EXPERIMENT-10

STUDY OF NETWORK SECURITY

Explore GPG tool to implement email security

Date of Performance:
Date of Submission:

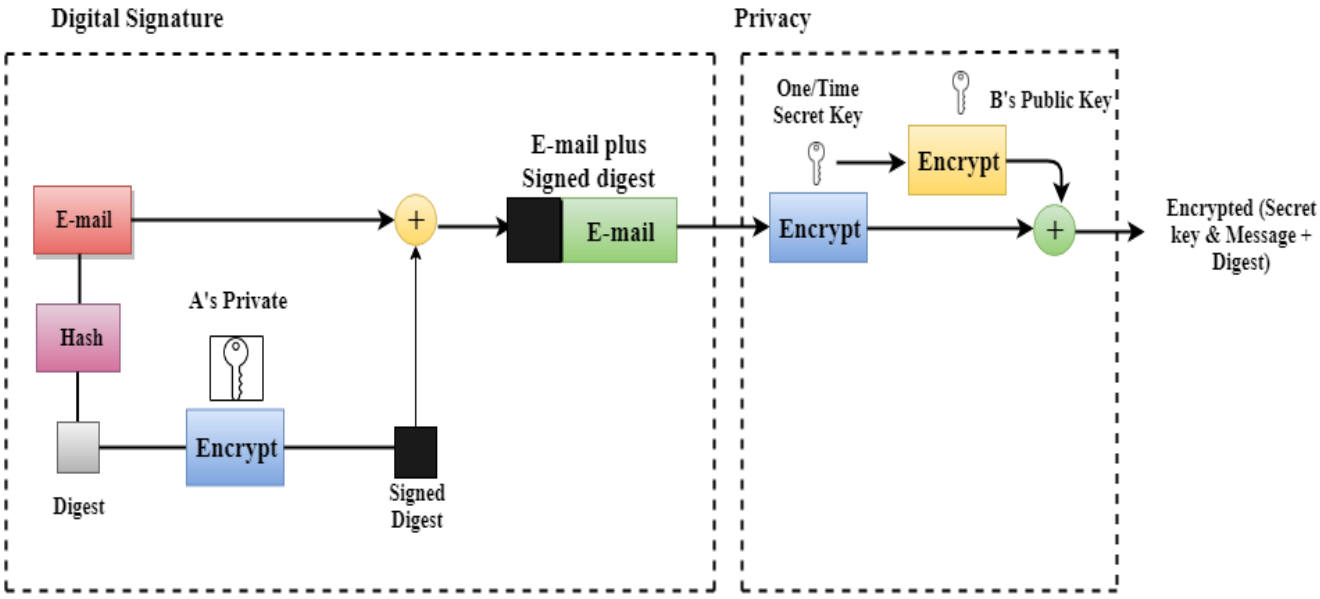
Aim:

" WRITE THE AIM"

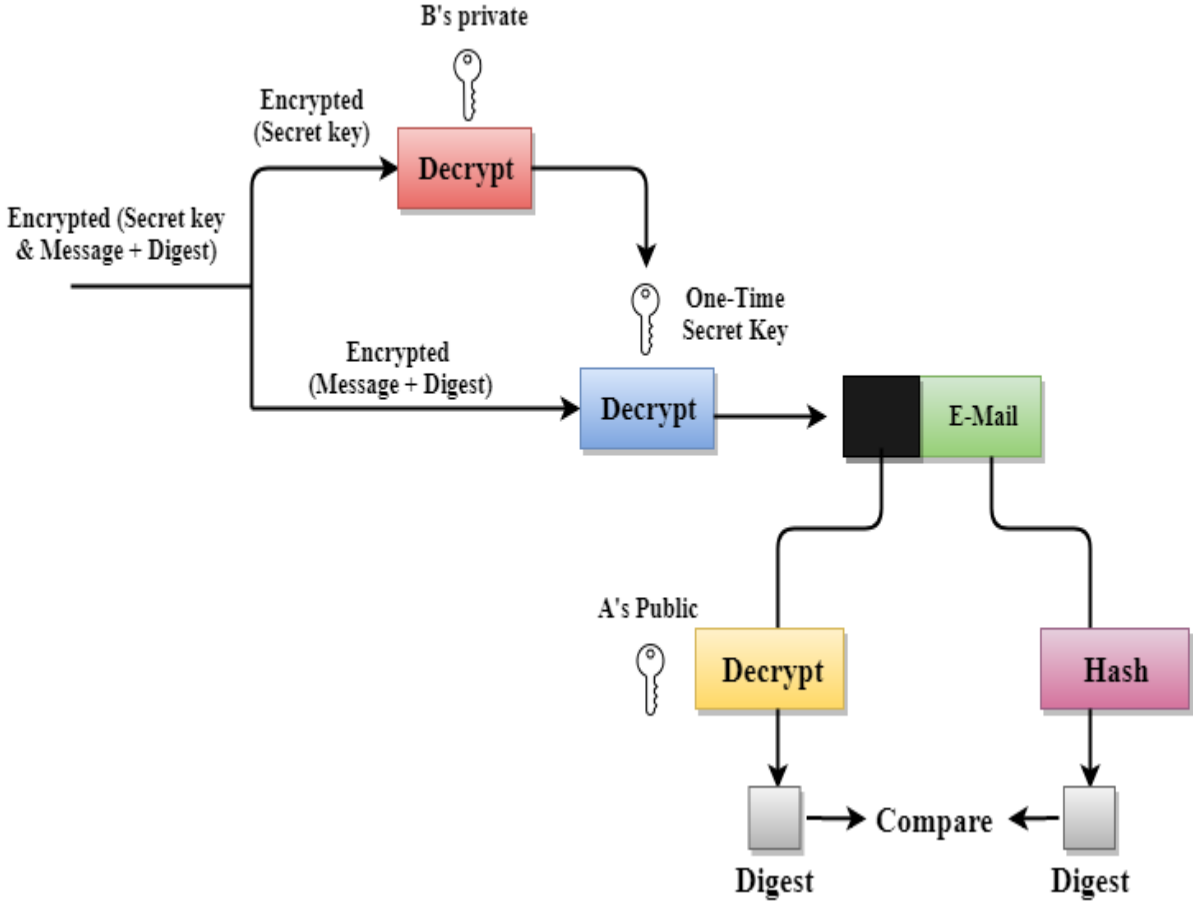
Theory:

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

PGP at Sender Site:



PGP at Receiver Site:

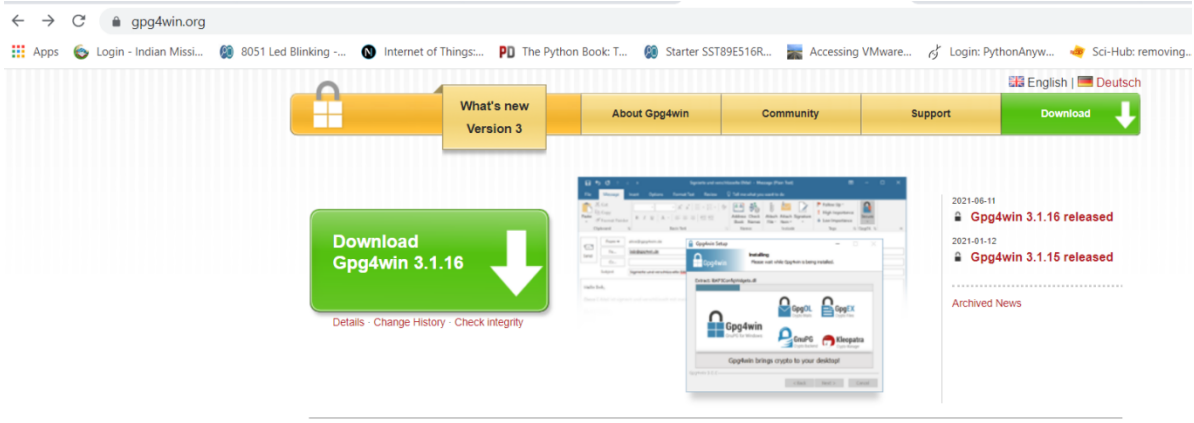


Procedure:

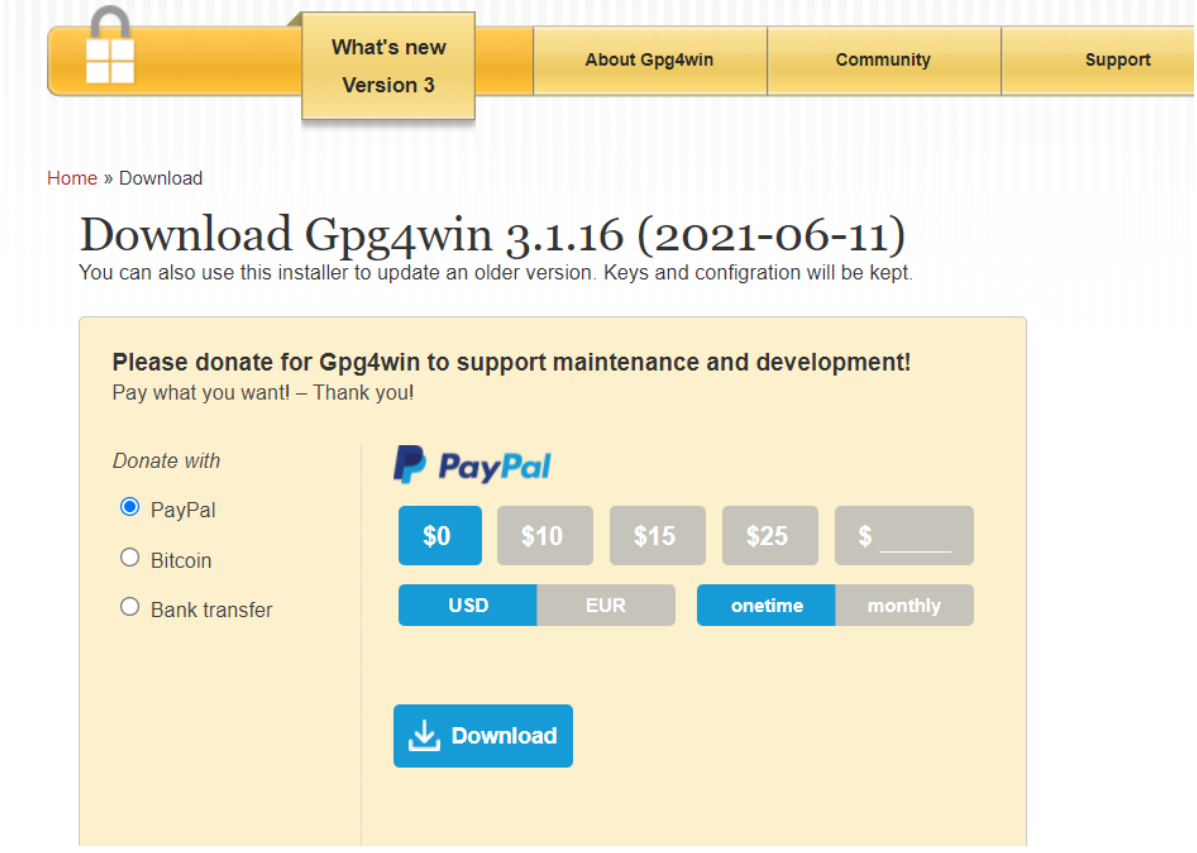
Step 1:

Install gPg4win Tool by clicking the link (https://www.gpg4win.org/thanks-for-download.html)

Click Download



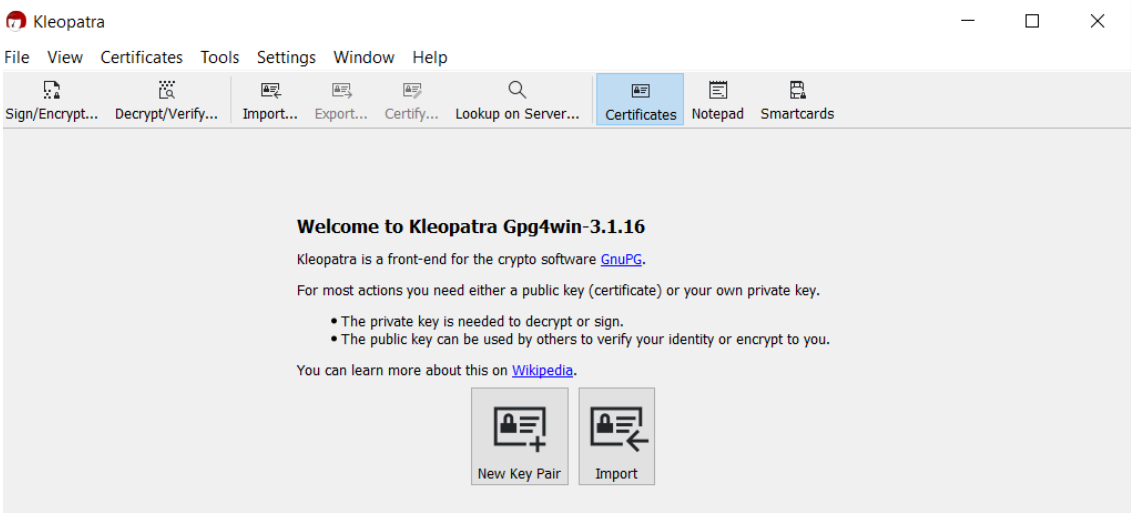
Click on 0 dollar and download



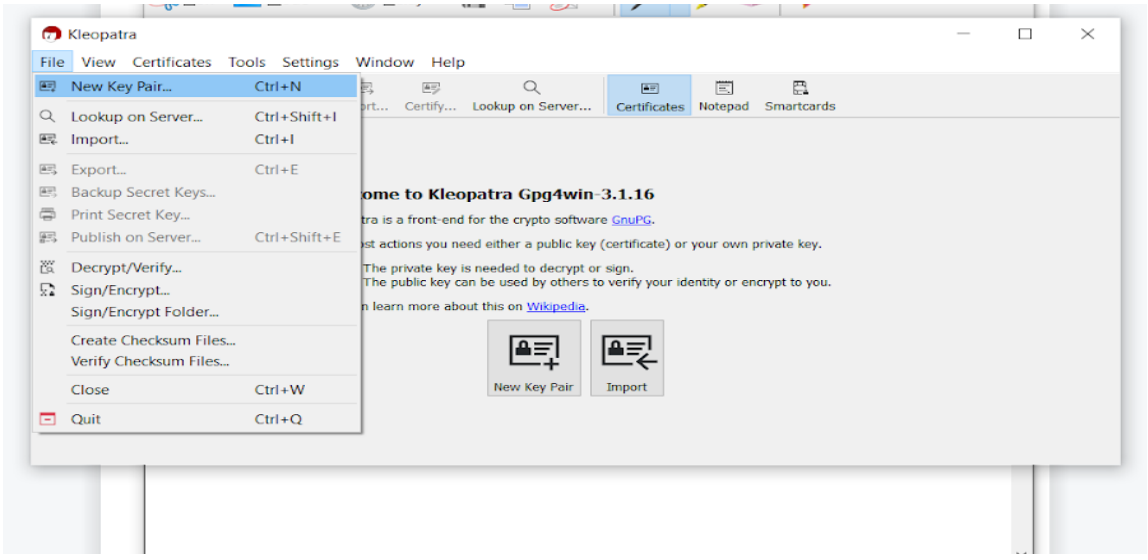
Click ok ------> Next ------> Select GPA and Browser Integration -----> Install -----> Finish

Step 2:

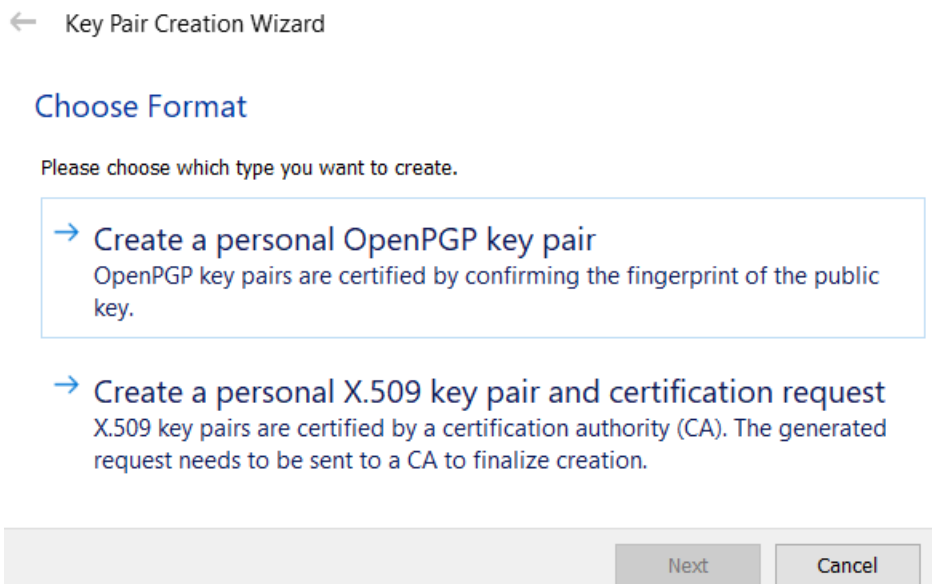
Click Kleopatra Software



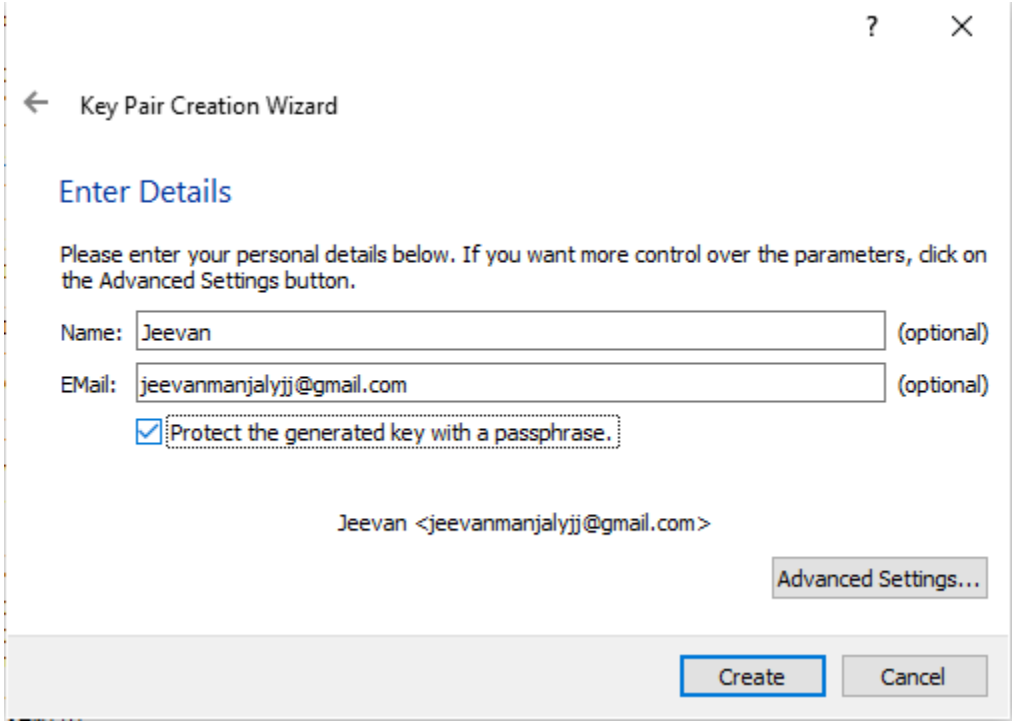
Click on File ------> New Key Pair



Select Create a OpenPGP Key Pair

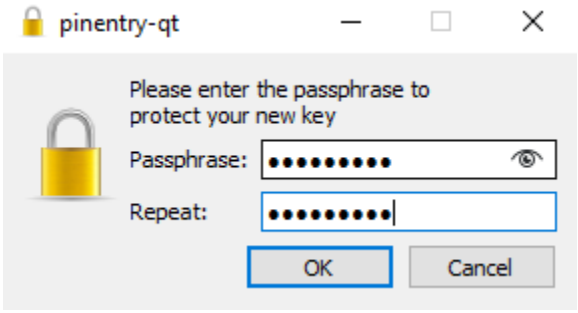


Click Next and give User name “your name”
Mail as “yourname@gamail.com”



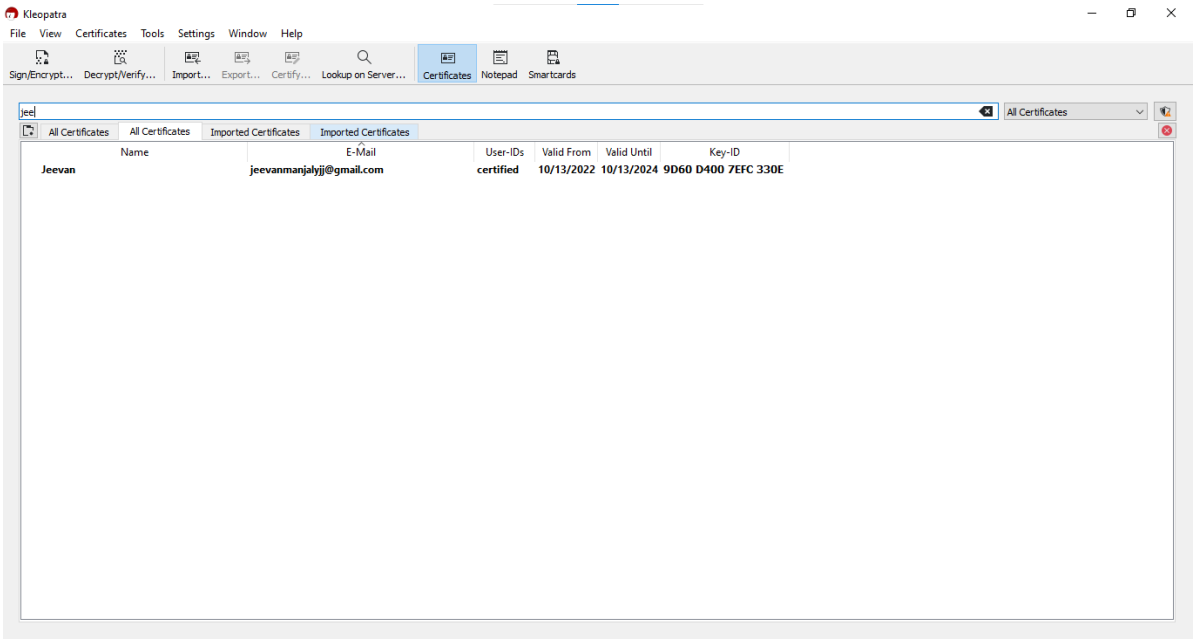
Click on **Protect the generated key with a passphrase**

Give the password

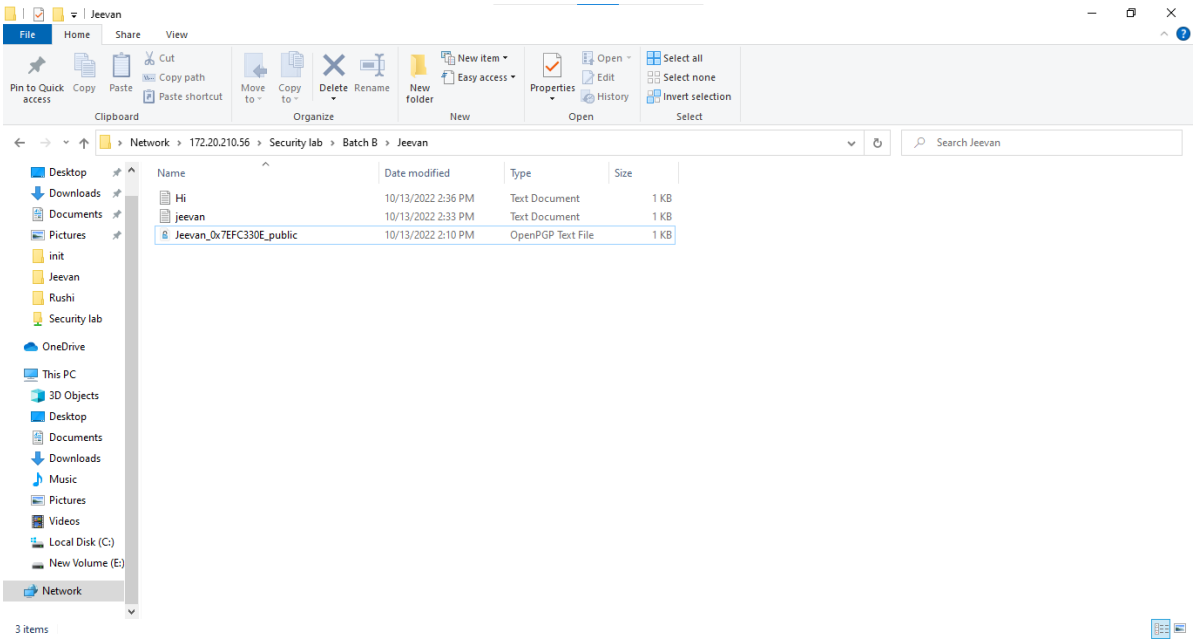


Key pair will be created Successfully.

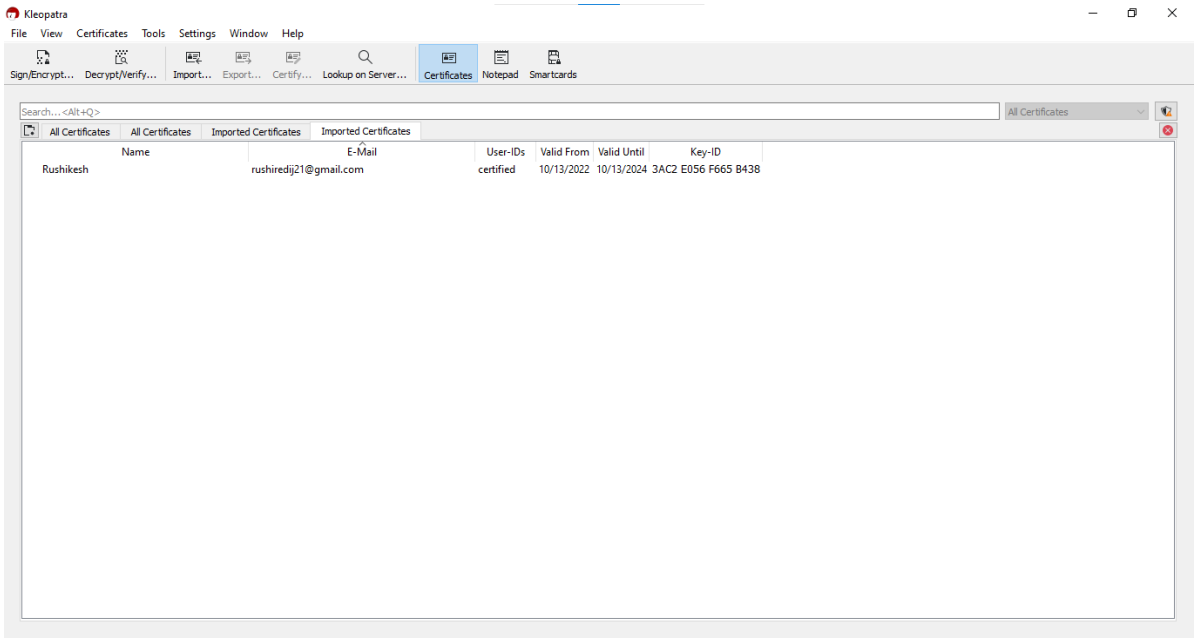
Step 3: Kleopatra(save public key private key):



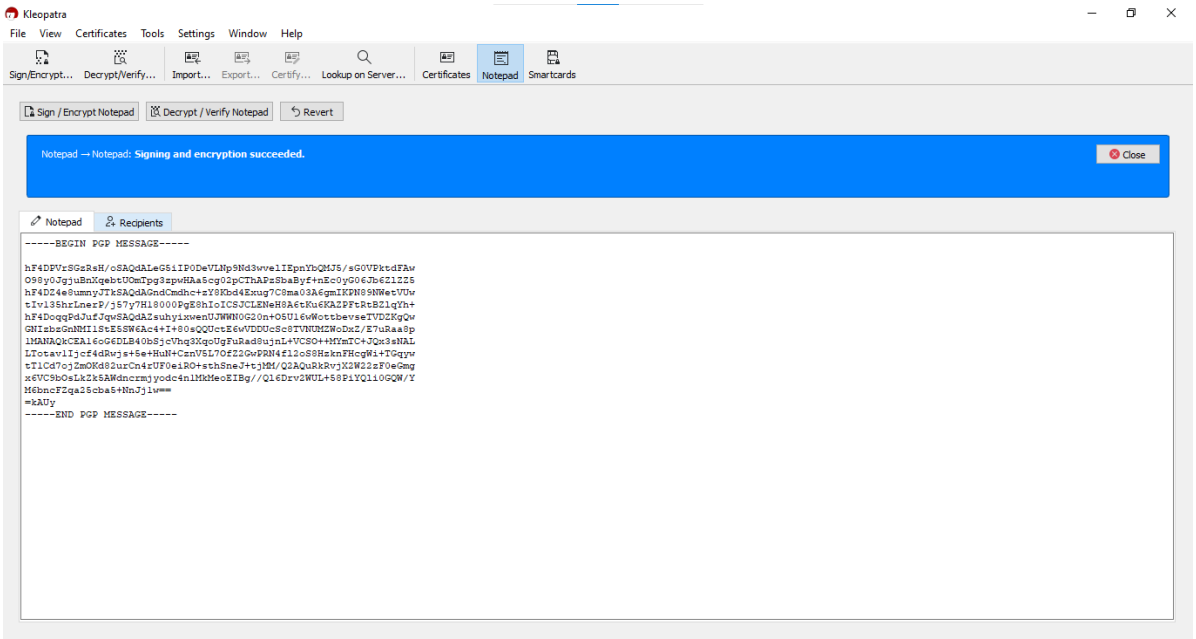
Paste the public key in folder:



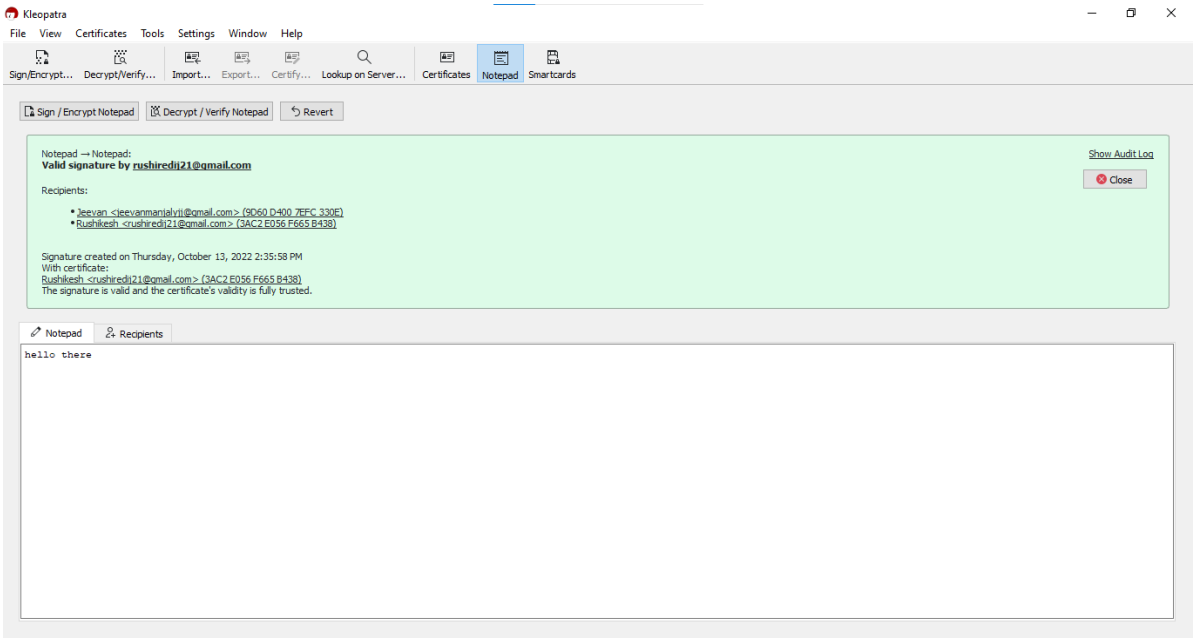
Go to the kleopatra software and click import and select the public key of the user



Click notepad type message and encrypt with the users public key

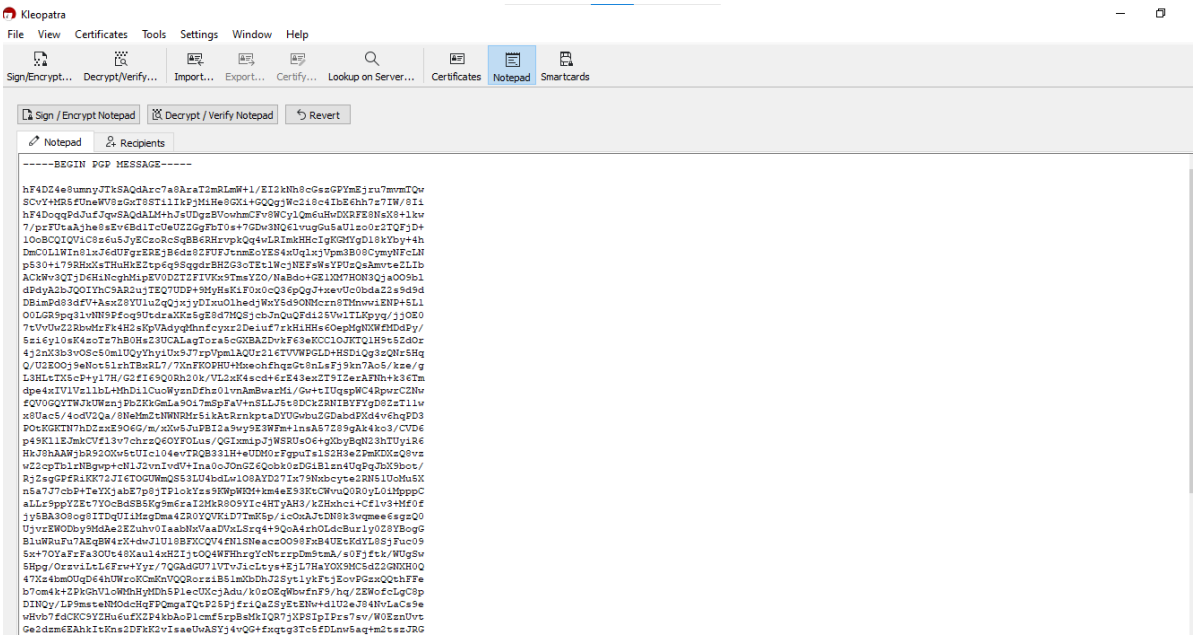


Step 6: Do the Same procedure for the Decryption



Output:

TASK : "ENCRYPT THE FILE WITH YOUR FRIENDS PUBLIC KEY and DECRYPT IT"


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Sign / Encrypt Notepad
Decrypt / Verify Notepad
Revert
Notepad
Recipients
-----BEGIN PGP MESSAGE-----
hF4DZ4e8umnyJTkSAQdArc7a8AraT2mRLmW+l/EI2kNh8cGszGPYmEjru7mvmTQw
SCvY+MR5fUneW8zGxT8STilIkPjMiHe8GXi+GQQgjWc2i8c4IbE6hh7z7IW/8Ii
hF4DoqqPdJufJqvSAQdALM+hJsUDgzBVowhmCFv8WCylQm6uHwDXRFE9NsX8+lkw
7/prFUtaAjhe8sEv6BdiTcfeUZZGgFbT0s+7GDw3HQ6lvugGu5aU1zo0r2TQfjD+
lOoBCQIQViC8z6u5JyECzoRcSqBB6RHrvpkQq4wLRImkHHcIgKGMYgD18kYby+4h
DmC0LlWIn8lxJ6dUFgrEREjB6dz8ZFUFJtnmEoYES4xUqlxjVpm3B08CymyNFcLN
p530+i79RHxXsTHuHkEZtp6q9SqqdrBHZG3oTEt1WcjNEFsWsYPUzQsAmvteZLIb
ACkWw3QTjD6HiNcghMipEV0DZTZFIVKx9TmsYZO/NaBdo+GEiXM7HON3QjaOO9bl
dPdyA2bJQOIYhC9AR2ujTEQ7UDP+9MyHsKiF0x0cQ36pQgJ+xevUc0bdaZ2s9d9d
DBimPd83dfV+AsxZ8YUluZqQjxjyDIxuOlhedjWxY5d9ONMcrn8TMnwwiENP+5Ll
O0LGR9pq3lvNN9PfcqUtdraXKz5gE8d7MQSjcbJnQuQFdi2SVwlTLKpyq/jjOE0
7tVvUwZ2RbwMrFk4H2sKpVAdyqHnfcyxr2Deiuf7rkHiHHs6OepMgNXWfMDdPy/
5zi6y1OsK4scYz7hBOHxZ3UCALagTora5cGXBAZDvkFG3eKCc1OJKTQlH9t5Zd0r
4j2nX9b3vOSc5OmlUQyYhyiUx9J7rpVpmlAQUr2lETVUWPGLD+HSD1Qg3zQNr5Hq
Q/U2EOOj9eNotSlrhTBxRL7/7KnFKOPHU+MxeohfhqxGt8nLsFj9kn7Ao5/kze/g
L3HLtTX5cP+yl7H/G2fI69Q0Rh20k/VL2xK4scd+6zE43exZT9IZerAFNh+k36Tm
dpe4xIV1VzllbL+MhDilCuoWyznDfhz0lvnAmBwarMi/Gw+tIUqspWC4RpwrCZNw
fQV0GQYTWJkUWznjPbZKkGmLa9Oi7mSpFaV+nSLLJ5t8DCkZRNIBYFYgD8ZzTllw
x8Uac5/4odV2Qa/8NeMmZtNWNRMr5ikAtRrnkptaDYUGwbuZGDabdPXd4v6hqPD3
POtKGKTN7hDZxxE9O6G/m/xXw5JuPBI2a9wy9E3WFm+lnsA67Z89gAk4ko3/CVD6
p49K1lEJmkCVfl3v7chrzQ6OYFOLus/QGIxmipjWSRUsO6+gXbyBqN23hTUyiR6
HkJ0hAAWjbR92OXw5tUIc104evTRQB33lH+eUDMOrFgpuTslS2H3eZPmKDXsQ8vz
wZ2cpTblxNBgwp+cNlJ2vnIvdV+Ina0oJOnGZ6QobO8D5L2n4UgPqJbX9bot/
RjZsgDfRiKK7JJI6TOGUWmQS53LU4bdLvlO8AYD27Ix79Nxbcyte2RN5lUoMu5X
n5a7J7cbP+IeYXjabE7p8jTPlokYzs9KWpWKM+km4eE93KtCWvuQ0R0yL0iMpppC
aLLr9ppYZEt7YOcBdSB5Kg9m6raI2MkR8O9YIc4HTyAH3/kZHxhci+Cflv3+Mf0f
jy5BA3O8cg8ITDqUIiMzgDma4ZR0YQVKiD7TmK5p/icOxAJtDN8k3wqmee6sgzQ0
UjvrEWODby9MdAe2EZuhv0IaabNxVaaDVxLSrq4+9QoA4rhOLdcBurly0Z8YBogG
BluWRuFu7AEqBW4rX+dwJlU18BFXCQV4fNlSNeaczOO98FxB4UEtKdYL8SjFuc09
5x+70YaFrFa3OUt48Xaul4xHZIjtOQ4WFHhrgYcNtrrpDm9tmA/s0Fjftk/WUgSw
5Hpg/OrzviLtL6Frv+Yyz/7QGAdGU7lVTvJicLtys+EjL7HaYOX9MC5d23GNXH0Q
47Xz4bmOUqD64hUWroKGmKnVQQRorziB5lmXbDhJZSytlykFtjEovPGzxQQthFFe
b7cm4k+ZPkGhVloWHbHyMDh5PlecUXcjAdu/k0zOEqWwfnF9/hq/ZEWofcLgC9p
DINQy/LP9msteNMOdcHqFPQmgaTQtP25PjfriQaZSyEtENw+diUZeJ84NvLaCs9e
wHvb7fdCKC9YZHu6ufXZP4kbAoP1cmf5rpBsMkIQR7jXPSIpIPrs7sv/W0EznUvt
Ge2dzm6EAhkItKns2DFkK2vIsaeUwASYj4vQG+fxqtg3Tc5fDLnw5aq+m2tszJRG
Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Sign / Encrypt Notepad
Decrypt / Verify Notepad
Revert
Notepad → Notepad:
Valid signature by rushiredji21@gmail.com
Show Audit Log
Close
Recipients:
Jeevan <jeevanmanjalvji@gmail.com> (9D60 D400 7EFC 330E)
Rushikesh <rushiredji21@gmail.com> (3AC2 E056 F665 B438)
Signature created on Thursday, October 13, 2022 2:35:58 PM
With certificate:
Rushikesh <rushiredji21@gmail.com> (3AC2 E056 F665 B438)
The signature is valid and the certificate's validity is fully trusted.
Notepad
Recipients
hello there