Lab 4 ; OpenPGP

Name: Sushma Shivshankar Nandiyawar – sushnand@iu.edu

Q1.

a. **Write a brief report of what you have done. In the report, include your OpenPGP key ID and signature (Your public key will be downloaded from the key** servers **and checked for signatures.) Also, answer the question below**

Answer:

Being a Windows user, I installed Gpg4win, which is a freely available software package encompassing various essential tools for secure communication.

1. **GnuPG Encryption Software**
   This tool empowers users to encrypt their emails, thereby bolstering the security of their communication.
2. **Kleopatra**
   I utilized Kleopatra to create both my public and private keys. Additionally, it simplified the process of adding public keys from other users, along with their key identifiers and email addresses.
3. **GnuPG for Outlook (GpgOL)**
   I incorporated the GpgOL extension into Microsoft Outlook, enabling me to send emails with digital signatures and encryption, thus assuring the privacy and integrity of my messages.

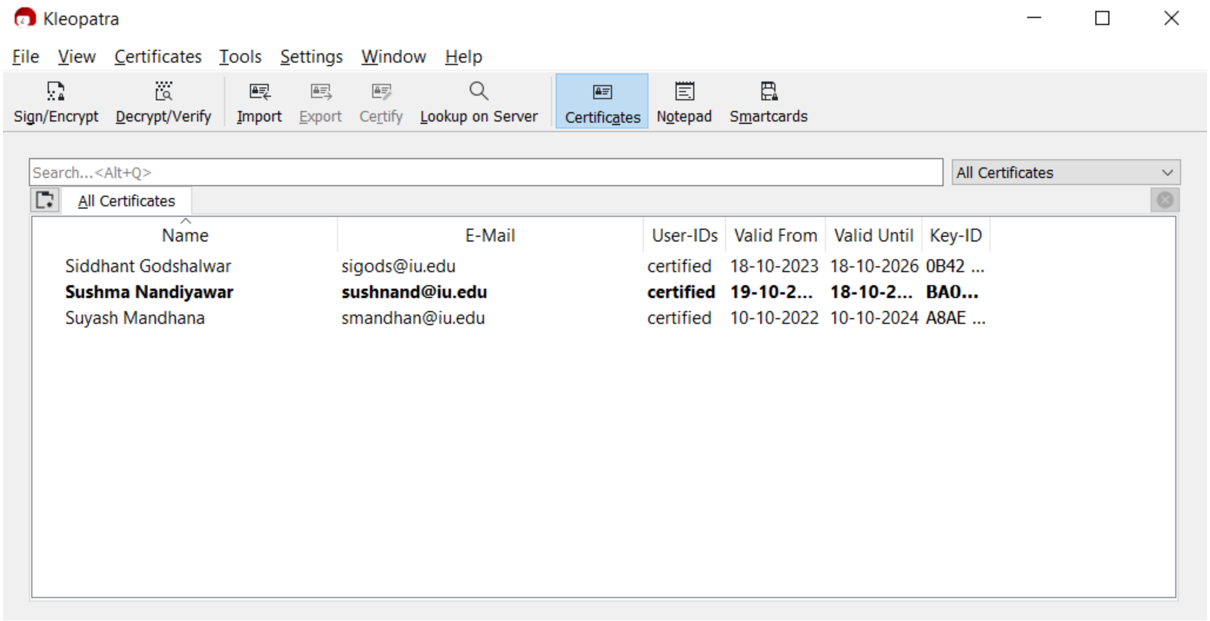
For ensuring secure communication, Gpg4win relies on two essential elements: public and private keys. I generated my own set of public and private keys using Kleopatra. To increase the availability of my public keys, I uploaded them to the designated servers as instructed in the assignment. Furthermore, I bolstered the reliability of my public keys by obtaining signatures from other users' private keys. In return, I provided signatures for their private keys. These mutually signed public keys were subsequently made available on the servers for others to utilize.

