A

## NON SYLLABUS PROJECT REPORT

## ON

## Keylogger

**BachelorofComputer Application**



**PoornimaUniversity,JaipurSession:2020-2023**

### SubmittedBy:

**Name – Ravindra Singh Shekhawat**

**Reg number – 2021PUSCEBCEX10576**

**Name – Yash Kumar Yadav**

**Reg number – 2021PUSCEBCEX10603**

### SubmittedTo:

**DEPARTMENTOFCOMPUTER SCIENCE & ENGINEERING**

### SchoolofEngineering&Technology,PoornimaUniversity

**RamchandraPura,SitapuraExtension,Jaipur,Rajasthan**

# CANDIDATE’S DECLARATION

Weherebydeclarethattheworkpresentedinthemajorprojectreportentitled“**Keylogger**”issubmittedby**Ravindra Singh Shekhawat (2021PUSCEBCEX10576) & Yash Kumar Yadav (2021PUSCEBCEX10603)**is in the fulfillment of the requirements for the award of the degree of Bachelor of Technology In Computer Science Engineerng ,Poornima University, Jaipur. The work has been found satisfactory, authentic of my own work carried out during my degree and approved for submission.

The work reported in this has not been submitted by me for award of any other degreeordiploma.

Date**:**17/05/2022

**Name:**

**Ravindra Singh Shekhawat &**

**Yash Kumar Yadav**

### CERTIFICATE

This is to certify that the major project report entitled “**Keylogger**” is submitted by **Ravindra Singh Shekhawat (2021PUSCEBCEX10576) & Yash Kumamr Yadav (2021PUSCEBCEX10603)** students of 2nd year III semester in partial fulfillment of the degree of Bachelor of Technology in Computer Engineering of Poornima University , Jaipur during the academic year 2020-2024.The work has been found satisfactory and is approved for submission.

### Guide name

Dr. Anuradha Raheja

Department of CSE

### 

HeadofDepartment DeanSCE

DepartmentofCSE

### ACKNOWLEDGEMENT

It is our privilege to express our sincerest regards to our project coordinator, **Mr.,**forhisvaluableinputs,ableguidance,encouragement,whole-heartedcooperation and constructive criticism throughout the duration of our project. Manythankstoourprojectguide,Chandarshekhar Kothari & Priya Kothari(Asst.Professor),who hasgivenhisfull effort in guiding the team for achieving the goal as well as his encouragement tomaintainour progress intrack.

We would like to express our hearts felt appreciation to all faculty members whosedirect or indirect suggestions helped us to develop this project. We pay our respect andlovetoourparentsandallotherfamilymembersandfriendsfortheirloveandencouragement throughout our career.

**Ravindra Singh Shekhawat (2021PUSCEBCEX10576)**

**Yash Kumar Yadav (2021PUSCEBCEX10603)**

### ABSTRACT

The development of technology is very fast, especially in the field of Internet technology that at any time experiencing significant changes, The development also supported by the ability of human resources, Keylogger is a tool that most developed because this application is very rarely recognized a malicious program by antivirus, keylogger will record all activities related to keystrokes, the recording process is accomplished by using string matching method. The application of string matching method in the process of recording the keyboard is to help the admin in knowing what the user accessed on the computer.

The keylogging program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. Using keylogger we prevent the miscellaneous use of system. Using this we capture all information in text and image form.

Key-logging can also be used to study human–computer interaction. Numerous key-logging methods exist: they range from hardware and software-based approaches to acoustic analysis.

•Keyloggers can be installed when a user clicks on a link or opens an attachment/file from a phishing mail

•Keyloggers can be installed through webpage script. This is done by exploiting a vulnerable browser and the keylogger is launched when the user visits the malicious website.

•a keylogger can be installed when a user opens a file attached to an email

•a keylogger can be installed via a web page script which exploits a browser vulnerability. The program will automatically be launched when a user visits an infected site

•a keylogger can exploit an infected system and is sometimes capable to download and install other malware to the system.

