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 –
- Design 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.

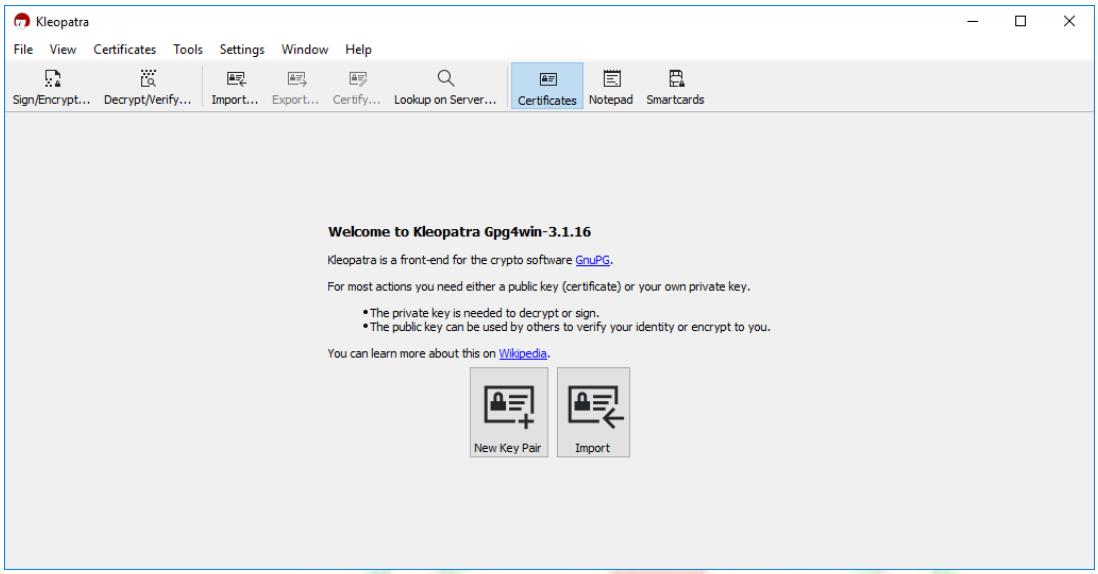
References:

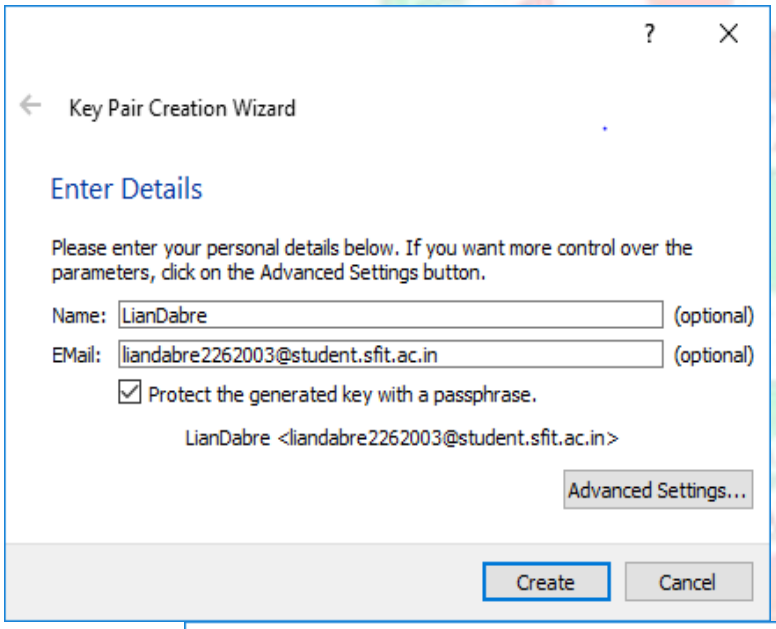
[1] "Gpg4win - a secure solution", https://www.gpg4win.org

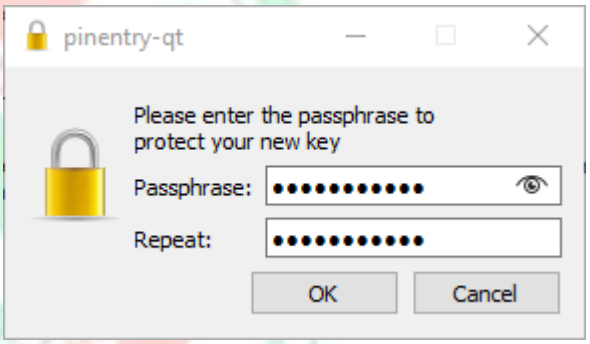
[2] "Kleopatra", https://www.openpgp.org/software/kleopatra/

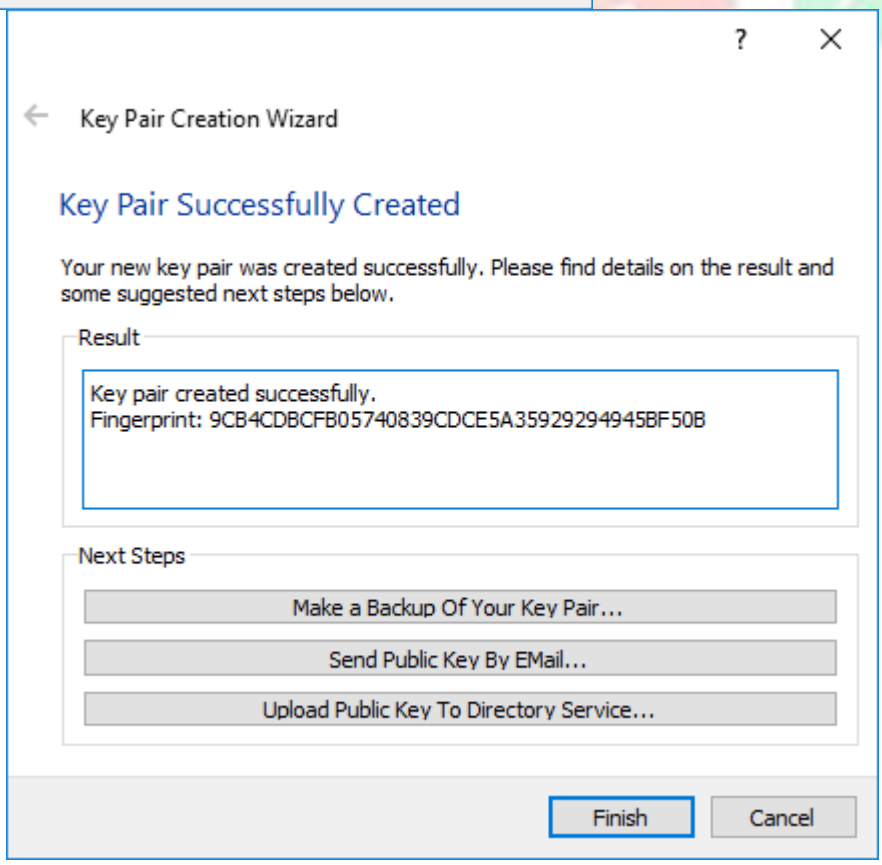
[3] "Pretty Good Privacy", https://en.wikipedia.org/wiki/Pretty_Good_Privacy

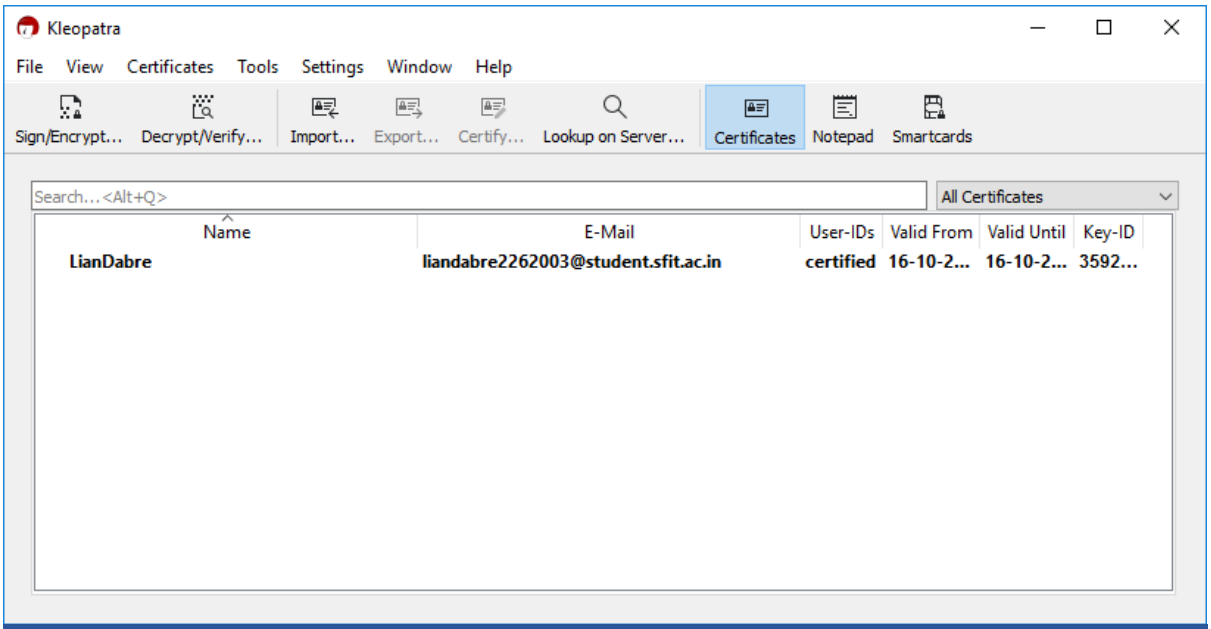
[4] "The Complete PGP Encryption Tutorial | Gpg4win & GnuPG ", https://youtu.be/CEADq-B8KtI

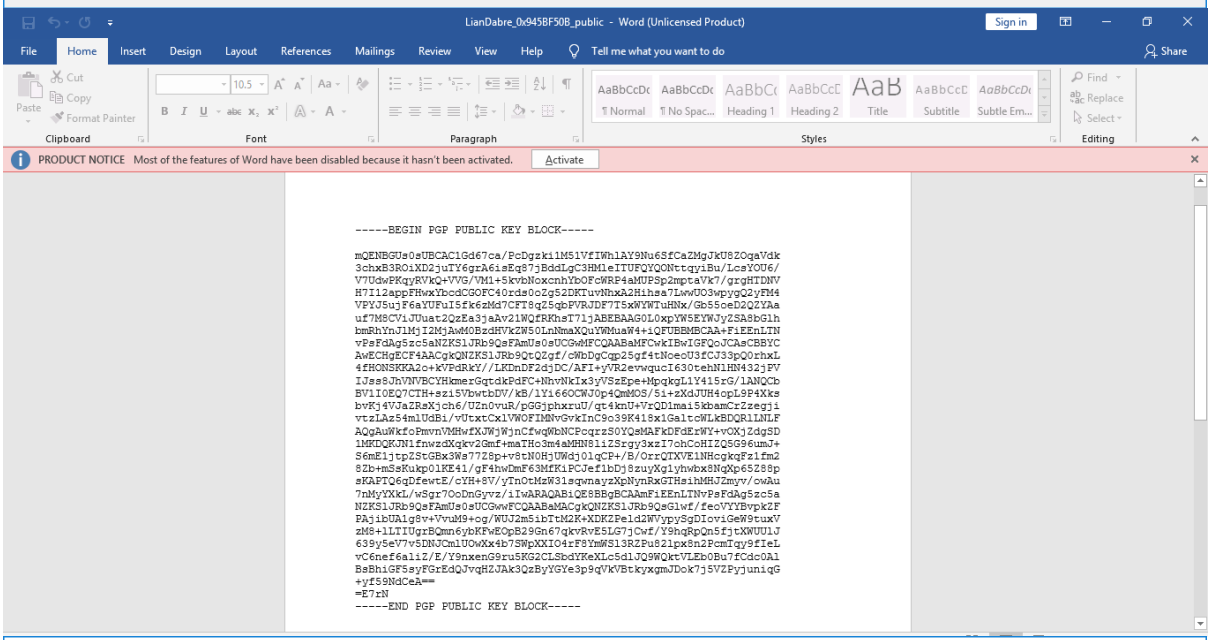

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Welcome to Kleopatra Gpg4win-3.1.16
Kleopatra is a front-end for the crypto software GnuPG.
For most actions you need either a public key (certificate) or your own private key.
• The private key is needed to decrypt or sign.
• The public key can be used by others to verify your identity or encrypt to you.
You can learn more about this on Wikipedia.
New Key Pair
Import

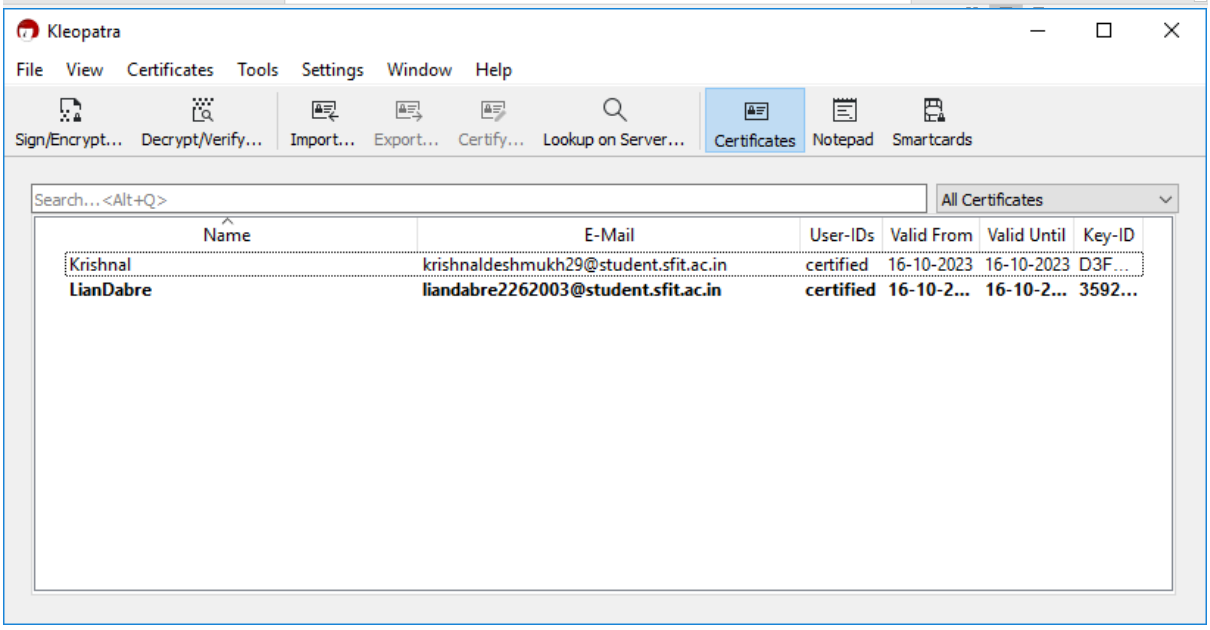

Key Pair Creation Wizard
Enter Details
Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.
Name: LianDabre (optional)
EMail: liandabre2262003@student.sfit.ac.in (optional)
Protect the generated key with a passphrase.
LianDabre <liandabre2262003@student.sfit.ac.in>
Advanced Settings...
Create
Cancel


pinentry-qt
Please enter the passphrase to protect your new key
Passphrase:
Repeat:
OK
Cancel


Key Pair Creation Wizard
Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
Result
Key pair created successfully.
Fingerprint: 9CB4CDBCFB05740839CDCE5A35929294945BF50B
Next Steps
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
LianDabre liandabre2262003@student.sfit.ac.in certified 16-10-2... 16-10-2... 3592...


LianDabre_0x945BF50B_public - Word (Unlicensed Product)
Sign in
File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do
Share
PRODUCT NOTICE Most of the features of Word have been disabled because it hasn't been activated.
Activate
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBGUs0sUBCAC1Gd67ca/PcDgzki1M51VfIWhlAY9Nu6SfCaZMgJkU8ZOqaVdk
3chxB3ROiXD2uTY6grA6isEq87jBddLgC3HMleIIUFQYQONttqyiBu/LcsYOU6/
V7UdwPKqyRVkQ+VVG/VM1+5kvbNoxcnhYbOFcWRP4aNUPSp2mptaVk7/grqHTDNV
H7I12apgFHwxIbcdCGOFC4Ords0oZg52DKTuvNbaA2Hihs47LwwUO3wpygQ2yFM4
VPYJ5ujF6aYUFuI5fk6zMd7CFT8q25qbPVRJDF7TSxWYWTuHNx/Gb55oeD2Q2YAa
uf7M8CViJUuat2QzEa3jaAv21WQfRKhsT7ljABEBAAG0L0xpYW5EYWJyZSA8bGlh
bmRhYnJlMjI2MjAwM0BzdHVkZW50LnNmaXQuYWuaW4+iQFUBBMBCAA+FiEEnLTN
vPsFdAg5zc5aNZKSlJRb9QsFAmUs0sUCGwMFCQAABaMFCwkIBwIGFQoJCAsCBBYC
AwECHgECF4AACgkQNZKSlJRb9QtQZgf/cWbDgCqp25gf4tNoeoU3fCJ33pQ0rhxL
4fHONSKKA2o+kVPdRkY//LKDnDF2djDC/AFI+yVR2evwqucI630tehN1HN432jFV
IJss8JhVNVBCYHkmerGqtdkPdFC+NhvNkIx3yVSzEpe+MpqkgL1Y415rG/lANQCb
BVlIOEQ7CTH+szi5VbwtbDV/kB/lY166OCWJOp4QmMOS/5i+zXdJUH4opL9P4Xks
bvKj4VJaZRsXjch6/UZn0ruR/pGGjphxruU/qt4kmU+VrQDlmai5kbamCrZzegji
vtzLAz54mlUdBi/vUtxtCxlVWOFIMNvGvkInC9o38K418x1GaltcWLkBDQRlLNLF
AQgAuWkfoPmvnVMHwfXJWjWjnCfwqWbNCPcqrzS0YQsMAFkDFdErWY+vOXjZdgSD
1MKDQKJN1fnwzdXqkv2Gmf+maTHo3m4aMHN81iZSrgy3xzI7ohCoHIZQ5G96umJ+
S6mEljtpZStGBx3Ws77Z8p+v8tN0HjUWdj0lqCP+/B/OrrQTXVE1NHcgkqFz1fm2
8Zb+mSsKukp0lKE41/gF4hwDmF63MfKiPCJef1bDj8zuyXg1yhwbx8NqXp65Z88p
sKAPTQ6qDfewtE/cYH+8V/yTnOtMzW31sqwnayzXpNynRxGTHsihMHJZmyv/owAu
7nMyYXkL/wSgr7OoDnGyvz/iIwARAQABiQE8BBgBCAAmFiEEnLTNvPsFdAg5zc5a
NZKSlJRb9QsFAmUs0sUCGwwFCQAABaMACgkQNZKSlJRb9QsGlwf/feoVYYBvpkZF
PAjibUAlg8v4VvuM9+og/WUU2m5ibTtM2K+XDKZPeld2WVypySgDIoviGeW9tuxV
zM8+LLIIUgrBQmn6ybKFwEOgB29Gn67qkvRvE5LG7jCwf/Y9hqRpQn5fjtXWUlJ
639y5eV7v5DNJCmlUOwXx4b7SWpXXIO4rF8YmWSl3RZPu821px8n2PcmTqy9fIeL
vC6nef6aliZ/E/Y9nxenG9ru5KG2CLSbdYKeXLc5dlJQ9WQktVLEbOBu7fCdcOAl
BsBhiGF5syFGrEdQJvqHZJAk3QzByYGYe3p9qVkVBtkyxgmJDok7j5VZPyjuniqG
+yf59NdCeA==
=E7rN
-----END PGP PUBLIC KEY BLOCK-----


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Krishnal krishnaldeshmukh29@student.sfit.ac.in certified 16-10-2023 16-10-2023 D3F...
LianDabre liandabre2262003@student.sfit.ac.in certified 16-10-2... 16-10-2... 3592...