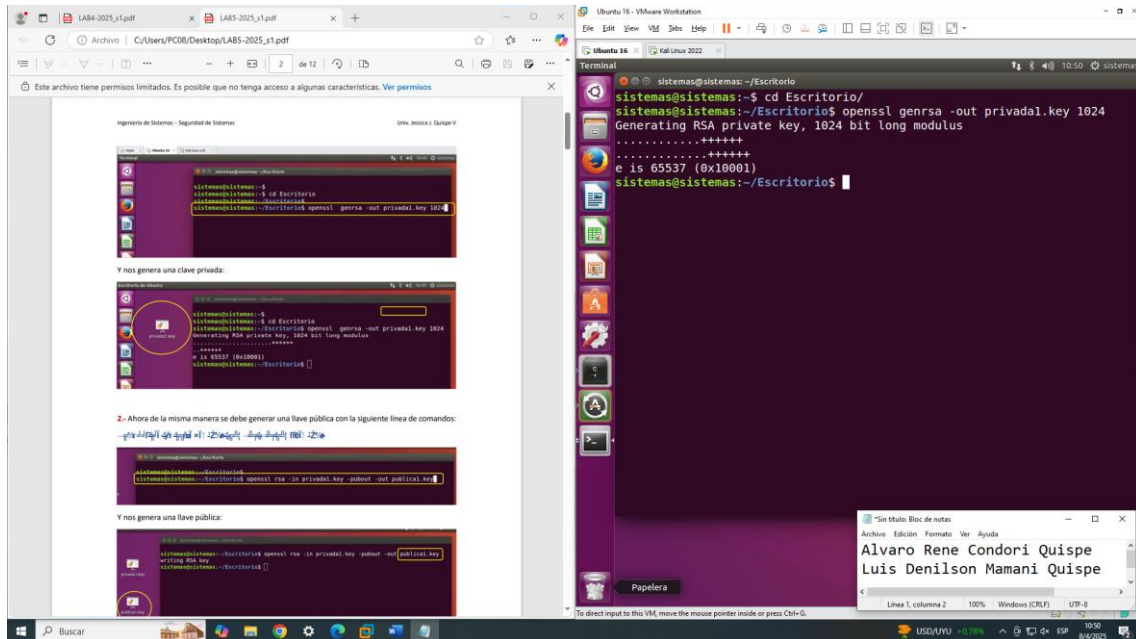


Lab 5

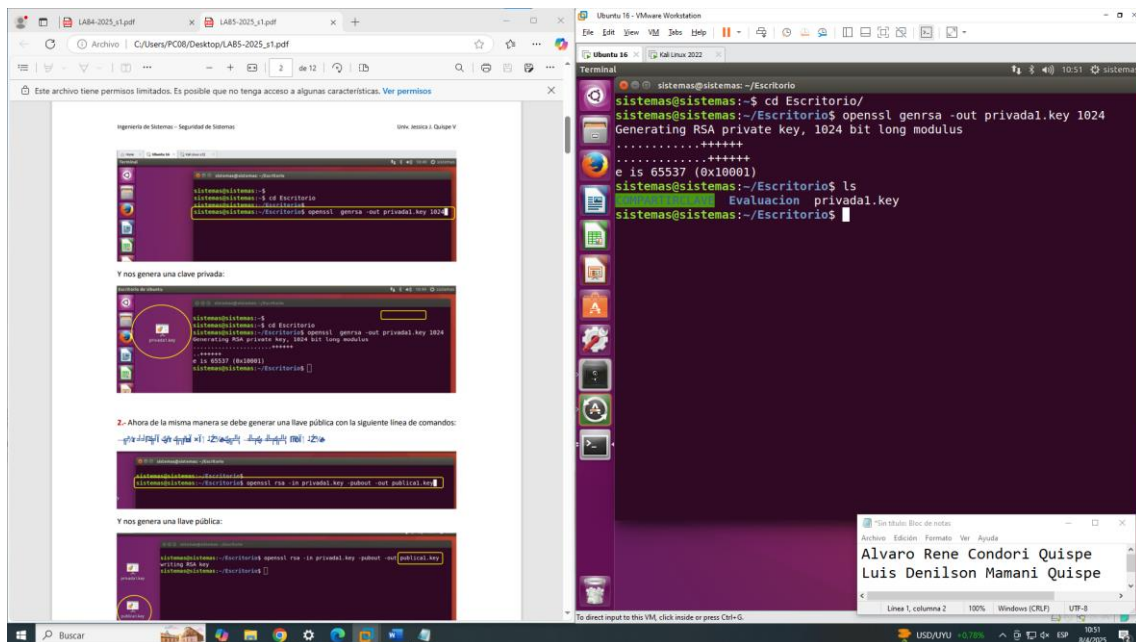
