Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Install and configure GNU privacy guard (GNUPG)

```
┌[henryfbp@pop-os]-(~/D/from-randy)
└> gpg --list-keys                                                    (base)
/home/henryfbp/.gnupg/pubring.kbx
--------------------------------
pub   rsa3072 2018-09-13 [SC] [expires: 2021-10-17]
      0A40840912135F815BD26155C3B02D99C1C244C3
uid           [ultimate] Henry Post <HenryFBP@gmail.com>
sub   rsa3072 2018-09-13 [E] [expires: 2020-09-12]

pub   rsa3072 2018-09-13 [SC] [expires: 2020-09-12]
      36EB77CBFCB9FAB819D7A9CA79FC9B69844EF44A
uid           [ultimate] Henry Post <hpost@hawk.iit.edu>
sub   rsa3072 2018-09-13 [E] [expires: 2020-09-12]

pub   rsa4096 2017-08-14 [SCE]
      128CF232A9371991C8A65695E08E7E629DB62FB1
uid           [ unknown] Fedora 28 (28) <fedora-28@fedoraproject.org>

pub   rsa4096 2018-02-17 [SCE]
      5A03B4DD8254ECA02FDA1637A20AA56B429476B4
uid           [ unknown] Fedora 29 (29) <fedora-29@fedoraproject.org>

pub   rsa4096 2018-08-11 [SCE]
      F1D8EC98F241AAF20DF69420EF3C111FCFC659B9
uid           [ unknown] Fedora (30) <fedora-30-primary@fedoraproject.org>

pub   rsa4096 2010-04-23 [SCE]
      8C3BE96AF2309184DA5C0DAE3B49DF2A0608B895
uid           [ unknown] EPEL (6) <epel@fedoraproject.org>

pub   rsa4096 2013-12-16 [SCE]
      91E97D7C4A5E96F17F3E888F6A2FAEA2352C64E5
uid           [ unknown] Fedora EPEL (7) <epel@fedoraproject.org>

pub   rsa4096 2018-11-13 [SCE] [expires: 2028-12-31]
      C2A3FA9DC67F68B98BB543F47BB90722DBBDCF7C
uid           [ unknown] Fedora (iot 2019) <fedora-iot-2019@fedoraproject.org>

pub   rsa4096 2015-01-18 [C] [expires: 2020-01-11]
      A490D0F4D311A4153E2BB7CADBB802B258ACD84F
uid           [  full  ] Tails developers (offline long-term identity key)
<tails@boum.org>
uid           [  full  ] Tails developers <tails@boum.org>
sub   rsa4096 2017-08-28 [S] [expires: 2020-01-11]
sub   rsa4096 2017-08-28 [S] [expires: 2020-01-11]
sub   ed25519 2017-08-28 [S] [expires: 2020-01-11]
sub   rsa4096 2018-08-30 [S] [expires: 2020-01-11]

pub   rsa4096 2010-09-27 [SC] [expires: 2020-02-07]
      4900707DDC5C07F2DECB02839C31503C6D866396
uid           [ unknown] Stefano Zacchiroli <zack@upsilon.cc>
```

