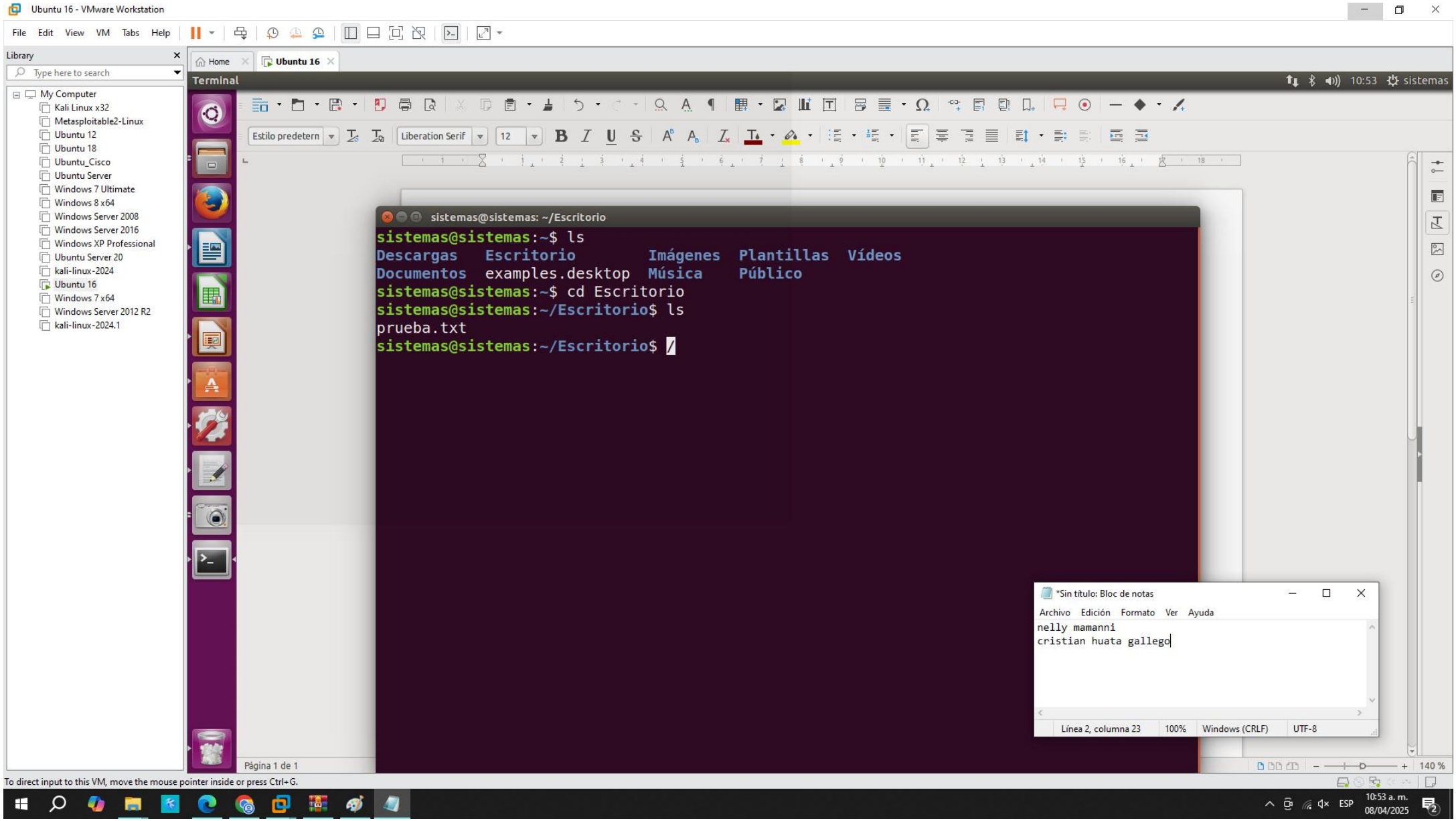

Ubuntu 16 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux x32
Metasploitable2-Linux
Ubuntu 12
Ubuntu 18
Ubuntu_Cisco
Ubuntu Server
Windows 7 Ultimate
Windows 8 x64
Windows Server 2008
Windows Server 2016
Windows XP Professional
Ubuntu Server 20
kali-linux-2024
Ubuntu 16
Windows 7 x64
Windows Server 2012 R2
kali-linux-2024.1
Home
Ubuntu 16
Terminal
10:53
sistemas
Estilo predetern
Liberation Serif
12
sistemas@sistemas: ~/Escritorio
sistemas@sistemas:~$ ls
Descargas Escritorio Imágenes Plantillas Vídeos
Documentos examples.desktop Música Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$
*Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda
nelly mamanni
cristian huata gallego
Línea 2, columna 23
100%
Windows (CRLF)
UTF-8
Página 1 de 1
140 %
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ESP
10:53 a. m.
08/04/2025

Ubuntu 16 - VMware Workstation

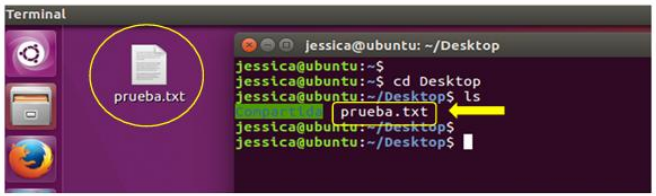
```
sistemas@sistemas:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
```

*Sin título: Bloc de notas

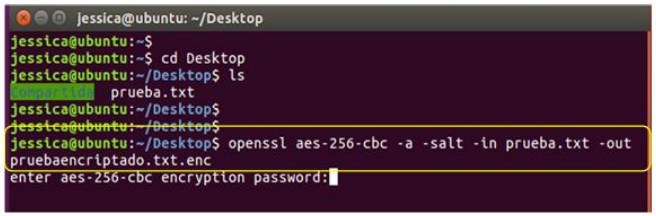
```
nelly mamanni
cristian huata gallego
```

LAB4-2025_s1.pdf

Ingeniería de Sistemas – Seguridad de Sistemas — Univ. Jessica J. Quispe V



3.- Una vez ubicado procedemos a encriptar el mensaje con el siguiente comando:



Nos pedirá una contraseña, ponemos una contraseña la misma que utilizaremos para desencriptar el archivo encriptado que se genere.

Donde:

openssl: Es el comando principal de OpenSSL, utilizado para realizar diversas operaciones criptográficas.

Ubuntu 16 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Kali Linux x32
- Metasploitable2-Linux
- Ubuntu 12
- Ubuntu 18
- Ubuntu_Cisco
- Ubuntu Server
- Windows 7 Ultimate
- Windows 8 x64
- Windows Server 2008
- Windows Server 2016
- Windows XP Professional
- Ubuntu Server 20
- kali-linux-2024
- Ubuntu 16
- Windows 7 x64
- Windows Server 2012 R2
- kali-linux-2024.1

Home | Ubuntu 16

sistemas@sistemas: ~/Escritorio — 11:00 sistemas

```
sistemas@sistemas:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

*Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
nelly mamanni
cristian huata gallego
```

Línea 2, columna 23 | 100% | Windows (CRLF) | UTF-8

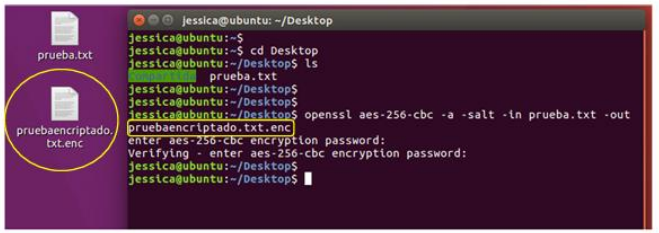
LAB4-2025_s1.pdf | Novedades de Microsoft Edge

Archivo | 192.168.55.254/lab/LAB4-2025_s1.pdf

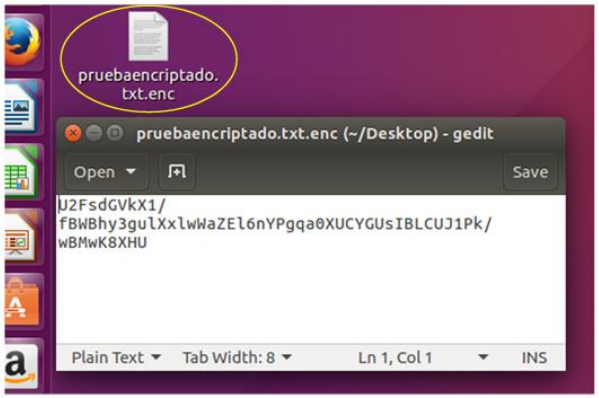
3 de 5

e permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

4.- Y al concluir nos generará un nuevo archivo encriptado:



Se puede ver que el contenido se cifró en el nuevo archivo:



3.- Ahora se desencriptará el archivo con el contenido encriptado con el siguiente comando:

Ponemos la misma contraseña con la cual se cifró el archivo y nos genera un nuevo archivo con el contenido desencriptado.