Nombres: Alvaro Rene Condori Quispe

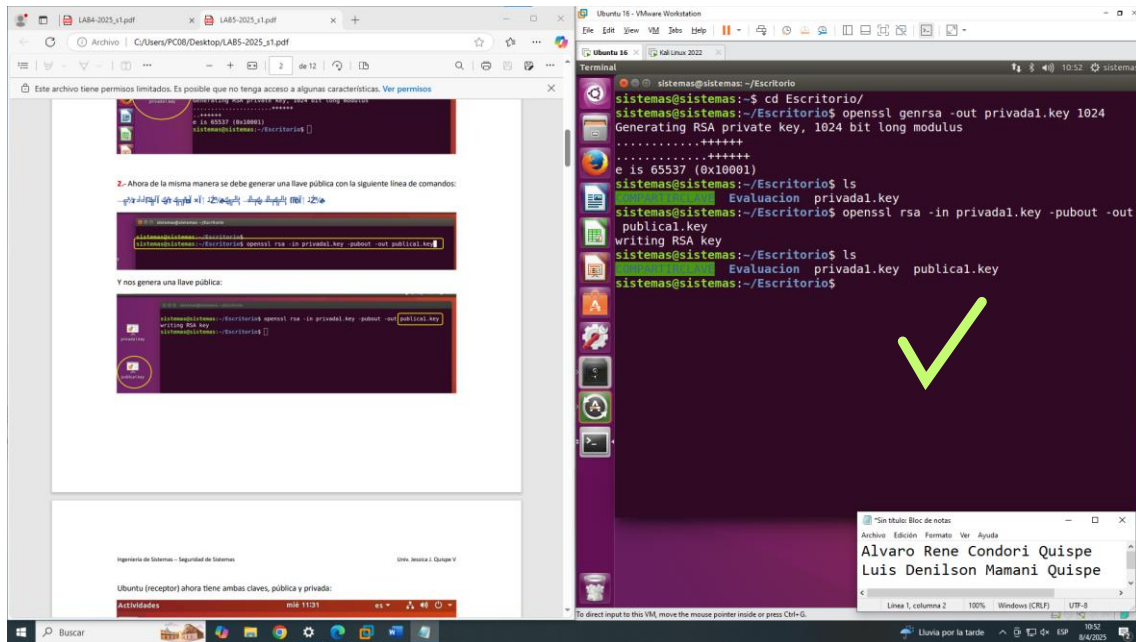
