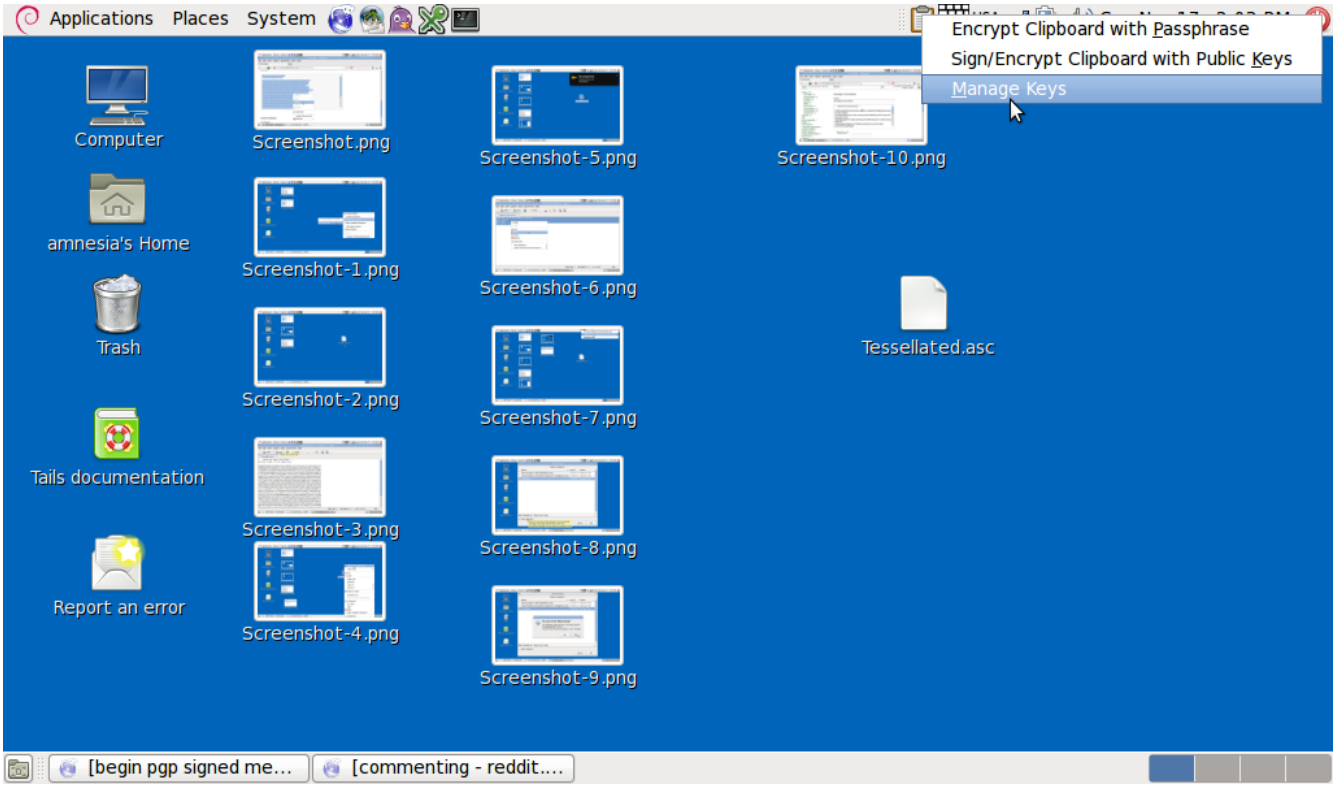
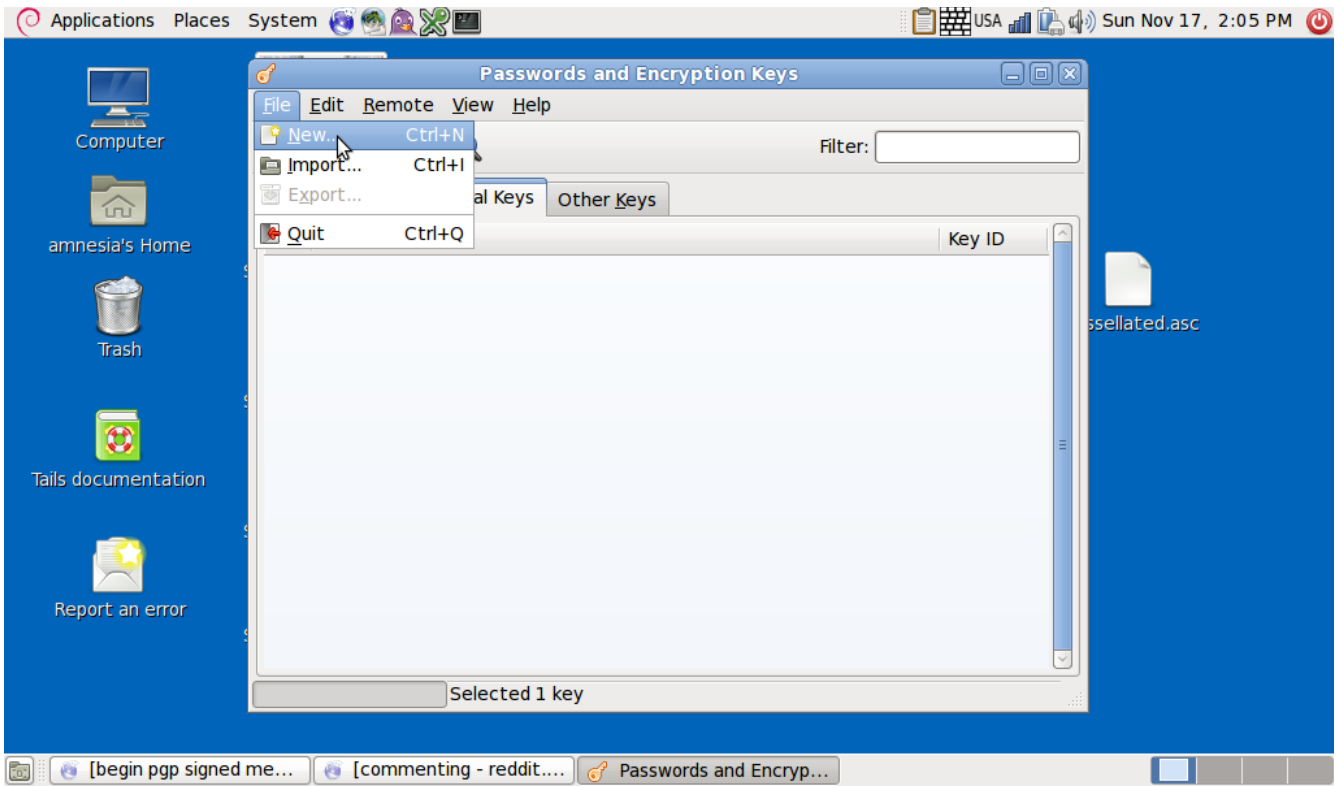
PGP on Tails Guide 4.22.17

https://www.reddit.com/r/SilkRoad/comments/1qtuy6/guide_for_the_pgp_tool_preinstalled_in_tails_with/ (edited from this source)

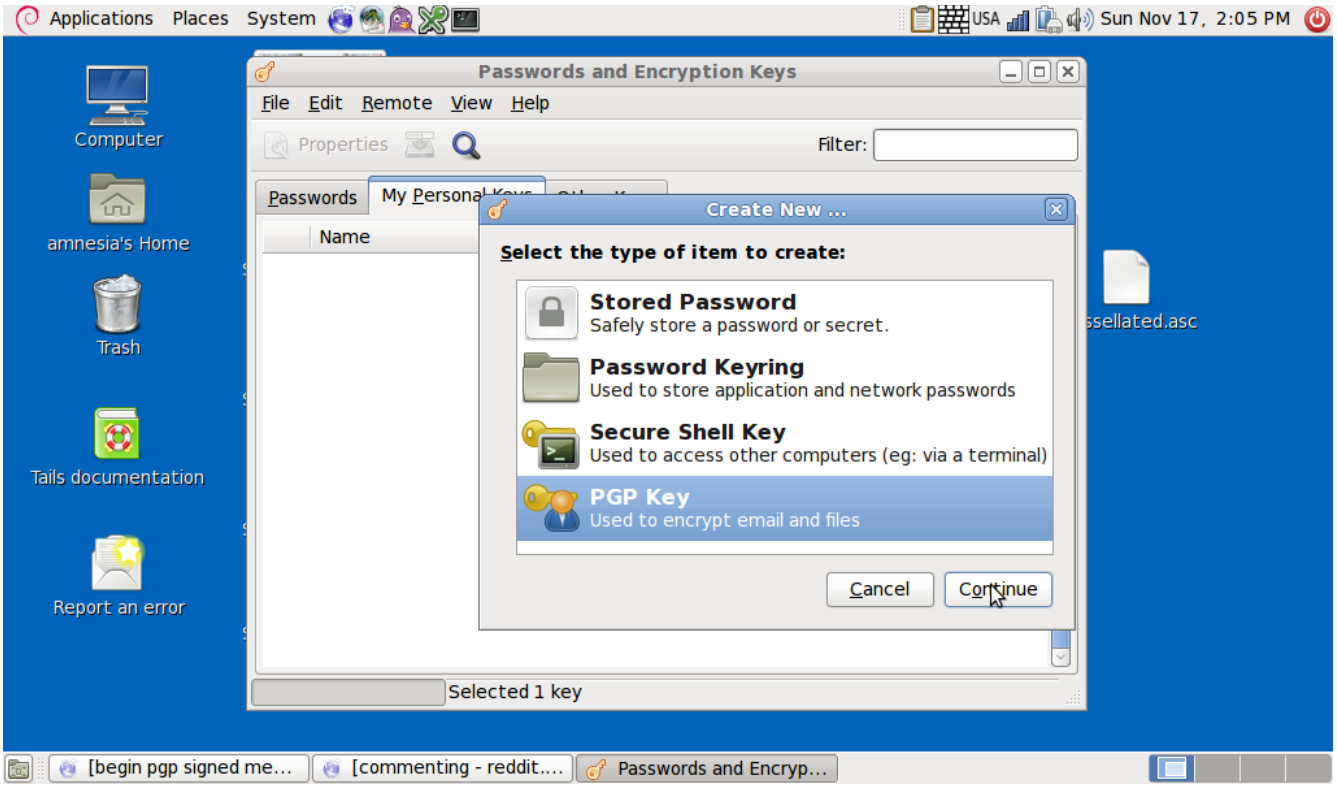
(1) **Create a pair of Keys**

-In order to receive messages, you have to create a pair of Public/Private keys. To do so, click on the Clipboard icon in the top bar and select "Manage Keys"

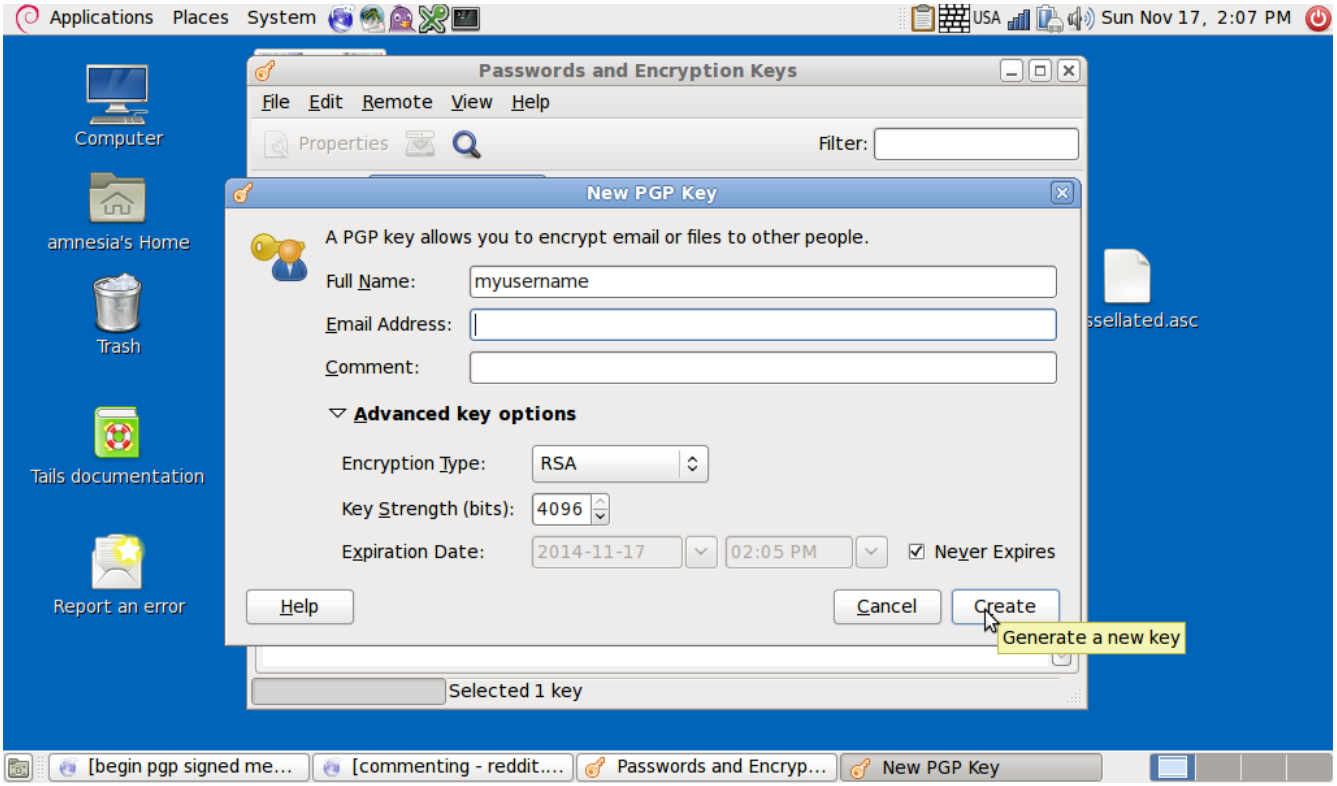




- Switch to the "My personal keys" tab. Click File -> New -> PGP Key

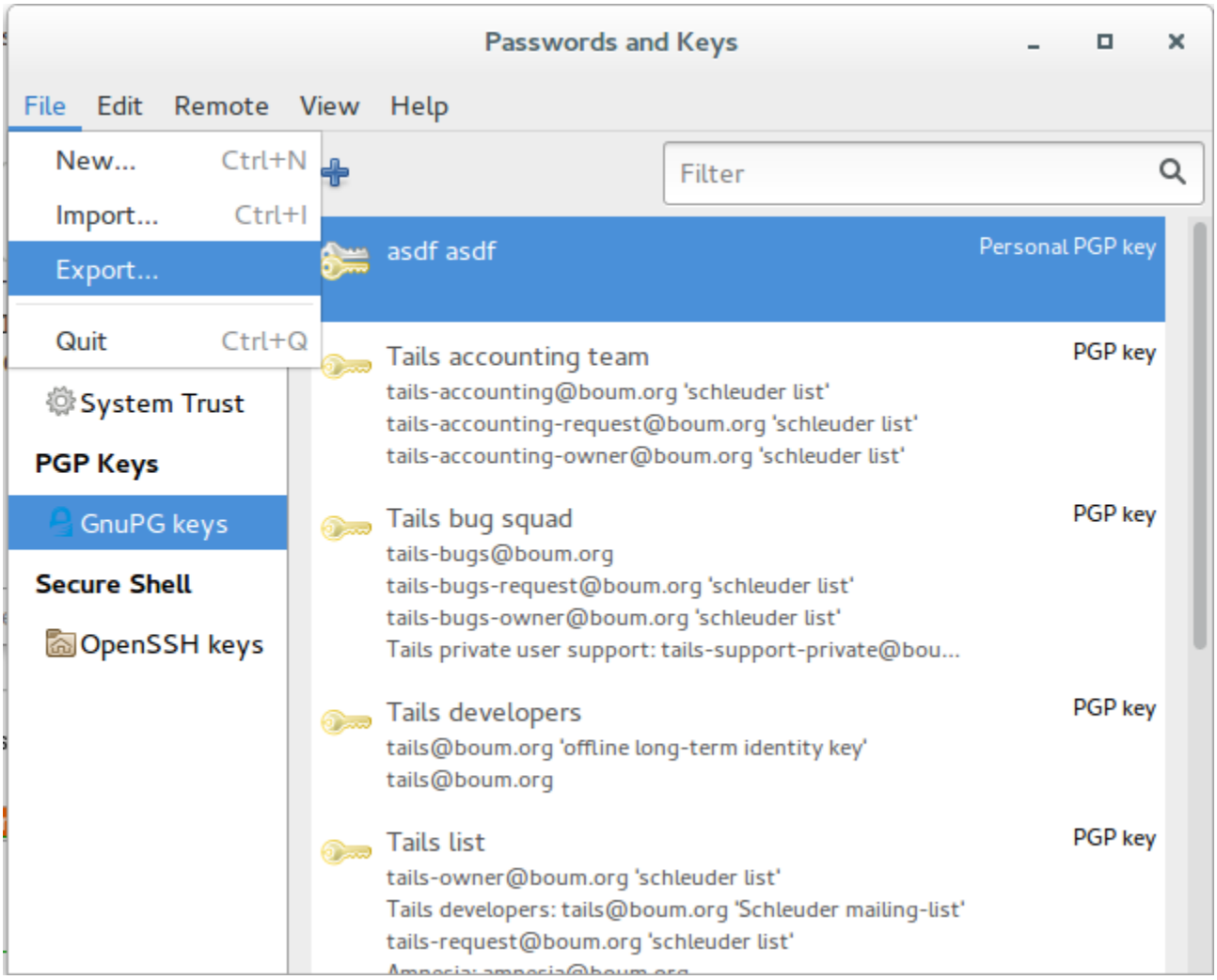


- You can choose *any* name. Key Strength 4096 should be enough, click Create. You can put your email address or not, depends on if you want your email attached to this key.

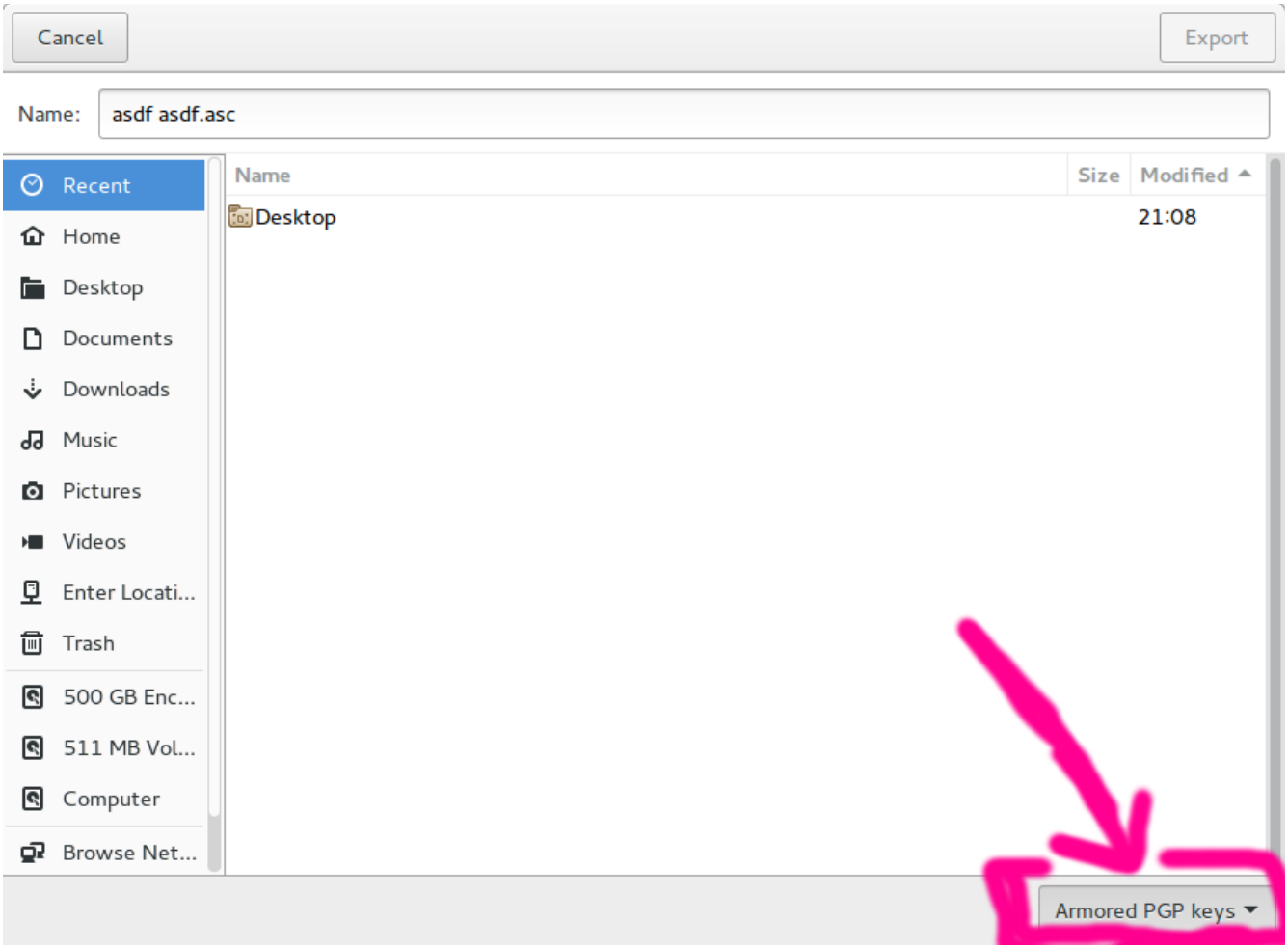


- Choose the friggin' passphrase and damn don't forget it, then wait for it to generate the key. Don't worry, it won't last long.

- To give someone else your public key, find your key in “GnuPG keys”. Then select your key and click “File” then “Export”. You can paste it wherever you need to.



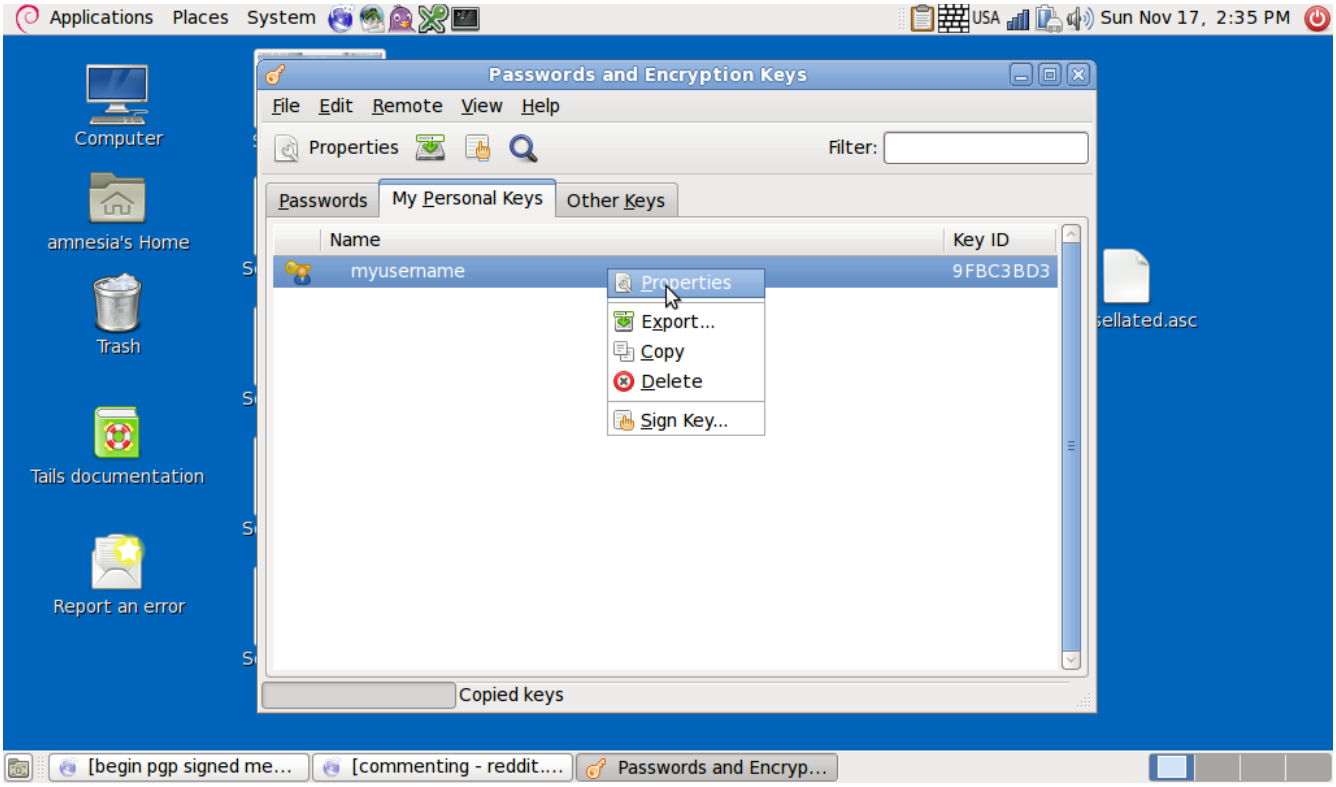
Make sure you save it as “Armored PGP keys”



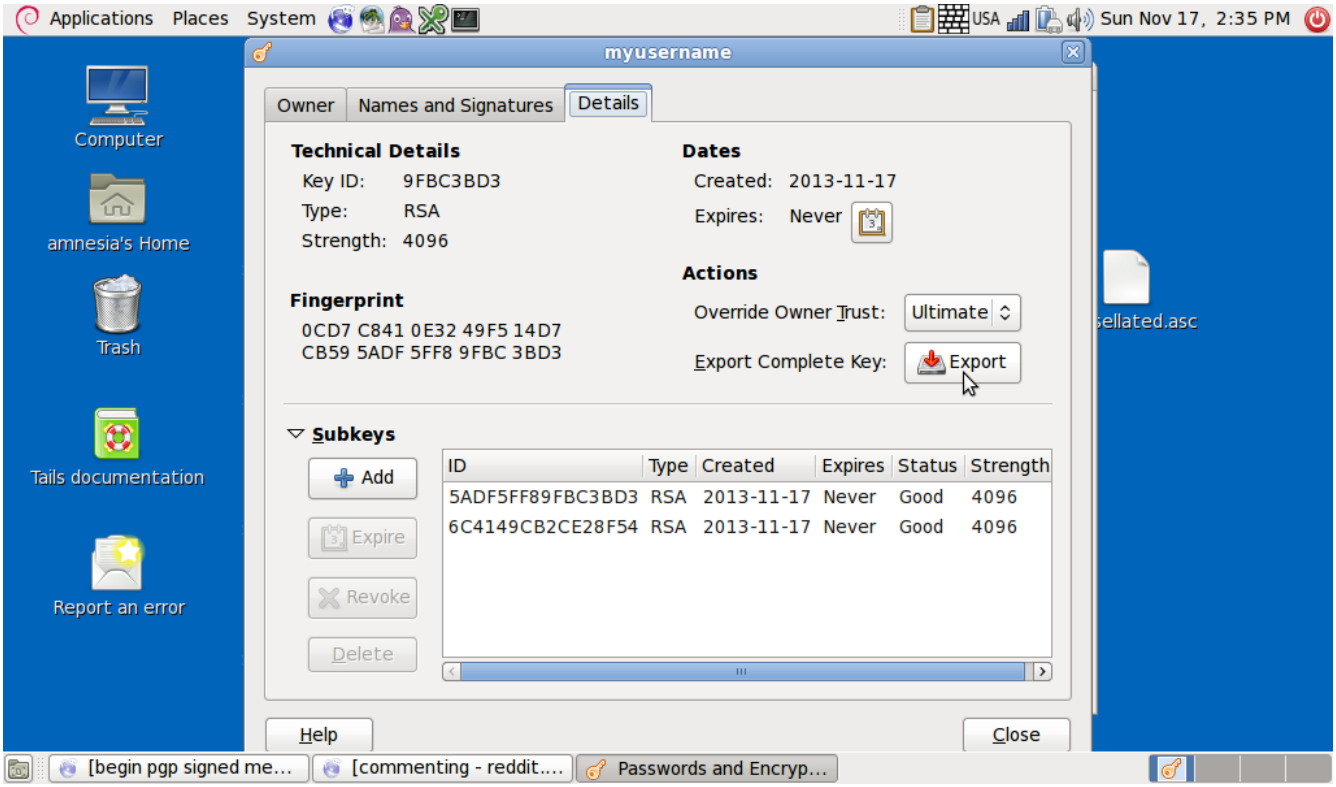
(2) **Exporting/Importing your private key**

If this is not a throwaway key, I highly recommend to export it. This is because if you don't, even when you create a new key using the same parameters it will never be the same key and you will never be able to decrypt your messages once it gets deleted. Now, do you remember the "Export" thing that appeared when you were copying your key? Yeah, forget that. That will only export your public key. You need to export the private one. So here's how to do it:

- On the "My personal keys" tab, right click on your key and select Properties.



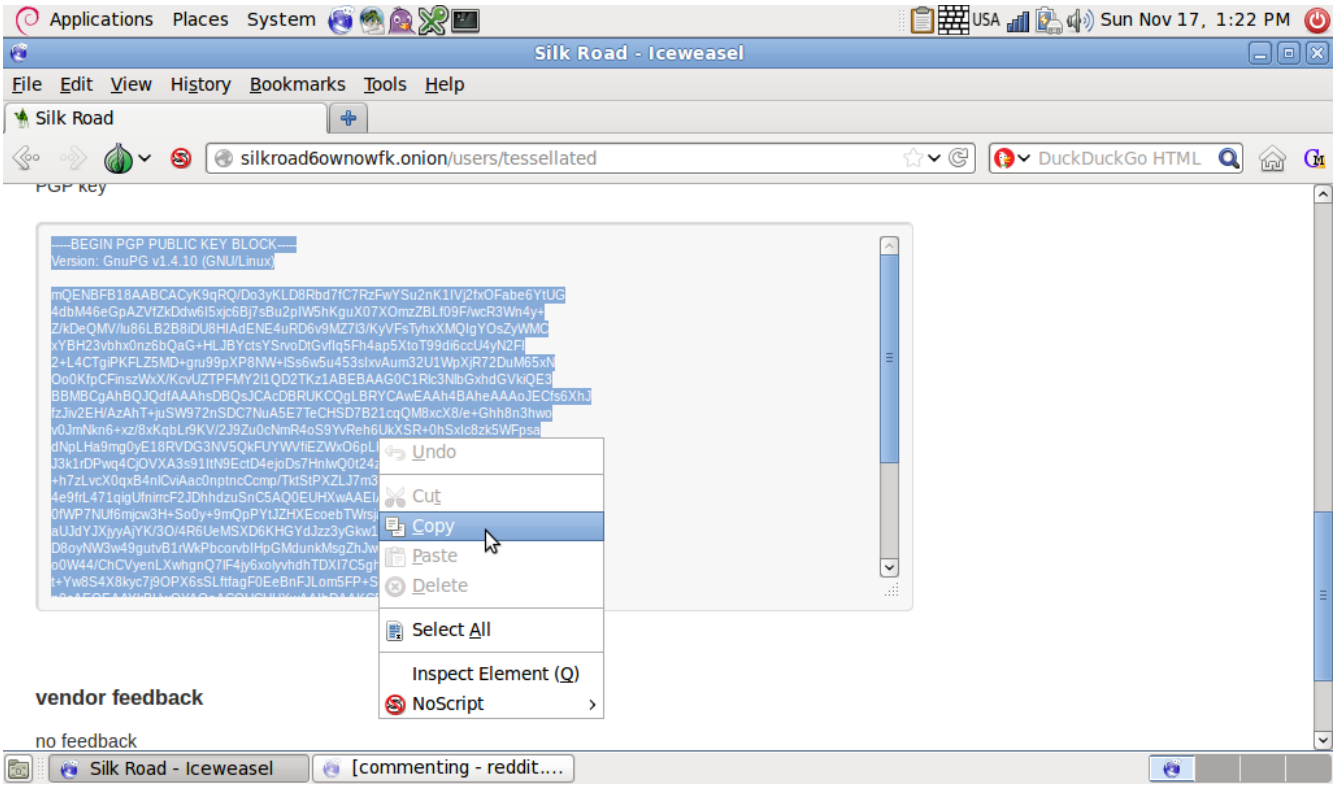
- Switch to the "Details" tab, then select "Export Complete Key". I'd suggest to save it on a USB stick or something else safe, that only you will use and that is easy to destroy.



-Every time you boot TAILS and the previous key has been deleted, you just plug the USB stick and right click on the exported keys you need to import, then select "Open with Import Key".

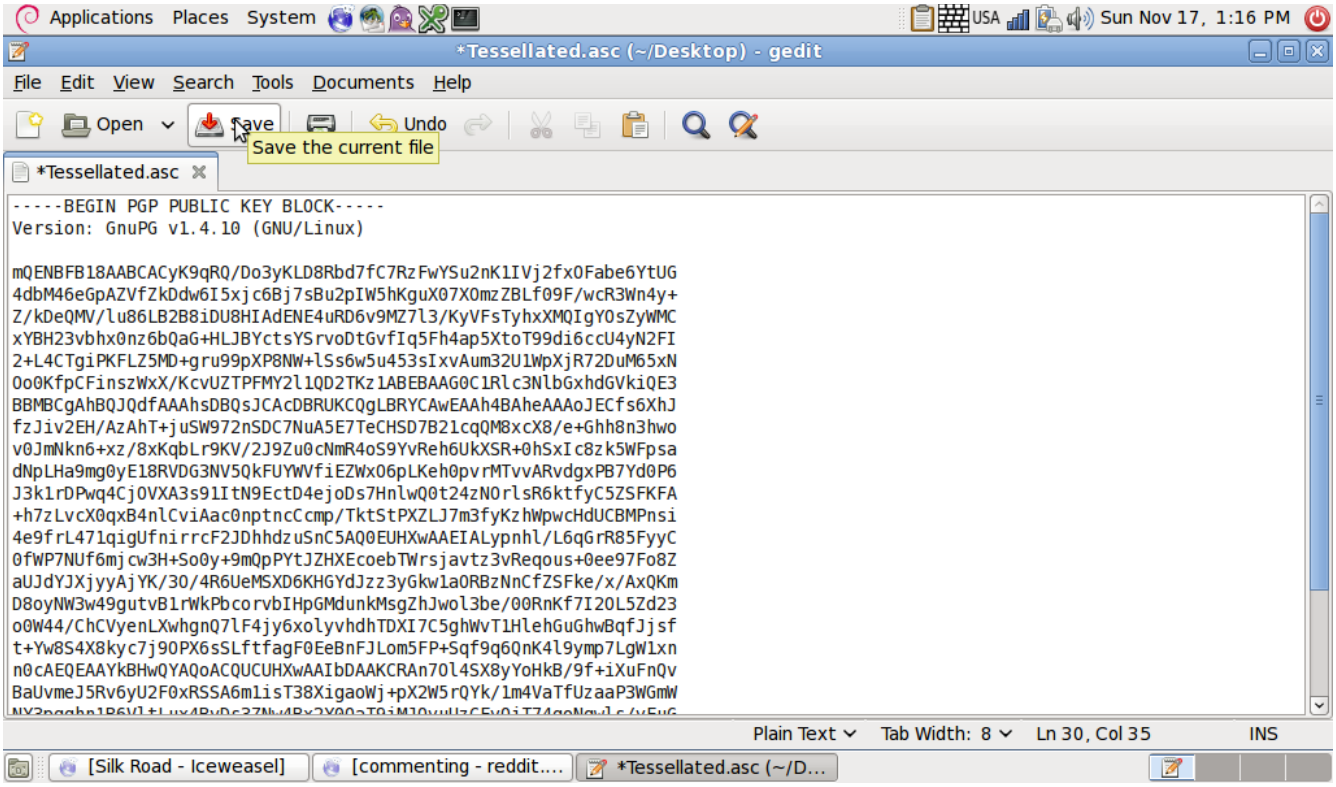
(3) **I want to message a friend.**

- Get your friend's public key, **including** the lines where it says "begin pgp public key block" and "end pgp public key block"

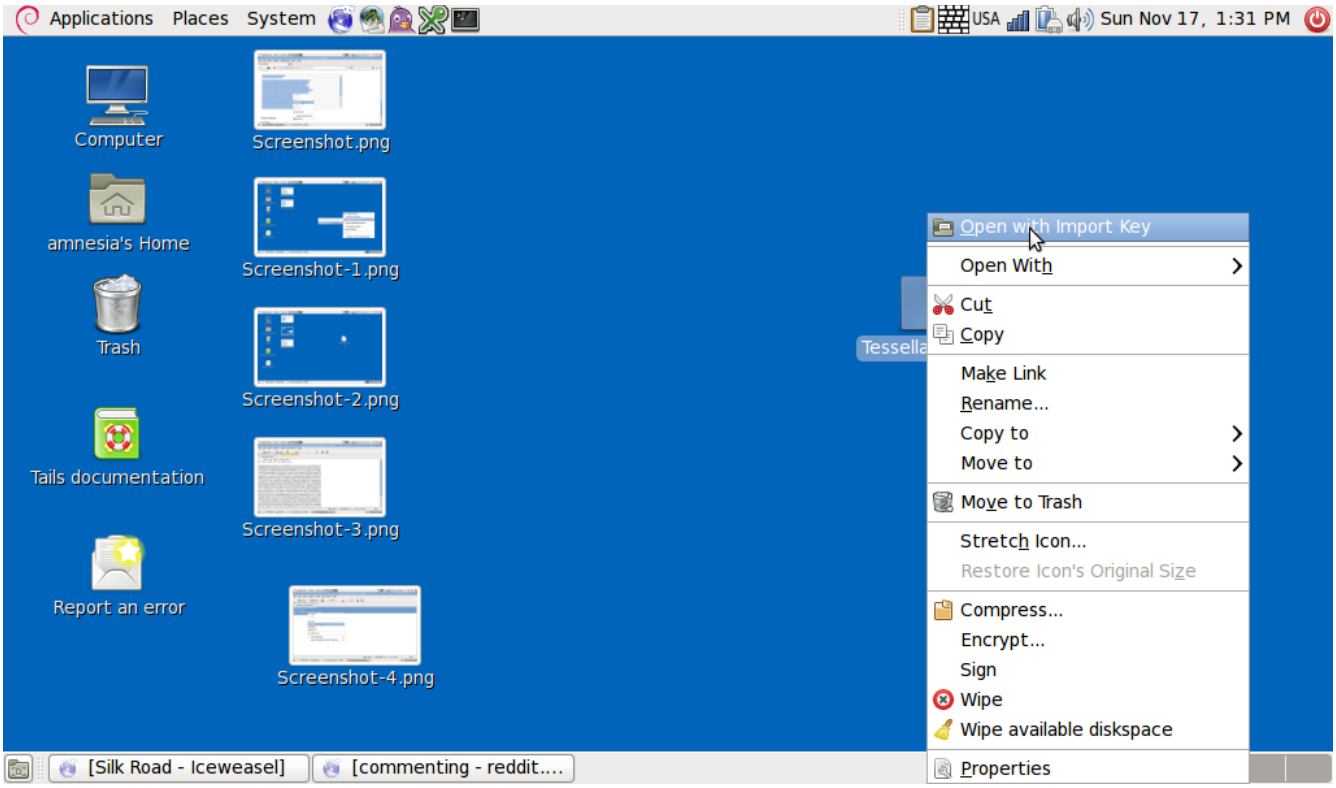


- Right click the file you just created, choose Open with -> gedit

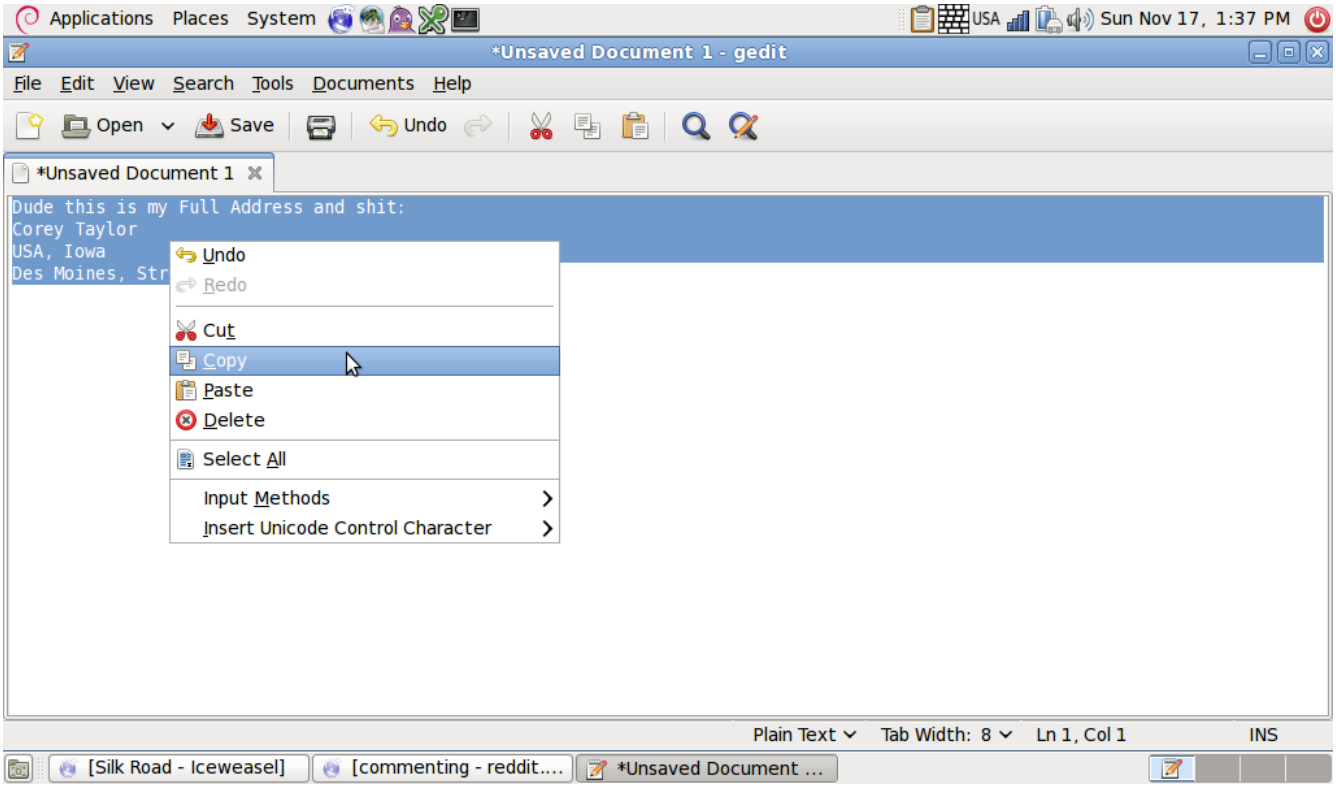
Right click inside the file, and Paste the key you just copied. Then save and name the extension .asc which makes things easier. Close!



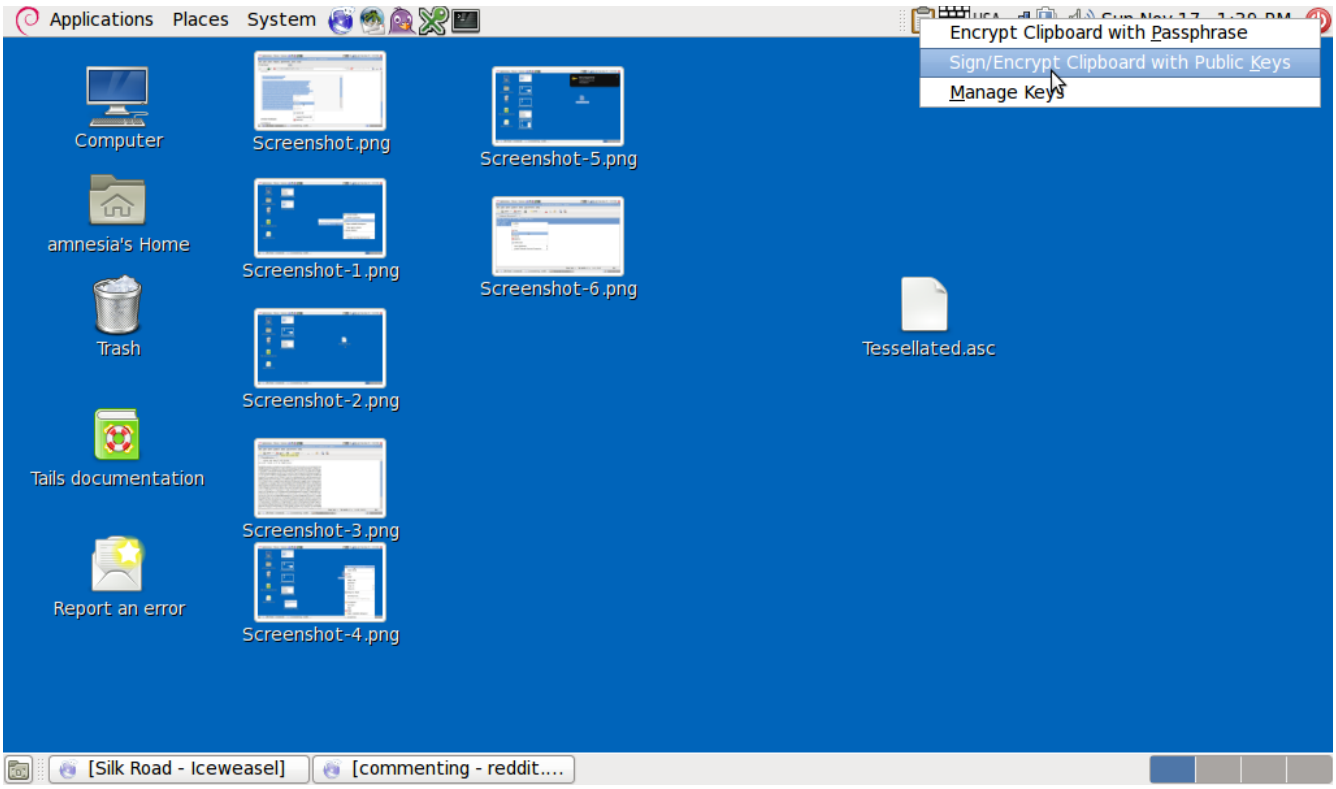
- Right click the file and select "Open with Import Key".



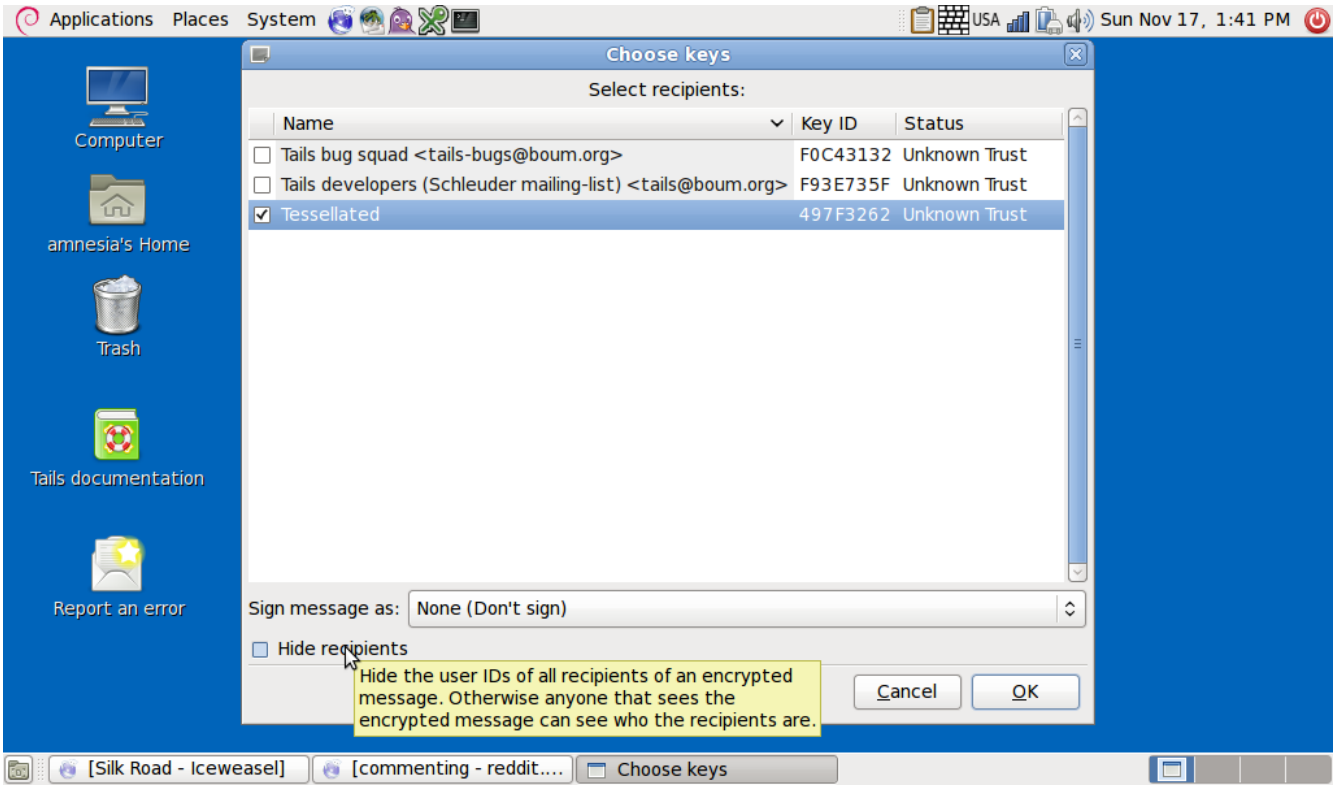
- Go into gedit or libre office and *just type* the message you like to send, then copy it.

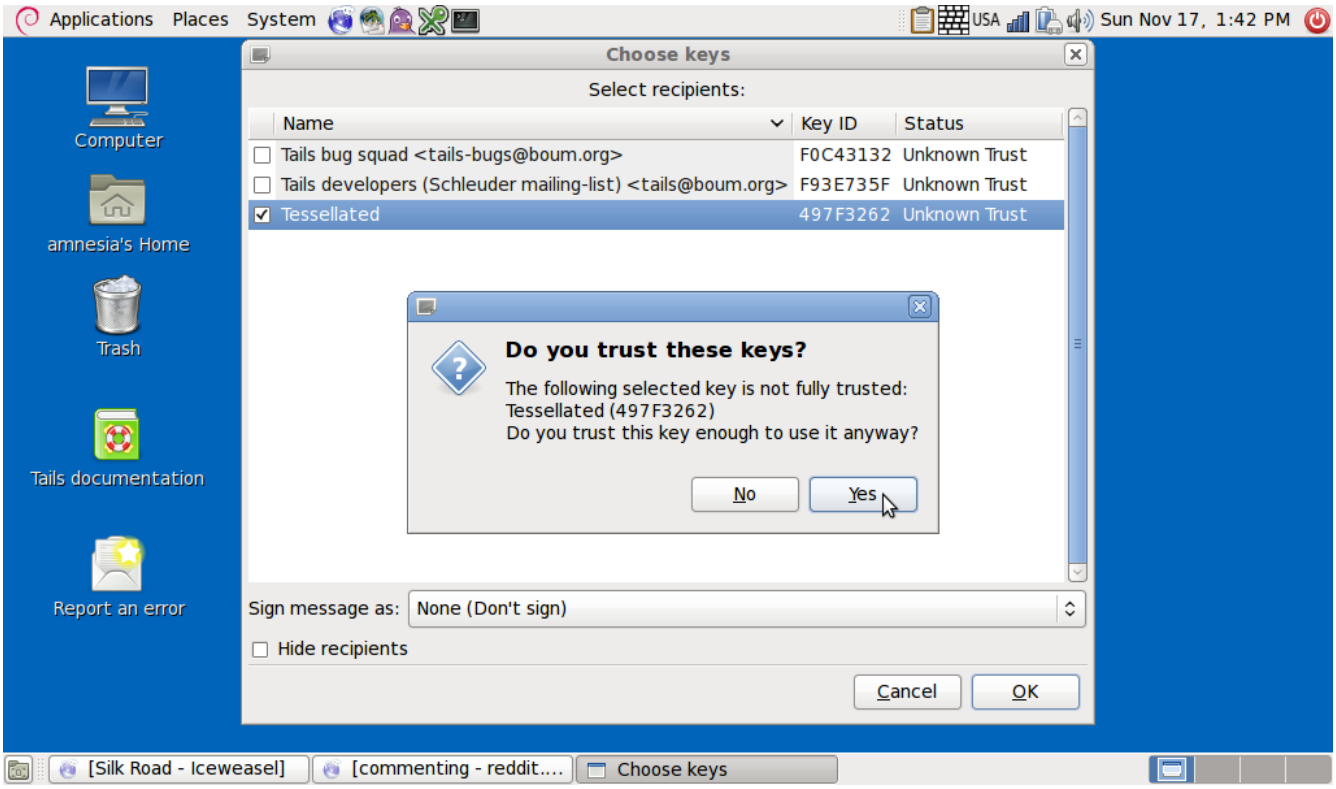


- In the top bar, click the clipboard icon, then select "Sign/Encrypt Clipboard with Public Keys". We're going to encrypt the message



- Select the friend you'd like to send the message to in the list (select "hide recipients" if you want that nobody sees who that message is sent to) and click OK, then Yes.

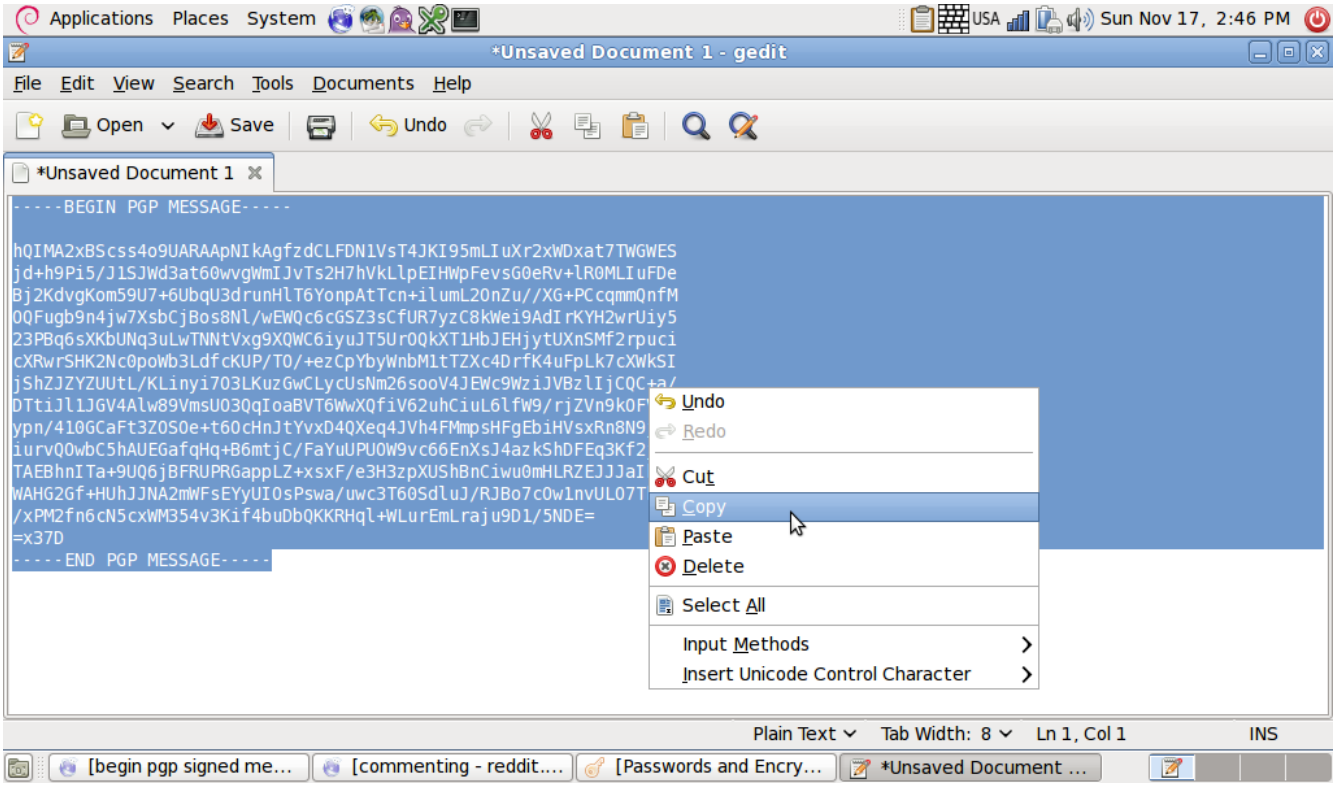




-If you yourself want to decrypt (read) the message, select *yourself* as a recipient as well!

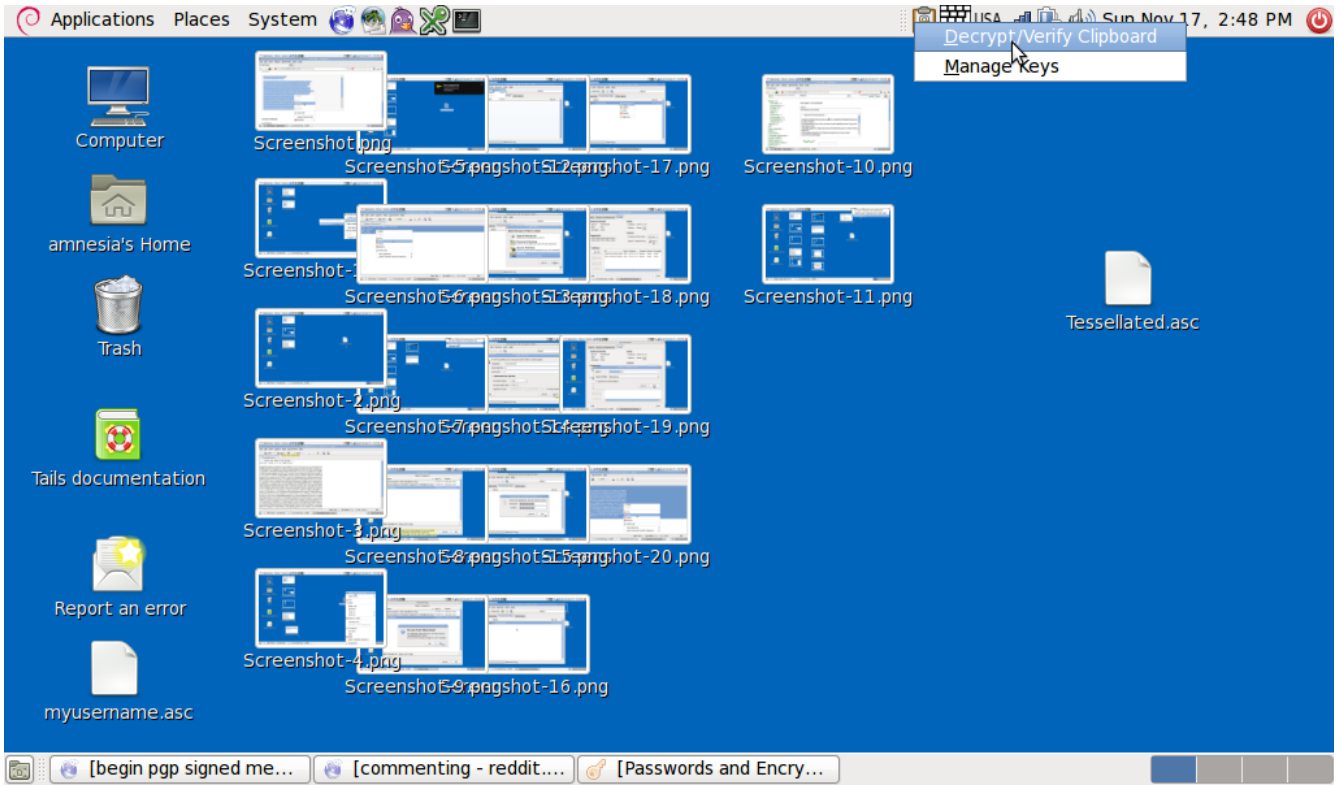
(4) **I want to decrypt a message that someone sent to me**

- Copy the message you received **including** the lines where it says "begin pgp message" and "end pgp message"

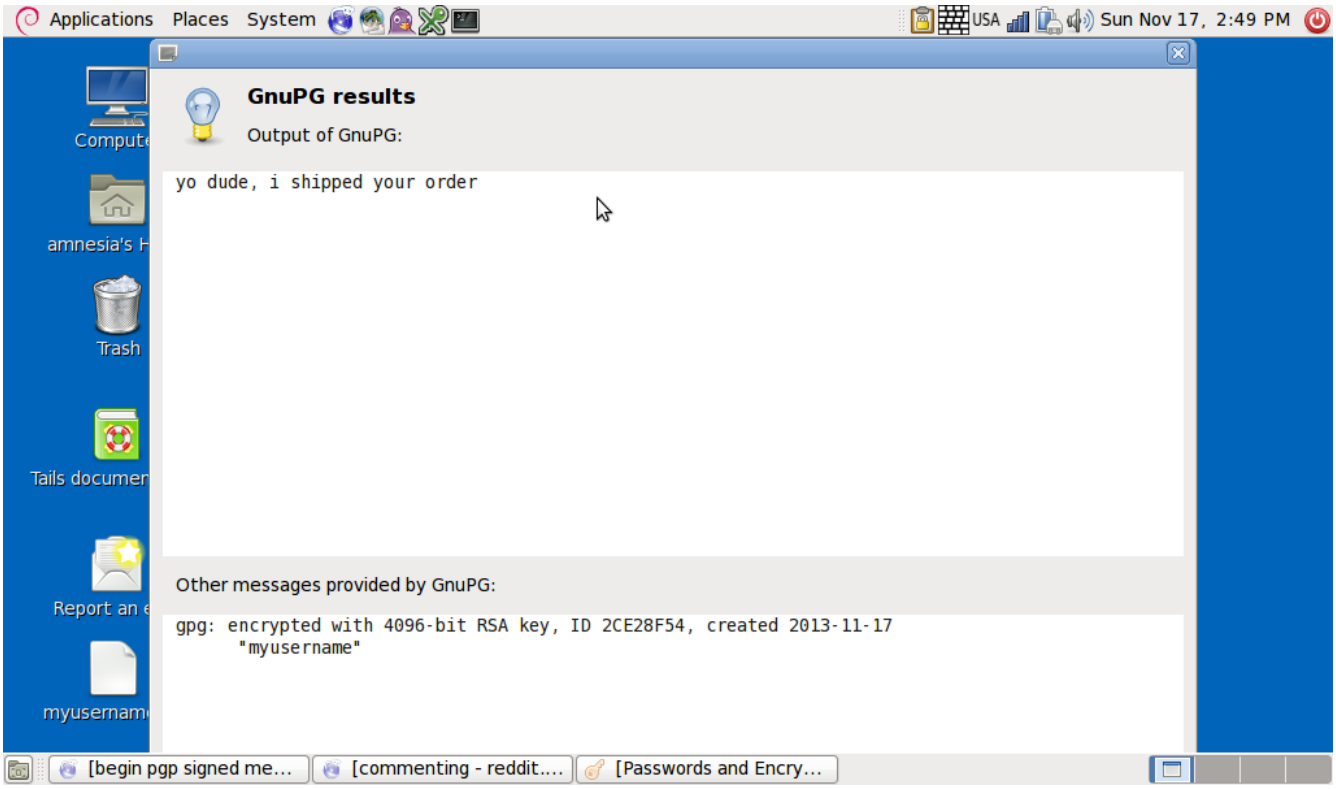


- In the top bar, select "Decrypt/Verify Clipboard"

://i.imgur.com/TfSuc38.png



- Select your key and insert your passphrase - A window will appear, showing you the decrypted message



Error?

- I'm trying to import a key or decrypt a message but it throws me an error.

Most of the times this is caused by text formatting. In fact, the PGP tool only accept perfectly formatted text.

-Have you imported your private key?

-Have you imported you friends' public key(s)?