# Major Project

## Classroom Name - CS04B1

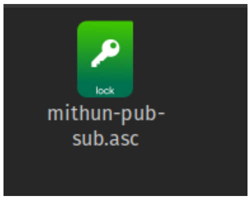
Activity:

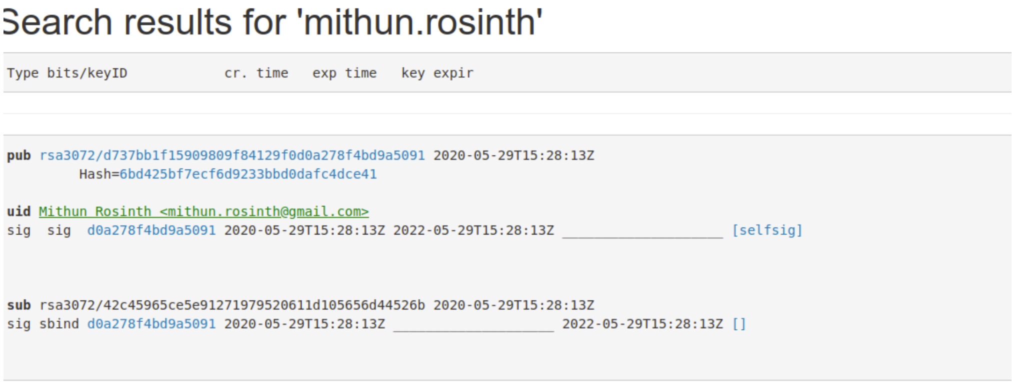
Install and send a message using PGP.

http://openpgp.org/ There are many options for using PGP, try different ones

and see how they work together.

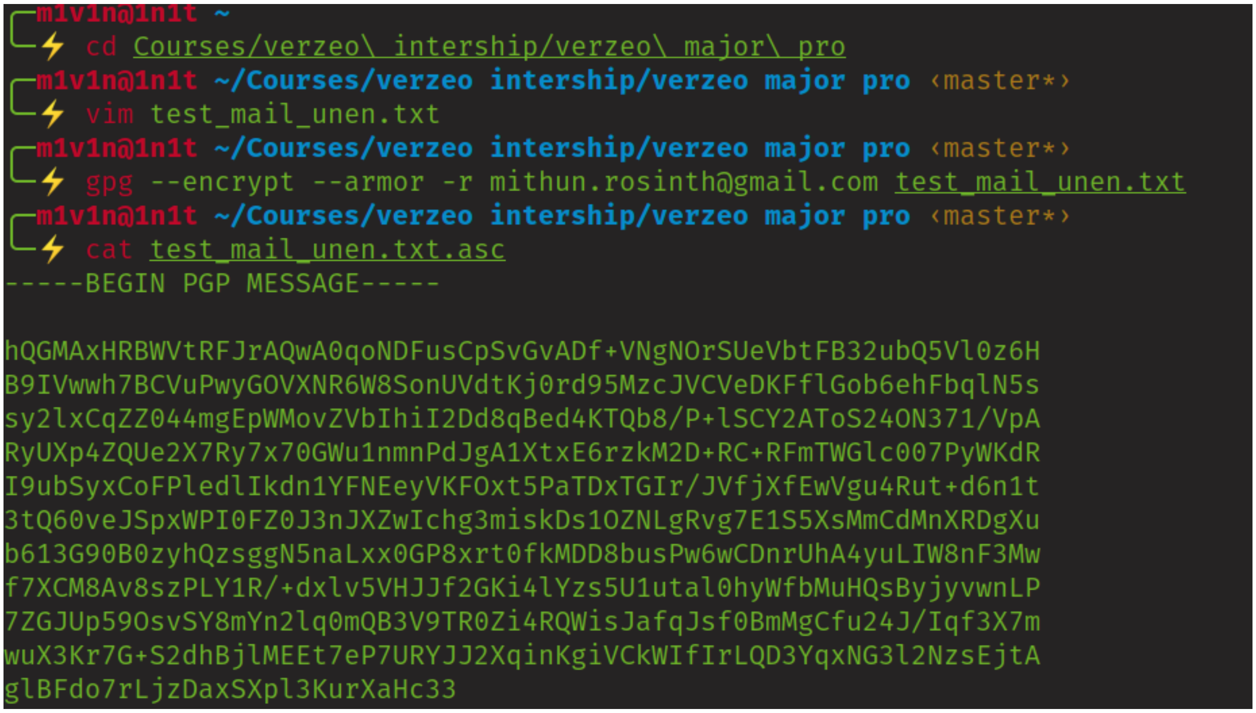
After Generating my public and private key pair I uploaded the public key into the ubuntu Keyserver





