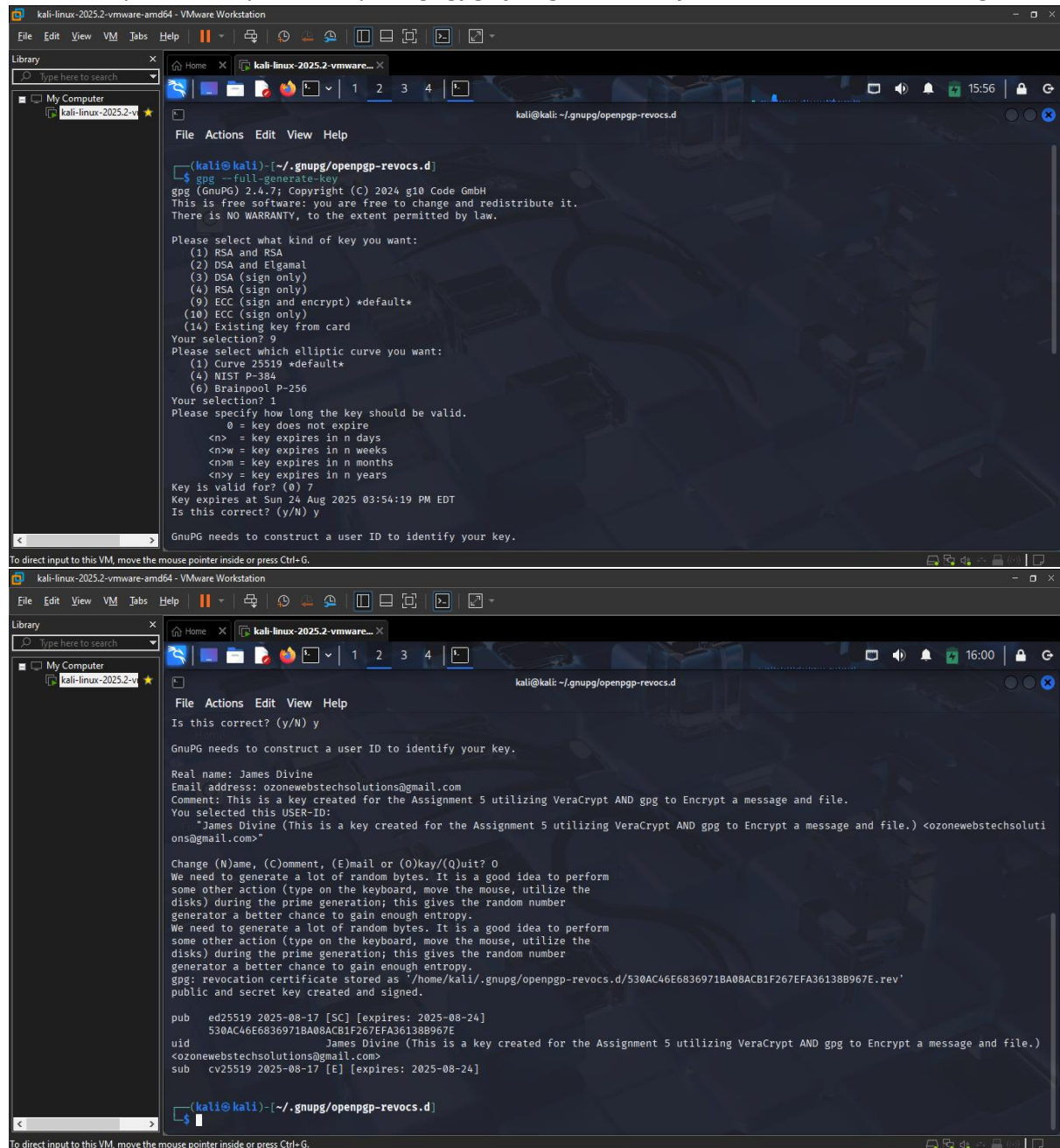


ASSIGNMENT 5
UTILIZING VERACRYPT AND GPG FOR ENCRYPTION OF FILES AND MESSAGES
BY
IJEI, CHUKWUMA FUMNANYA DIVINE JAMES
VeraCrypt Passkey: Starboy10.#

My Approach is to utilize GPG on Kali UI to encrypt a message using a public key and thereafter utilize VeraCrypt to encrypt the this file where I will be pasting the encrypted message hereby creating a kind of DOUBLE AUTHETICATION regarding the message I want to share with the recipient (which is the tutor) in this case.

The initial stage is the encryption stage utilizing GPG:

Successfully created my Public Key using ***“gpg --full-generate-key”*** and the default sub-settings.



```
(kali@kali)-[~/gnupg/openpgp-revocs.d]
$ gpg --full-generate-key
gpg (GnuPG) 2.4.7; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
(1) RSA and RSA
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (sign only)
(14) Existing key from card
Your selection? 9
Please select which elliptic curve you want:
(1) Curve 25519 *default*
(4) NIST P-384
(6) Brainpool P-256
Your selection? 1
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 7
Key expires at Sun 24 Aug 2025 03:54:19 PM EDT
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

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

(kali@kali)-[~/gnupg/openpgp-revocs.d]
$ gpg --full-generate-key
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: James Divine
Email address: ozonwebstechsolutions@gmail.com
Comment: This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.
You selected this USER-ID:
  "James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.) <ozonwebstechsolutions@gmail.com>"

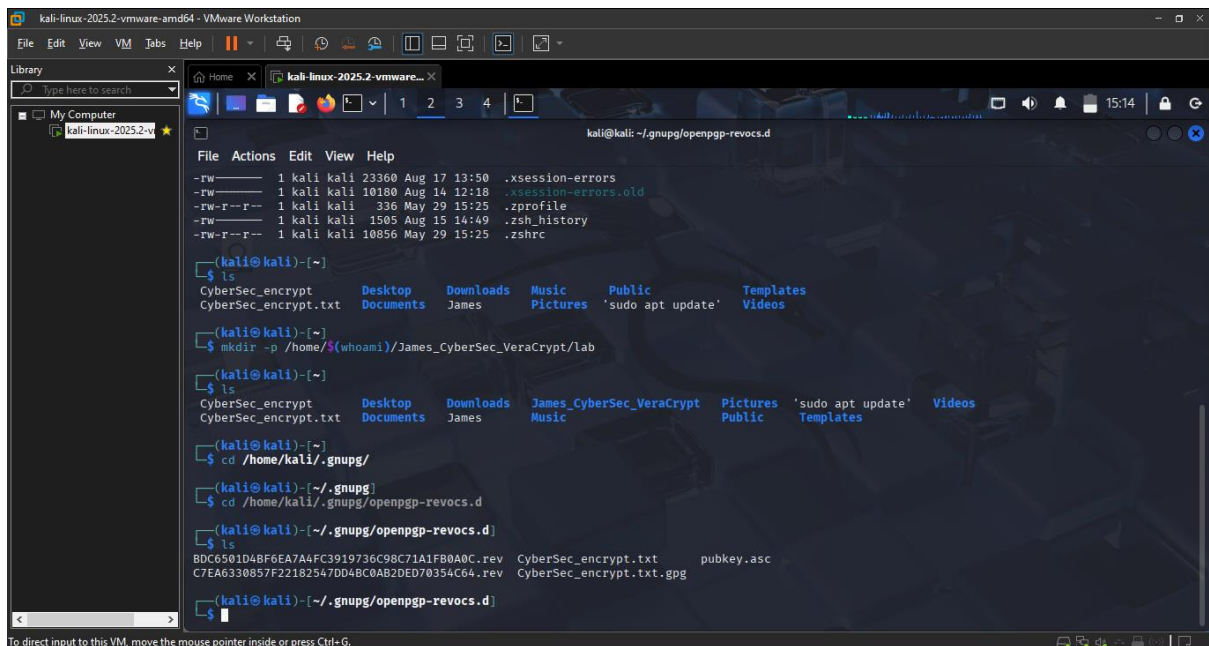
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/530AC46E68369718A08ACB1F267EFA36138B967E.rev'
public and secret key created and signed.

pub  ed25519 2025-08-17 [SC] [expires: 2025-08-24]
     530AC46E68369718A08ACB1F267EFA36138B967E
uid  James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.)
     <ozonwebstechsolutions@gmail.com>
sub  cv25519 2025-08-17 [E] [expires: 2025-08-24]

(kali@kali)-[~/gnupg/openpgp-revocs.d]
$
```

I have been able to successfully create new directory and also get the created public key from the “*openpgp-revocs.d*” folder inside the “*.gnupg*” folder.

Public Key: 530AC46E6836971BA08ACB1F267EFA36138B967E.rev



The screenshot shows a terminal window with the following commands and output:

```
kali@kali:~$ ls
CyberSec_encrypt
CyberSec_encrypt.txt

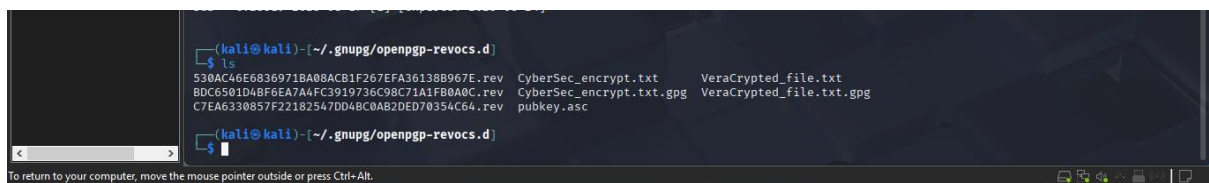
(kali@kali)~$ mkdir -p /home/$whoami/James_CyberSec_VeraCrypt/lab

(kali@kali)~$ ls
CyberSec_encrypt
CyberSec_encrypt.txt

(kali@kali)~$ cd /home/kali/.gnupg/

(kali@kali)~/.gnupg$ cd /home/kali/.gnupg/openpgp-revocs.d

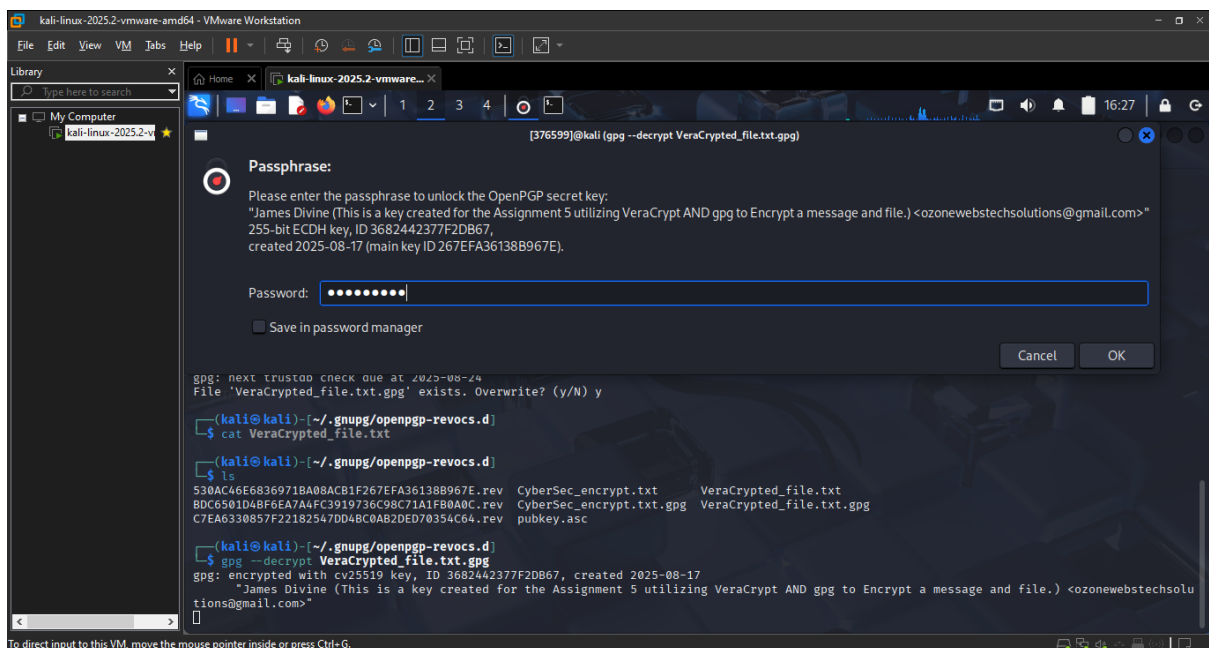
(kali@kali)~/.gnupg/openpgp-revocs.d$ ls
BDCE6501D48F6EA7A4FC3919736C98C71A1F80A0C.rev  CyberSec_encrypt.txt  pubkey.asc
C7EA6330857F22182547DD4BC0AB2DE070354C64.rev  CyberSec_encrypt.txt.gpg
```