Ubuntu 16 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Kali Linux x32
- Metasploitable2-Linux
- Ubuntu 12
- Ubuntu 18
- Ubuntu_Cisco
- Ubuntu Server
- Windows 7 Ultimate
- Windows 8 x64
- Windows Server 2008
- Windows Server 2016
- Windows XP Professional
- Ubuntu Server 20
- kali-linux-2024
- Ubuntu 16
- Windows 7 x64
- Windows Server 2012 R2
- kali-linux-2024.1

Home | Ubuntu 16

sistemas@sistemas: ~/Escritorio — 11:00 sistemas

```
sistemas@sistemas:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

*Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
nelly mamanni
cristian huata gallego
```

Línea 2, columna 23 | 100% | Windows (CRLF) | UTF-8

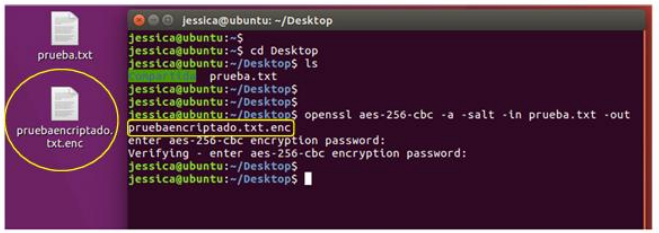
LAB4-2025_s1.pdf | Novedades de Microsoft Edge

Archivo | 192.168.55.254/lab/LAB4-2025_s1.pdf

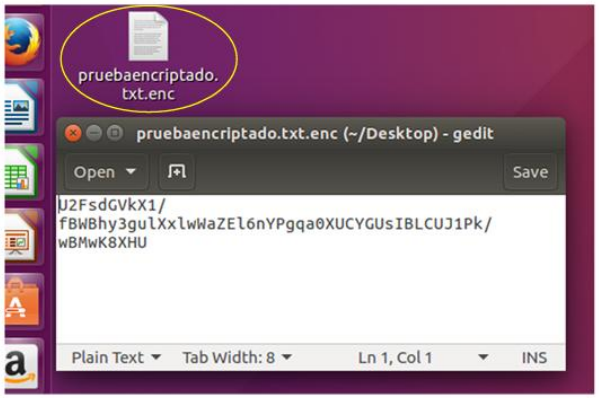
3 de 5

e permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

4.- Y al concluir nos generará un nuevo archivo encriptado:

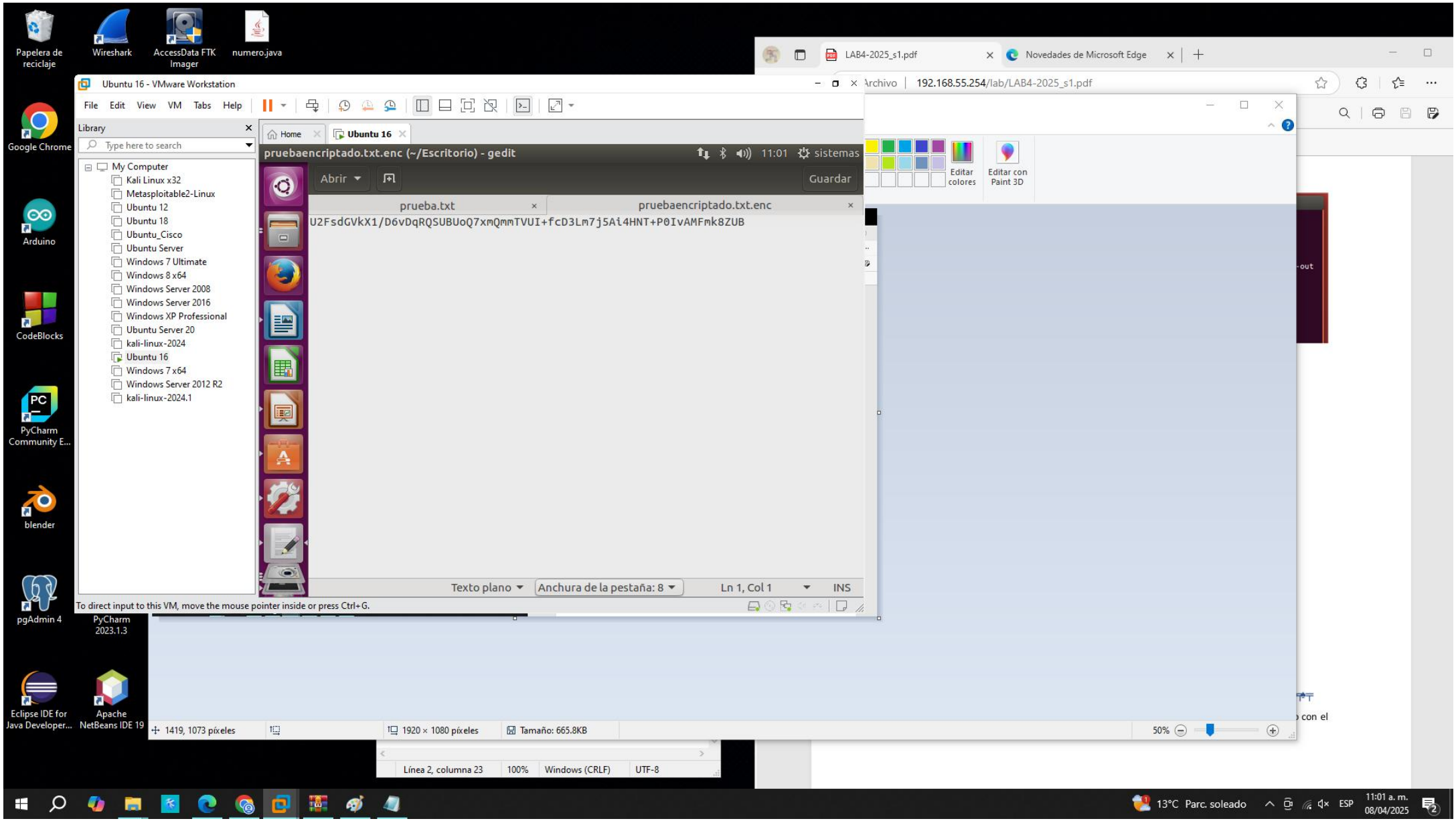


Se puede ver que el contenido se cifró en el nuevo archivo:



3.- Ahora se desencriptará el archivo con el contenido encriptado con el siguiente comando:

Ponemos la misma contraseña con la cual se cifró el archivo y nos genera un nuevo archivo con el contenido desencriptado.


Papelera de reciclaje
Wireshark
AccessData FTK Imager
numero.java
Google Chrome
Arduino
CodeBlocks
PyCharm Community E...
blender
pgAdmin 4
PyCharm 2023.1.3
Eclipse IDE for Java Developer...
Apache NetBeans IDE 19
Ubuntu 16 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux x32
Metasploitable2-Linux
Ubuntu 12
Ubuntu 18
Ubuntu_Cisco
Ubuntu Server
Windows 7 Ultimate
Windows 8 x64
Windows Server 2008
Windows Server 2016
Windows XP Professional
Ubuntu Server 20
kali-linux-2024
Ubuntu 16
Windows 7 x64
Windows Server 2012 R2
kali-linux-2024.1
Home
Ubuntu 16
pruebaencriptado.txt.enc (~/Escritorio) - gedit
11:01
sistemas
Abrir
Guardar
prueba.txt
pruebaencriptado.txt.enc
U2FsdGVkX1/D6vDqRQSUBUoQ7xmQmmTVUI+fcD3Lm7j5Ai4HNT+P0IvAMFmk8ZUB
Texto plano
Anchura de la pestaña: 8
Ln 1, Col 1
INS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
LAB4-2025_s1.pdf
Novedades de Microsoft Edge
Archivo
192.168.55.254/lab/LAB4-2025_s1.pdf
Editar colores
Editar con Paint 3D
1419, 1073 píxeles
1920 × 1080 píxeles
Tamaño: 665.8KB
50%
Línea 2, columna 23
100%
Windows (CRLF)
UTF-8
13°C Parc. soleado
ESP
11:01 a. m.
08/04/2025

```
sistemas@sistemas:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -d -a -i
n pruebaencriptado.txt.enc -out pruebadesencriptado.txt
enter aes-256-cbc decryption password:
sistemas@sistemas:~/Escritorio$
```

```
nelly mamanni
cristian huata gallego
```

Donde:

openssl: Es el comando principal de OpenSSL, utilizado para realizar div operaciones criptográficas.

aes-256-cbc: Especifica el algoritmo de cifrado que se utilizó previamente para encriptar el archivo. En este caso, AES con una clave de 256 bits en modo CBC (Cipher Block Chaining).