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

```
uid            [ unknown] Stefano Zacchiroli <zack@debian.org>
uid            [ unknown] Stefano Zacchiroli <stefano.zacchiroli@inria.fr>
uid            [ unknown] Stefano Zacchiroli <zack@softwareheritage.org>
uid            [ unknown] Stefano Zacchiroli <zack@irif.fr>
sub   rsa4096 2010-09-27 [E]
sub   rsa4096 2012-12-01 [S] [expires: 2020-02-07]

pub   rsa3072 2019-10-17 [SC] [expires: 2021-10-16]
      C2299344CB37649D814509E902FDD80B802CEAA1
uid            [ unknown] Randy Random <randyrandom62435123@gmail.com>
sub   rsa3072 2019-10-17 [E] [expires: 2021-10-16]
```
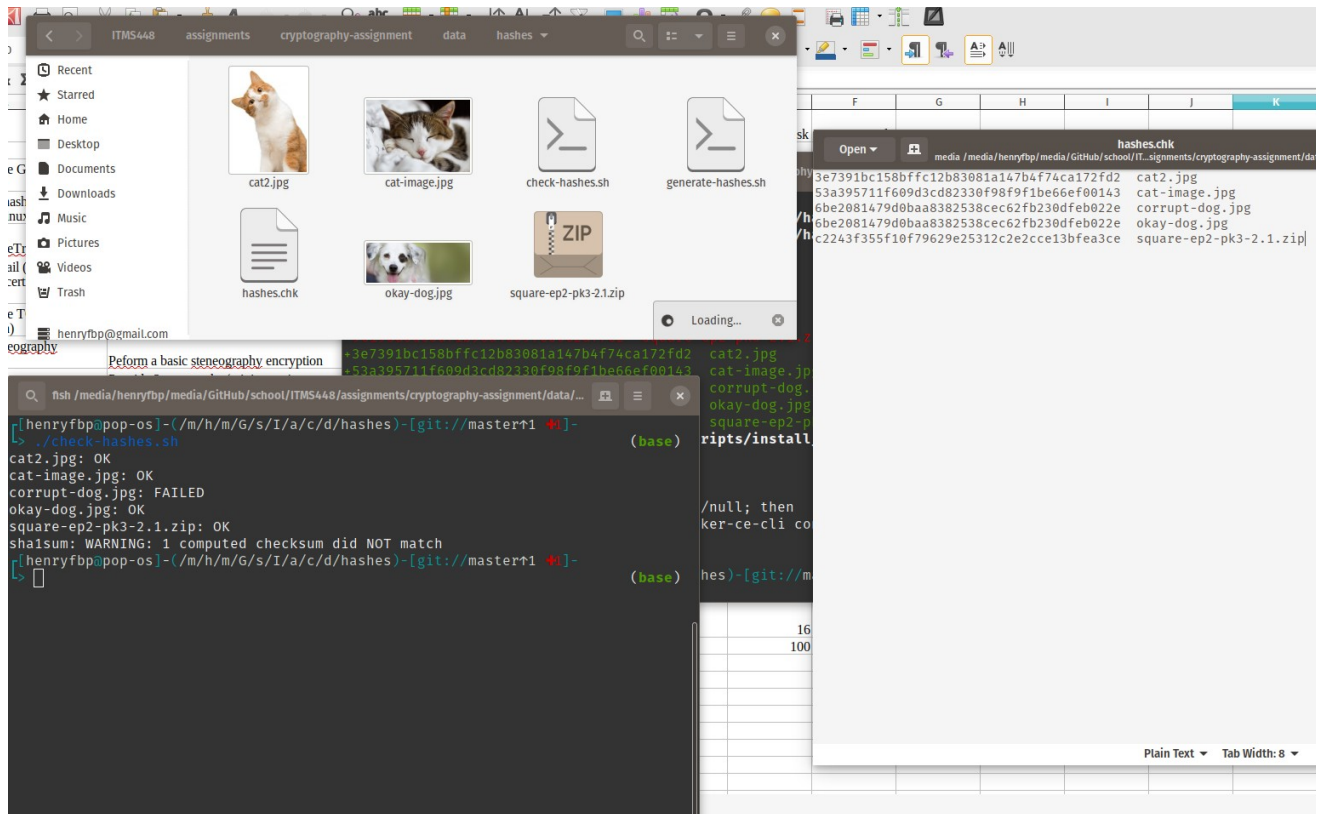
Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Generate a SHA1 hash from the command-line in Linux

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Install and configure TrueCrypt

Volume inside image file info:

```
┌[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/truecrypt)-[git://master …2]-
└> ls my-volume.img  -lh                                          (base)
-rwxrwxrwx 1 root root 48M Oct 17 22:46 my-volume.img
┌[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/truecrypt)-[git://master …2]-
└> cat creds.txt                                                  (base)
outerpassword
```