The screenshot shows a terminal window with the following commands and output:

```
(kali@kali)~/.gnupg/openpgp-revocs.d$ ls
530AC46E6836971BA08ACB1F267EFA36138B967E.rev  CyberSec_encrypt.txt  VeraCrypt_file.txt
BDCE6501D48F6EA7A4FC3919736C98C71A1F80A0C.rev  CyberSec_encrypt.txt.gpg  VeraCrypt_file.txt.gpg
C7EA6330857F22182547DD4BC0AB2DE070354C64.rev  pubkey.asc
```

At this stage I am trying to perform the encryption of the message



The screenshot shows a terminal window with a passphrase prompt and the following commands and output:

```
[376599]@kali (gpg --decrypt VeraCrypt_file.txt.gpg)

Passphrase:
Please enter the passphrase to unlock the OpenPGP secret key:
"James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.) <ozonewebstechnolutions@gmail.com>"
255-bit ECDH key, ID 3682442377F2DB67,
created 2025-08-17 (main key ID 267EFA36138B967E).

Password: [REDACTED]

Save in password manager

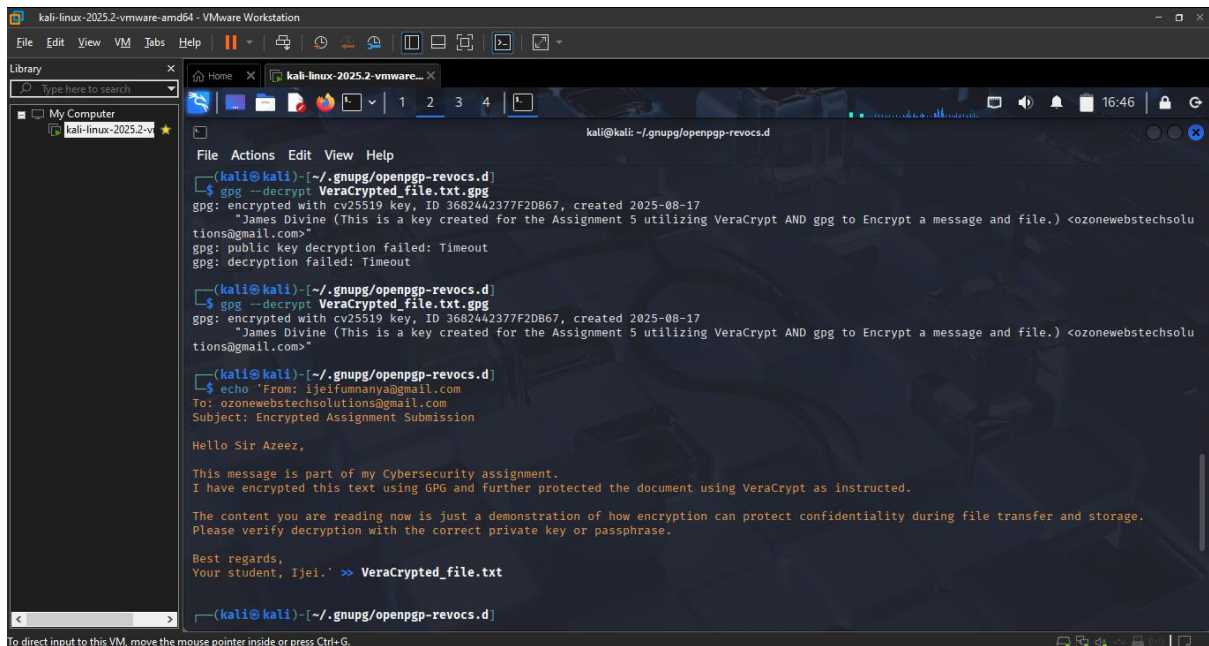
gpg: next trustsd check due at 2025-08-24
File 'VeraCrypt_file.txt.gpg' exists. Overwrite? (y/N) y

(kali@kali)~/.gnupg/openpgp-revocs.d$ cat VeraCrypt_file.txt

(kali@kali)~/.gnupg/openpgp-revocs.d$ ls
530AC46E6836971BA08ACB1F267EFA36138B967E.rev  CyberSec_encrypt.txt  VeraCrypt_file.txt
BDCE6501D48F6EA7A4FC3919736C98C71A1F80A0C.rev  CyberSec_encrypt.txt.gpg  VeraCrypt_file.txt.gpg
C7EA6330857F22182547DD4BC0AB2DE070354C64.rev  pubkey.asc

(kali@kali)~/.gnupg/openpgp-revocs.d$ gpg --decrypt VeraCrypt_file.txt.gpg
gpg: encrypted with cv25519 key, ID 3682442377F2DB67, created 2025-08-17
"James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.) <ozonewebstechnolutions@gmail.com>"
```