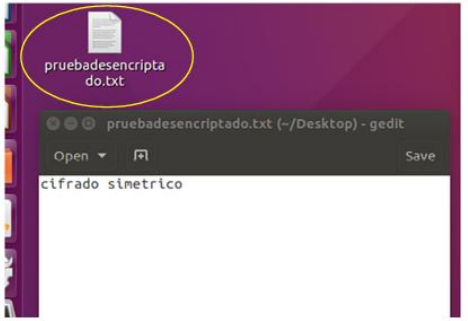
-d: Esta opción indica que OpenSSL debe realizar la operación de descifrado en lugar de cifrado.

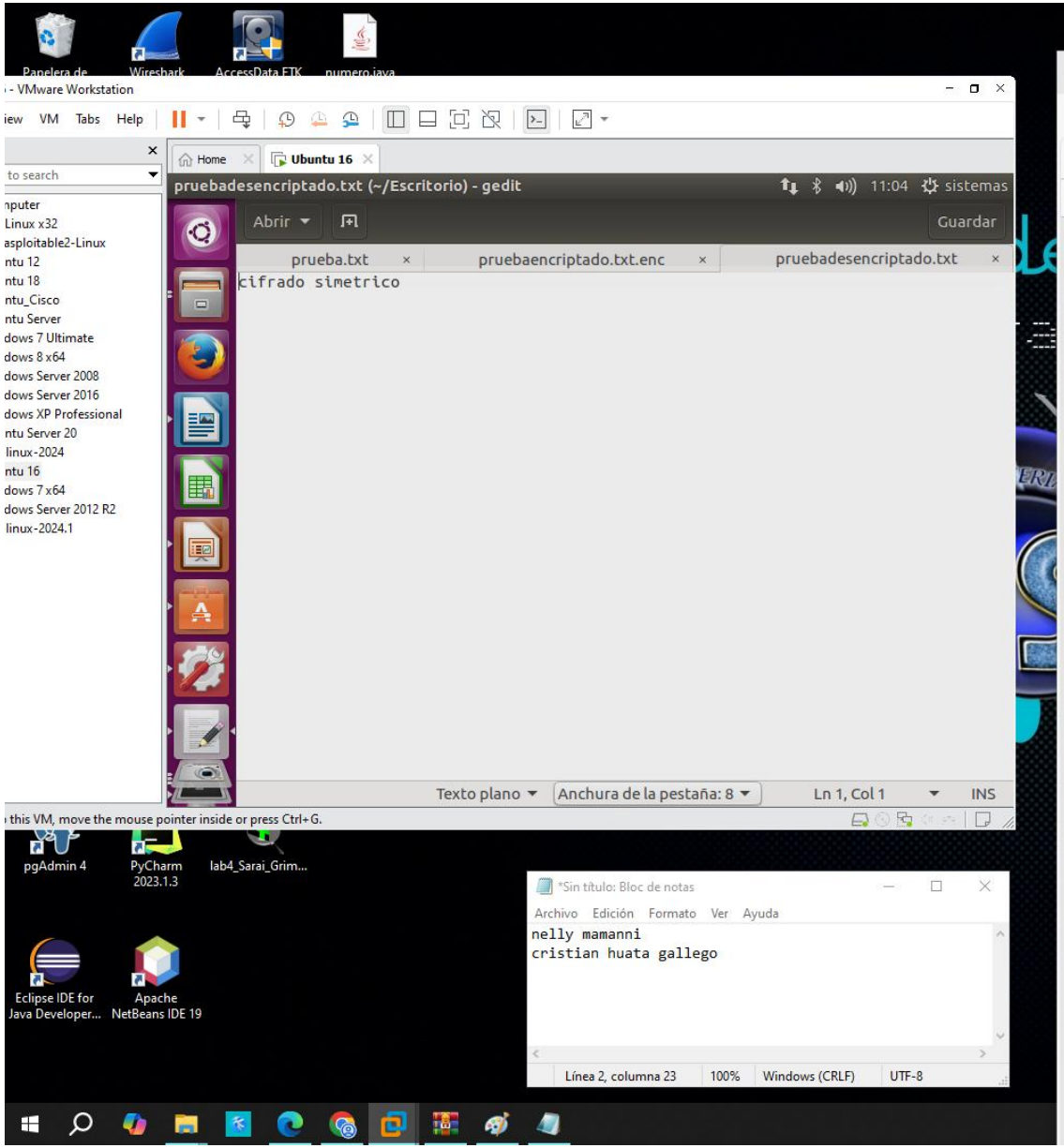
-a: Esta opción indica que el texto cifrado se codifica utilizando codificación de base64, por lo que OpenSSL debe decodificarlo antes de realizar el descifrado.

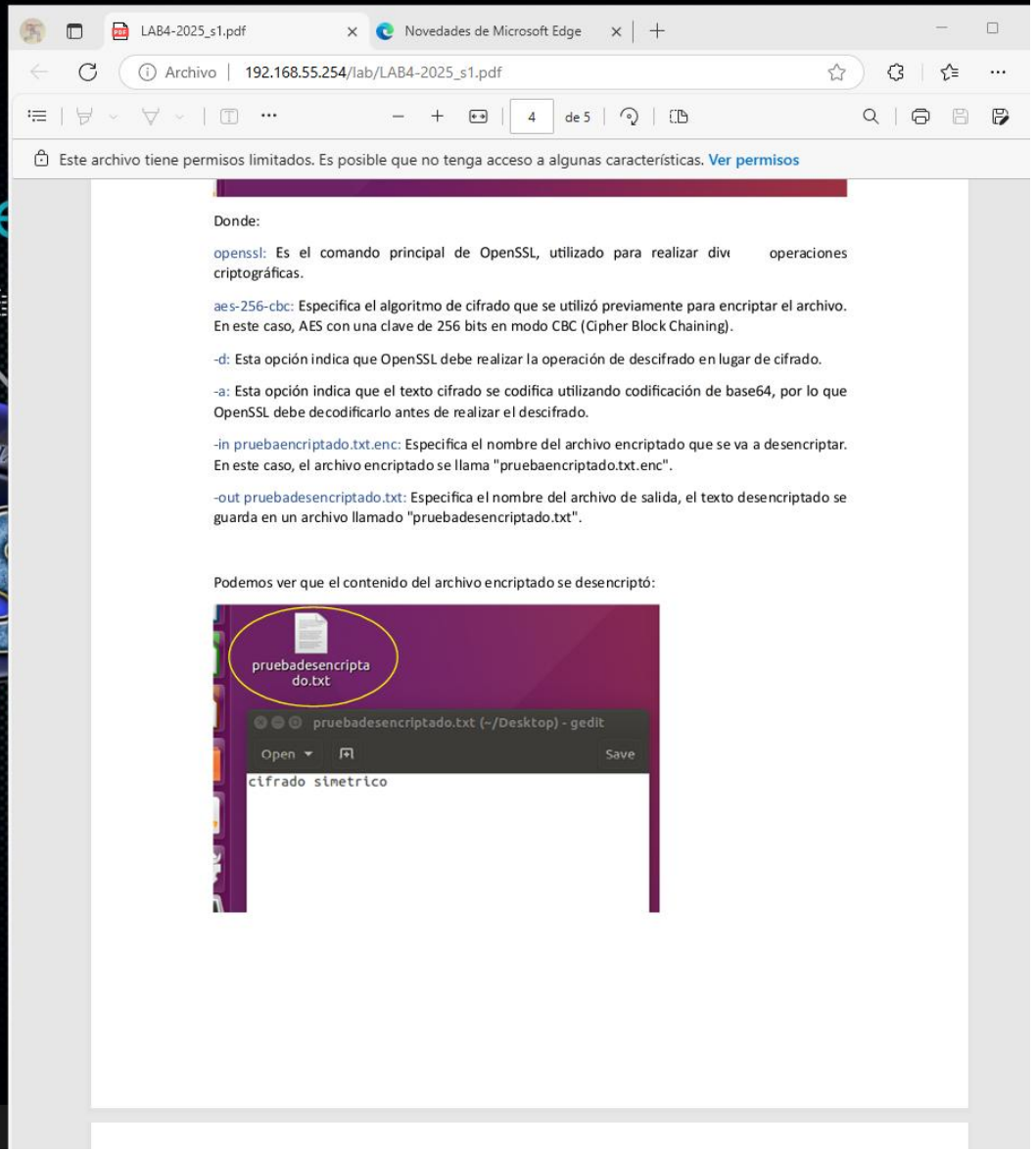
-in pruebaencriptado.txt.enc: Especifica el nombre del archivo encriptado que se va a desencriptar. En este caso, el archivo encriptado se llama "pruebaencriptado.txt.enc".

