Please include the following in your lab writeup:
- Lab number, your full name and Student ID.
- Clearly labelled answers to the questions (Core 1, Challenge 99, etc).
- Report is submitted in electronic form as a PDF file.

LAB NUMBER: 2
FULL NAME : Elisha Jones
STUDENT ID: 300573902

CREATE A KEYPAIR
- List the commands used and provide the output from the commands.

```
 cashmere-lounge% gpg2 --gen-key
   gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
   This is free software: you are free to change and redistribute it.
   There is NO WARRANTY, to the extent permitted by law.

   gpg: directory '/home/joneselis1/.gnupg' created
   gpg: keybox '/home/joneselis1/.gnupg/pubring.kbx' created
   Note: Use "gpg2 --full-generate-key" for a full featured key generation dialog.

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

   Real name: Elijones
   Email address: joneselis1@ecs.vuw.ac.nz
   You selected this USER-ID:
       "Elijones <joneselis1@ecs.vuw.ac.nz>"

   Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
   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: /home/joneselis1/.gnupg/trustdb.gpg: trustdb created
   gpg: key 395E4E835B0C7300 marked as ultimately trusted
   gpg: directory '/home/joneselis1/.gnupg/openpgp-revocs.d' created
   gpg: revocation certificate stored as
'/home/joneselis1/.gnupg/openpgp-revocs.d/DD95B8C0392B2AE1CA4162B3395E4E835B0C73
00.rev'
   public and secret key created and signed.
   pub   rsa3072 2021-03-18 [SC] [expires: 2023-03-18]
      DD95B8C0392B2AE1CA4162B3395E4E835B0C7300
   uid                      Elijones <joneselis1@ecs.vuw.ac.nz>
   sub   rsa3072 2021-03-18 [E] [expires: 2023-03-18]
```

passphrase = ChloeCrowe02

CREATE A REVOCATION KEY

- List the commands used and provide the output from the commands.

```
  cashmere-lounge% gpg2 --gen-revoke --armor --output=RevocationCertificate.asc
joneselis1@ecs.vuw.ac.nz
```

- Paste the revocation key into this sheet.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: This is a revocation certificate

iQG2BCABCAAgFiEE3ZW4wDkrKuHKQWKzOV5Og1sMcwAFAmBSoF4CHQIACgkQOV5O
g1sMcwBlYQwAt9LdK6tz8CZrIm4ukvB9HXEgJwgu8bEbGRwuyU2P8fyU+cTUWzcU
284VwyXflPRxGKwRlqjYZgE50vGoYJ/UE5yJIYx4OvUfSOuqyrUWrVumWdVGyI3y
2CQeUbuWS1tmJ5VG96zhIXIQ7FuJTgipDUmJ7OlLInN8xrye4o3Isze4qu1AE4pQ
iVsMZoUfXrh6gVEd0+9ffLMATgk1PdI6fmTsoHJL4JiSff0uHephQg8DXUiPsM0J
iZCi7gxvqFRrlIc6TAIRDZN3ikvxzWZBoHbPxOYHynwVO8tHOg+46BBN6vpg04J5
CSW6zQZA2DVRhRDv4IBtgAVostx+pCdM7EM4Y+8hiO84IFVbbPc89qVUXZAXSUO8
SO800oUT6bU9Z6IPqhnqhqpoEhixuhOoiisIw/EQsMZfEcV+GLp83IqKRq1qEzSG
iJctlQe7/z13mA4uC8DInGhg9yWXXvkFGmrThJJmxHj7LOogB+yEBUFV8VGX5z19
ACEPg1UzxuEo
=+8LW
-----END PGP PUBLIC KEY BLOCK-----
```

EXPORT YOUR PUBLIC KEY

- List the commands used and provide the output from the commands.
- Paste your public key into this sheet.

```
  cashmere-lounge% gpg2 --gen-revoke --armor --output=RevocationCertificate.asc
joneselis1@ecs.vuw.ac.nz
   sec  rsa3072/395E4E835B0C7300 2021-03-18 Elijones <joneselis1@ecs.vuw.ac.nz>

   Create a revocation certificate for this key? (y/N) y
   Please select the reason for the revocation:
   0 = No reason specified
   1 = Key has been compromised
   2 = Key is superseded
   3 = Key is no longer used
   Q = Cancel
   (Probably you want to select 1 here)
   Your decision? 1
   Enter an optional description; end it with an empty line:
   >
   Reason for revocation: Key has been compromised
   (No description given)
   Is this okay? (y/N) y
   Revocation certificate created.