Luis Denilson Mamani Quispe

1

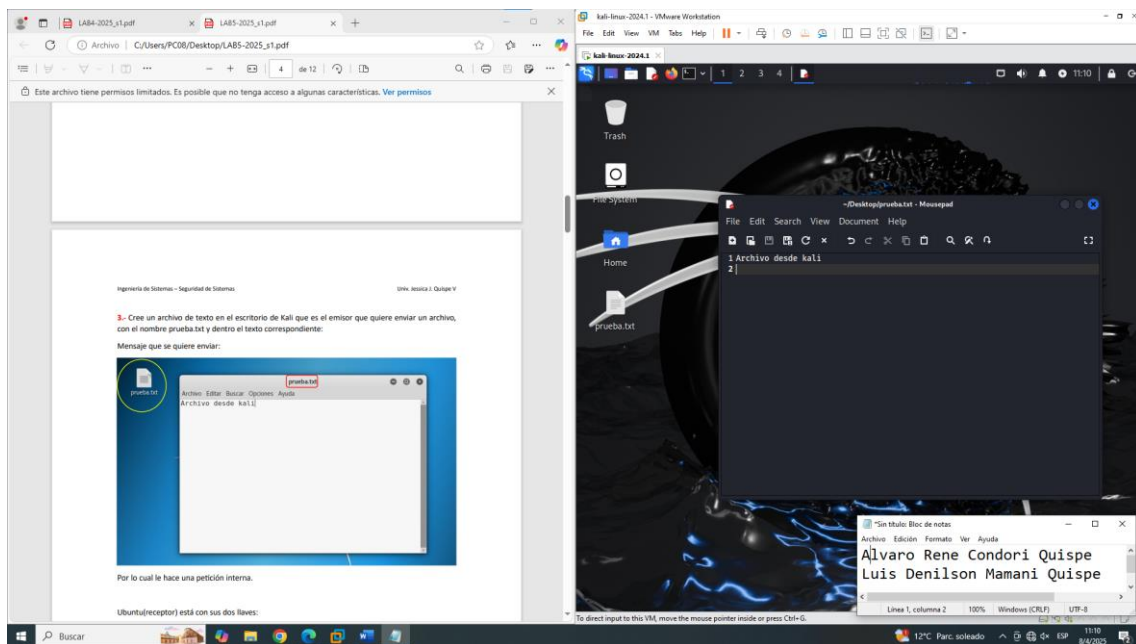


2