Mounting outer volume:
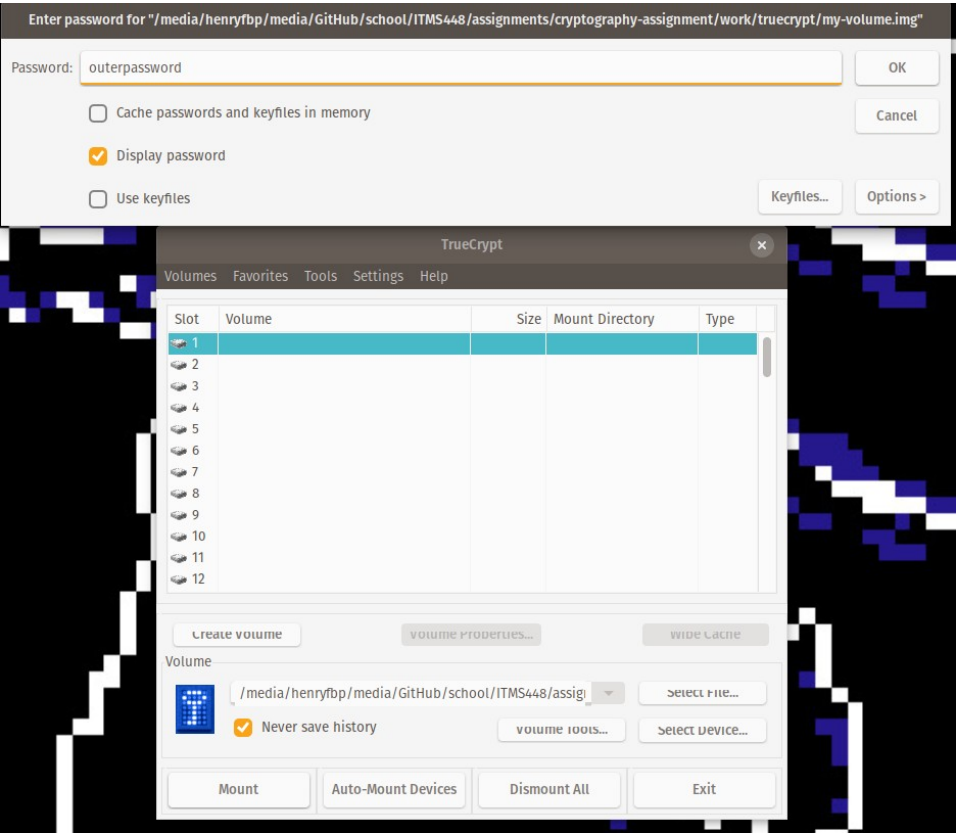
Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Writing to the volume:

```
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/truecrypt)-[git://master …1]-
└> echo 'secret' > /media/truecrypt1/secrets.txt                    (base)
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/truecrypt)-[git://master +1…2]-
└> ls                                                               (base)
creds.txt  my-volume.img
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/truecrypt)-[git://master +1…2]-
└> cd /media/truecrypt1/                                            (base)
[henryfbp@pop-os]-(/m/truecrypt1)
└> ls                                                               (base)
secrets.txt
[henryfbp@pop-os]-(/m/truecrypt1)
└> cat secrets.txt                                                  (base)
secret
```

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Send encrypted email (includes exchanging digital certificates and decrypting email)