-out pruebadesencriptado.txt: Especifica el nombre del archivo de salida, el texto desencriptado se guarda en un archivo llamado "pruebadesencriptado.txt".

Podemos ver que el contenido del archivo encriptado se desencriptó:







Donde:

openssl: Es el comando principal de OpenSSL, utilizado para realizar div operaciones criptográficas.

aes-256-cbc: Especifica el algoritmo de cifrado que se utilizó previamente para encriptar el archivo. En este caso, AES con una clave de 256 bits en modo CBC (Cipher Block Chaining).

-d: Esta opción indica que OpenSSL debe realizar la operación de descifrado en lugar de cifrado.

-a: Esta opción indica que el texto cifrado se codifica utilizando codificación de base64, por lo que OpenSSL debe decodificarlo antes de realizar el descifrado.

-in pruebaencriptado.txt.enc: Especifica el nombre del archivo encriptado que se va a desencriptar. En este caso, el archivo encriptado se llama "pruebaencriptado.txt.enc".

-out pruebadesencriptado.txt: Especifica el nombre del archivo de salida, el texto desencriptado se guarda en un archivo llamado "pruebadesencriptado.txt".

Podemos ver que el contenido del archivo encriptado se desencriptó:

- VMware Workstation

iew VM Tabs Help

Home | Ubuntu 16

sistemas@sistemas: ~/Escritorio 11:07 sistemas

```
sistemas@sistemas:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt
 -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -d -a -i
n pruebaencriptado.txt.enc -out pruebadesencriptado.txt
enter aes-256-cbc decryption password:
sistemas@sistemas:~/Escritorio$ ls
nely.txt                pruebaencriptado.txt.enc
pruebadesencriptado.txt  prueba.txt
sistemas@sistemas:~/Escritorio$
```

this VM, move the mouse pointer inside or press Ctrl+G.

*Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
nelly mamanni
cristian huata gallego
```

Línea 2, columna 23 | 100% | Windows (CRLF) | UTF-8

LAB4-2025_s1.pdf | Novedades de Microsoft Edge

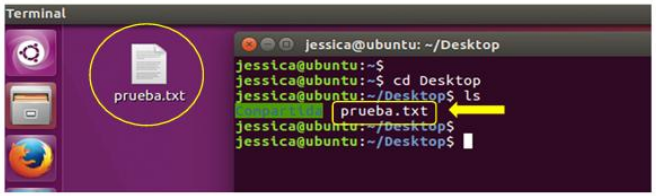
Archivo | 192.168.55.254/lab/LAB4-2025_s1.pdf

2 de 5

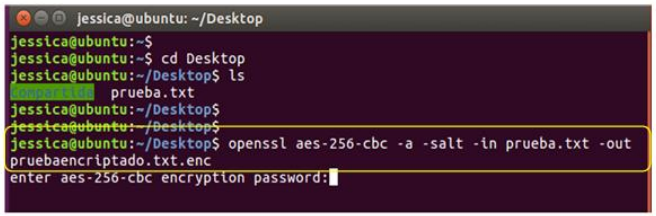
Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

2.- Una vez se halla creado el archivo, procedemos a utilizar un algoritmo de cifrado en este caso el primero que se va a utilizar es el algoritmo AES que es para cifrado simétrico.

En la terminal de comandos nos ubicamos donde tenemos nuestro archivo.

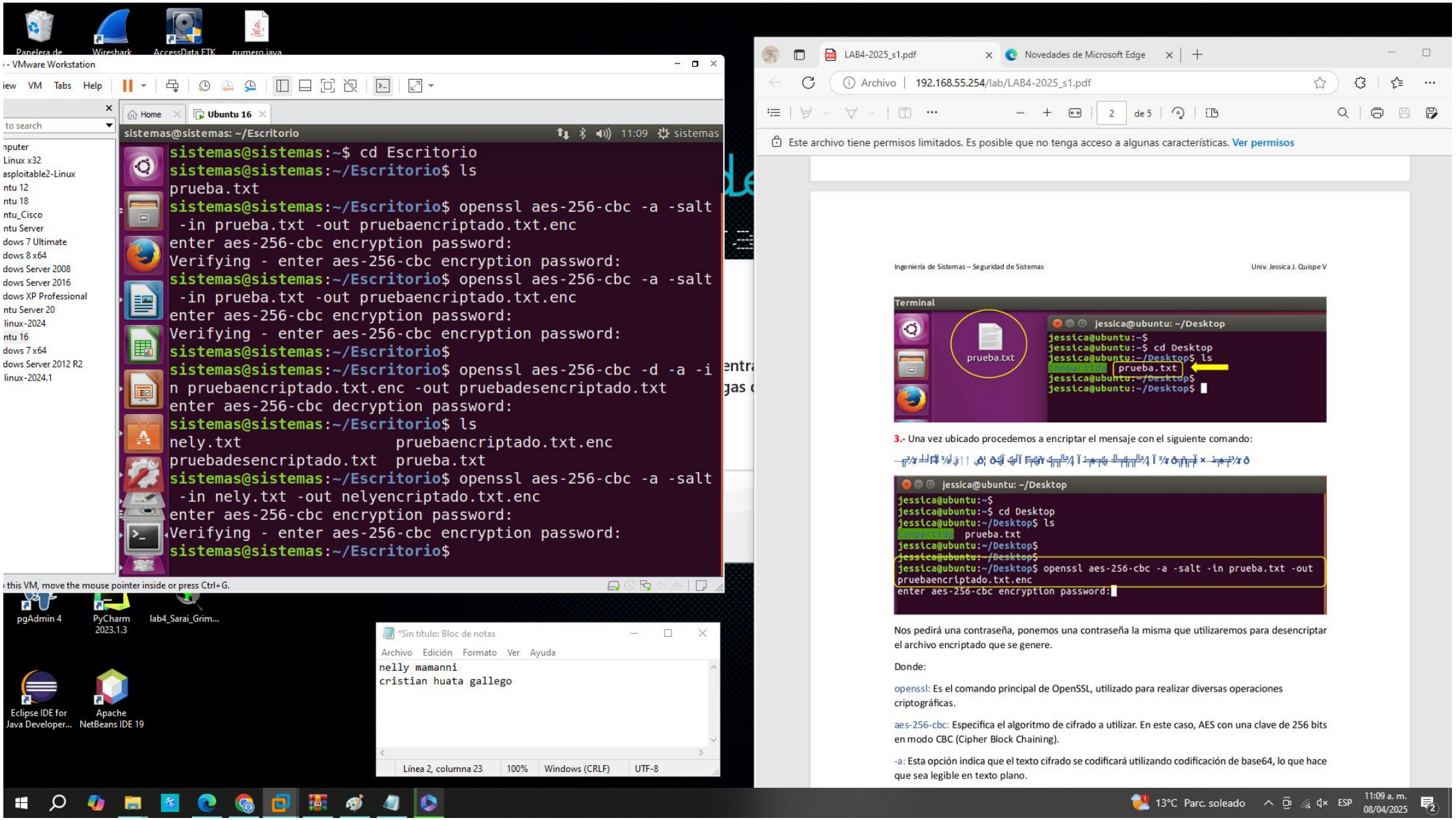


3.- Una vez ubicado procedemos a encriptar el mensaje con el siguiente comando:



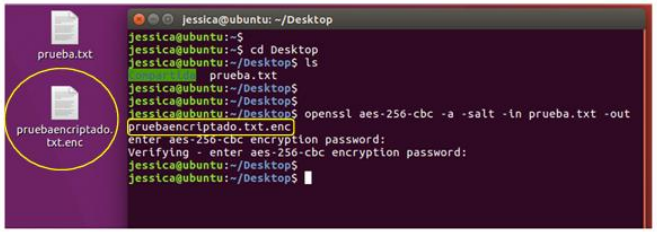
Nos pedirá una contraseña, ponemos una contraseña la misma que utilizaremos para desencriptar

13°C Parc. soleado ESP 11:07 a. m. 08/04/2025

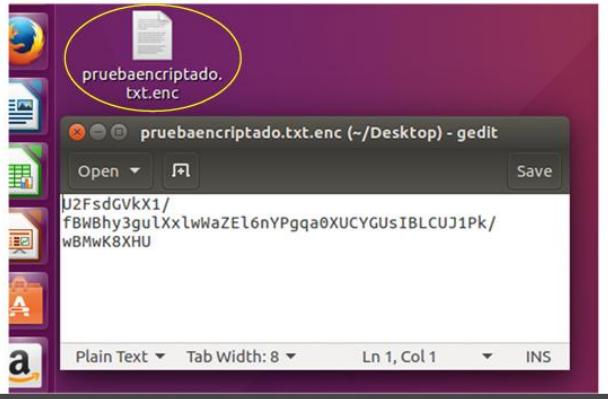

- VMware Workstation
Ubuntu 16
sistemas@sistemas: ~/Escritorio
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ ls
prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -d -a -in pruebaencriptado.txt.enc -out pruebadesencriptado.txt
enter aes-256-cbc decryption password:
sistemas@sistemas:~/Escritorio$ ls
nely.txt pruebaencriptado.txt.enc
pruebadesencriptado.txt prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt -in nely.txt -out nelyencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$
*Sin título: Bloc de notas
nelly mamanni
cristian huata gallego
LAB4-2025_s1.pdf
Novedades de Microsoft Edge
192.168.55.254/lab/LAB4-2025_s1.pdf
Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos
Ingeniería de Sistemas – Seguridad de Sistemas
Univ. Jessica J. Quispe V
Terminal
prueba.txt
jessica@ubuntu: ~/Desktop
jessica@ubuntu:~$ cd Desktop
jessica@ubuntu:~/Desktop$ ls
prueba.txt
3.- Una vez ubicado procedemos a encriptar el mensaje con el siguiente comando:
jessica@ubuntu:~/Desktop$ openssl aes-256-cbc -a -salt -in prueba.txt -out pruebaencriptado.txt.enc
enter aes-256-cbc encryption password:
Nos pedirá una contraseña, ponemos una contraseña la misma que utilizaremos para desencriptar el archivo encriptado que se genere.
Donde:
openssl: Es el comando principal de OpenSSL, utilizado para realizar diversas operaciones criptográficas.
aes-256-cbc: Especifica el algoritmo de cifrado a utilizar. En este caso, AES con una clave de 256 bits en modo CBC (Cipher Block Chaining).
-a: Esta opción indica que el texto cifrado se codificará utilizando codificación de base64, lo que hace que sea legible en texto plano.

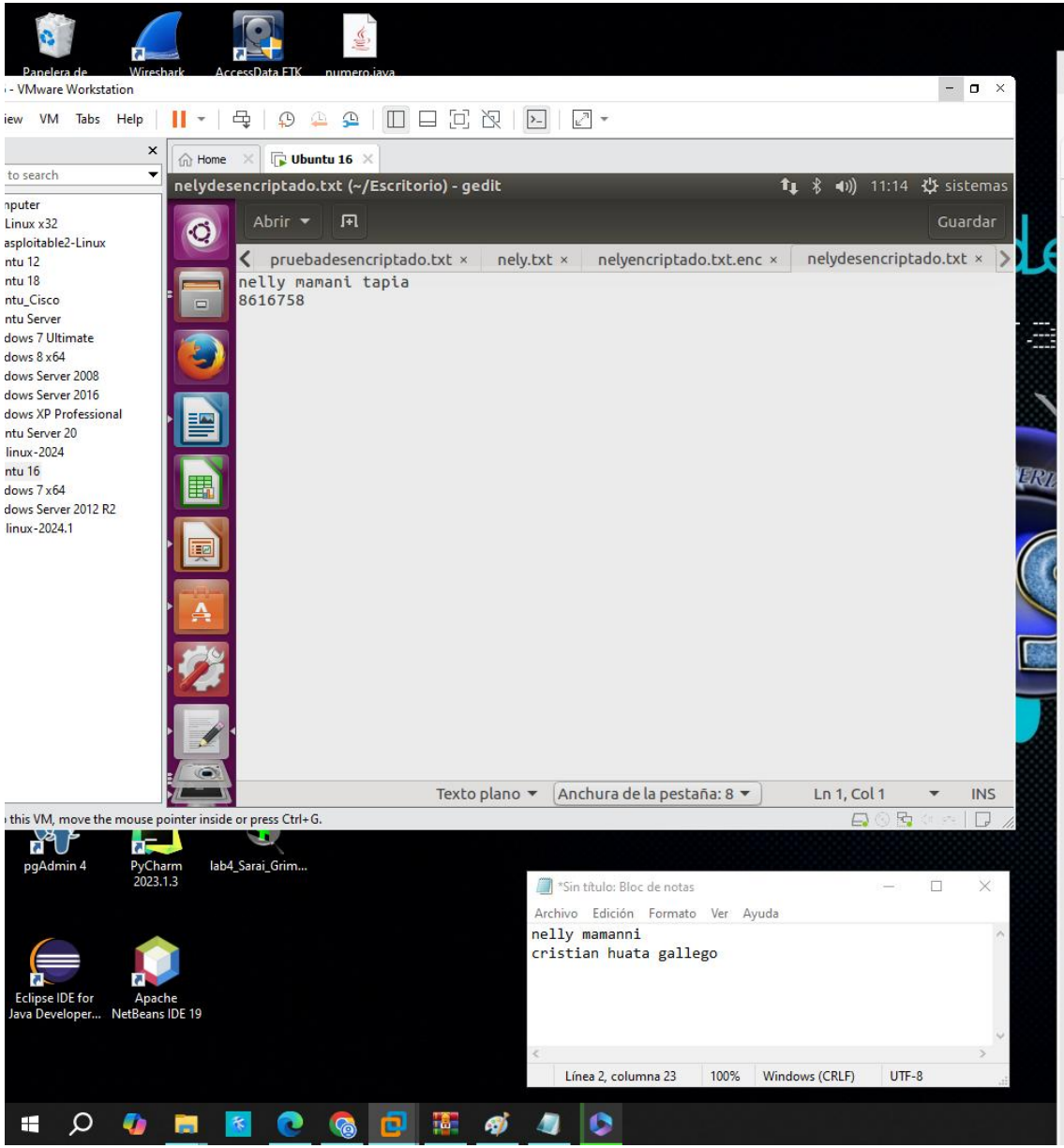
Ingeniería de Sistemas – Seguridad de Sistemas Univ. Jessica J. Quispe V

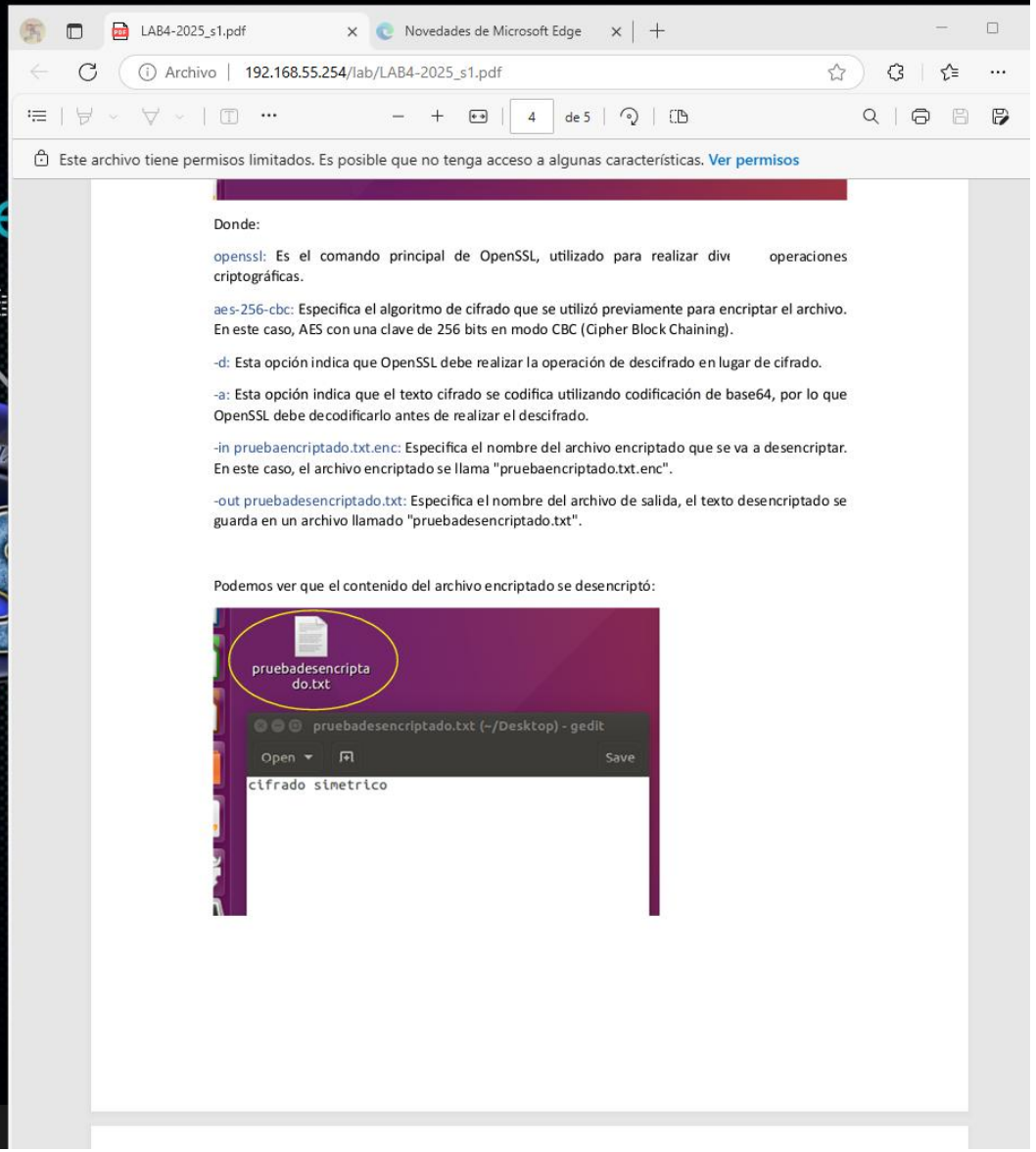
4.- Y al concluir nos generará un nuevo archivo encriptado:



Se puede ver que el contenido se cifró en el nuevo archivo:







Donde:

openssl: Es el comando principal de OpenSSL, utilizado para realizar div operaciones criptográficas.

aes-256-cbc: Especifica el algoritmo de cifrado que se utilizó previamente para encriptar el archivo. En este caso, AES con una clave de 256 bits en modo CBC (Cipher Block Chaining).

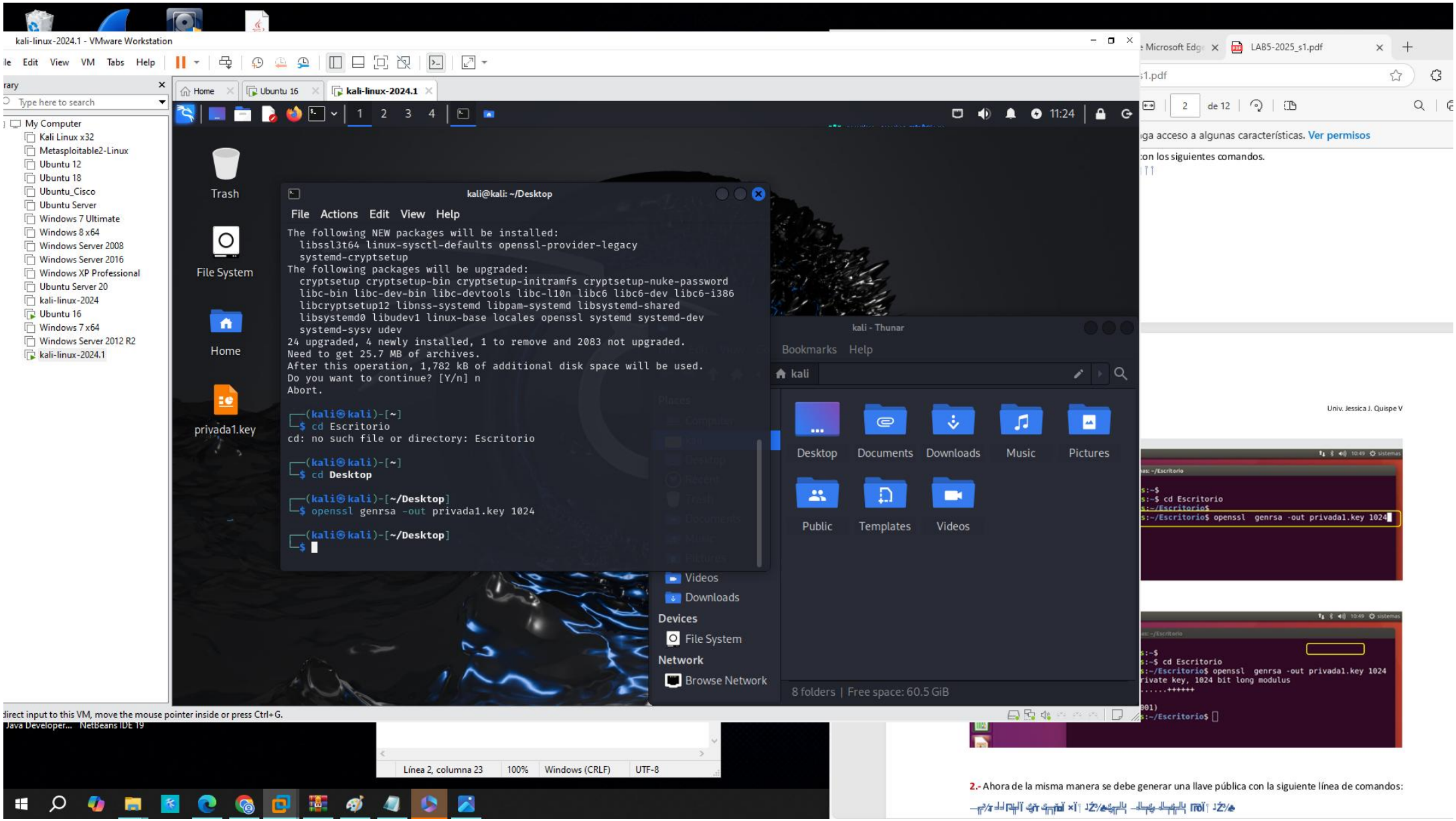
-d: Esta opción indica que OpenSSL debe realizar la operación de descifrado en lugar de cifrado.

-a: Esta opción indica que el texto cifrado se codifica utilizando codificación de base64, por lo que OpenSSL debe decodificarlo antes de realizar el descifrado.