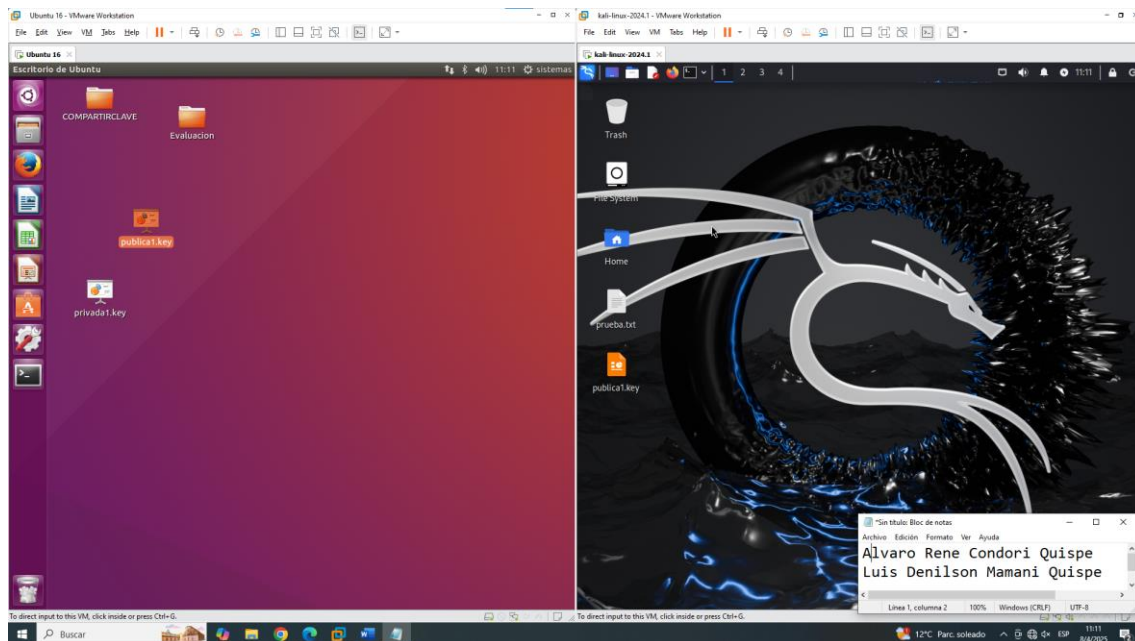




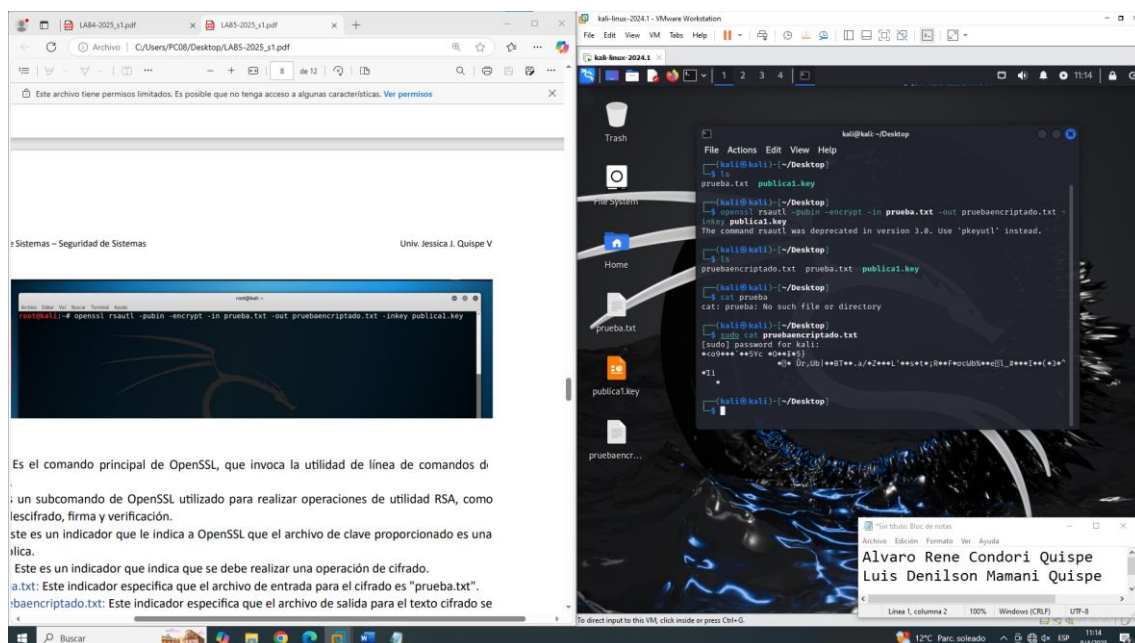
3.