As we can see here the public key decryption is timed and can timeout of session so we need to be time conscious when trying to perform the encryption process. Thereafter we have our message which we have just **“echoed” using “echo”** into our **“VeraCrypted_file.txt”**



```
kali@kali: ~/gnupg/openpgp-revocs.d
$ gpg --decrypt VeraCrypted_file.txt.gpg
gpg: encrypted with cv25519 key, ID 3682442377F2DB67, created 2025-08-17
"James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.) <ozonewebstechnolutions@gmail.com>"
gpg: public key decryption failed: Timeout
gpg: decryption failed: Timeout

(kali@kali)~/gnupg/openpgp-revocs.d
$ gpg --decrypt VeraCrypted_file.txt.gpg
gpg: encrypted with cv25519 key, ID 3682442377F2DB67, created 2025-08-17
"James Divine (This is a key created for the Assignment 5 utilizing VeraCrypt AND gpg to Encrypt a message and file.) <ozonewebstechnolutions@gmail.com>"

(kali@kali)~/gnupg/openpgp-revocs.d
$ echo "From: ijeifumanya@gmail.com
To: ozonewebstechnolutions@gmail.com
Subject: Encrypted Assignment Submission

Hello Sir Azeez,

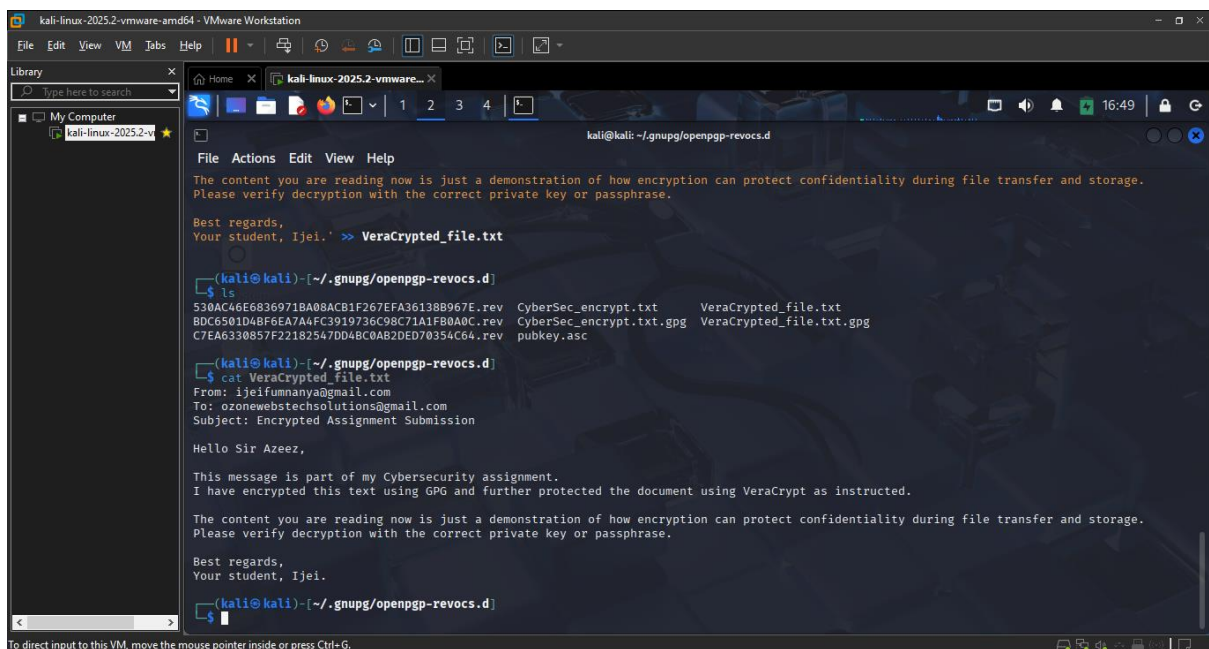
This message is part of my Cybersecurity assignment.
I have encrypted this text using GPG and further protected the document using VeraCrypt as instructed.

The content you are reading now is just a demonstration of how encryption can protect confidentiality during file transfer and storage.
Please verify decryption with the correct private key or passphrase.

Best regards,
Your student, Ijei." >> VeraCrypted_file.txt

(kali@kali)~/gnupg/openpgp-revocs.d
```