   Please move it to a medium which you can hide away; if Mallory gets
   access to this certificate he can use it to make your key unusable.
   It is smart to print this certificate and store it away, just in case
   your media become unreadable.  But have some caution:  The print system of
   your machine might store the data and make it available to others!
   cashmere-lounge%
```

```
cashmere-lounge% gpg2 --fingerprint joneselis1@ecs.vuw.ac.nz
   gpg: checking the trustdb
   gpg: marginals needed: 3  completes needed: 1  trust model: pgp
   gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
   gpg: next trustdb check due at 2023-03-18
   pub   rsa3072 2021-03-18 [SC] [expires: 2023-03-18]
      DD95 B8C0 392B 2AE1 CA41  62B3 395E 4E83 5B0C 7300
   uid           [ultimate] Elijones <joneselis1@ecs.vuw.ac.nz>
   sub   rsa3072 2021-03-18 [E] [expires: 2023-03-18]
```

my signed public key: cashmere-lounge% gpg2 --export --armor joneselis1@ecs.vuw.ac.nz > joneselis1.publickey.asc

```
betsy% gpg2 --import kriletmila.asc
gpg: key 47613C6DC0607F4D: public key "Milan Kriletich
<kriletmila@myvuw.ac.
nz>" imported
gpg: Total number processed: 1
gpg:               imported: 1
betsy% gpg2 --fingerprint kriletmila@myvuw.ac.nz
pub   rsa3072 2021-03-25 [SC] [expires: 2023-03-25]
      90BE 29F2 0A46 A735 E269  7AFB 4761 3C6D C060 7F4D
uid           [ unknown] Milan Kriletich <kriletmila@myvuw.ac.nz>
sub   rsa3072 2021-03-25 [E] [expires: 2023-03-25]
```

```
betsy% gpg2 --sign-key kriletmila@myvuw.ac.nz

pub  rsa3072/47613C6DC0607F4D
    created: 2021-03-25  expires: 2023-03-25  usage: SC
    trust: unknown       validity: unknown
sub  rsa3072/B48872928079FB31
    created: 2021-03-25  expires: 2023-03-25  usage: E
[ unknown] (1). Milan Kriletich <kriletmila@myvuw.ac.nz>

gpg: using "395E4E835B0C7300" as default secret key for signing

pub  rsa3072/47613C6DC0607F4D
    created: 2021-03-25  expires: 2023-03-25  usage: SC
    trust: unknown       validity: unknown
Primary key fingerprint: 90BE 29F2 0A46 A735 E269  7AFB 4761 3C6D
C060 7F4D

    Milan Kriletich <kriletmila@myvuw.ac.nz>

This key is due to expire on 2023-03-25.
Are you sure that you want to sign this key with your
key "Elijones <joneselis1@ecs.vuw.ac.nz>" (395E4E835B0C7300)

Really sign? (y/N) y

betsy% gpg2 --export --armor kriletmila@myvuw.ac.nz > signed_key.asc
betsy% gpg2 --import signed_keyjones.asc
gpg: key 395E4E835B0C7300: "Elijones <joneselis1@ecs.vuw.ac.nz>" 1
new signa
ture
gpg: Total number processed: 1
gpg:         new signatures: 1
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2023-03-18
betsy%
```

SWAP SIGNED VERSIONS OF PLAIN.TXT

- List the commands used and provide the output from the commands.
- You must demonstrate the steps taken to securely do this and ensure that no modifications have taken place in transit.
- As part of your proof paste the signed messages into this sheet.

```
betsy% gpg2 --clearsign plaintext.txt  - my
gpg: using "395E4E835B0C7300" as default secret key for signing
betsy% gpg2 --verify mila.plaintext.txt.asc
gpg: Signature made Thu 25 Mar 2021 14:10:19 NZDT
gpg:                using RSA key
90BE29F20A46A735E2697AFB47613C6DC0607F4D
gpg: Good signature from "Milan Kriletich <kriletmila@myvuw.ac.nz>"
[full]
```

SECURELY SWAPPED ENCRYPTED VERSIONS

- List the commands used and provide the output from the commands.
- You must demonstrate the steps taken to securely do this and ensure that no modifications have taken place in transit.
- As part of your proof paste the encrypted messages into this sheet.

```
betsy% gpg2 --encrypt -r kriletmila@myvuw.ac.nz encrypt.txt betsy%
gpg2 --decrypt encrypt.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID 0ECAB1B62D3196AD, created
2021-03-1
8
     "Elijones <joneselis1@ecs.vuw.ac.nz>"
Yourself off its pleasant ecstatic now law. Ye their mirth seems of
songs. Prospect out bed contempt separate. Her inquietude our shy yet
sentiments collecting. Cottage fat beloved himself arrived old. Grave
widow hours among him? no you led. Power had these met least nor
young. Yet match drift wrong his our. %
betsy%
```