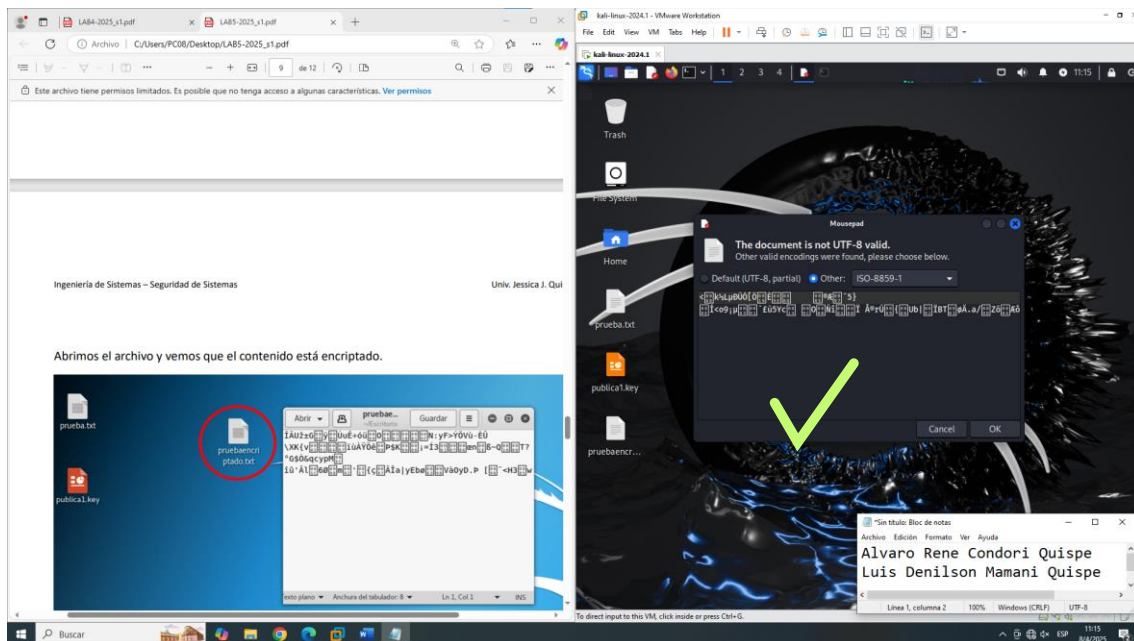


4.

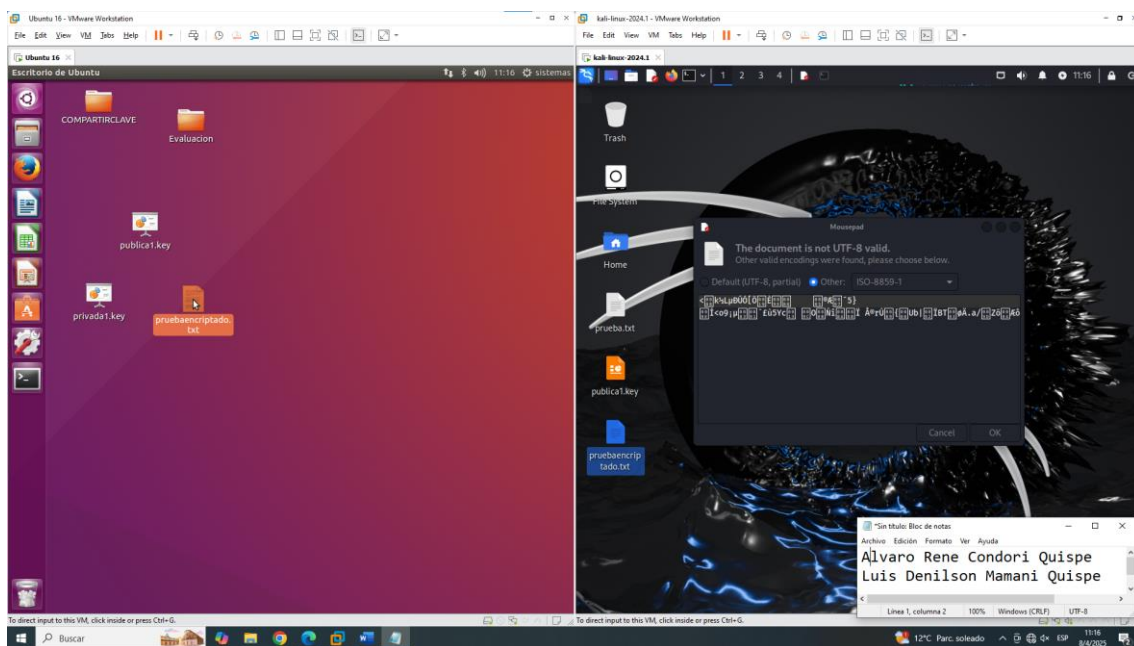


5.





5.