Sending pubkey as Randy to Henry
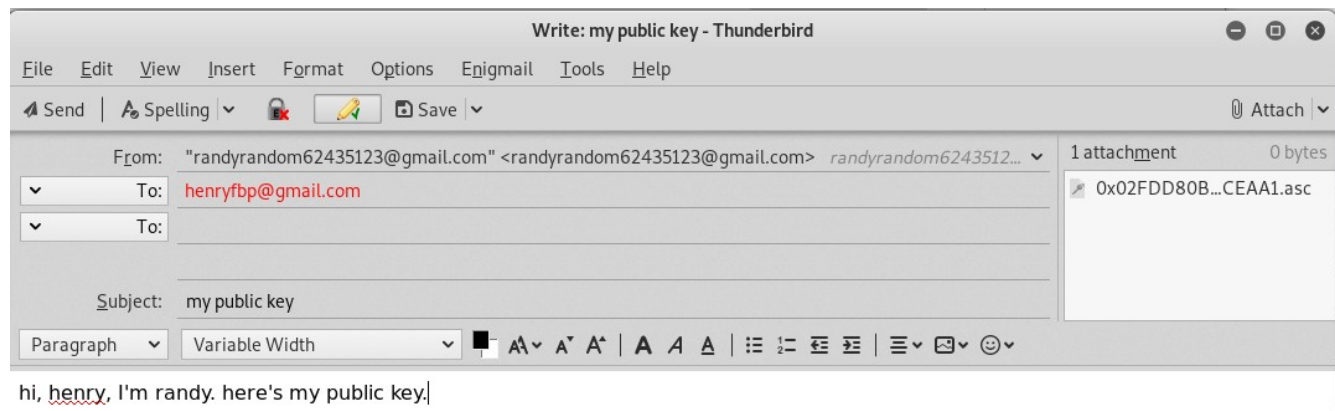


Receiving pubkey as Henry
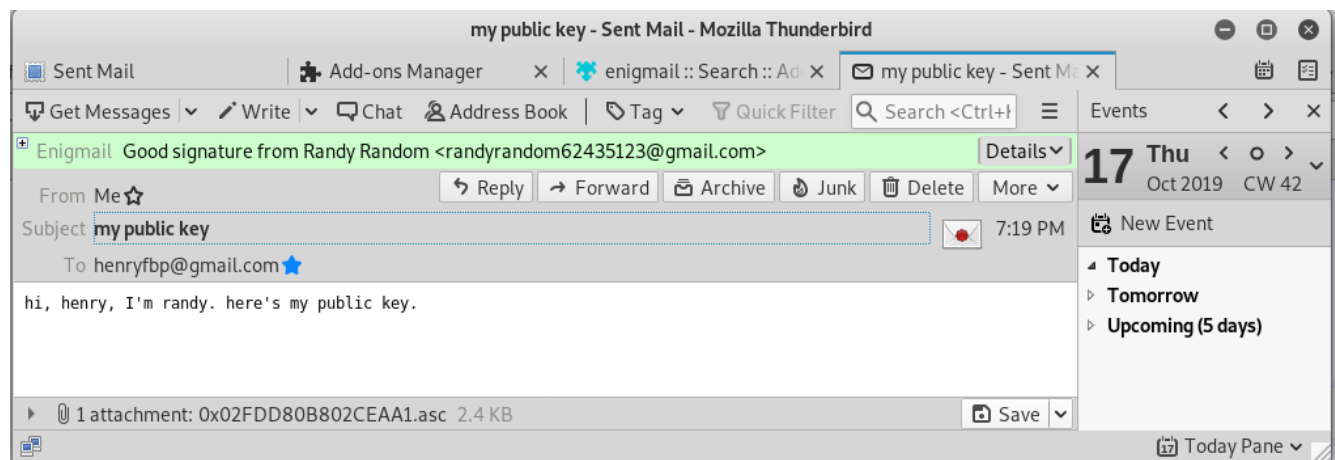
Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Importing Randy's pubkey
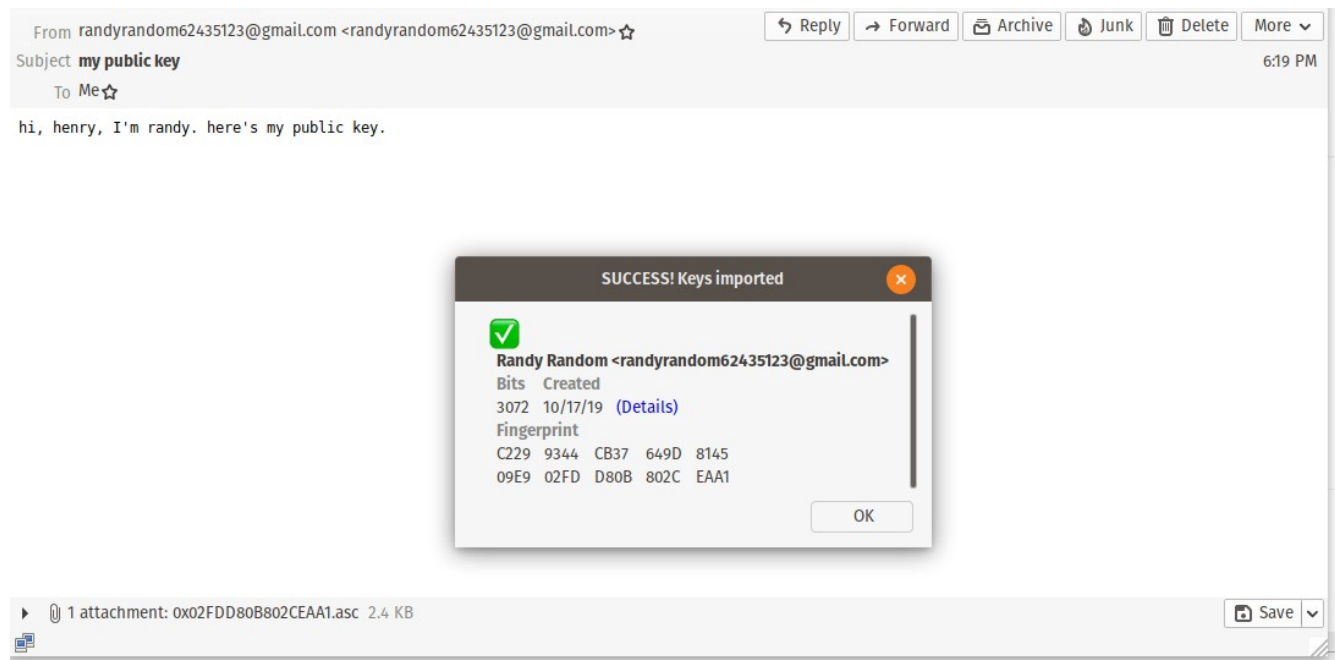