-in pruebaencriptado.txt.enc: Especifica el nombre del archivo encriptado que se va a desencriptar. En este caso, el archivo encriptado se llama "pruebaencriptado.txt.enc".

-out pruebadesencriptado.txt: Especifica el nombre del archivo de salida, el texto desencriptado se guarda en un archivo llamado "pruebadesencriptado.txt".

Podemos ver que el contenido del archivo encriptado se desencriptó:


kali-linux-2024.1 - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 16
kali-linux-2024.1
My Computer
Kali Linux x32
Metasploitable2-Linux
Ubuntu 12
Ubuntu 18
Ubuntu_Cisco
Ubuntu Server
Windows 7 Ultimate
Windows 8 x64
Windows Server 2008
Windows Server 2016
Windows XP Professional
Ubuntu Server 20
kali-linux-2024
Ubuntu 16
Windows 7 x64
Windows Server 2012 R2
kali-linux-2024.1
Trash
File System
Home
privada1.key
kali@kali: ~/Desktop
File Actions Edit View Help
The following NEW packages will be installed:
libssl3t64 linux-sysctl-defaults openssl-provider-legacy
systemd-cryptsetup
The following packages will be upgraded:
cryptsetup cryptsetup-bin cryptsetup-initramfs cryptsetup-nuke-password
libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386
libcryptsetup12 libnss-systemd libpam-systemd libsystemd-shared
libsystemd0 libudev1 linux-base locales openssl systemd systemd-dev
systemd-sysv udev
24 upgraded, 4 newly installed, 1 to remove and 2083 not upgraded.
Need to get 25.7 MB of archives.
After this operation, 1,782 kB of additional disk space will be used.
Do you want to continue? [Y/n] n
Abort.
(kali㉿kali)-[~]
$ cd Escritorio
cd: no such file or directory: Escritorio
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ openssl genrsa -out privada1.key 1024
(kali㉿kali)-[~/Desktop]
$
kali - Thunar
Bookmarks Help
kali
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
Devices
File System
Network
Browse Network
8 folders | Free space: 60.5 GiB
direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Línea 2, columna 23
100%
Windows (CRLF)
UTF-8
LAB5-2025_s1.pdf
de 12
Ver permisos
con los siguientes comandos.
Univ. Jessica J. Quispe V
2.- Ahora de la misma manera se debe generar una llave pública con la siguiente línea de comandos:

Ubuntu 16 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Kali Linux x32
- Metasploitable2-Linux
- Ubuntu 12
- Ubuntu 18
- Ubuntu_Cisco
- Ubuntu Server
- Windows 7 Ultimate
- Windows 8 x64
- Windows Server 2008
- Windows Server 2016
- Windows XP Professional
- Ubuntu Server 20
- kali-linux-2024
- Ubuntu 16
- Windows 7 x64
- Windows Server 2012 R2
- kali-linux-2024.1

Home | Ubuntu 16 | kali-linux-2024.1

Escritorio 11:36 sistemas

Carpeta personal > Escritorio

Recientes
Carpeta personal
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Papelera
Red
Equipo
Conectarse con un ...

nely.txt
nelydesencriptado.txt
nelyencriptado.txt.enc
privada1.key
prueba.txt
pruebadesencriptado.txt
pruebaencriptado.txt.enc

«nelydesencriptado.txt» seleccionado (27 bytes)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

pgAdmin 4
PyCharm 2023.1.3
lab4_Sarai_Grim...
Eclipse IDE for Java Developer...
Apache NetBeans IDE 19

*Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda

nelly mamanni
cristian huata gallego

Línea 2, columna 23 | 100% | Windows (CRLF) | UTF-8

LAB4-2025_s1.pdf | Novedades de Microsoft Edge | LAB5-2025_s1.pdf

Archivo | 192.168.55.254/lab/LAB5-2025_s1.pdf

2 de 12

tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

Ingeniería de Sistemas – Seguridad de Sistemas Univ. Jessica J. Quispe V

