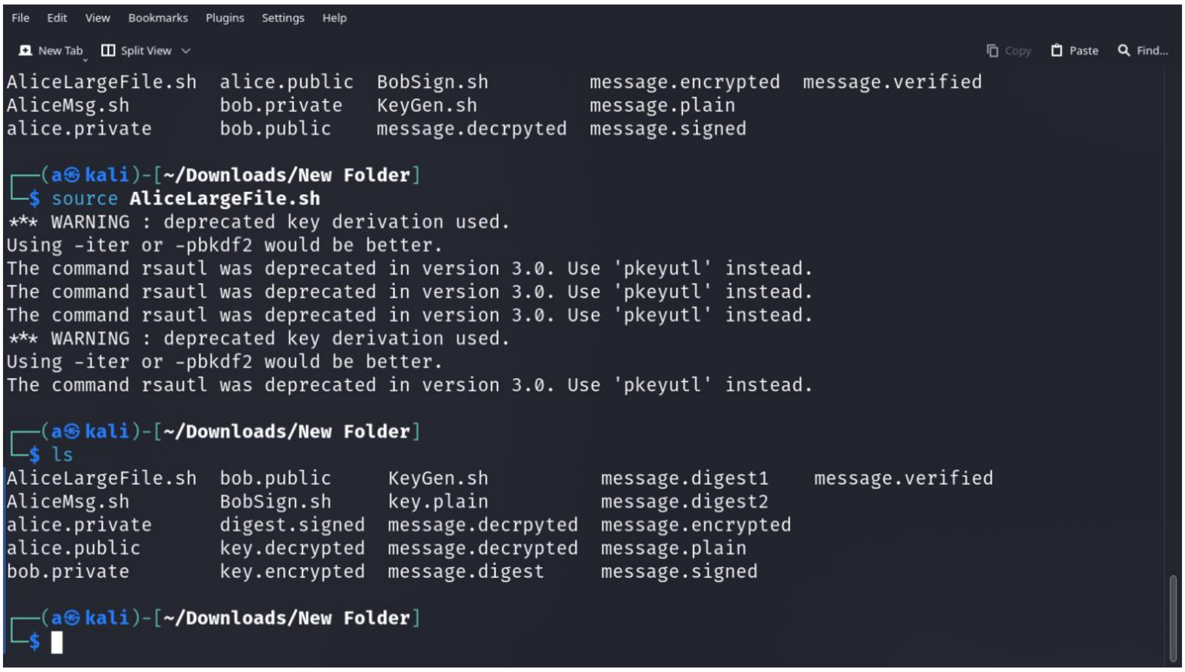
```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat message.decrpyted
Alice Loves you

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat BobSign.sh
#!/bin/sh

# Name: Mohan Patil
# Roll No.: 19141267

# Bob sends a short signed message

# Message Bob wants to sign
echo "Will you marry me ?" > message.plain

# Bob signs the message using his private key
openssl rsautl -sign -in message.plain -out message.signed -inkey bob.private

# Alice verifies Bob's message using his public key
openssl rsautl -verify -in message.signed -out message.verified -pubin -inkey bob.public


┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ 
```



```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat AliceMsg.sh
#!/bin/sh
# Name: Mohan Patil
# Roll No.: 19141267

# Alice sends a short confidential message

# Secret message Alice wants to send to Bob
echo "Alice Loves you" > message.plain

# Alice encrypts the message using Bob's public key
openssl rsautl -encrypt -in message.plain -out message.encrypted                            -pubin -inkey bob.p
ublic

# Bob decrypts Alice's message using his private key
openssl rsautl -decrypt -in message.encrypted -out message.decrpyted                        -inkey bob.private


┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ ls
AliceLargeFile.sh  alice.private  bob.private  BobSign.sh  message.decrpyted  message.plain
AliceMsg.sh        alice.public   bob.public   KeyGen.sh   message.encrypted


┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ source AliceMsg.sh
```


New Folder : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab
Split View
Copy
Paste
Find...
1:42 AM
10/17/22

```
┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ cat KeyGen.sh
#!/bin/sh

# Name: Mohan Patil
# Roll No.: 19141267

# Key generation

# Create Alice's key pair
openssl genrsa > alice.private

# Obtain Alice's public key
openssl rsa -in alice.private -pubout -out alice.public

# Create Bob's key pair
openssl genrsa > bob.private

# Obtain Bob's public key
openssl rsa -in bob.private -pubout -out bob.public

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ source KeyGen.sh
writing RSA key
writing RSA key

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ ls
AliceLargeFile.sh  AliceMsg.sh  alice.private  alice.public  bob.private  bob.public  BobSign.sh  KeyGen.sh
```



```
AliceLargeFile.sh  alice.public  BobSign.sh        message.encrypted  message.verified
AliceMsg.sh        bob.private   KeyGen.sh         message.plain
alice.private      bob.public    message.decrpyted  message.signed

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ source AliceLargeFile.sh
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ ls
AliceLargeFile.sh  bob.public      KeyGen.sh          message.digest1    message.verified
AliceMsg.sh        BobSign.sh      key.plain          message.digest2
alice.private      digest.signed   message.decrpyted  message.encrypted
alice.public       key.decrypted   message.decrypted  message.plain
bob.private        key.encrypted   message.digest     message.signed

┌──(a㉿kali)-[~/Downloads/New Folder]
└─$ 
```