I additionally brought in Suyush's public keys, following the fingerprint verification procedure as outlined in the assignment, with the assistance of Kleopatra. To conclude, I utilized the GpgOL extension integrated into Outlook to send Suyush emails with either digital signatures, encryption, or both, thereby ensuring the utmost level of security in our communication.

My Finger Print: 543B 964A 9654 6244 A632 057D BA0C F6DB E29C 07B5

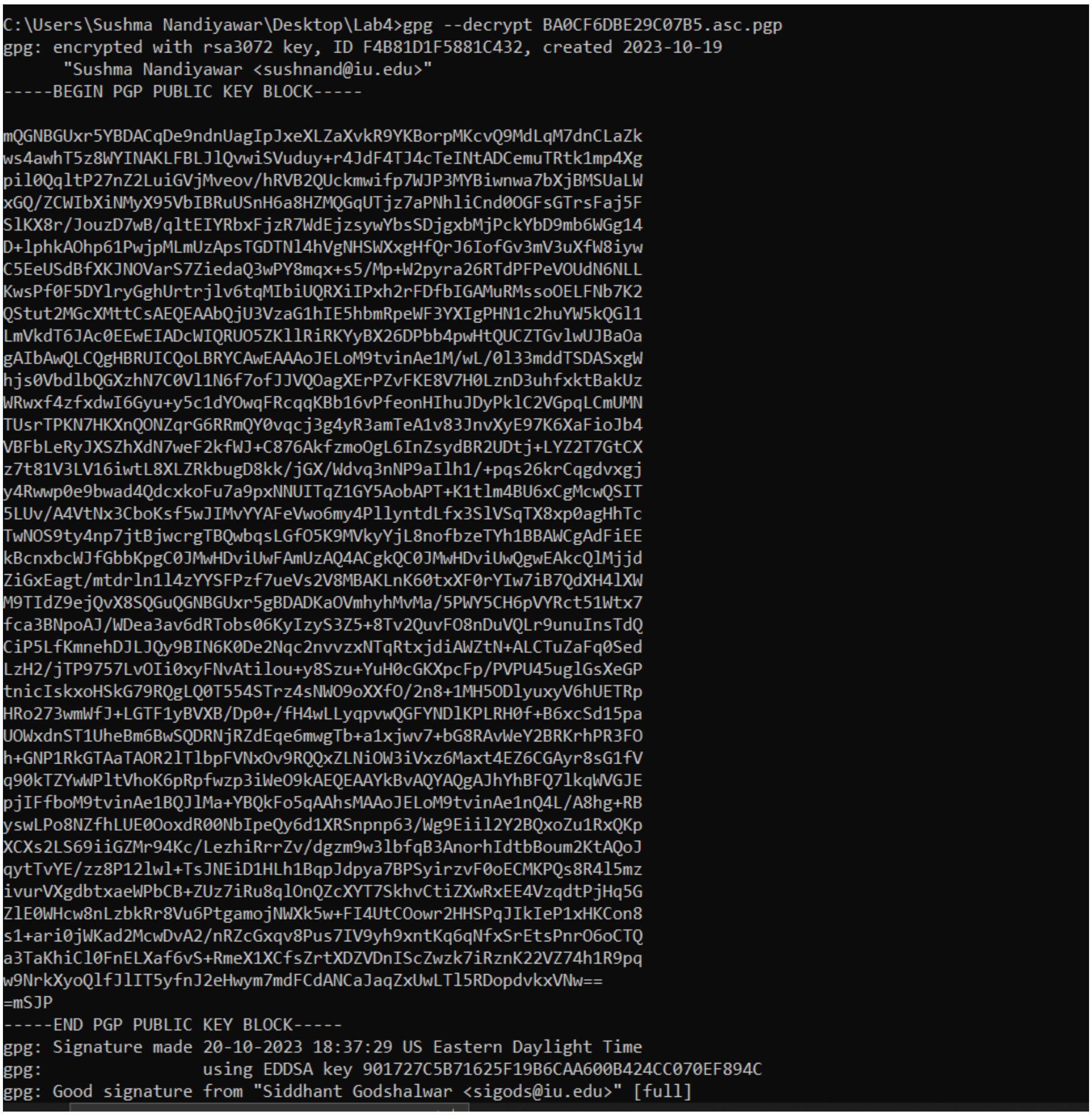
Key ID: BA0C F6DB E29C 07B5

Imported Suyash's (smandhan@iu.edu) Public key and sent email to him.



Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Siddhant Godshalwar	sigods@iu.edu	certified	18-10-2023	18-10-2026	0B42 ...
Sushma Nandiyawar	**sushnand@iu.edu**	**certified**	**19-10-2...**	**18-10-2...**	**BA0...**
Suyash Mandhana	smandhan@iu.edu	certified	10-10-2022	10-10-2024	A8AE ...

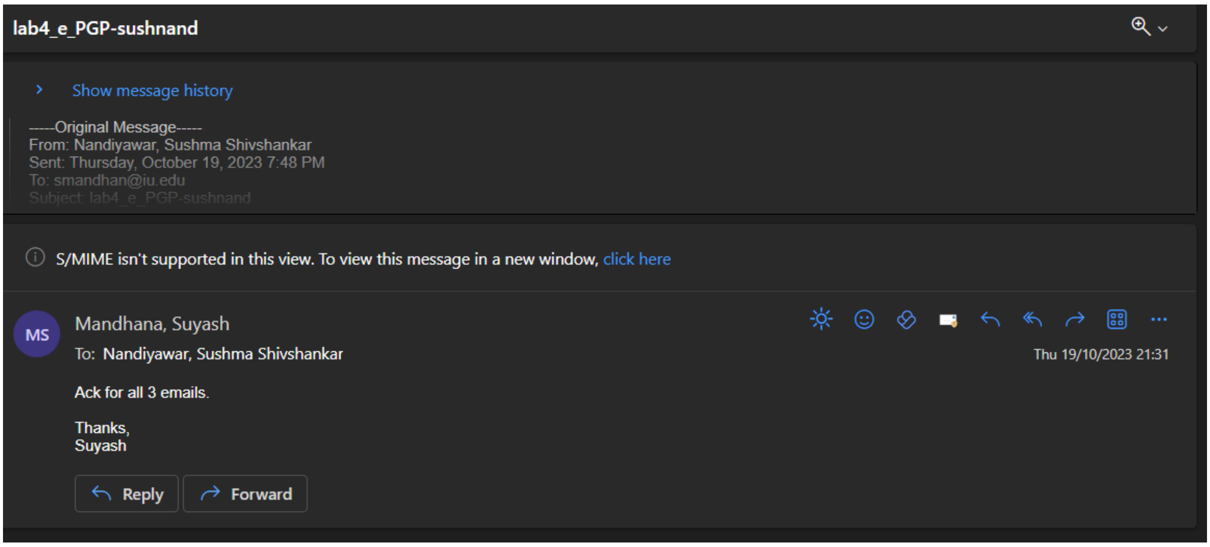
Siddhanth Godshalwar signed my key



```
C:\Users\Sushma Nandiyawar\Desktop\Lab4>gpg --decrypt BA0CF6DBE29C07B5.asc.pgp
gpg: encrypted with rsa3072 key, ID F4B81D1F5881C432, created 2023-10-19
      "Sushma Nandiyawar <sushnand@iu.edu>"
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGUxr5YBDACqDe9ndnUagIpJxeXLZaXvkR9YKBorpMKcvQ9MdLqM7dnCLaZk
ws4awhT5z8WYINAKLFBLJlQvwiSVuduy+r4JdF4TJ4cTeINtADCemuTRtk1mp4Xg
pil0QqltP27nZ2LuiGVjMveov/hRVB2QUckmwifp7WJP3MYBiwnwa7bXjBMSUaLW
xGQ/ZCWIbXiNMyX95VbIBRuUSnH6a8HZMQGqUTjz7aPNhliCnd0OGFsGTrsFaj5F
SlKX8r/JouzD7wB/qltEIYRbxFjzR7WdEjzsywYbsSDjgxbMjPckYbD9mb6WGg14
D+lphkAOhp61PwjpMLmUzApsTGDTNl4hVgNHSWXxgHfQrJ6IofGv3mV3uXfW8iyw
C5EeUSdBfXKJNOVarS7ZiedaQ3wPY8mqx+s5/Mp+W2pyra26RTdPFPeVOUdN6NLL
KwsPf0F5DYlryGghUrtrjlv6tqMIbiUQRXiIPxh2rFDfbIGAMuRMssoOELFNb7K2
QStut2MGcXMttCsAEQEAAbQjU3VzaG1hIE5hbmRpeWF3YXIgPHN1c2huYW5kQGl1
LmVkdT6JAc0EEwEIADcWIQRUO5ZKllRiRKYyBX26DPbb4pwHtQUCZTGvlwUJBaOa
gAIbAwQLCQgHBRUICQoLBRYCAwEAAAoJELoM9tvinAe1M/wL/0l33mddTSDASxgW
hjs0VbdlbQGXzhN7C0Vl1N6f7ofJJVQOagXErPZvFKE8V7H0LznD3uhfxktBakUz
WRwxf4zfxdwI6Gyu+y5c1dYOwqFRcqqKBb16vPfeonHIhuJDyPklC2VGpqLCmUMN
TUsrTPKN7HKXnQONZqrG6RRmQY0vqcj3g4yR3amTeA1v83JnvXyE97K6XaFioJb4
VBFbLeRyJXSZhXdN7weF2kfWJ+C876AkfzmoOgL6InZsydBR2UDtj+LYZ2T7GtCX
z7t81V3LV16iwtL8XLZRkbugD8kk/jGX/Wdvq3nNP9aIlh1/+pqs26krCqgdvxgj
y4Rwwp0e9bwad4QdcxkoFu7a9pxNNUITqZ1GY5AobAPT+K1tlm4BU6xCgMcwQSIT
5LUv/A4VtNx3CboKsf5wJIMvYYAFeVwo6my4PllyntdLfx3SlVSqTX8xp0agHhTc
TwNOS9ty4np7jtBjwcrgTBQwbqsLGfO5K9MVkyYjL8nofbzeTYh1BBAWCgAdFiEE
kBcnxbcWJfGbbKpgC0JMwHDviUwFAmUzAQ4ACgkQC0JMwHDviUwQgwEAkcQlMjjd
ZiGxEagt/mtdrln1l4zYYSFPzf7ueVs2V8MBAKLnK60txXF0rYIw7iB7QdXH4lXW
M9TIdZ9ejQvX8SQGuQGNBGUxr5gBDADKaOVmhyhMvMa/5PWY5CH6pVYRct51Wtx7
fca3BNpoAJ/WDea3av6dRTobs06KyIzyS3Z5+8Tv2QuvFO8nDuVQLr9unuInsTdQ
CiP5LfKmnehDJLJQy9BIN6K0De2Nqc2nvvzxNTqRtxjdiAWZtN+ALCTuZaFq0Sed
LzH2/jTP9757LvOIi0xyFNvAtilou+y8Szu+YuH0cGKXpcFp/PVPU45uglGsXeGP
tnicIskxoHSkG79RQgLQ0T554STrz4sNWO9oXXfO/2n8+1MH5ODlyuxyV6hUETRp
HRo273wmWfJ+LGTF1yBVXB/Dp0+/fH4wLLyqpvwQGFYNDlKPLRH0f+B6xcSd15pa
UOWxdnST1UheBm6BwSQDRNjRZdEqe6mwgTb+a1xjwv7+bG8RAvWeY2BRKrhPR3FO
h+GNP1RkGTAaTAOR2lTlbpFVNxOv9RQQxZLNiOW3iVxz6Maxt4EZ6CGAyr8sG1fV
q90kTZYwWPltVhoK6pRpfwzp3iWeO9kAEQEAAYkBvAQYAQgAJhYhBFQ7lkqWVGJE
pjIFfboM9tvinAe1BQJlMa+YBQkFo5qAAhsMAAoJELoM9tvinAe1nQ4L/A8hg+RB
yswLPo8NZfhLUE0OoxdR00NbIpeQy6d1XRSnpnp63/Wg9Eiil2Y2BQxoZu1RxQKp
XCXs2LS69iiGZMr94Kc/LezhiRrrZv/dgzm9w3lbfqB3AnorhIdtbBoum2KtAQoJ
qytTvYE/zz8P12lwl+TsJNEiD1HLh1BqpJdpya7BPSyirzvF0oECMKPQs8R4l5mz
ivurVXgdbtxaeWPbCB+ZUz7iRu8qlOnQZcXYT7SkhvCtiZXwRxEE4VzqdtPjHq5G
ZlE0WHcw8nLzbkRr8Vu6PtgamojNWXk5w+FI4UtCOowr2HHSPqJIkIeP1xHKCon8
s1+ari0jWKad2McwDvA2/nRZcGxqv8Pus7IV9yh9xntKq6qNfxSrEtsPnrO6oCTQ
a3TaKhiCl0FnELXaf6vS+RmeX1XCfsZrtXDZVDnIScZwzk7iRznK22VZ74h1R9pq
w9NrkXyoQlfJlIT5yfnJ2eHwym7mdFCdANCaJaqZxUwLTl5RDopdvkxVNw==
=mSJP
-----END PGP PUBLIC KEY BLOCK-----
gpg: Signature made 20-10-2023 18:37:29 US Eastern Daylight Time
gpg:                using EDDSA key 901727C5B71625F19B6CAA600B424CC070EF894C
gpg: Good signature from "Siddhant Godshalwar <sigods@iu.edu>" [full]
```

Sent the 3 different mails signed, encrypted, signed&encrypted:



lab4_e_PGP-sushnand

-----Original Message-----
From: Nandiyawar, Sushma Shivshankar
Sent: Thursday, October 19, 2023 7:48 PM
To: smandhan@iu.edu
Subject: lab4_e_PGP-sushnand

S/MIME isn't supported in this view. To view this message in a new window, click here

Mandhana, Suyash
To: Nandiyawar, Sushma Shivshankar
Thu 19/10/2023 21:31

Ack for all 3 emails.

Thanks,
Suyash

b. **Can you send signed/encrypted email using webmail such as Gmail? Why, or why not? What are the challenges?**

Answer:

Indeed, sending emails with digital signatures and encryption using Gmail is possible, thanks to its incorporation of S/MIME features. Nevertheless, there are some difficulties connected to this procedure:

Activation Requirement:

Both the sender and receiver need to enable S/MIME for encrypted and signed email communication. This activation is attainable through G Suite, but it's important to highlight that this feature is exclusively accessible for users with paid Google accounts.

Reliance on External Solutions

Gmail lacks built-in support for digital signatures or email encryption.

Consequently, users frequently turn to external solutions to incorporate these security features.

1. **Compatibility Issues**
   Ensuring that both the sender and recipient employ encryption techniques and keys that are compatible can pose a challenge.
2. **Usability Challenges**
   Everyday users might encounter difficulties when attempting to set up email encryption, which could result in adoption problems.
3. **Key Handling**
   Handling public and private keys, verifying their reliability, and securely exchanging keys are three vital yet intricate components of email encryption.
4. **Limited Endorsement**
   Some email clients do not offer complete support for encrypted emails, potentially requiring the utilization of third-party apps for decryption.

Q2. Given fingerprint of the key, why are you convinced that the key file you downloaded must not have been-tampered with? (Answer in one sentence)

Answer:

I would trust the downloaded key file because each key has a unique fingerprint, which functions as a cryptographic checksum. Any changes to this fingerprint would result in a completely different key.