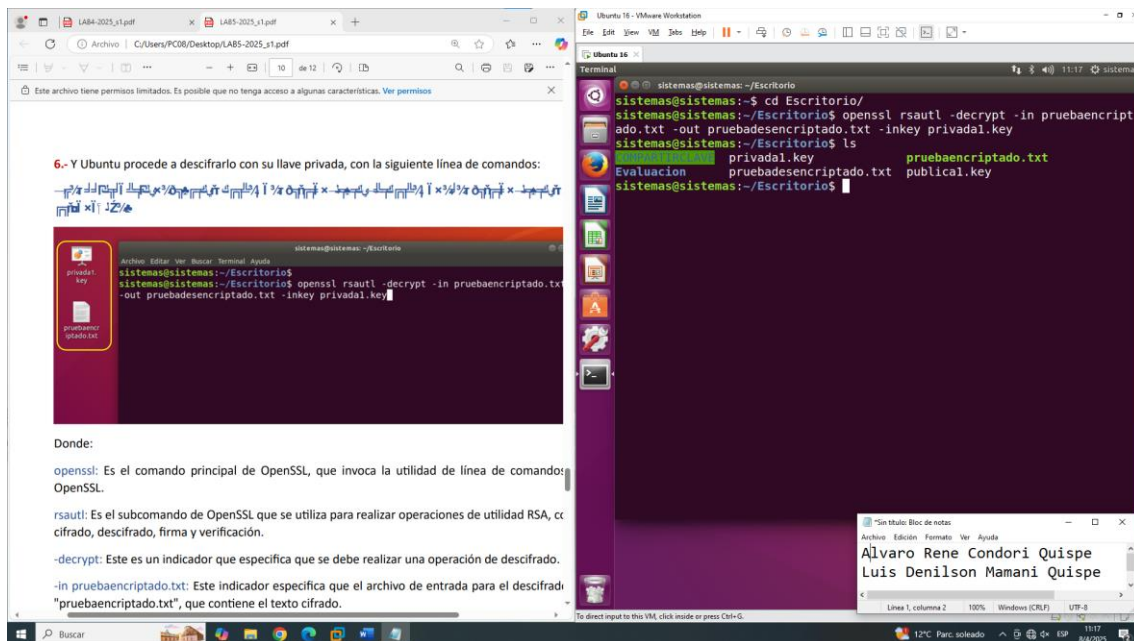
6.

6.- Y Ubuntu procede a descifrarlo con su llave privada, con la siguiente línea de comandos:

```
openssl rsautl -decrypt -in pruebaencrptado.txt -out prueba-descriptado.txt -inkey privada1.key
```

Donde:

- openssl: Es el comando principal de OpenSSL, que invoca la utilidad de línea de comandos OpenSSL.
- rsautl: Es el subcomando de OpenSSL que se utiliza para realizar operaciones de utilidad RSA, cifrado, descifrado, firma y verificación.
- decrypt: Este es un indicador que especifica que se debe realizar una operación de descifrado.
- in pruebaencrptado.txt: Este indicador especifica que el archivo de entrada para el descifrado "pruebaencrptado.txt", que contiene el texto cifrado.



7.