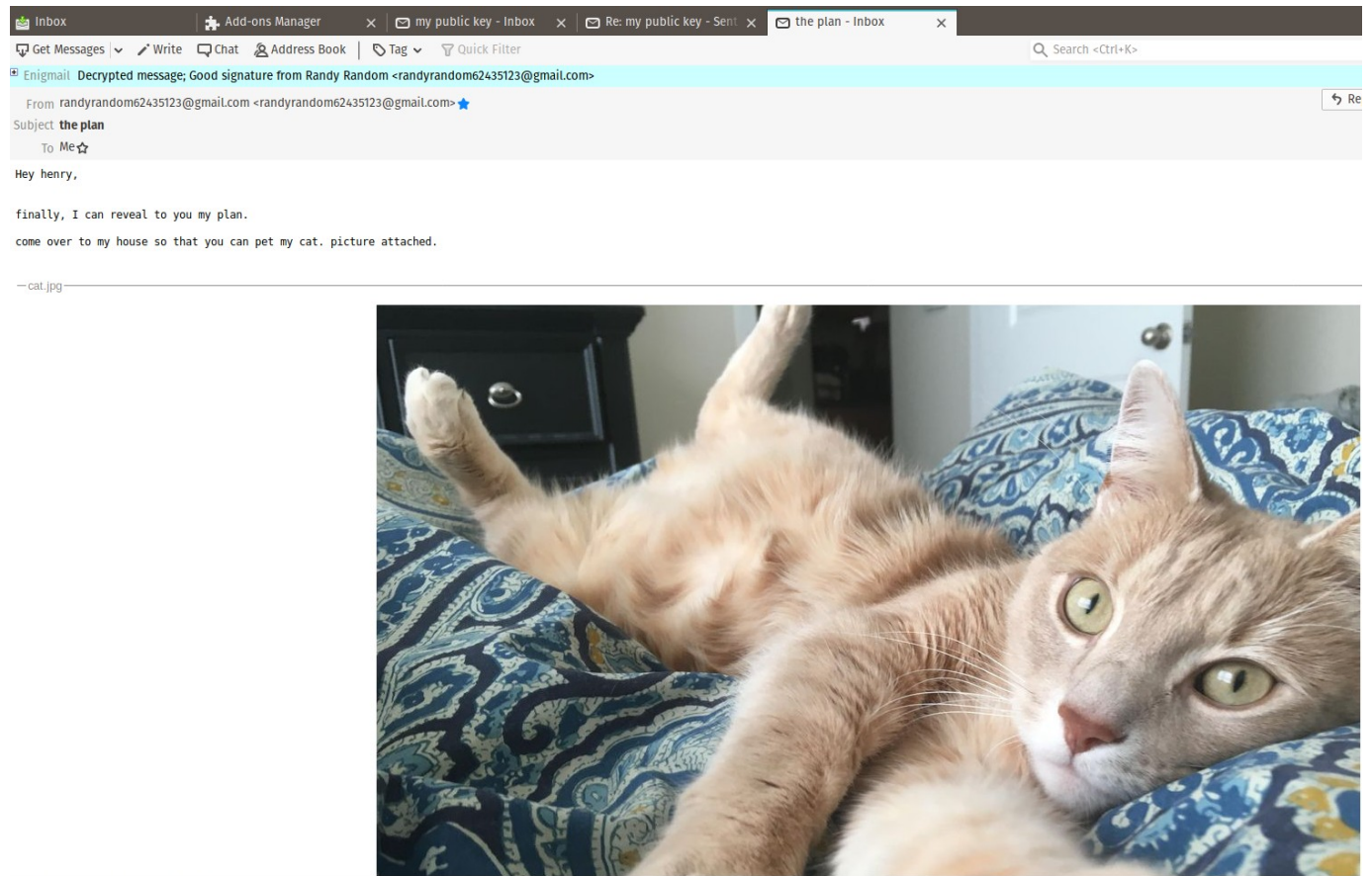Henry sending his encrypted pubkey to Randy
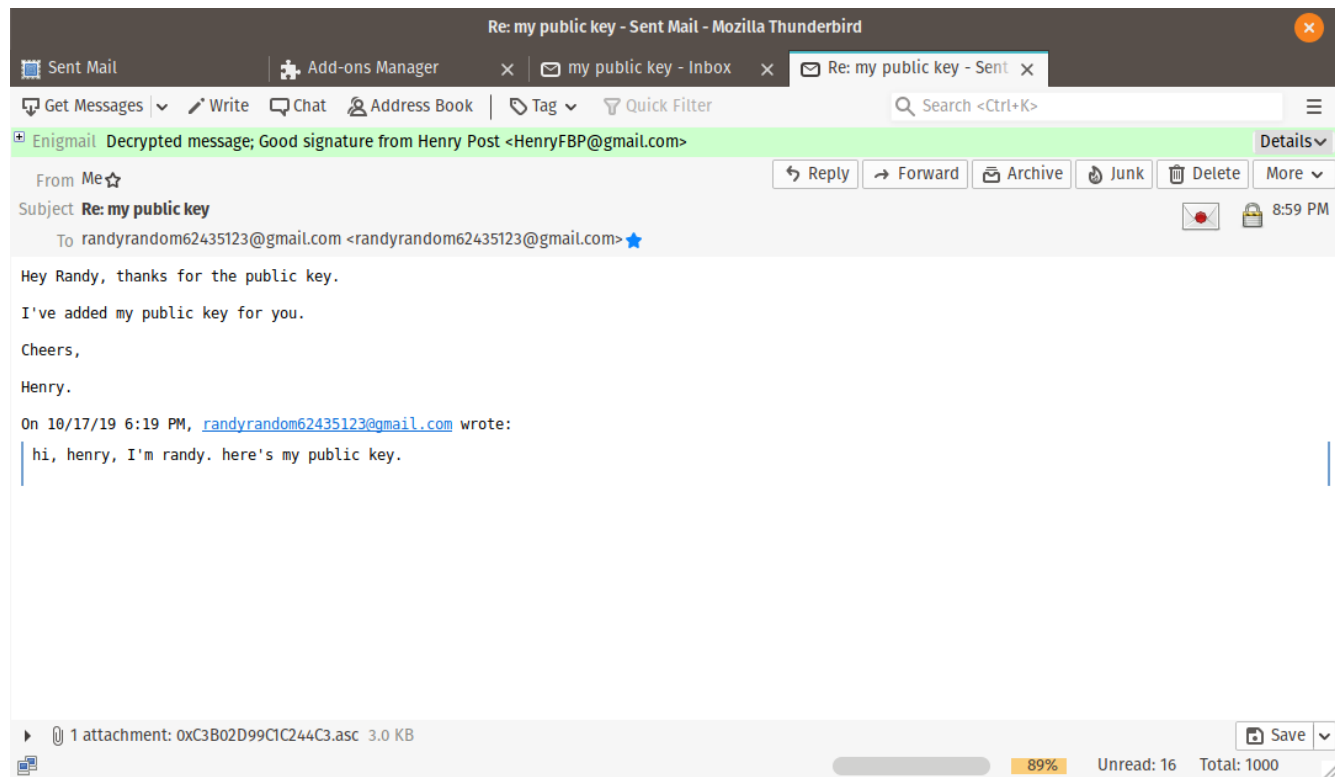
Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Randy sending a secret plan to Henry using Henry's pubkey