**TableofContents**

FrontPage i

[CANDIDATE’SDECLARATION ii](#_TOC_250001)

[CERTIFICATE iii](#_bookmark0)

[ACKNOWLEDGEMENT iv](#_bookmark1)

[ABSTRACT v](#_bookmark2)

[TableofContents vi](#_bookmark3)

[ListofFigures viii](#_bookmark4)

[ListofTables ix](#_bookmark5)

Chapter 1 Introduction

Chapter 2 Working of project

Chapter 3 Result analysis

[Chapter4FutureScope](#_bookmark56)

[Chapter5Conclusion](#_bookmark57)

[References](#_TOC_250000)

# 

# Chapter 1 : Introduction

Ourprojectis **Keyloggers**

# We have chosen to focus on keyloggers because most students have very little experience with keyloggers. Many of the students who do have experience with keyloggers have not used them in the professional industry; thus, lacking the context of how and when they are used. It is also important for students to know which software keylogging programs are available, and most importantly how they are used.

# Computer Forensics consists of the art of examining digital media to preserve, recover, and analyze the data in an effective manner. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers are available in software or hardware form, and are used to capture and compile a record of all typed keys. The information gathered from a keystroke logger can be saved on the system as a hidden file, or ailed to the hacker/forensic analyst. Generic keystroke loggers typically record the application name, time and date when the application was accessed, as well as all keystrokes associated with the application. Advanced keystroke loggers have many additional features.

# Our chosen keylogger has the following features:

# Monitors Keystrokes

# Encrypt the Keylogger file as data.txt

# Send the E-mail file

# A Keylogger is a tool or a technology that monitors and logs consecutive keystrokes made on a keyboard. It normally operates in a covert so that potential victims wouldn’t suspect that their activities are being monitored. Hackers can use this tool to record their target’s browsing activity and obtain their personal information, which they can then use for their own financialgain by blackmailing the target, withdrawing funds from their bank account,or selling the info to other cybercriminals on the dark web.

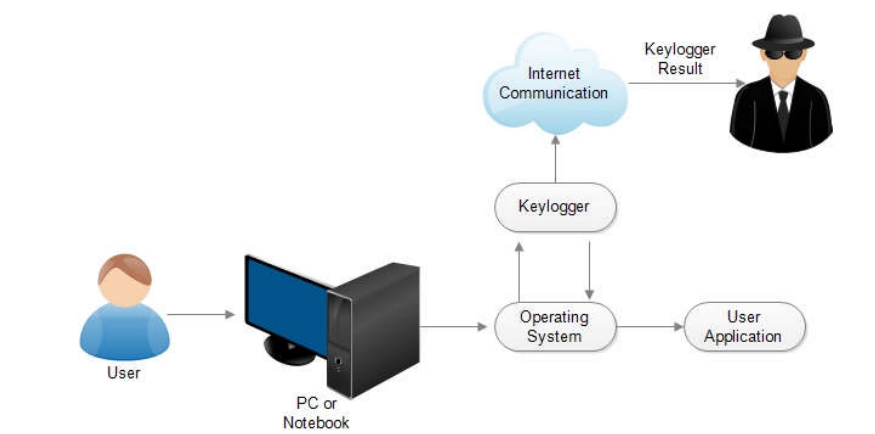
# Often erroneously described as malicious software, keyloggers aren’t always software-based. Theycan also be hardware-based, in which case they either built into hardware or available as a separate device. As far as software-based keyloggers are concerned, unless they are legitimate, they are usually bundled with malware, spyware, or a virus. Hackers typically distribute this malicious keylogging software via phishing emails that include compromised attachments and/or links to infected websites.