Decided to **“cat”** it to cross-check if the text to be encrypted is inside the folder **“VeraCrypted_file.txt”**



```
kali@kali: ~/gnupg/openpgp-revocs.d
$ ls
530AC46E6836971BA08ACB1F267EFA36138B967E.rev  CyberSec_encrypt.txt  VeraCrypted_file.txt
BDC6501D48F6EA7A4FC3919736C98C71A1FB0A0C.rev  CyberSec_encrypt.txt.gpg  VeraCrypted_file.txt.gpg
C7EA6330857F22182547DD4BC0A82DED70354C64.rev  pubkey.asc

(kali@kali)~/gnupg/openpgp-revocs.d
$ cat VeraCrypted_file.txt
From: ijeifumanya@gmail.com
To: ozonewebstechnolutions@gmail.com
Subject: Encrypted Assignment Submission

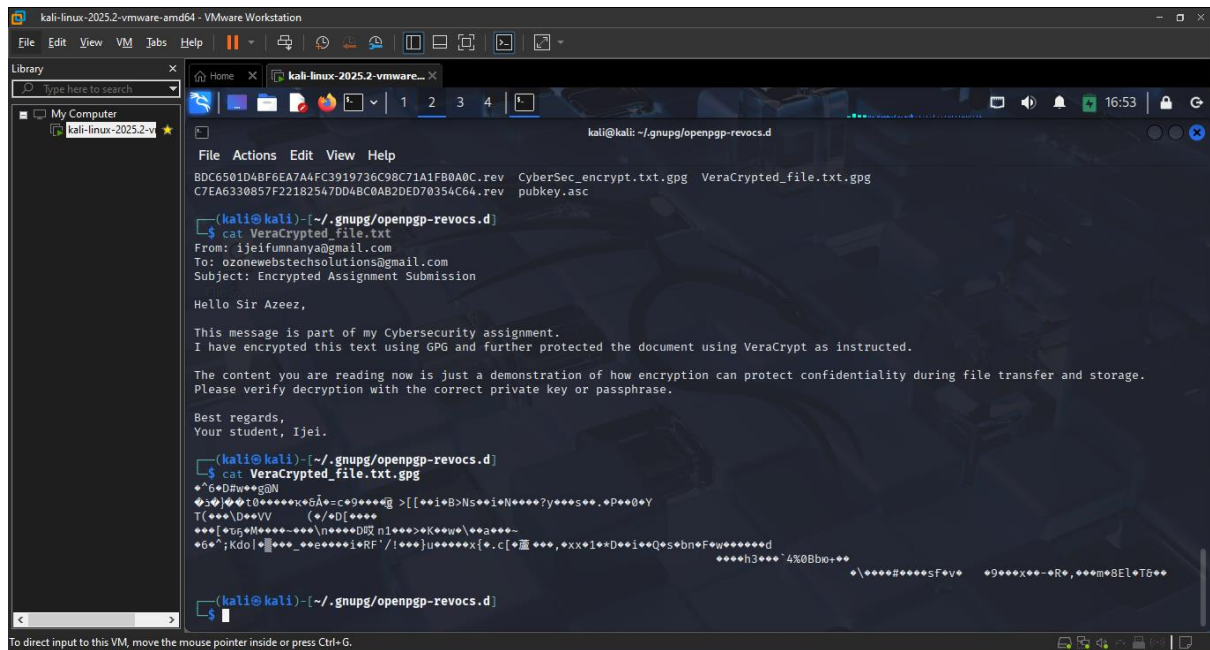
Hello Sir Azeez,

This message is part of my Cybersecurity assignment.
I have encrypted this text using GPG and further protected the document using VeraCrypt as instructed.

The content you are reading now is just a demonstration of how encryption can protect confidentiality during file transfer and storage.
Please verify decryption with the correct private key or passphrase.

Best regards,
Your student, Ijei.
```


Then afterwards, checked the encrypted message in the **“.gpg”** file and we have our cipher-text in it.



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali: ~/gnupg/openpgp-revocs.d
File Actions Edit View Help
BDC6501D4BF6EA7A4FC3919736C98C71A1F80A0C.rev CyberSec_encrypt.txt.gpg VeraCrypted_file.txt.gpg
C7EA6330857F22182547DD4BC0AB2DE070354C64.rev pubkey.asc

(kali@kali)~/gnupg/openpgp-revocs.d
$ cat VeraCrypted_file.txt
From: ijeifumnanya@gmail.com
To: ozonewebstechsolutions@gmail.com
Subject: Encrypted Assignment Submission

Hello Sir Azeez,

This message is part of my Cybersecurity assignment.
I have encrypted this text using GPG and further protected the document using VeraCrypt as instructed.

The content you are reading now is just a demonstration of how encryption can protect confidentiality during file transfer and storage.
Please verify decryption with the correct private key or passphrase.

Best regards,
Your student, Ijei.

(kali@kali)~/gnupg/openpgp-revocs.d
$ cat VeraCrypted_file.txt.gpg
^G^D#w^g@N
^5^0^0t0+++++;e5A^=-c+0++++@ >[[+i+B>N;s+e+i*N++++?y+++++.P+e@eY
T(++++D+VV (/+D[++++
+++{+u5+N+++++---\n++++D5R n|+++++K+g+e\+e+e+---
+6^";Kdo|+^+++++e++++i*RF'//!+++}u+++++x{+c[+^+ +x+e+D+e+Q+e+bn+F+e+e+e+d
++++h3+++4%0Bbo+++
e\++++Z++++sF+e+ +?+++x+++e+Re,+++m+8EL+TG+++

