**ST. FRANCIS INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SECURITY LAB**

**Experiment – 11: Implementation of Email security**

**Aim:** To implement Email security.

**Objective:** After performing the experiment, the students will be able to understand security methods to achieve Email security.

**Lab objective mapped:** L502.6: Students should be able to apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** Windows OS, Gpg4win, Kleopatra

**Pre-Experiment Theory:**

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, whole disk partitions and to increase the security of e-mail communications.

OpenPGP is a non-proprietary format for authenticating or encrypting data, using public key cryptography. It is based on the original PGP (Pretty Good Privacy) software. Beginning in 1997, the OpenPGP Working Group was formed in the Internet Engineering Task Force (IETF) to define this standard that had formerly been a proprietary product since 1991. Over the past decade, PGP, and later OpenPGP, has become the standard for nearly all of the world’s signed or encrypted email. OpenPGP also defines a standard format for certificates which, unlike most other certificate formats, enables webs of trust.

GnuPG (also known as GPG) is a complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows you to encrypt and sign your data and communications. It features a versatile key management system, along with access modules for all kinds of public key directories. GnuPG is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. GnuPG also provides support for S/MIME and Secure Shell (ssh).

Gpg4win is a Windows version of GnuPG featuring a context menu tool, a crypto manager, and an Outlook plugin to send and receive standard PGP/MIME mails. The current version of Gpg4win is 4.2.0.

**Implementation:**

For implementation of Email security through GPG we will use Kleopatra. Kleopatra is a certificate manager and GUI for GnuPG. The software helps to store OpenPGP certificates and keys. It is available for Windows and Linux.

1. Download and Install Gpg4win from its official website [1]. Choose ‘Kleopatra’ as a key manager component during installation.
2. Open Kleopatra interface from desktop icon.
3. Create a new key pair (choose open PGP key pair if prompted)
4. Save the keys on the desktop and observe the keys.
5. Import your secret communication partner’s (your friend’s) key in Kleopatra.
6. Write your secret message in any word processing software. (e.g. Microsoft Word, notepad, WordPad etc.)
7. Encrypt this message file with recipient’s public key. Save and send it to the recipient through any preferred communication medium.
8. Decrypt and observe the message received by you.

**Output:**

Attach following screenshots (SS) as the output. Write a brief explanation for each.

1. Welcome window of Kleopatra interface.
2. SS with new key pair created.
3. SS of private and public key.
4. SS with imported public key.
5. SS with message and encrypted message.
6. SS with message decryption.

**Post Experimental Exercise-** *(to be handwritten on journal sheets.)*

Write answers to following questions.

1. What is PGP?
2. What is S/MIME?

**Conclusion:**

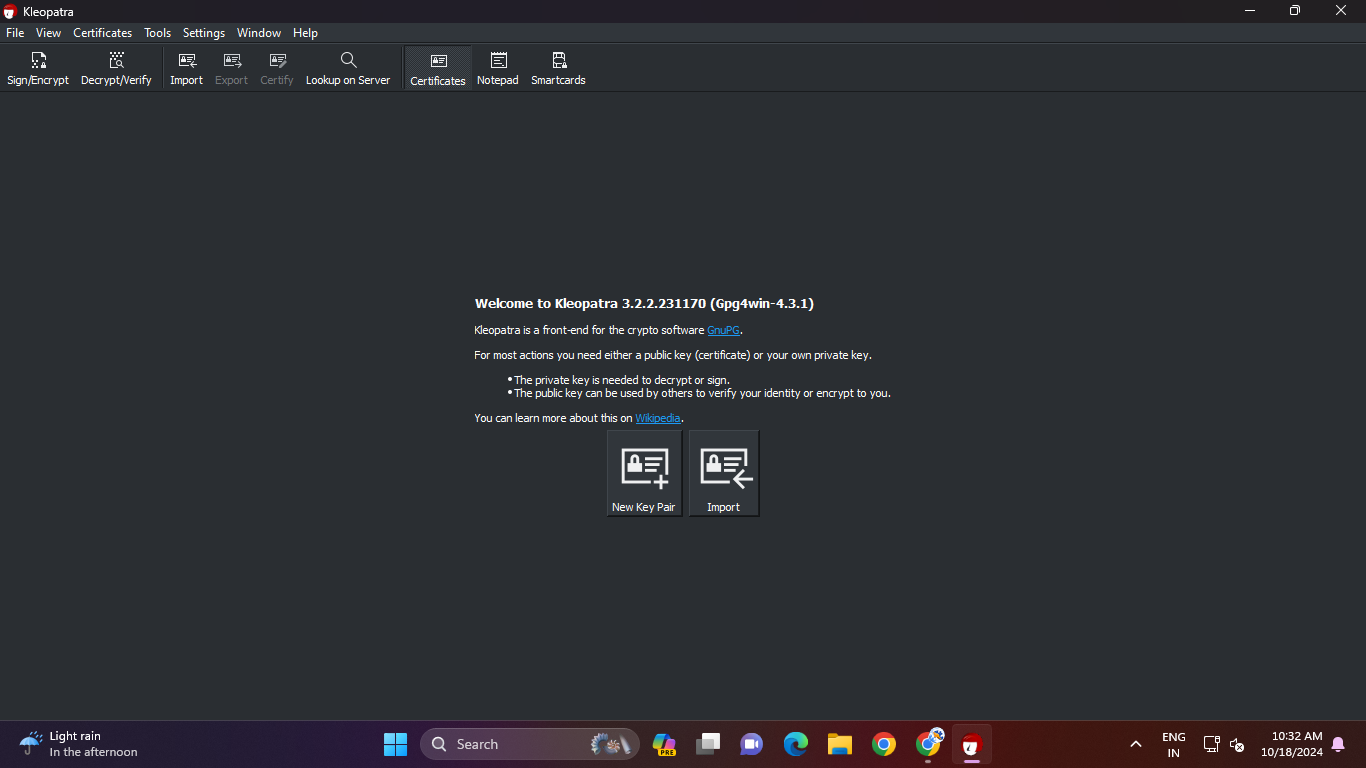
GPG is used for authentication and privacy to messages over the internet. GPG was originated to address the security concerns of plain e-mail or text messages. Gnupg is used to demonstrate usage of GPG. Kleopatra helps to store OpenPGP certificates and keys.

**References:**

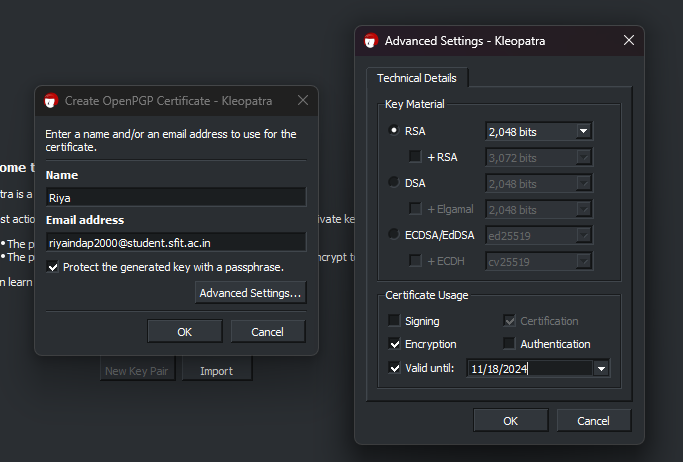
1. “Gpg4win - a secure solution”, <https://www.gpg4win.org>
2. “Kleopatra”, <https://www.openpgp.org/software/kleopatra/>
3. “Pretty Good Privacy”, <https://en.wikipedia.org/wiki/Pretty_Good_Privacy>
4. “The Complete PGP Encryption Tutorial | Gpg4win & GnuPG “, <https://youtu.be/CEADq-B8KtI>

Post-Experiment Screenshots

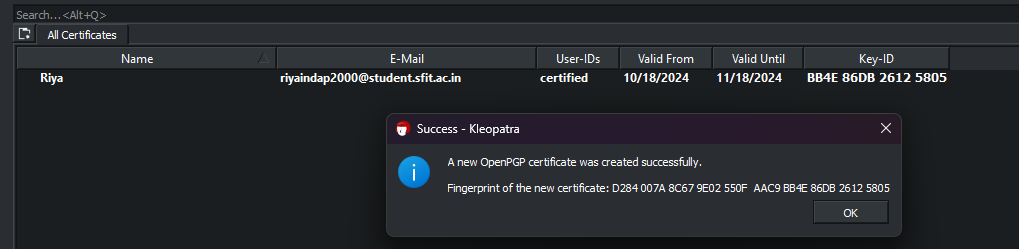
1.Welcome window of Kleopatra interface.



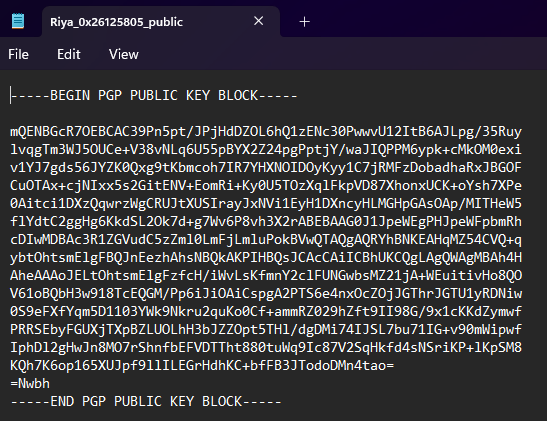
This is the welcome window of cleopatra interface,that is seen in the certificate tab.

2.SS with new key pair created.

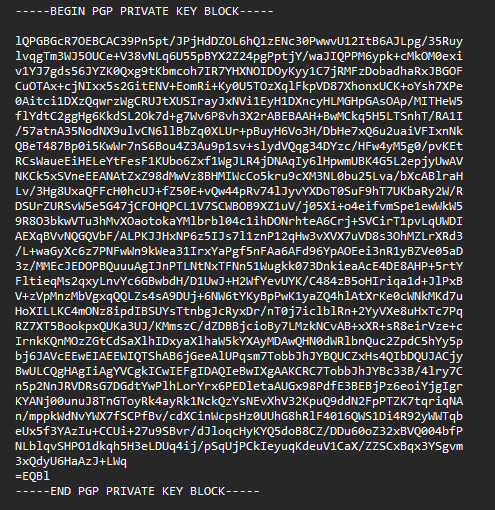
On clicking the create new key pair option on the welcome screen tha tab opened in which own name and email address has been entered.In the advance settings option the the the technical details is set to RSA with the size of key as 2048 bits and the certificate usage is set to only encryption with validity set to next month for the generated key.



On clicking ok the key-pair is generated and is visible in the certificate tab.

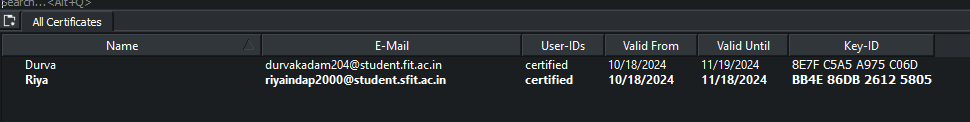
3.SS of private and public key. 

By right clicking on the certificate and exporting it to the the folder on desktop and the public can be viewed by opening it in the notepad with the option edit in notepad.The attached is the public key of riya(my own) that has been generated.This is file with .asc extension.

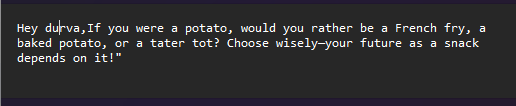


similarly for private key,through the option of expprting secret keys the secret was stored in the desktop and viewed by the option of edit in notepad.The attached is the private key of riya(my own).

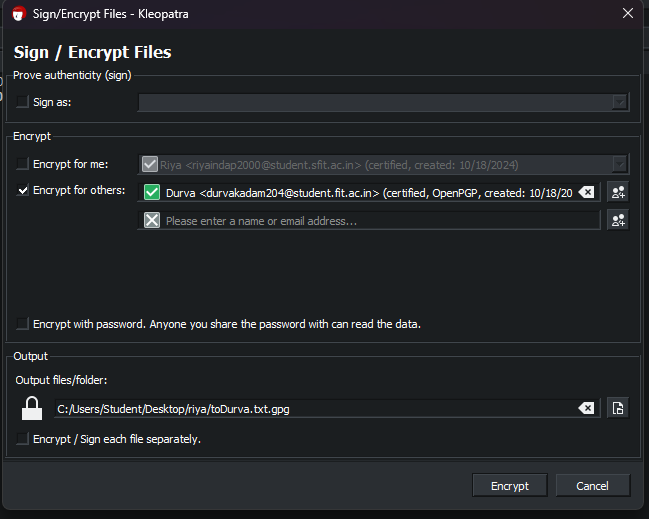
4.SS with imported public key.



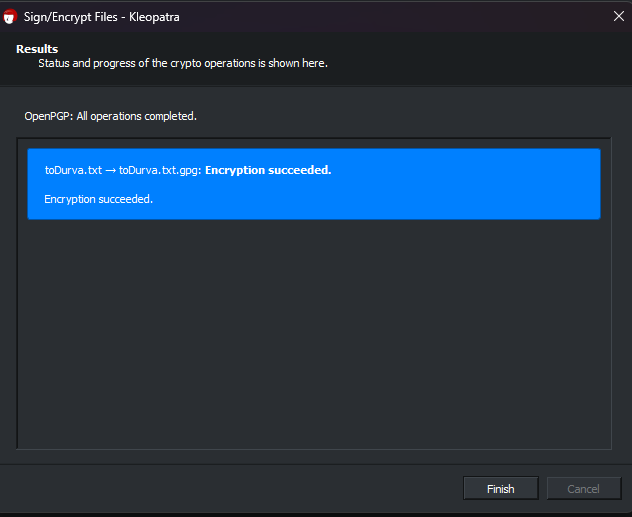
The person to which we wish to send the encrypted message,we need the public key of that person.Here the person is durva.So by downloading the public key sent import we selected the durva’s public key and imported in the kleopatra.Thus as seen in the attached screenshot we now have my own public key and the receiver of my message’s public key.

5.SS with message and encrypted message.

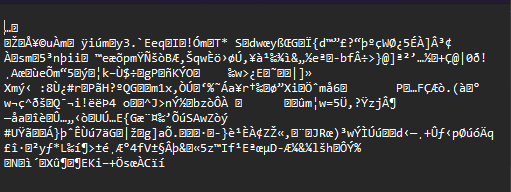
This is the message that I wish to encrypt and send to durva.I have wrote it in a text file and stored in my folder.



Now through the sign/encrypt option of kleopatra i selected the the text file containing my message to encrypt.The above prompt opened and by encrypting for others i encrypted the message fo the durva .

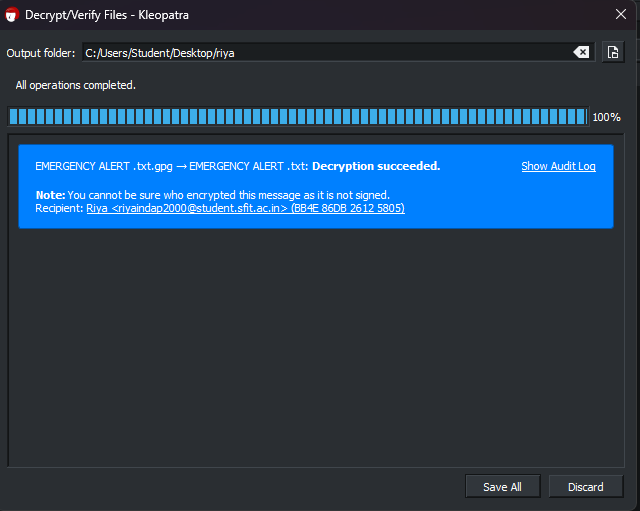


On completing the encryption I saved the file in my own folder.



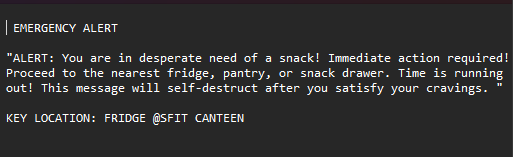
The is the encrypted message of my original message.I sent it to durva by attaching it to her through mail.

6.SS with message decryption.



The perform decryption of a encrypted message sent by durva I downloaded the the attachment she sent through mail and saved in my own folder.On kleopatra through th option of decrypt and verify i chose the encrypted message sent by durva and decrypted it.

On completing the decryption ,saved the message in my folder.



On opening the decrypted message sent by durva in noted,the message was read.