# Key logging program also known as keyloggers is a kind of malware that has capability to maliciously track input of the user from the keyboard in aim to retrieve private information. Keyloggers thus cause a major threat to business and personal activities of kind like transactions, online banking, email and chat. The keyboard is the prime target as it allows keyloggers to retrieve user input to the system as it is the most common way user interacts with a computer. There are two types of keyloggers that exists in market, a software keylogger and a hardware keylogger among which software keylogger are widely used and are easy to plant and cause substantial damage. Keyloggers essentially performs two tasks that

# is guiding into client input stream to get keystrokes and moving the information to a distant area (for example- mail). The fundamental goal of keyloggers is to meddle in the chain of occasions that happen when a key is squeezed and when the information is shown on the screen because of a keystroke. Keylogger can be used for legitimate as well as illegitimate purposes, it basically depends on user who is using it. System administrators can use keyloggers for systems, i.e. for detecting suspicious users. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers can be used to capture and compile a record of all typed keys. Keyloggers can at times be utilized as a spying instrument to bargain business and state-possessed organization's information. Attackers can utilize keylogger to gain admittance to the clients' private and delicate data, they can exploit the separated information to perform online cash exchange the client's record or different vindictive stuff.

# Chapter 2 : Working of project

Keylogger is a device either hardware or software used to monitor keyboard keystrokes. A keylogger will usually store the monitoring results of the keyboard keystrokes into alog/record/record file. Some specific keylogger can even send the recording to specific e-mail periodically. Keylogger can be used for the benefit of usefulor even can be used for the benefit of evil. Right interestsinclude monitoring employee productivity for law enforcementand the search for evidence of the crime.

****

We create a keylogger system which will capture the keystrokes of the system and send aemail to our system which is in the encrypted form whose key is unique and only owner has it.

**Step – 1:**

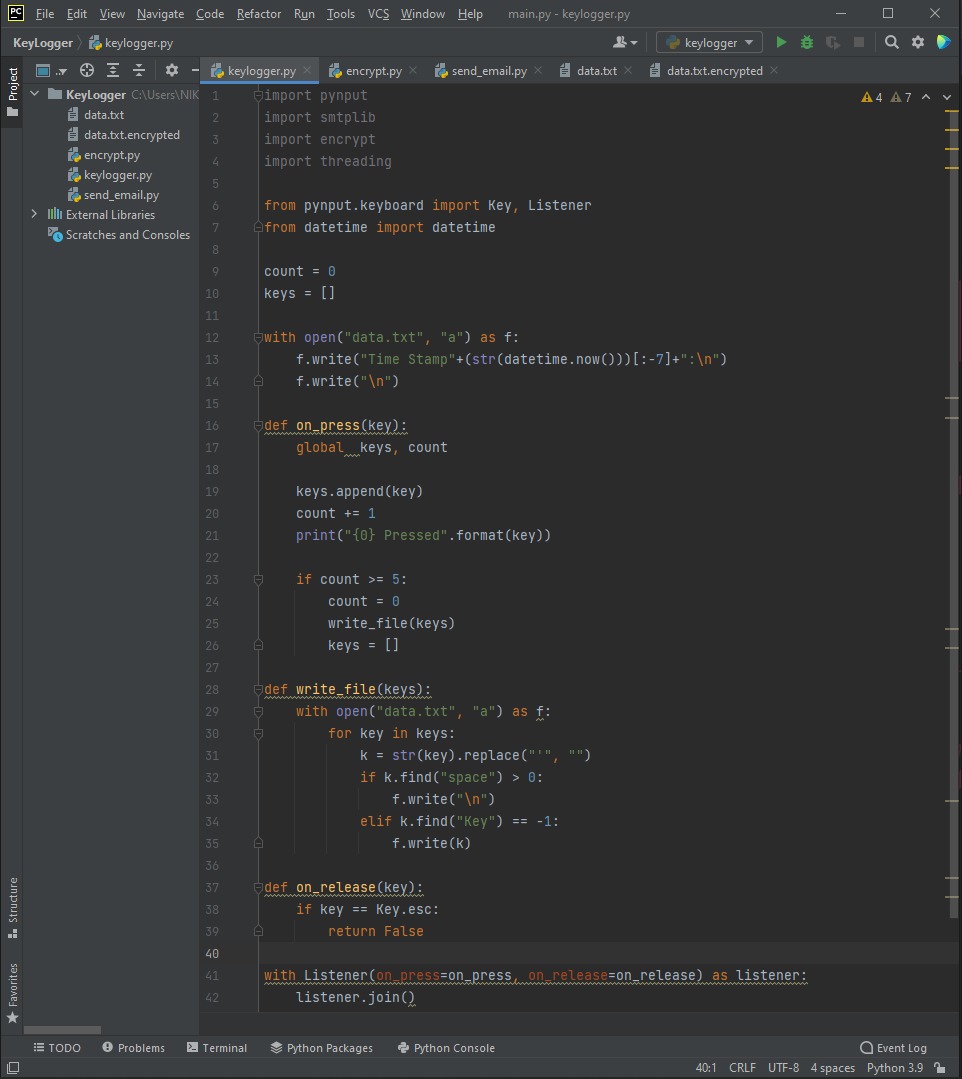
In first, create a data file in which all the keylogs/keystrokes will be saved and with the time stamp.

**Step – 2:**

Program will start as the system boots up and monitors the keystrokes.

**Step – 3:**

We will create the main file as **keylogger.py**

****

**Step – 4:**

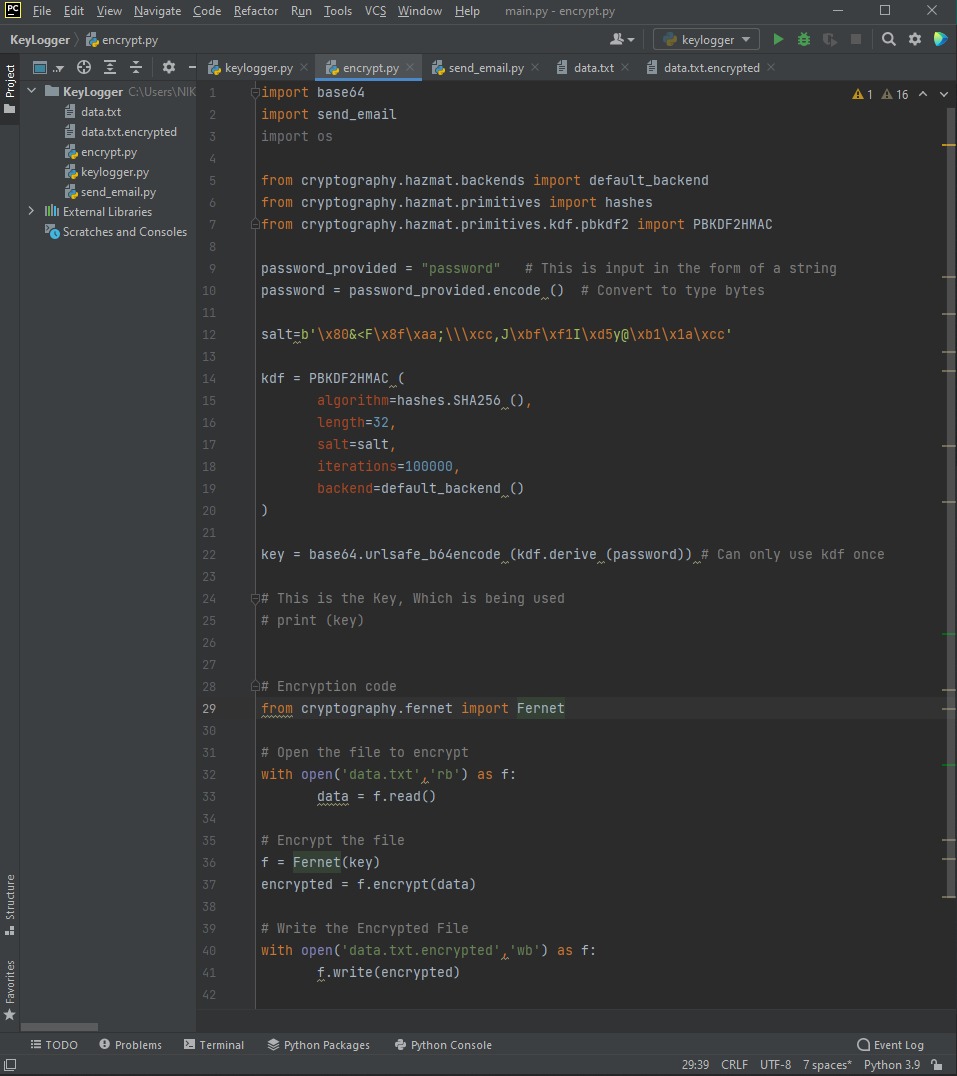
Program will end at the press of esc key

**Step – 5:**

Import the encrypt file to encrypt the data stored in the data.txt with the help of symmetric encryption.

**Step – 6:**

Create encrypt file as **encrypt.py**

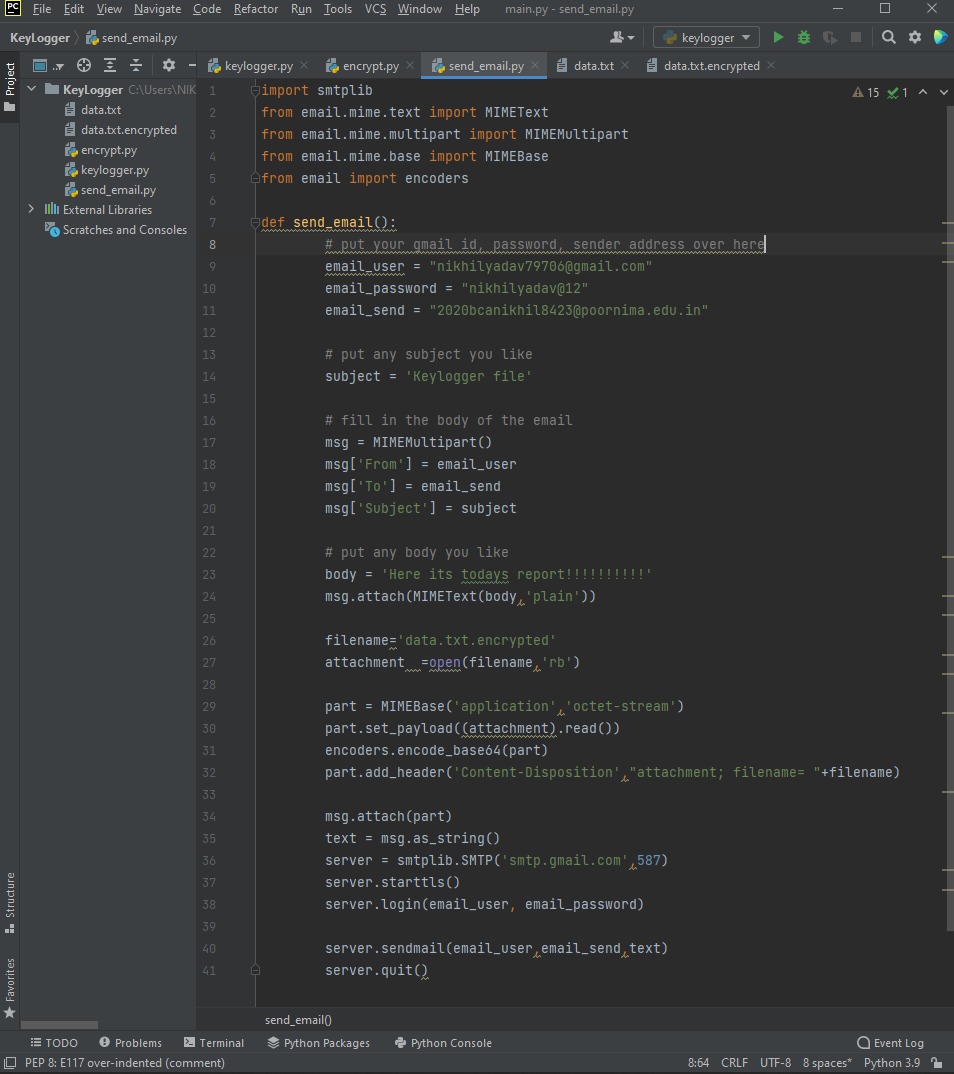


**Step – 7:**

Connect to Send\_email file with the encrypt file.

**Step-8:**

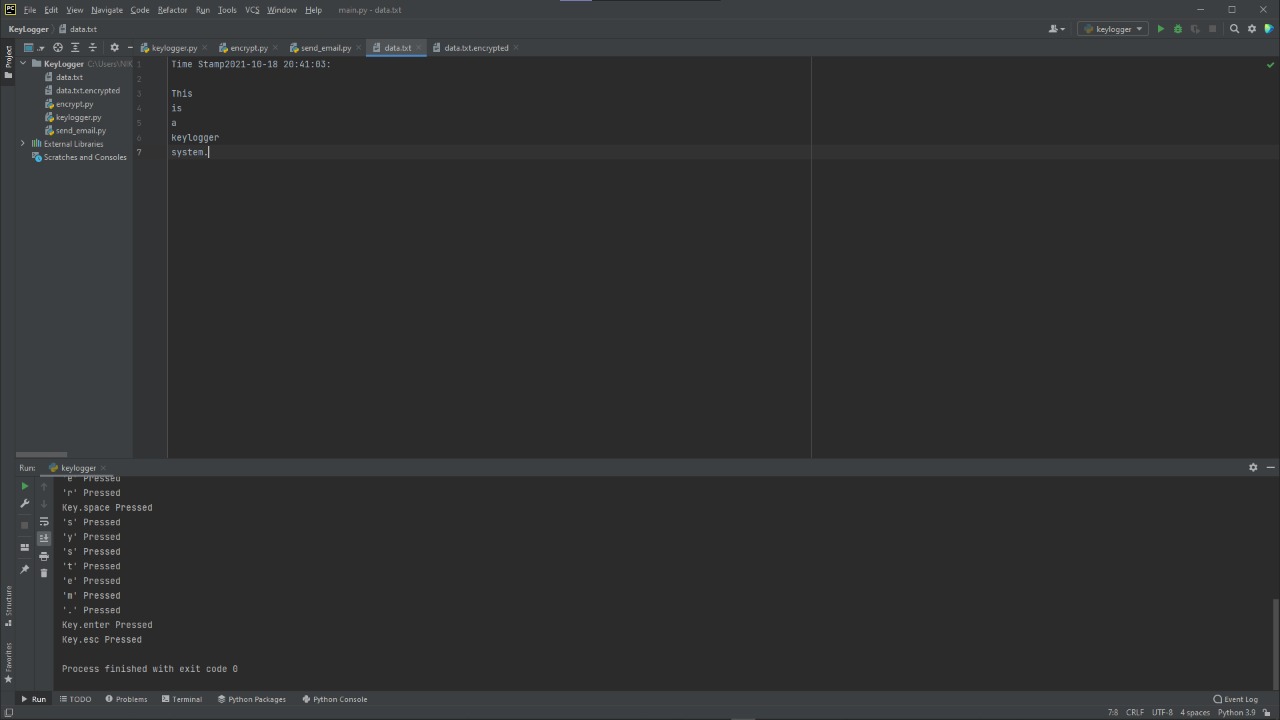
Create the **send\_emial.py** file to automatically send the mail to system without user knowledge by putting your mail id, password, sender email address.



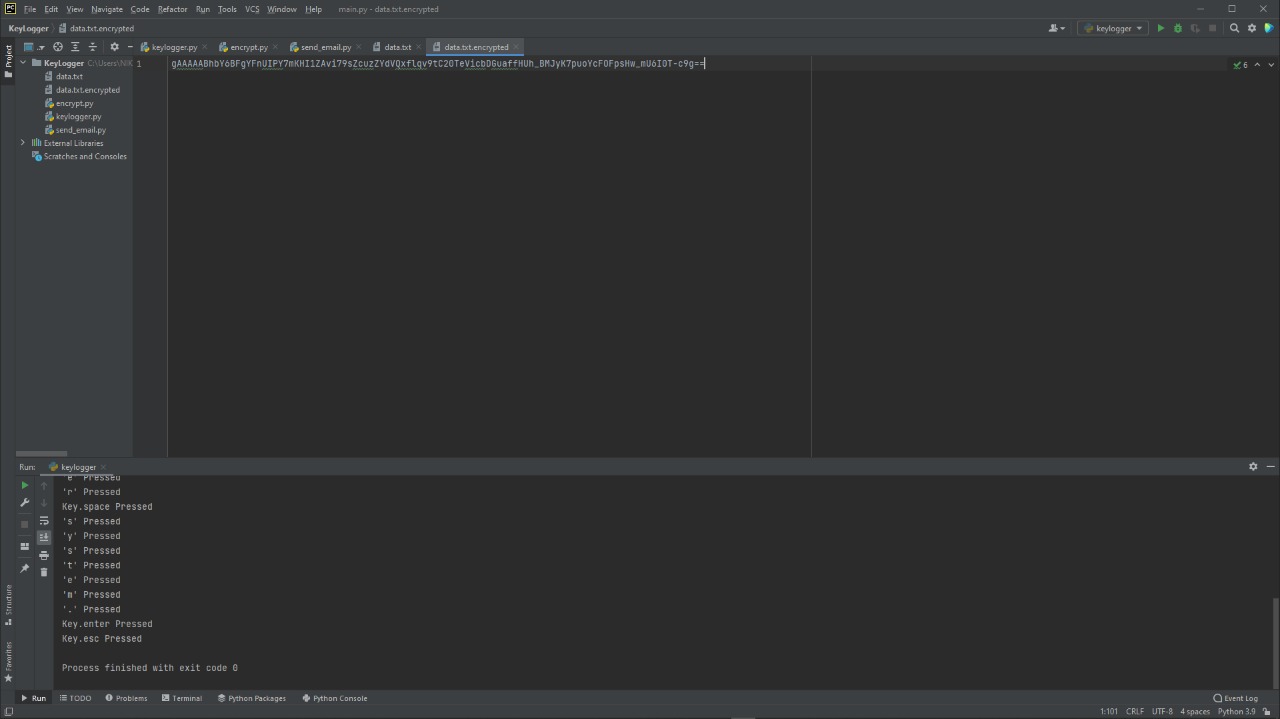
* For Program to work in background without getting noticed we put an extension **“.pyw”** by that it will run program in no console mode means invisible working and quit the program with the **“esc”** key.

# Chapter 3 : Result analysis

* Our keystrokes get stored in the "**data.txt**" file and with the timestamp**.**



* stored file data.txt now goes to encrypt program to get encrypted and saves in "**data.txt.encrypted**"file and only person with key can decrypt it.

****

* Now the encrypted file will get attached to the mail and send it to the mail address provided.

# 

* mail has been sent to owner and now download it to save the file on your system and with help of the key we have we can decrypt it.
* With the help of decryptfilewe decrypt the file content send by mail to us.

# 

# Chapter 4 : Future Scope

Cyber Security is a vast domain and is developing day by day.

Future scope of our project includes:-

* Android support
* Linux support
* Image, video file
* Browser history
* Access control
* Trojan

# Chapter 5 : Conclusion

The product can play out the proposed work like a fundamental keylogger does to get all secret data from client of the framework by getting their keystrokes occasions and mouse clicks without the information on the client. So client of the framework is ignorant of things occurring in foundation. The software is able to monitor data and store the data in a specific folder or send the data to the owner’s mail id. The software is also able to hide itself from the owner if the system while it runs in background. Thus, I accept that my methodology extensively increases current standards for observing the information and gathering it for either lawful or unlawful reason.

Software that can not only monitor every keystroke and action performed at a PC but also be used as legally binding evidence of wrong-doing has been unveiled. Worries about cyber-crime and sabotage have prompted many employers to consider monitoring employees. They have joined forces to create a system which can monitor computer activity, store it and retrieve disputed files within minutes… "People need to recognize that you are using a PC as a representative of a company and that employers have a legal requirement to store data.

# References

Youtube

Github

Google

Books