(kali@kali)~/gnupg/openpgp-revocs.d
```

Original Text:

From: ijeifumnanya@gmail.com

To: ozonewebstechsolutions@gmail.com

Subject: Encrypted Assignment Submission

Hello Sir Azeez,

This message is part of my Cybersecurity assignment.

I have encrypted this text using GPG and further protected the document using VeraCrypt as instructed.

The content you are reading now is just a demonstration of how encryption can protect confidentiality during file transfer and storage.

Please verify decryption with the correct private key or passphrase.

Best regards,

Your student, Ijei.

Cipher-text:

^6D#wg@N

};}t0k&Ã=c9g>[[iB>NsiiN??y?s
.P0Y

T(\\D VV (/D[

[5M~\\nDn1>Kw\`a~

6^;Kdo|_eiiRF'/{u}x{.c[蘆

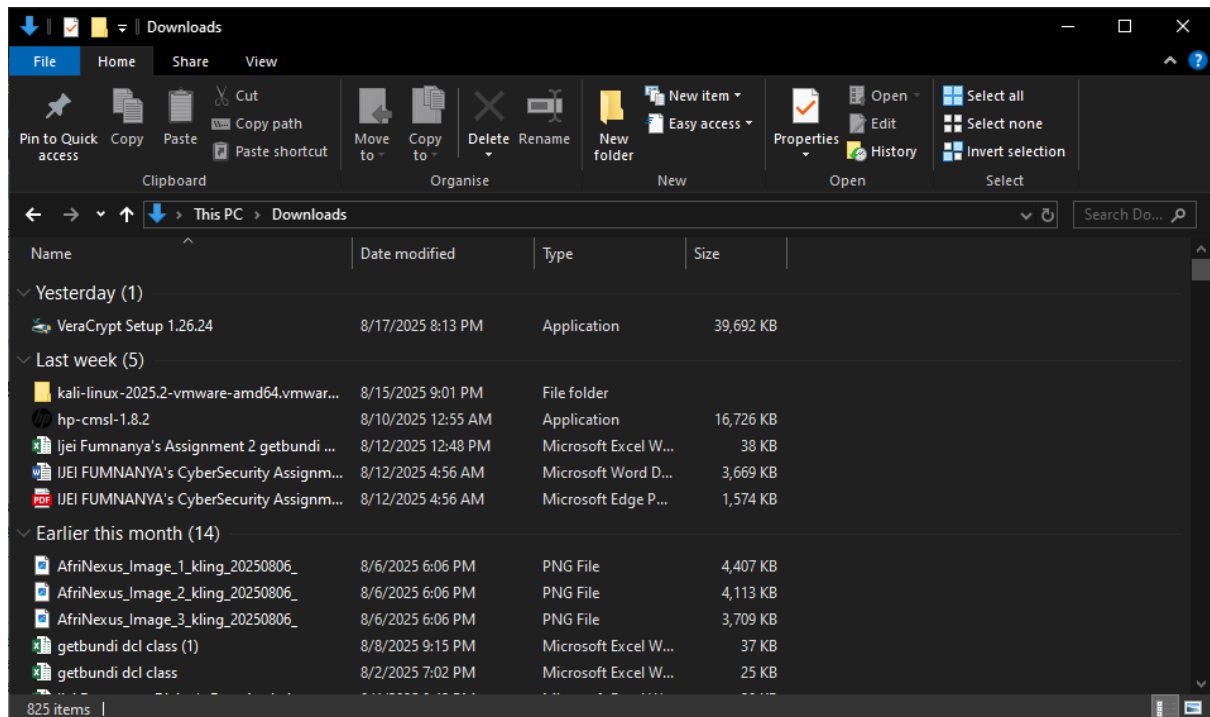
,xx1*DiiQsbnFwdd

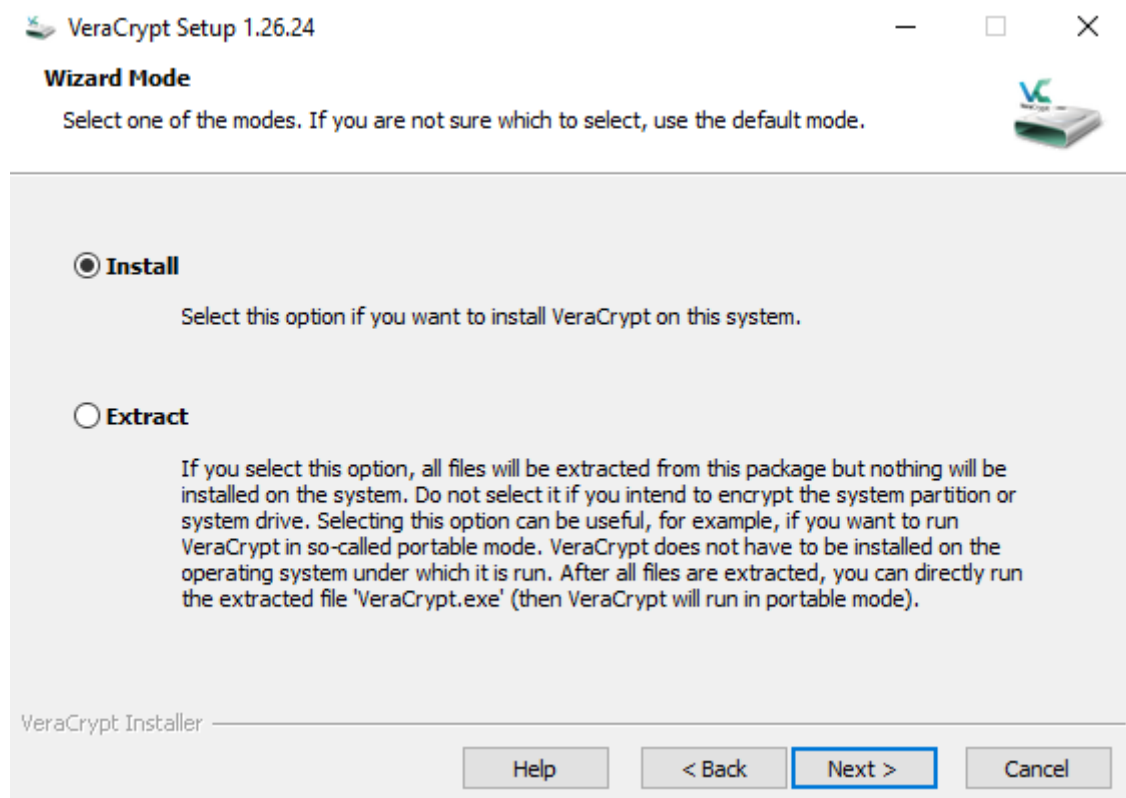
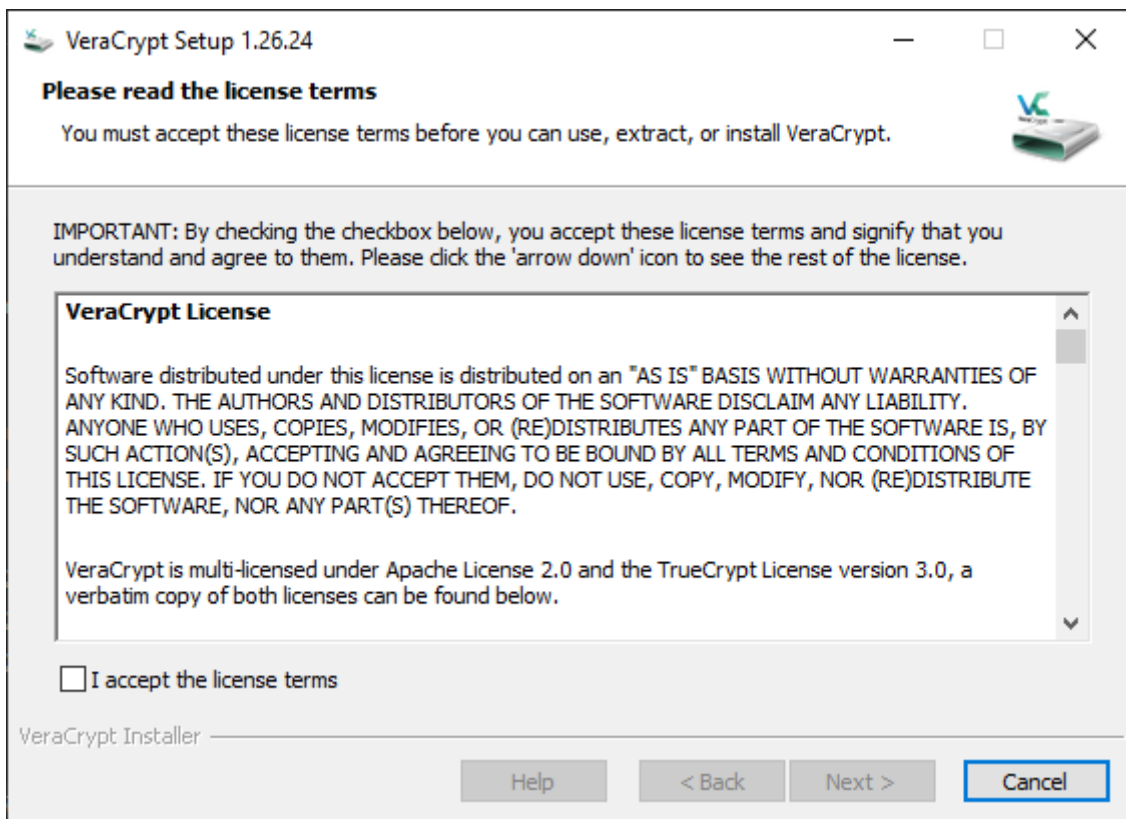