Ingeniería de Sistemas – Seguridad de Sistemas

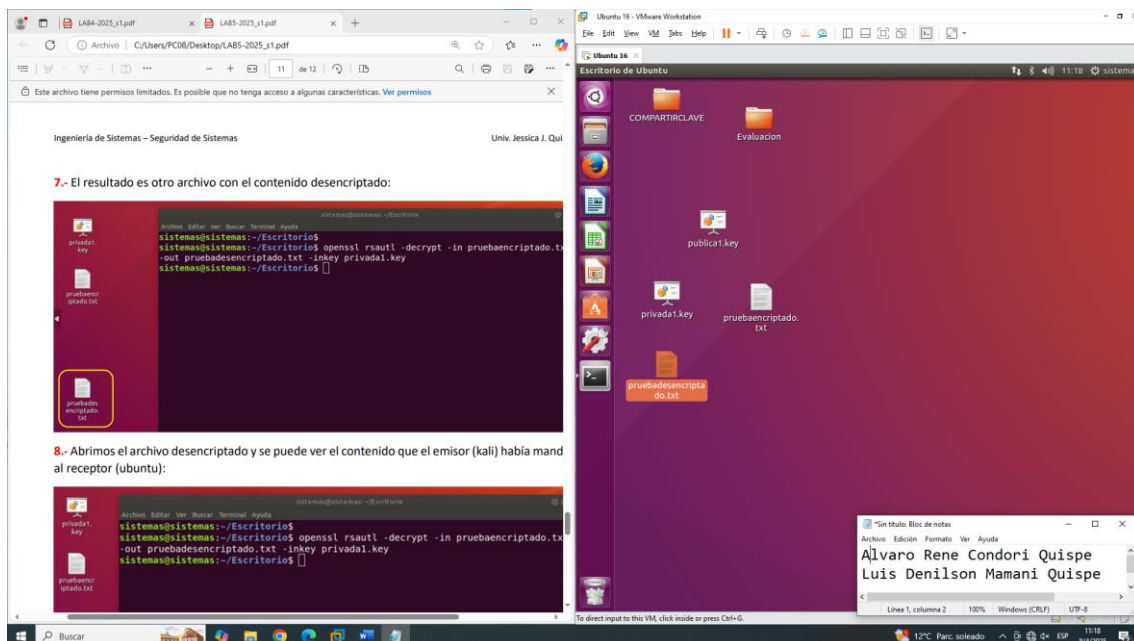
Univ. Jessica J. Qui

7.- El resultado es otro archivo con el contenido descifrado:

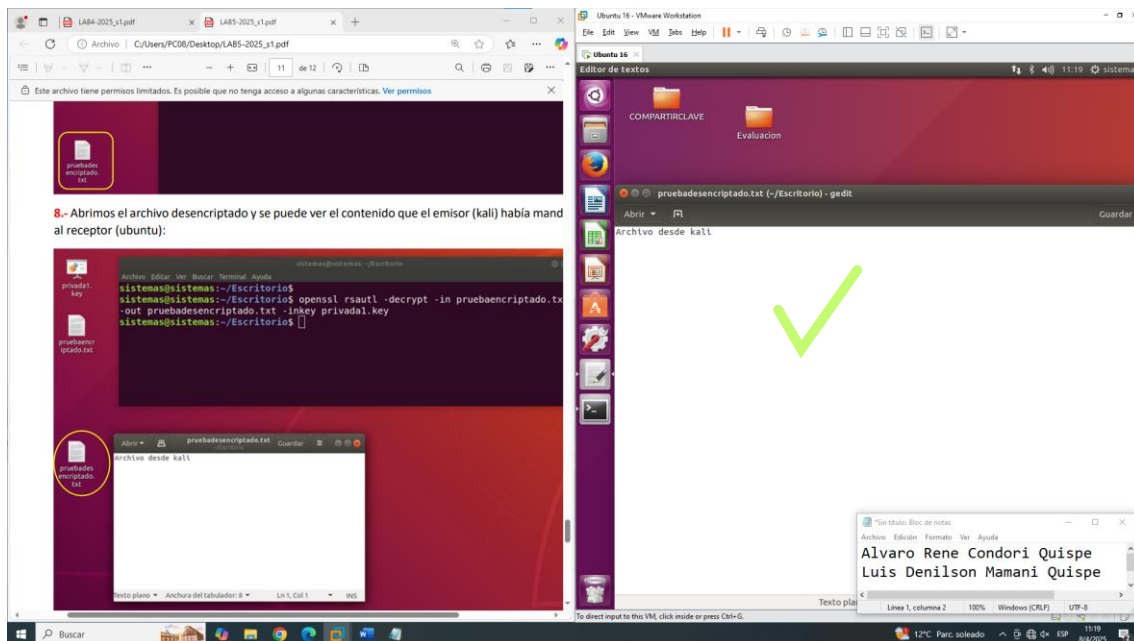
```
openssl rsautl -decrypt -in pruebaencrptado.txt -out prueba-descriptado.txt -inkey privada1.key
```

8.- Abrimos el archivo descifrado y se puede ver el contenido que el emisor (kali) había mandado al receptor (ubuntu):

```
openssl rsautl -decrypt -in pruebaencrptado.txt -out prueba-descriptado.txt -inkey privada1.key
```



8.



Evaluacion