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

The email without decrypting it:

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate
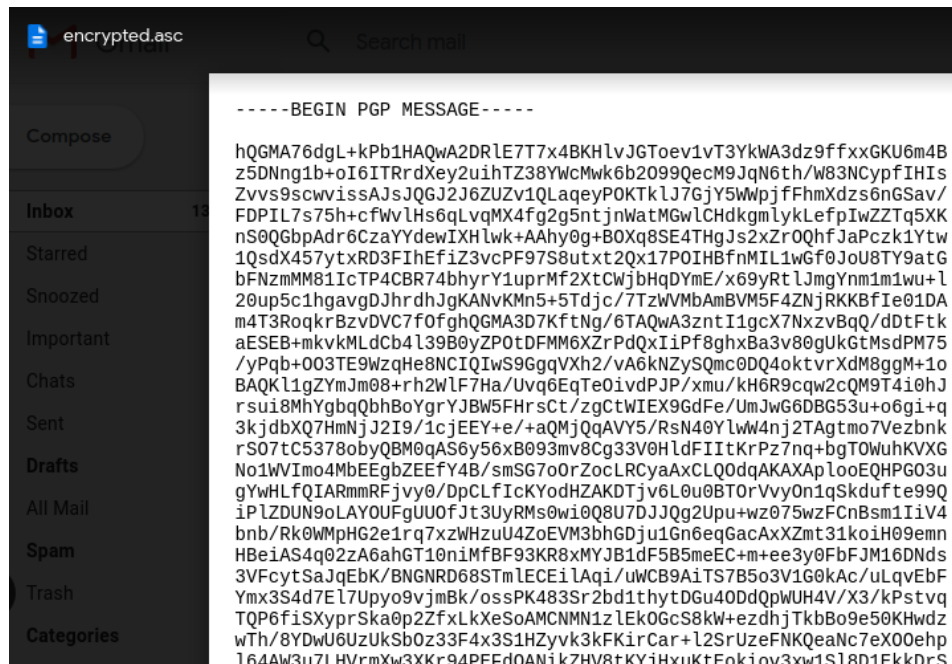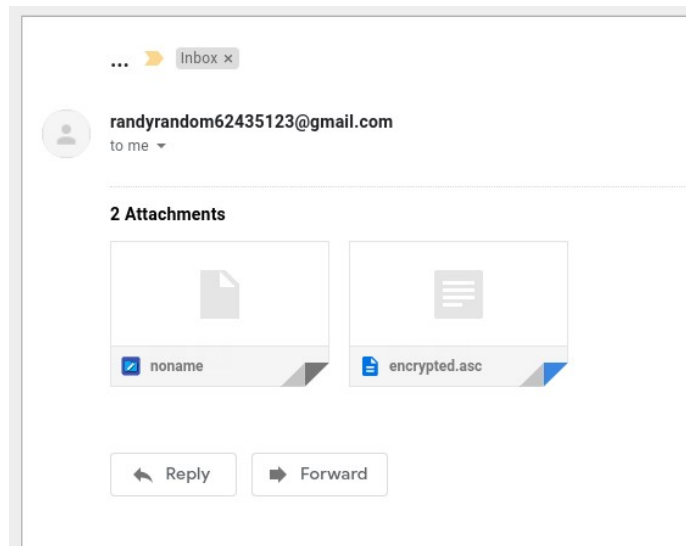
# Install and configure TOR (includes performing a search)

## Tor log:

10/18/19, 02:52:58.852 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down all existing connections.

10/18/19, 02:52:58.852 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down all existing connections.

10/18/19, 02:52:58.852 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down all existing connections.

10/18/19, 02:52:58.852 [NOTICE] Opening Socks listener on 127.0.0.1:9150

10/18/19, 02:52:58.852 [NOTICE] Opened Socks listener on 127.0.0.1:9150

10/18/19, 02:52:58.852 [NOTICE] Renaming old configuration file to "/home/vagrant/Downloads/tor-browser_en-US/Browser/TorBrowser/Data/Tor/torrc.orig.1"

10/18/19, 02:52:59.749 [NOTICE] Bootstrapped 5% (conn): Connecting to a relay

10/18/19, 02:53:00.250 [NOTICE] Bootstrapped 10% (conn_done): Connected to a relay

10/18/19, 02:53:00.580 [NOTICE] Bootstrapped 14% (handshake): Handshaking with a relay

10/18/19, 02:53:00.860 [NOTICE] Bootstrapped 15% (handshake_done): Handshake with a relay done

10/18/19, 02:53:00.861 [NOTICE] Bootstrapped 20% (onehop_create): Establishing an encrypted directory connection

10/18/19, 02:53:01.147 [NOTICE] Bootstrapped 25% (requesting_status): Asking for networkstatus consensus

10/18/19, 02:53:01.431 [NOTICE] Bootstrapped 30% (loading_status): Loading networkstatus consensus

10/18/19, 02:53:03.186 [NOTICE] I learned some more directory information, but not enough to build a circuit: We have no usable consensus.

10/18/19, 02:53:03.475 [NOTICE] Bootstrapped 40% (loading_keys): Loading authority key certs

10/18/19, 02:53:03.820 [NOTICE] The current consensus has no exit nodes. Tor can only build internal paths, such as paths to onion services.

10/18/19, 02:53:03.820 [NOTICE] Bootstrapped 45% (requesting_descriptors): Asking for relay descriptors

10/18/19, 02:53:03.821 [NOTICE] I learned some more directory information, but not enough to build a circuit: We need more microdescriptors: we have 0/5700, and can only build 0% of likely paths. (We have 0% of guards bw, 0% of midpoint bw, and 0% of end bw (no exits in consensus, using mid) = 0% of path bw.)

10/18/19, 02:53:04.729 [NOTICE] Bootstrapped 50% (loading_descriptors): Loading relay descriptors

10/18/19, 02:53:05.456 [NOTICE] The current consensus contains exit nodes. Tor can build exit and internal paths.