```
sistemas@sistemas:~$
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$
sistemas@sistemas:~/Escritorio$ openssl  genrsa -out privada1.key 1024
```

Y nos genera una clave privada:

```
sistemas@sistemas:~$
sistemas@sistemas:~$ cd Escritorio
sistemas@sistemas:~/Escritorio$ openssl  genrsa -out privada1.key 1024
Generating RSA private key, 1024 bit long modulus
.....................++++++
..++++++
e is 65537 (0x10001)
sistemas@sistemas:~/Escritorio$
```

2.- Ahora de la misma manera se debe generar una llave pública con la siguiente línea de comandos:

13°C Mayorm. soleado ESP 11:36 a. m. 08/04/2025

Descargas

Ubuntu 16 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer
- Kali Linux x32
- Metasploitable2-Linux
- Ubuntu 12
- Ubuntu 18
- Ubuntu_Cisco
- Ubuntu Server
- Windows 7 Ultimate
- Windows 8 x64
- Windows Server 2008
- Windows Server 2016
- Windows XP Professional
- Ubuntu Server 20
- kali-linux-2024
- Ubuntu 16
- Windows 7 x64
- Windows Server 2012 R2
- kali-linux-2024.1

Home | Ubuntu 16 | kali-linux-2024.1

Escritorio 11:38 sistemas

Carpeta personal | Escritorio

Recientes
Carpeta personal
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Papelera
Red
Equipo
Conectarse con un ...

nely.txt
nelydesencriptado.txt
nelyencriptado.txt.enc
privada1.key
prueba.txt
pruebadesencriptado.txt
pruebaencriptado.txt.enc
publica1.key

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Disco local (C:)
Disco local (D:)
Nuevo vol (E:)
Red

96 elementos

Eclipse IDE for Java Developer...
Apache NetBeans IDE 19

16 elementos

*Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda

nelly mamanni
cristian huata gallego

Línea 2, columna 23 | 100% | Windows (CRLF) | UTF-8

LAB4-2025_s1.pdf | Novedades de Microsoft Edge | LAB5-2025_s1.pdf

Archivo | 192.168.55.254/lab/LAB5-2025_s1.pdf

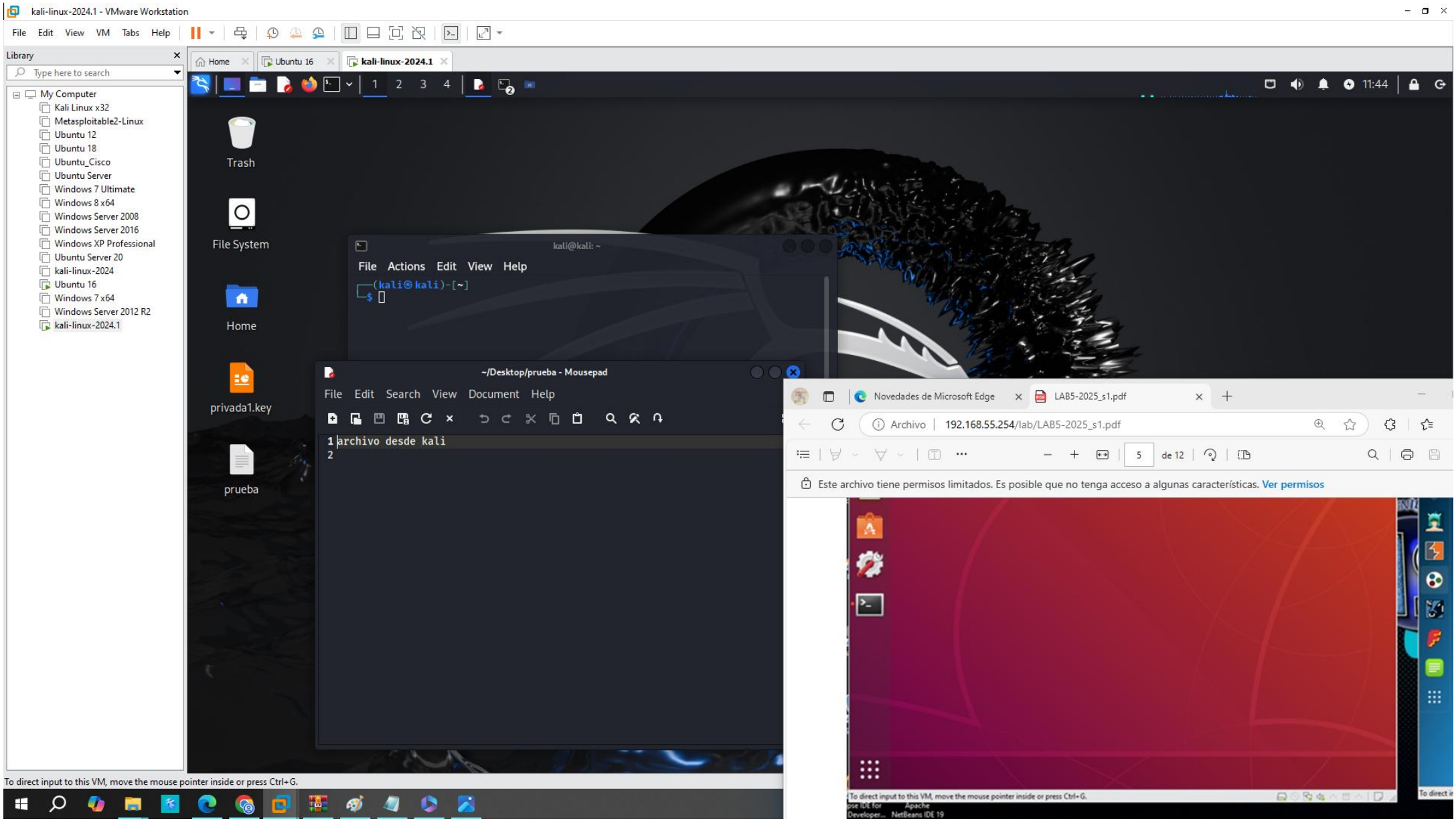
3 de 12

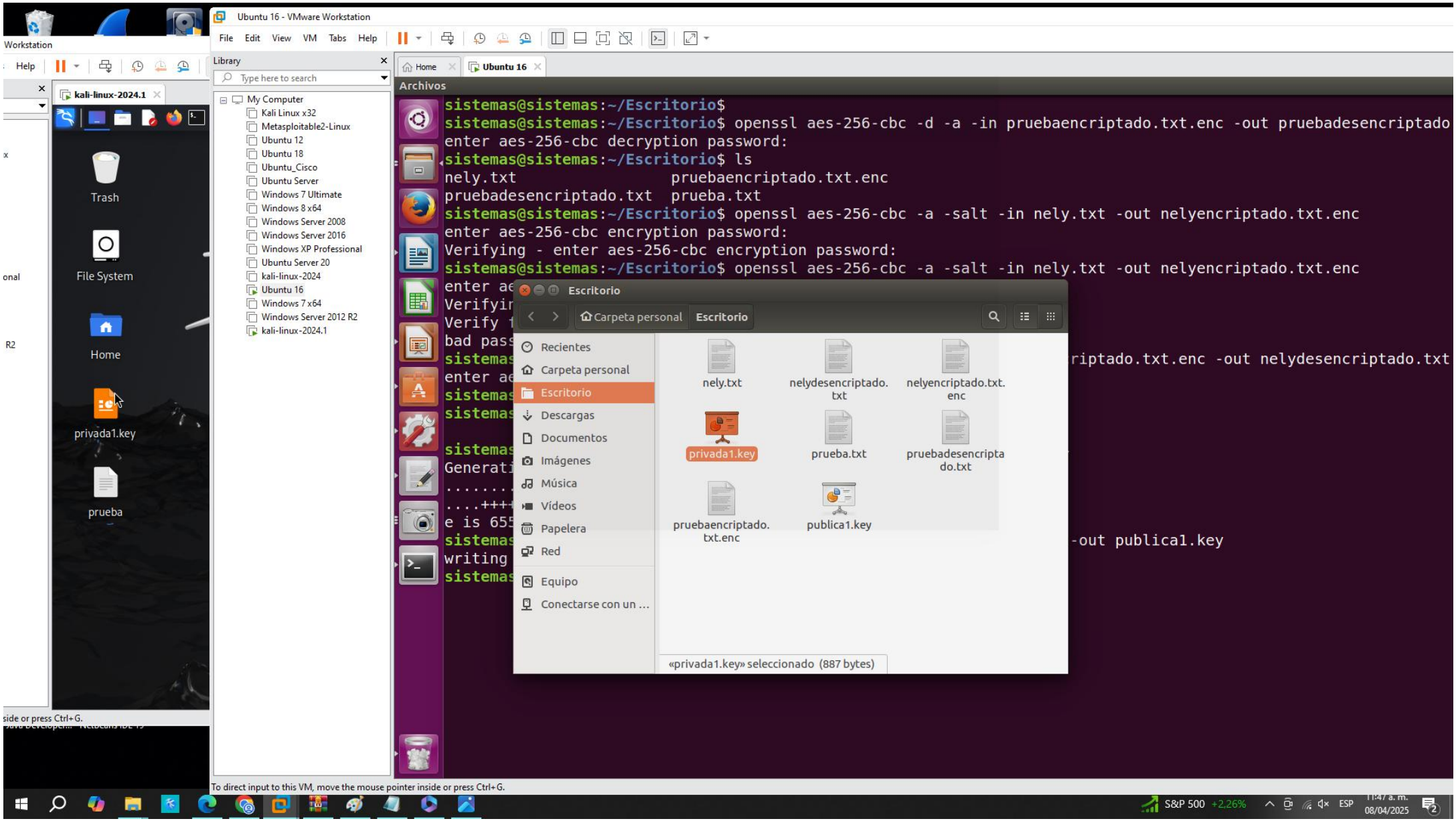
tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

Ubuntu (receptor) ahora tiene ambas claves, pública y privada:

El mecanismo de cifrado asimétrico consiste en que el emisor quiere enviar un archivo cifrado al

13°C Mayorm. soleado ESP 11:38 a. m. 08/04/2025


kali-linux-2024.1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux x32
Metasploitable2-Linux
Ubuntu 12
Ubuntu 18
Ubuntu_Cisco
Ubuntu Server
Windows 7 Ultimate
Windows 8 x64
Windows Server 2008
Windows Server 2016
Windows XP Professional
Ubuntu Server 20
kali-linux-2024
Ubuntu 16
Windows 7 x64
Windows Server 2012 R2
kali-linux-2024.1
Home
Ubuntu 16
kali-linux-2024.1
1 2 3 4
11:44
Trash
File System
Home
privada1.key
prueba
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$
~/Desktop/prueba - Mousepad
File Edit Search View Document Help
1 archivo desde kali
2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Novedades de Microsoft Edge
LAB5-2025_s1.pdf
Archivo | 192.168.55.254/lab/LAB5-2025_s1.pdf
5 de 12
Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Ubuntu 16 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux x32
Metasploitable2-Linux
Ubuntu 12
Ubuntu 18
Ubuntu_Cisco
Ubuntu Server
Windows 7 Ultimate
Windows 8 x64
Windows Server 2008
Windows Server 2016
Windows XP Professional
Ubuntu Server 20
kali-linux-2024
Ubuntu 16
Windows 7 x64
Windows Server 2012 R2
kali-linux-2024.1
Home
Ubuntu 16
Archivos
kali-linux-2024.1
Trash
File System
Home
privada1.key
prueba
sistemas@sistemas:~/Escritorio$
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -d -a -in pruebaencriptado.txt.enc -out pruebadesencriptado
enter aes-256-cbc decryption password:
sistemas@sistemas:~/Escritorio$ ls
nely.txt pruebaencriptado.txt.enc
pruebadesencriptado.txt prueba.txt
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt -in nely.txt -out nelyencriptado.txt.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
sistemas@sistemas:~/Escritorio$ openssl aes-256-cbc -a -salt -in nely.txt -out nelyencriptado.txt.enc
riptado.txt.enc -out nelydesencriptado.txt
-out publica1.key
Escritorio
Carpeta personal
Escritorio
Recientes
Carpeta personal
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Papelera
Red
Equipo
Conectarse con un ...
nely.txt
nelydesencriptado.txt
nelyencriptado.txt.enc
privada1.key
prueba.txt
pruebadesencriptado.txt
pruebaencriptado.txt.enc
publica1.key
«privada1.key» seleccionado (887 bytes)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
S&P 500 +2,26%
ESP
08/04/2025

Ubuntu 16 - VMware Workstation

File Edit View VM Tabs Help

Library

Home | Ubuntu 16

kali-linux-2024.1

1 2 3 4 11:56

Trash

File System

Home

privada1.key

prueba

root@kali: /home/kali

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# openssl rsautl -pubin -encrypt -in prueba.txt -out pruebaencriptado.txt -
inkey publica1.key
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
Could not open file or uri for loading private key of public key from publica
1.key: No such file or directory

┌──(root㉿kali)-[/home/kali]
└─# openssl rsautl -pubin -encrypt -in prueba.txt -out pruebaencriptado.txt -
inkey publica1.key
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
Could not open file or uri for loading private key of public key from publica
1.key: No such file or directory

┌──(root㉿kali)-[/home/kali]
└─# openssl pkeyutl -pubin -encrypt -in prueba.txt -out pruebaencriptado.txt
-inkey publica1.key
Could not open file or uri for loading private key of public key from publica
1.key: No such file or directory
pkeyutl: Error initializing context

┌──(root㉿kali)-[/home/kali]
└─#
```

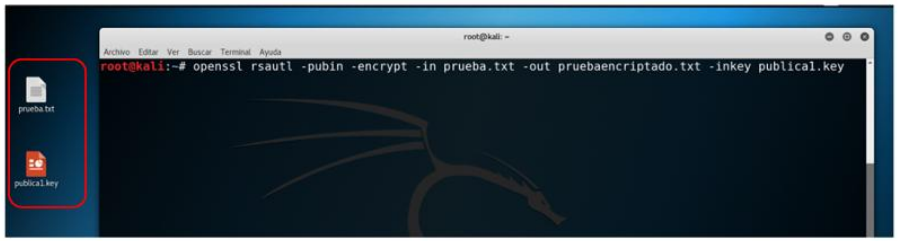
ter inside or press Ctrl+G.

Novedades de Microsoft Edge | LAB5-2025_s1.pdf

Archivo | 192.168.55.254/lab/LAB5-2025_s1.pdf

8 de 12

Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos



Donde:

openssl: Es el comando principal de OpenSSL, que invoca la utilidad de línea de comandos d OpenSSL.
rsautl: Es un subcomando de OpenSSL utilizado para realizar operaciones de utilidad RSA, como cifrado, descifrado, firma y verificación.
-pubin: Este es un indicador que le indica a OpenSSL que el archivo de clave proporcionado es una clave pública.
-encrypt: Este es un indicador que indica que se debe realizar una operación de cifrado.
-in prueba.txt: Este indicador especifica que el archivo de entrada para el cifrado es "prueba.txt".
-out pruebaencriptado.txt: Este indicador especifica que el archivo de salida para el texto cifrado se llamará "pruebaencriptado.txt".
-inkey publica1.key: Éste cifra el contenido del archivo "prueba.txt" utilizando la clave públic contenida en el archivo "publica1.key" y guarda el texto cifrado en un nuevo archivo llamado "pruebaencriptado.txt"

Y el resultado será un nuevo archivo encriptado: