GPG Install and Basic Use

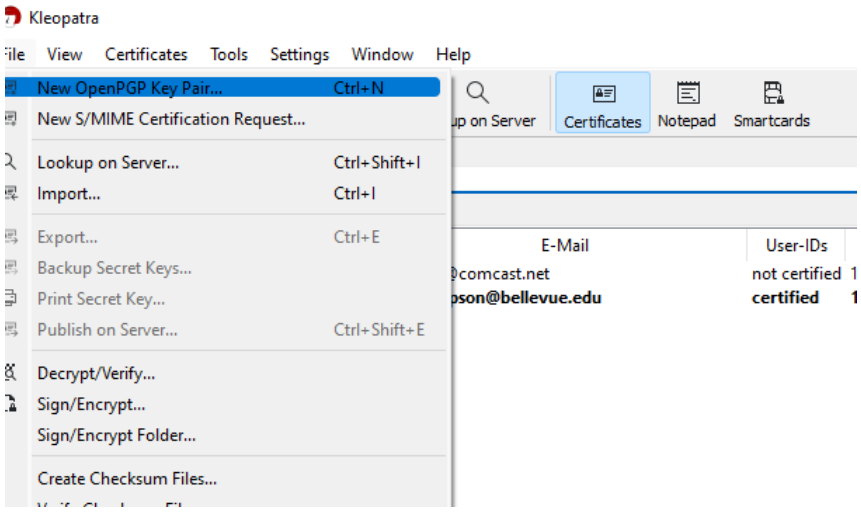
This assignment has five steps:

1. Download/install the application, create your key.
2. Send a message to your instructor that includes your public key. Don't worry, by default the public key is sent.
3. Wait for a message back from your instructor that includes their public key. Add it to your keyring.
4. Send your instructor an encrypted message.
5. Wait for a message back. Follow the instructions!

---

1. Download/install the application, create your key

- Get GPG4Win from https://www.gpg4win.org
- You'll see a message to donate. If you click on $0, you'll get a button to download without donating.
- Save in a local folder.
- Double click the downloaded file, this will start the install process.
- Select the language, welcome screen ->Next
- Continuing the install process, using defaults. May take a few minutes…….
- Reboot now or later, your choice.
- In Windows, look for recently added and find Kleopatra.
- Click on File menu item and select New OpenPGP KeyPair.



- Input your first and last name and BU email address, and generate a passphrase/password for your key pair.
- It's time to generate a passphrase/password to protect your key, type one in..
- Type it again to confirm...
  Don't forget your passphrase/password! You'll need it to decrypt messages from people who have your public key. You may want to write it down. You might get a message about an insecure passphrase.. it's your decision.
- You'll now see that a new OpenPGP certificate was created successfully.

---

2. Send your public key to the Professor.

Now it's time to send your public key to someone so that they can send you encrypted messages, which you decrypt with your private key.

- In Kleopatra, click on certificates. Right click on your key and select Export and save the key on your local machine, name it LastName_FirstName.asc (delete all other characters in the filename).
- Create a message to your professor, using either an email client or a web-based client and attach your .asc file. If you open your .asc file with a text editor, you'll see a long string of characters, with the words: Begin PGP Public Key Block.

  -----BEGIN PGP PUBLIC KEY BLOCK-----
  Version: PGP Desktop 9.6.0 (Build 214) - not licensed for commercial use: www.pgp.com
  H9+kWpd+M/baoj0wxBDFMMARkkh0dWZIIEBCURLlWCBQeUJpmKCoY
  tVUtnW+uEGe
  njTUxw55W0l7N4wbkwyaynfAenmDv0qXP9L/NoTWx8t7Yr4A49xKYsJAY
  uVqNlCv
  dG1i/VbvWSH/tmB7GFOaXs8Jqrl/JtyBWCKFz7OV7XX3tpAihZfNZTEP2N
  bXaxTw
  e24uBTztgBuGh3hIPSK5RU3tNxr+y5uURYEKPqsZO1PL+fgv6VKAzVhC5
  EvdjA==
  =h6s0.....

  -----END PGP PUBLIC KEY BLOCK-----

- At this point, you only have your own keys, you have no one else's public key.. we're going to add one now.

3. Receive a public key from the Professor.

Receiving a Public key (.asc File)

- If you receive a message with an .asc attachment, save the attachment
- Go to Kleopatra and click on the Import icon. A window pops up, asking you to select the key to import into your keyring. Click Open to continue.
- Once you've imported the key, it will show up in/on your keyring. If not, restart Kleopatra, then open the app.

---

4. Send an encrypted message to the Professor.

You are now ready to send an encrypted message to your Professor.

- In Kleopatra, click on the Notepad icon. Type your message. Click on Recipients and deselect Sign As:.
- Click Encrypt for Others and click on the people icon to the right. Select the professor's key and click OK. .
- The encrypted text will now show up in the same area you typed the message. At this point, you should see a block that begins with -----BEGIN PGP MESSAGE-----
- **If you still see plain text, try this section again.**
- Select all the text, include header and footer being careful not to include any spaces after the final --- Copy the text.
- Using BU Mail, create a new message, type in the addressee, and paste your encrypted text into the text area of the message.

---

5. Decrypting a digest from the Professor.

When your correspondent sends you an encrypted message (using your public key), the beginning of the message has the phrase:

-----BEGIN PGP MESSAGE----- ..

  - To decrypt the digest (using your private key) select all the text (with no spaces before the -----BEGIN, and no spaces after BLOCK-----), copy, and paste into the Notepad tab in the Notepad menu of the Kleopatra.

- Click on the Decrypt/Verify menu item.You may be asked to type in your passphrase before the message can be decrypted. Again, this may be cached.
- Follow the final instructions to finish the assignment.