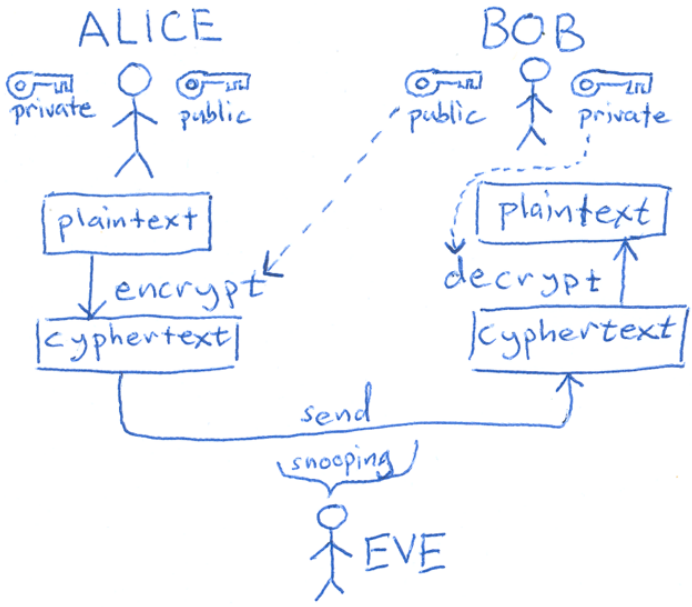
Note: This guide assumes you've set up your Ubuntu VM using the guides ***vm-v2-0 (Part-1)*** *and* ***vm-v2-0 (Part-2)****. If not, please complete those guides before proceeding.*

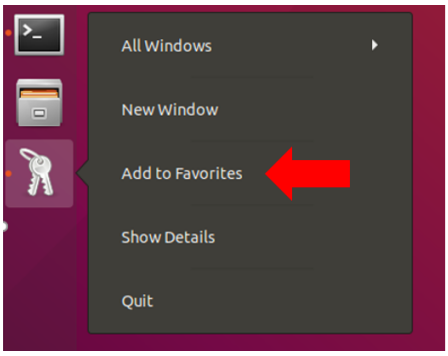
Public Key encryption works by creating a set of mathematically-related keys (long strings of characters) that permit encryption and decryption of files. A file encrypted with a public key can only be decrypted with the associated private key. In this way, we can share our public keys with anyone without being concerned about compromise, as long as we always keep our private keys secure.



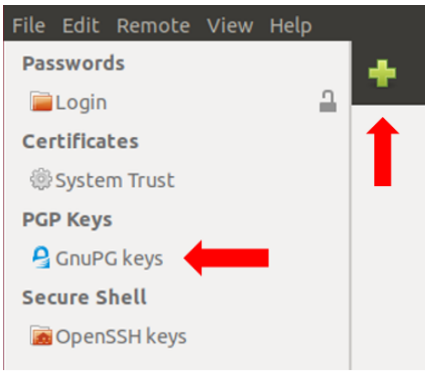
In this course, each of us will generate a key pair (public and private) and share our public keys with each other. We can then post encrypted files in a common, shared folder and only the intended recipients will be able to decrypt the files and read the contents.

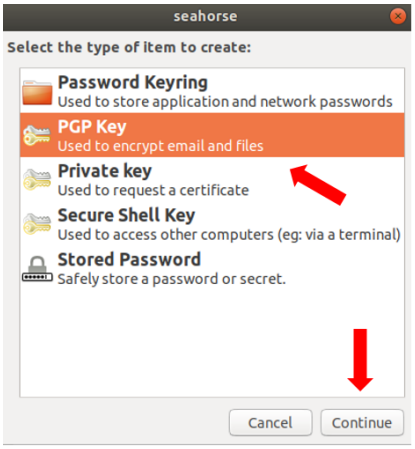
1. Start by opening Ubuntu's key manager. To get to it, click on the 3 x 3 grid of dots on the bottom left of your Ubuntu Desktop. Then, in the search box at the top of the window type, "***keys***". Look for the "***Passwords and Keys***" icon and click on it.

2. (OPTIONAL) Once the "***Passwords and Keys***" program starts, you can lock the icon to your application launcher to allow for quick access the next time you need it by right clicking on it and selecting "***Add to Favorites***".



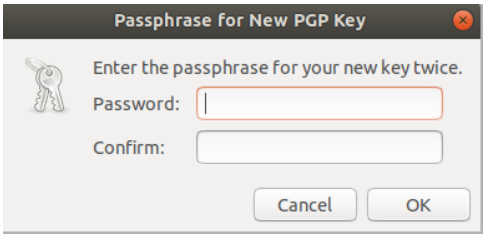
3. Click on the "***GnuPG keys***" item, then click on the green plus sign (**+**). In the pop-up window, select "***PGP Key***" and finally, click on "***Continue***"





4. In the next window, enter your full name, and USNA e-mail address. There's no need to adjust the "***Advanced key options***", but you can click on them to see what's there if you're curious; just don't change anything. When you're ready, click "***Create***"

5. Enter the same password you used for your VM login, and enter it again to confirm it. When you're ready, click on "***OK***".



6. Once your key pair is generated (it may take a little while), it will show up in your list of keys.

7. You're all set! Your instructor will guide you through importing public keys and encrypting / decrypting files.