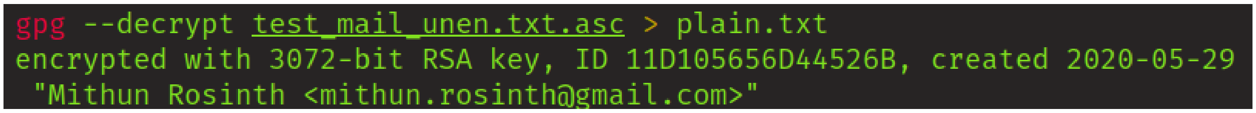
Search results for 'mithun.rosinth'

```
Type bits/keyID           cr. time   exp time   key expir

pub rsa3072/d737bb1f15909809f84129f0d0a278f4bd9a5091 2020-05-29T15:28:13Z
         Hash=6bd425bf7ecf6d9233bbd0dafc4dce41

uid Mithun Rosinth <mithun.rosinth@gmail.com>
sig  sig  d0a278f4bd9a5091 2020-05-29T15:28:13Z 2022-05-29T15:28:13Z ____________________ [selfsig]


sub rsa3072/42c45965ce5e91271979520611d105656d44526b 2020-05-29T15:28:13Z
sig sbind d0a278f4bd9a5091 2020-05-29T15:28:13Z ____________________ 2022-05-29T15:28:13Z []
```

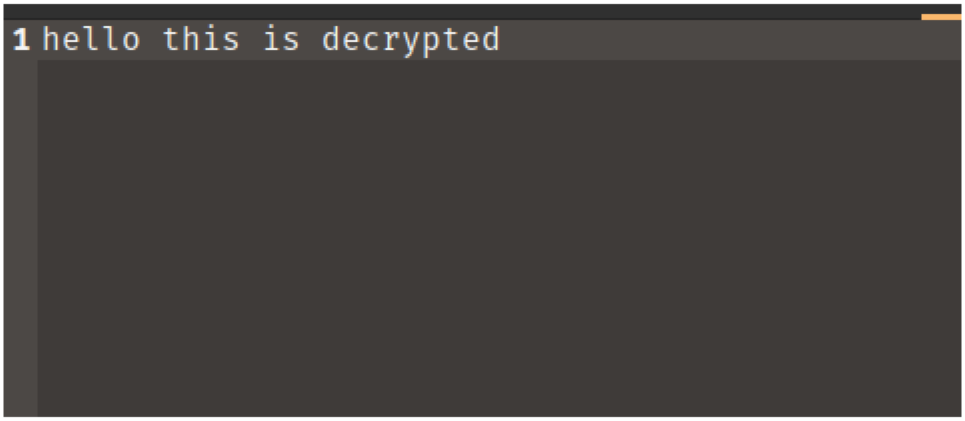


```
┌m1v1n@1n1t ~
└⚡ cd Courses/verzeo\ intership/verzeo\ major\ pro
┌m1v1n@1n1t ~/Courses/verzeo intership/verzeo major pro ‹master*›
└⚡ vim test_mail_unen.txt
┌m1v1n@1n1t ~/Courses/verzeo intership/verzeo major pro ‹master*›
└⚡ gpg --encrypt --armor -r mithun.rosinth@gmail.com test_mail_unen.txt
┌m1v1n@1n1t ~/Courses/verzeo intership/verzeo major pro ‹master*›
└⚡ cat test_mail_unen.txt.asc
-----BEGIN PGP MESSAGE-----

hQGMAxHRBWVtRFJrAQwA0qoNDFusCpSvGvADf+VNgNOrSUeVbtFB32ubQ5Vl0z6H
B9IVwwh7BCVuPwyGOVXNR6W8SonUVdtKj0rd95MzcJVCVeDKFflGob6ehFbqlN5s
sy2lxCqZZ044mgEpWMovZVbIhiI2Dd8qBed4KTQb8/P+lSCY2AToS24ON371/VpA
RyUXp4ZQUe2X7Ry7x70GWu1nmnPdJgA1XtxE6rzkM2D+RC+RFmTWGlc007PyWKdR
I9ubSyxCoFPledlIkdn1YFNEeyVKFOxt5PaTDxTGIr/JVfjXfEwVgu4Rut+d6n1t
3tQ60veJSpxWPI0FZ0J3nJXZwIchg3miskDs1OZNLgRvg7E1S5XsMmCdMnXRDgXu
b613G90B0zyhQzsggN5naLxx0GP8xrt0fkMDD8busPw6wCDnrUhA4yuLIW8nF3Mw
f7XCM8Av8szPLY1R/+dxlv5VHJJf2GKi4lYzs5U1utal0hyWfbMuHQsByjyvwnLP
7ZGJUp59OsvSY8mYn2lq0mQB3V9TR0Zi4RQWisJafqJsf0BmMgCfu24J/Iqf3X7m
wuX3Kr7G+S2dhBjlMEEt7eP7URYJJ2XqinKgiVCkWIfIrLQD3YqxNG3l2NzsEjtA
glBFdo7rLjzDaxSXpl3KurXaHc33
```

Then I encrypted a random text file with the intended public key and sent the mail. Upon receiving the attachment was downloaded and decrypted with the private key.



```
gpg --decrypt test_mail_unen.txt.asc > plain.txt
encrypted with 3072-bit RSA key, ID 11D105656D44526B, created 2020-05-29
 "Mithun Rosinth <mithun.rosinth@gmail.com>"
```

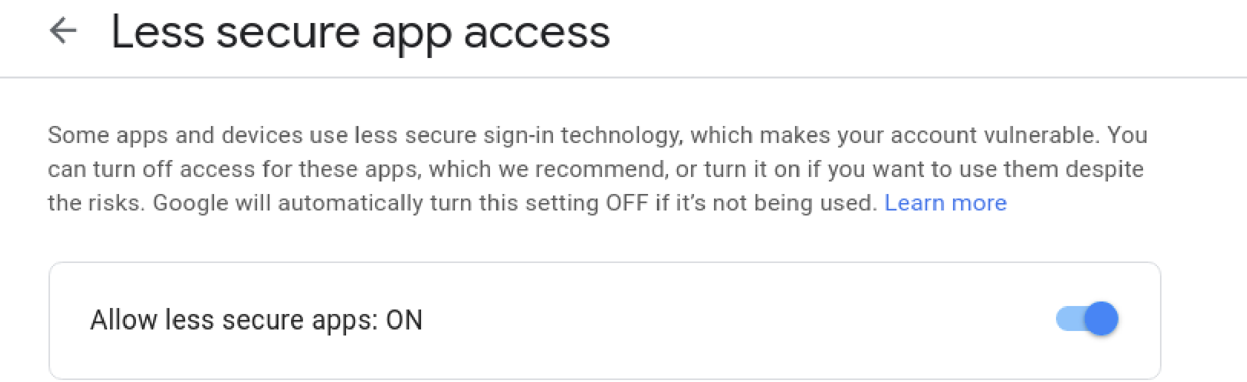


```
hello this is decrypted
```

The same can also be done without a hassle by using free encrypted mail services like Proton mail

# Activity

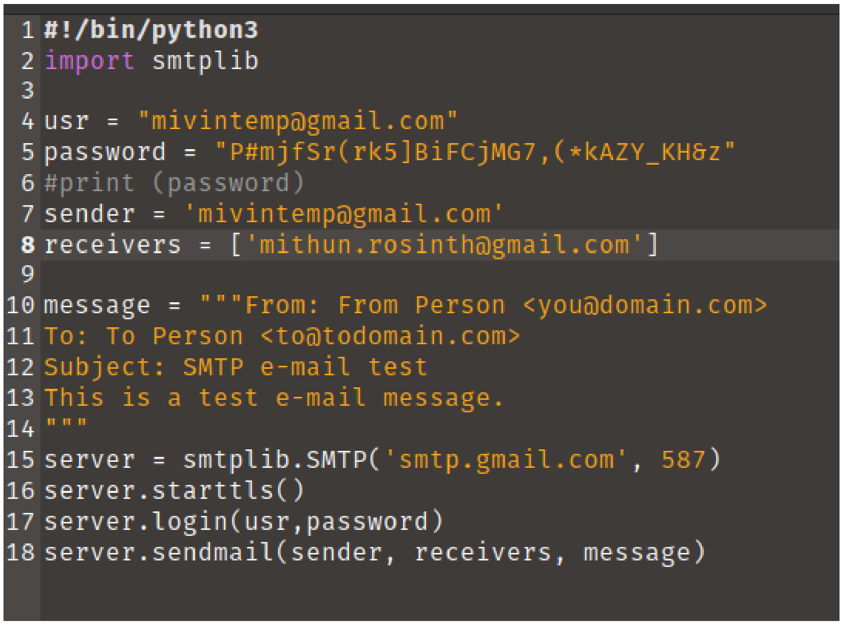
To use TLS on port 587 on Gmail, we need to toggle the “Allow less secure apps” option on for the receivers to be able to send emails. We can use SSL on port 465 also to send emails.



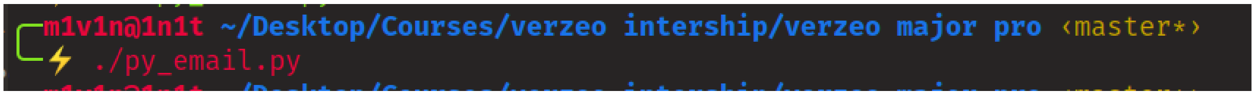
## ← Less secure app access

Some apps and devices use less secure sign-in technology, which makes your account vulnerable. You can turn off access for these apps, which we recommend, or turn it on if you want to use them despite the risks. Google will automatically turn this setting OFF if it’s not being used. Learn more

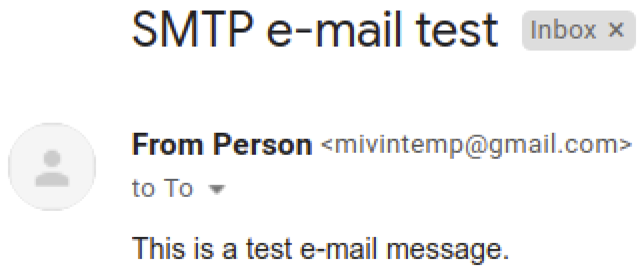
Allow less secure apps: ON



```python
#!/bin/python3
import smtplib

usr = "mivintemp@gmail.com"
password = "P#mjfSr(rk5]BiFCjMG7,(*kAZY_KH&z"
#print (password)
sender = 'mivintemp@gmail.com'
receivers = ['mithun.rosinth@gmail.com']

message = """From: From Person <you@domain.com>
To: To Person <to@todomain.com>
Subject: SMTP e-mail test
This is a test e-mail message.
"""
server = smtplib.SMTP('smtp.gmail.com', 587)
server.starttls()
server.login(usr,password)
server.sendmail(sender, receivers, message)
```



```
┌─m1v1n@1n1t ~/Desktop/Courses/verzeo intership/verzeo major pro ‹master*›
└─⚡ ./py_email.py
```



SMTP e-mail test

From Person <mivintemp@gmail.com>
to To

This is a test e-mail message.

- **Can you email multiple people?**
  - Yes, by putting all the receivers’ mail addresses in receivers list in the program above.
- **Could you pull the list of people to email from an external file?**
  - Yes, using csv files (excel sheets), we can send emails to various people. In python, using the csv library, we can read all the values and send emails by looping over the data.
- **How can you personalize the email for the recipient?**
  - We can personalize the email for recipients by adding HTML content and attachments using python’s email module.

# Discussion

## What could you do to ensure privacy when sending email?

Using PGP or similar encryption technology to ensure only the intended receiver can decrypt the message. This prevents attackers from gaining information even if he or she intercepts or sniffs the mail packets.

## What expectation of privacy do you have when sending e-mail?

None other than the intended receiver must be able to read the message. This even includes the e-mail service provider.

## If you had a secret message to send, how would you do it?

Using any encryption that abides the Public Key Infrastructure and a trusted and secure sharing platforms like proton mail or signal.

## How could you automate e-mailing many people?

Many modern email clients like outlook and mozilla thunderbird support such features for enterprise clients where a user can add all the desired receivers in a group and schedule emails for everyone in the group. For a general mail user though, who consumes the consumer version of the mailing service it is possible by using such clients or using small scripts programmed to do this.  Languages like python consist of libraries which facilitate the usage of common email protocols like smtp.

# Assessment Questions

## Why do email services "read" your email? What is their goal?

E-mail services term their mail inspection as a precautionary measure to detect malicious activities and prevent online crimes. But a few mail services also use this aggregated data as an input for running personalised ads and provide personalised services and connected services and keep users secure from account compromises.

## How does PGP secure email differently than GMail?

PGP secure mail does not allow even the mail provider to decrypt the mails that are intended for the receiver.

## Why don't people use services like PGP more often?

PGP services might require a bit of knowledge to set up. While most of the traditional mail providers don’t support such features out of the box, it is rare that people get to know about such things. And the setup steps for non-tech savvy people might seem daunting. More accessible PGP enabled mail services or traditional mail service providers adding the feature will only be the solution for this issue.

## What is phishing?

It is a form of social-engineering that is used to lure the victim into clicking malicious links and entering valid usernames and passwords into malicious look-alike websites created by the Attacker.

## What is spear-phishing?

It is a form of phishing in which the victim is a high profile target such as a CEO, political leader or a celebrity. This kind of phishing is usually done for monetary gains and defacement purposes.