h3`4%0Bbio+

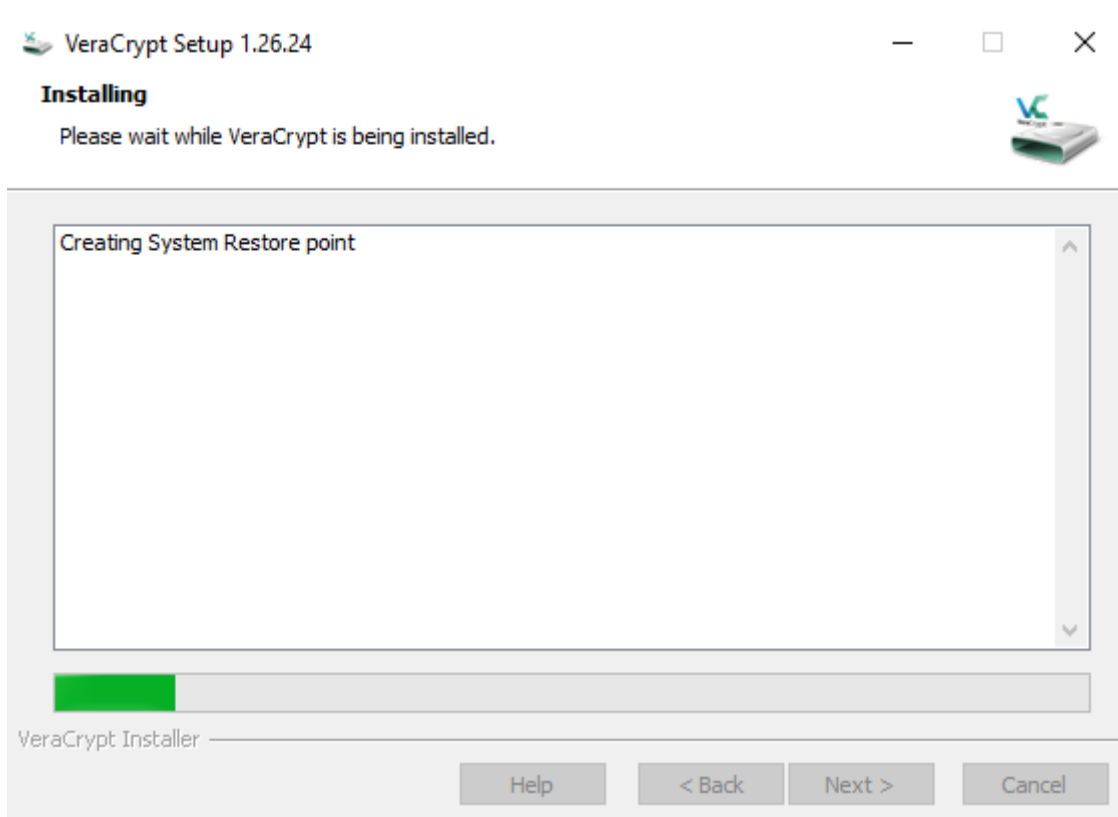
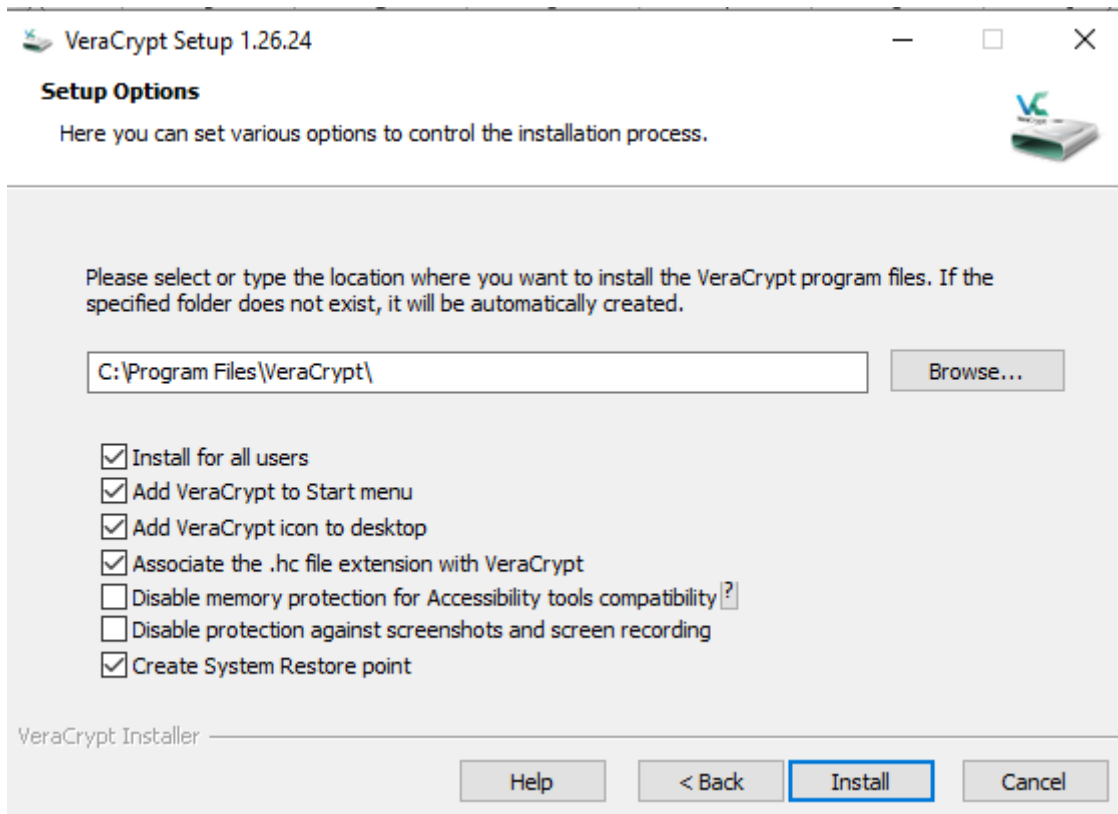
\#####sfv

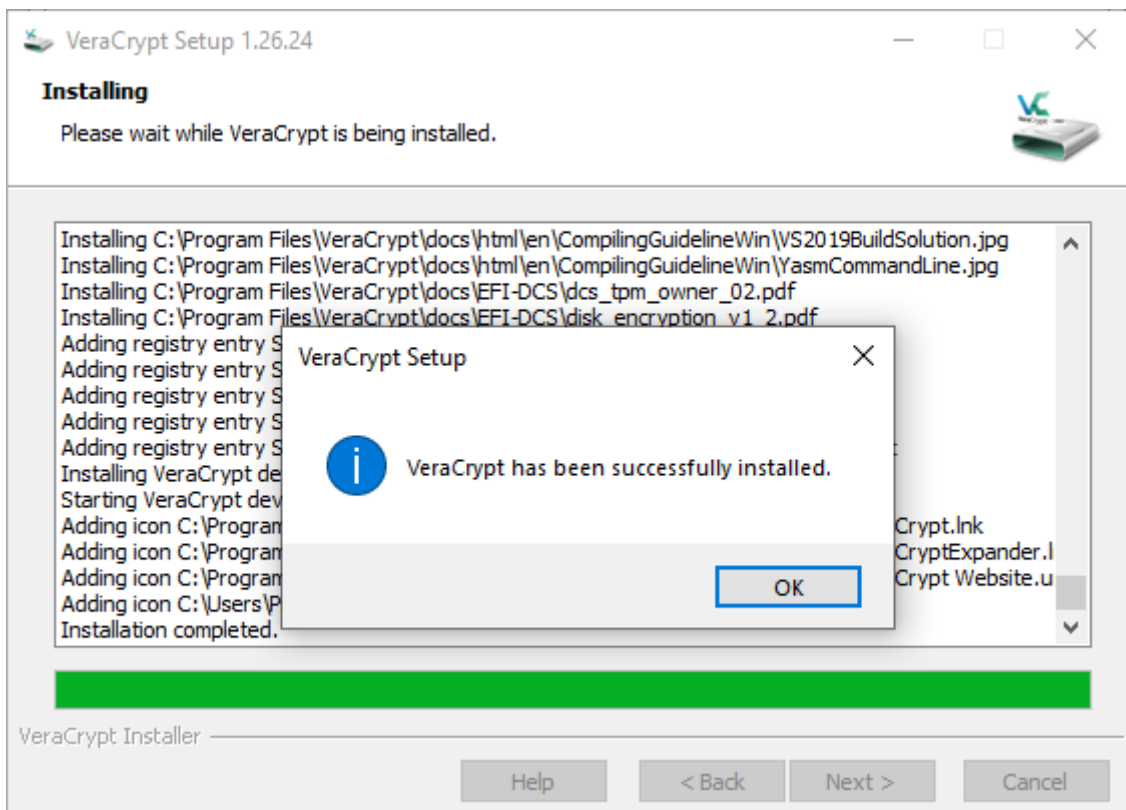
9xx-R,,m8ElT&

Next stage of the assignment with my approach is to download and install VeraCrypt.









Successfully installed and the PDF version of this particular file will be mounted in it on an encrypted volume using Advanced encryption standard (AES) encryption algorithm.