10/18/19, 02:53:06.290 [NOTICE] Bootstrapped 56% (loading_descriptors): Loading relay descriptors

10/18/19, 02:53:07.361 [NOTICE] Bootstrapped 64% (loading_descriptors): Loading relay descriptors

10/18/19, 02:53:07.361 [NOTICE] Bootstrapped 71% (loading_descriptors): Loading relay descriptors

10/18/19, 02:53:07.362 [NOTICE] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits

10/18/19, 02:53:07.827 [NOTICE] Bootstrapped 80% (ap_conn): Connecting to a relay to build circuits

10/18/19, 02:53:07.965 [NOTICE] Bootstrapped 85% (ap_conn_done): Connected to a relay to build circuits

10/18/19, 02:53:08.262 [NOTICE] Bootstrapped 89% (ap_handshake): Finishing handshake with a relay to build circuits

10/18/19, 02:53:08.427 [NOTICE] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circuits

10/18/19, 02:53:08.429 [NOTICE] Bootstrapped 95% (circuit_create): Establishing a Tor circuit

10/18/19, 02:53:09.353 [NOTICE] Bootstrapped 100% (done): Done

10/18/19, 02:53:10.198 [NOTICE] New control connection opened from 127.0.0.1.

10/18/19, 02:53:10.364 [NOTICE] New control connection opened from 127.0.0.1.

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Screenshots of pages

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

# Peform a basic steganography encryption

Files:



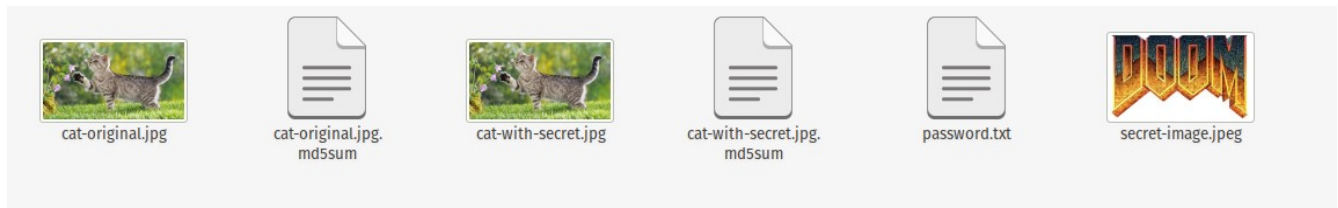Embedding a secret image with the password 'doom':

```
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑1 +1…2]-
L> steghide embed -cf cat-with-secret.jpg  -p doom -ef secret-image.jpeg
embedding "secret-image.jpeg" in "cat-with-secret.jpg"... done
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑1 +1…2]-
L>                                                                    (base)
```

Comparing file hashes:

```
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑1 +1…2]-
L> md5sum cat-with-secret.jpg > cat-with-secret.jpg.md5sum          (base)
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑1 +1…3]-
L> md5sum cat-original.jpg > cat-original.jpg.md5sum                (base)
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑1 +1…4]-
L> diff *.md5sum                                                    (base)
1c1
< 805a724aa60d663994046cdb885f4007  cat-original.jpg
---
> 4d020fd379161118166250ac8657ff4f  cat-with-secret.jpg
```
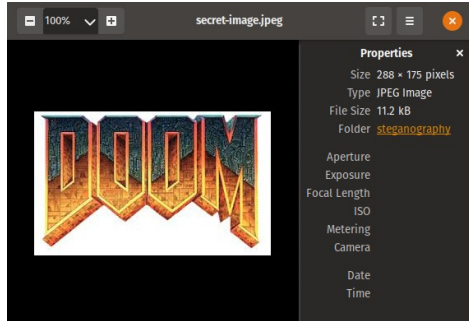
Cryptography Task
ITMS 448
Henry Post, hpost@hawk.iit.edu, Undergraduate

Extracting the secret file:

```
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +1]-
└> ls                                                              (base)
cat-original.jpg        cat-with-secret.jpg        password.txt
cat-original.jpg.md5sum  cat-with-secret.jpg.md5sum  secret-image.jpeg
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +1]-
└> rm secret-image.jpeg                                            (base)
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +2]-
└> ls secret-image.jpeg                                            (base)
ls: cannot access 'secret-image.jpeg' No such file or directory
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +2]-
└> man steghide                                                    (base)
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +2]-
└> steghide extract -sf cat-with-secret.jpg                        (base)
Enter passphrase: ↵
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +2]-
└> steghide extract -sf cat-with-secret.jpg -p doom               (base)
wrote extracted data to "secret-image.jpeg".
[henryfbp@pop-os]-(/m/h/m/G/s/I/a/c/w/steganography)-[git://master↑2 +1]-
└> xdg-open secret-image.jpeg                                      (base)
```

The secret image:



The image with the secret in it: