**ADVANCE KEYLOGGER IN PYTHON**

Submitted in partial fulfillment of the requirements of the degree

BACHELOR OF ENGINEERING IN COMPUTER ENGINEERING

By

Shyam Sanjay Thakur (TE2-59)

Siddharth Lahu Tayade (TE2-57)

Adarsh Ambuj Tripathi (TE2-61)

Devesh Sudhir Nikam (TE2-05)

Supervisor

Prof. Alka Srivastava

**CERTIFICATE**

This is to certify that the Mini Project entitled “Advance keylogger ” is a bonafide work of Siddharth Lahu Tayade (Roll no:-57), Shyam Sanjay Thakur (Roll no:-59), Devesh Sudhir Nikam (Roll no:-05), Adarsh Ambuj Tripathi (Roll no:-61) is submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of “Bachelor of Engineering” in “Computer Engineering” .

(Dr.Suvarna Pansambal) (Prof.Alka Srivastava ) (Dr Ramesh Kulkarni)

Head of Department Supervisor Principal

**Mini Project Approval**

This is to certify that mini project entitled ”Advanced keylogger” is the bonafide work of Siddharth Lahu Tayade (Roll no:57), Shyam Sanjay Thakur( Roll no: 59), Adarsh Ambuj Tripathi(Roll no: 61) , Devesh Sudhir Nikam (Roll no: 05) is approved for the degree of

“Bachelor Of Engineering” in Computer Engineering.

Examiners

1………………………………………

(Internal Examiner Name & Sign)

2………………………………………

(External Examiner name & Sign)

Date:

Place:

**Contents**

● Abstract

● Acknowledgments

1. Introduction

1.1 Introduction

1.2 Objectives

1.3 Specifications

1.4 Scope

1.5 Methodology

2. Literature Survey

2.1 Survey of Existing System

2.2 Limitation Existing system or research gap

3. Proposed System

3.1 Introduction

3.2 Flowcharts

3.3 Software and hardware Requirement

3.4 Implementation

3.5 Security

3.6 Future work.

• References

**ABSTRACT**

Keyloggers is the action of recording the key stroke on a keyboard, typically in a covert manner. Software Keyloggers are detected based on the behavioral characteristics. They don't provide root privileges; detection is based on permission from kernel and prone to many attacks. Software Keyloggers is a software program that can be installed onto a computer, which monitors all the user activities on computer.

Keyloggers steal the confidential information and they completely run in stealth mode. When Keyloggers is installed in a computer, it is not shown either in start-up icons or anywhere else on the computer that is being monitored.

Software Keyloggers have posed a great threat to user privacy and security. Detection of Keyloggers is difficult because they run in hidden mode. Detection of Software Keyloggers is done using various technique namely Anti-Hook techniques, Spyware detection, bot detection, safe access to password protected accounts and dendritic cell algorithm. These algorithms are used to detect the existence of Keyloggers in computer, which strengthens user privacy and security.

**ACKNOWLEDGEMENT**

We are thankful to all the faculty members, providing their valuable time and guidance in elaborating views of studying the project details and getting the right version for its implementation.

We would like to express a deep sense of thanks and gratitude to our project guide prof. Alka Srivastava for constantly guiding us throughout this project. Her constructive advice and constant motivation have been responsible for the successful completion of this project.

We have greatly benefited from the valuable guidance, encouragement and kind supervision given to us throughout this project which helped us to develop the project successfully.

Submitted By,

Shyam Sanjay Thakur, Roll no:-59

Adarsh Ambuj Tripathi, Roll no:-61 Siddharth Lahu Tayade, Roll no:-57

Devesh Sudhir Nikam, Roll No:-05

Under the guidance of Prof. Alka Srivastava

**1. INTRODUCTION**

**1.1 Introduction**

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. Working: Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970’s and was a hardware key logger and first software key-logger was developed in 1983.

Keylogging programs, commonly known as keylogger, are a type of malware that maliciously track user input from the keyboard in an attempt to retrieve personal and private information. The keyboard is the primary target for keylogger to retrieve personal and private information. The keylogger is the primary target for keylogger to retrieve user input from, because it is the most common user interface with a computer.

Keylogger is a program with which we monitor keystrokes. These keystrokes will be stored in a log file. We can record sensitive information like username and password using this keystroke. To create a keylogger we are going to use the pynput module.

**1.2 Objectives**

* The main objective of keyloggers is to interfere in the chain of events that happen when a key is pressed and when the data is displayed on the monitor as a result of a keystroke.
* Keyloggers are built for the act of keystroke logging — creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal.
* Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities.

**1.3 Specifications**

* The keylogger should be able to capture keystrokes made on the keyboard, and save them to a log file. This can be done using Python's built-in keyboard module, which provides functions for capturing keyboard events.
* For security reasons, the keylogger should be hidden from the user, so that they are not aware that their keystrokes are being logged. This can be done by running the keylogger as a background process.
* The keylogger should save the captured keystrokes to a log file, which can be in plain text or encrypted form. The log file should include the date and time of each keystroke.

**1.4 Scope**

* Educational project: The project could be designed as an educational tool to help students understand how keyloggers work and how they can be used to capture sensitive information.
* Research project: The project could be designed as a research tool to study user behavior and gather data on how users interact with their computers or mobile devices.
* Security project: The project could be designed as a security tool to monitor and track the activity of users on a network or system, with the aim of identifying potential threats or security breaches.
* Malware project: The project could be designed as a malware tool to be used for malicious purposes, such as stealing passwords, credit card information, or other sensitive data.

**1.5 Methodology**

**Planning:** This involves defining the scope and purpose of the keylogger project. The planning phase includes determining the type of keylogger to be developed,the platform it will run on, and the features it will have.

**Development:** This involves the actual implementation of the keylogger. The development phase includes writing the code, testing the program, and ensuring that it meets the design specifications.

**Deployment:** This involves installing the keylogger on the target system or network. The deployment phase includes selecting the appropriate method of installation, such as email, social engineering, or other tactics.

**Data collection:** This involves collecting the data that is logged by the keylogger. The data collected by the keylogger typically includes keystrokes, screenshots, and other information about the user's activity.

**Data storage:** This involves storing the data collected by the keylogger. The data may be stored locally on the target system or sent to a remote server for storage.

**2. LITERATURE SURVEY**

**2.1 Survey of existing system:**

Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities.

Some keyloggers can also capture your screen at random intervals; these are known as screen recorders. Whether for malicious intent or for legitimate uses, you should be aware how keyloggers are affecting you. First, we'll further define keystroke logging before diving into how keyloggers work. Then you'll be able to better understand how to secure yourself from unwanted eyes.

**2.2 Limitation in existing system:**

● Often flagged by antimalware software as malicious

● Incapable of logging BIOS inputs.

● Typically needs to be installed in line with the keyboard making it easy to detect.

● Requires direct access to the target device, making remote management impossible..

**3.PROPOSED SYSTEM**

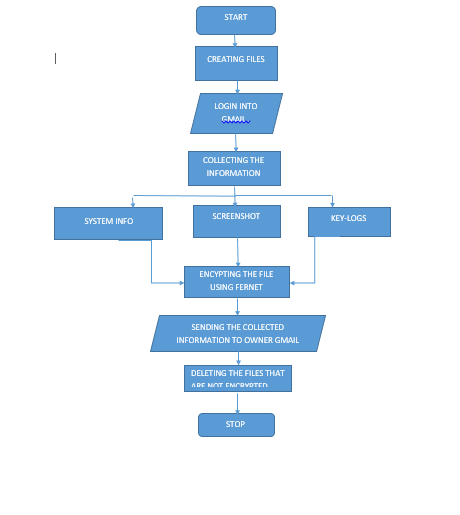
**3.1 Introduction**

Nowadays, computers are used everywhere to carry out daily routine tasks. The input devices i.e. keyboard or mouse are used to feed input to computers. The surveillance of input devices is much important as monitoring the users logging activity. A keylogger also referred as a keystroke logger, is a software or hardware device which monitors every keystroke typed by a user. Keylogger runs in the background that user cannot identify its presence. It can be used as monitoring software for parents to keep an eye on children activity on computers and for the owner to

monitor their employees. A keylogger (which can be either spyware or software) is a kind of surveillance software that has the ability to store every keystroke in a log file. It is very dangerous for those systems which use their system for daily transaction purpose i.e. Online Banking Systems. A keylogger is a tool, made to save all the keystroke generated through the machine which sanctions hackers to steal sensitive information without user’s intention. Privileged also relies on the access for both implementation and placement by Kernel keylogger, the entire message transmitted from the keyboard drivers, while the a programmer simply relies on kernel level facilities that interrupt. This certainly needs a large power and expertise for real and error-free execution. However, it has been observed that 90% of the current keyloggers are running in userspace so they do not need any permission for execution.

**3.2 Flowchart**

* System Flowchart



**3.3 Software and Hardware Requirements:**

* Software Requirements: Oracle virtual box, Windows 10 VM.
* Language: python
* Necessary Modules: SMTP, CRYPTOGRAPHY, SOCKET, PYNPUT.
* Hardware Requirements:INTEL i3
* Main Memory(RAM): 4GB
* Cache memory: 512KB

* Monitor : 14 inch Color

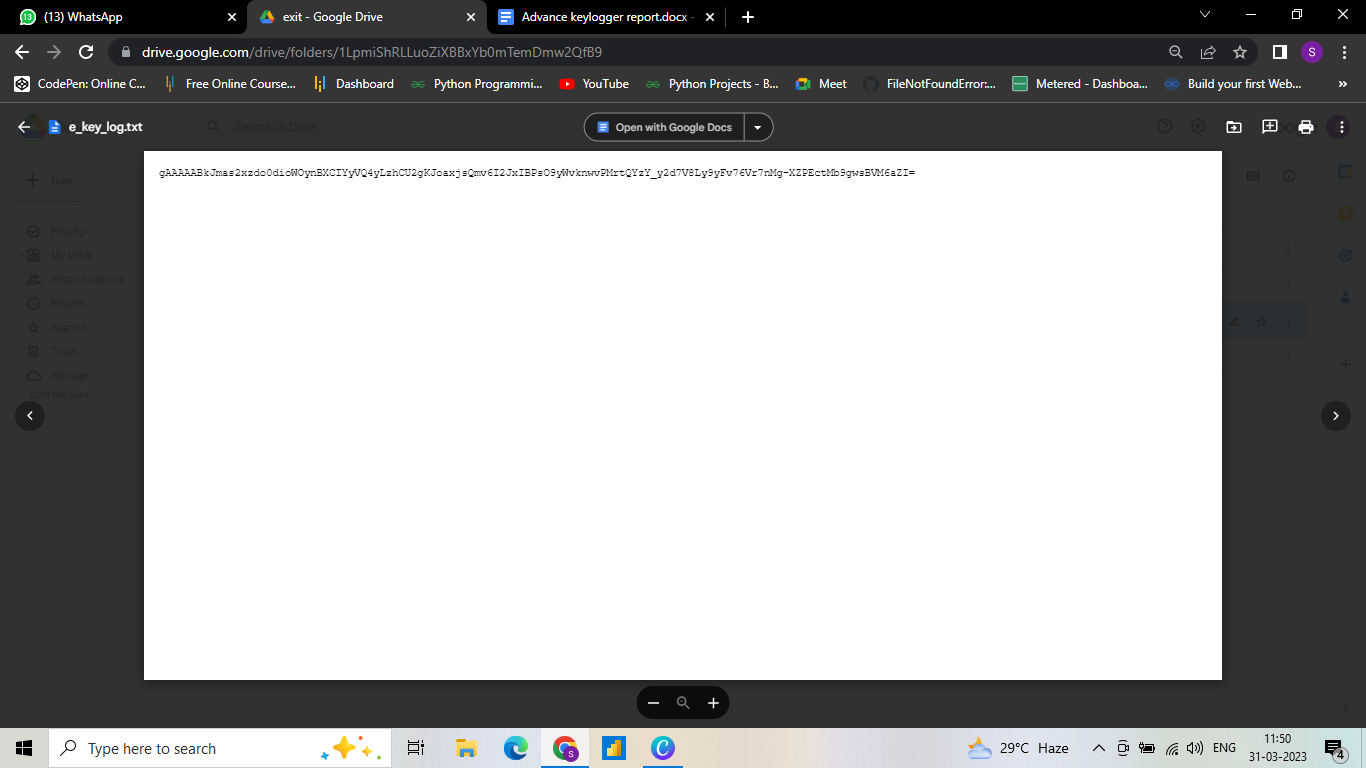
* Monitor Keyboard : 108 Keys

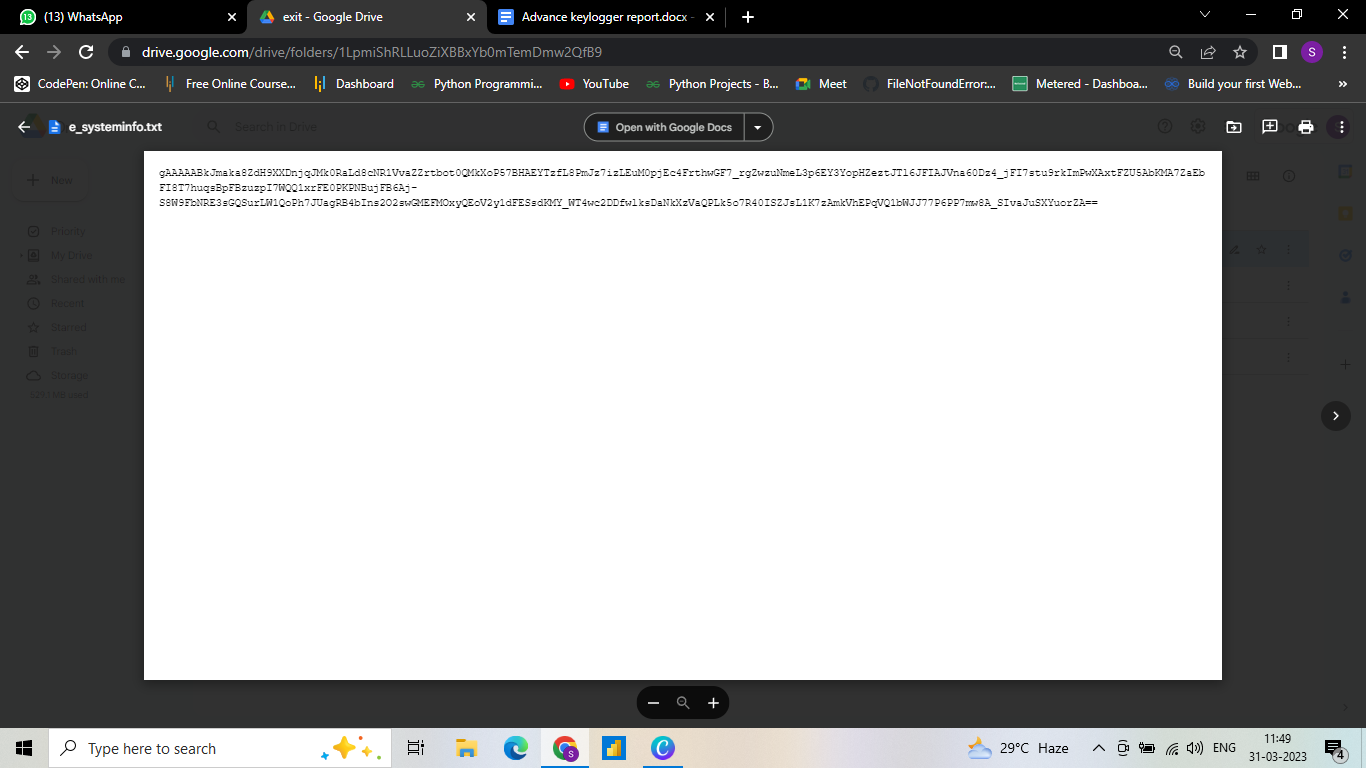
* Mouse : Optical Mouse

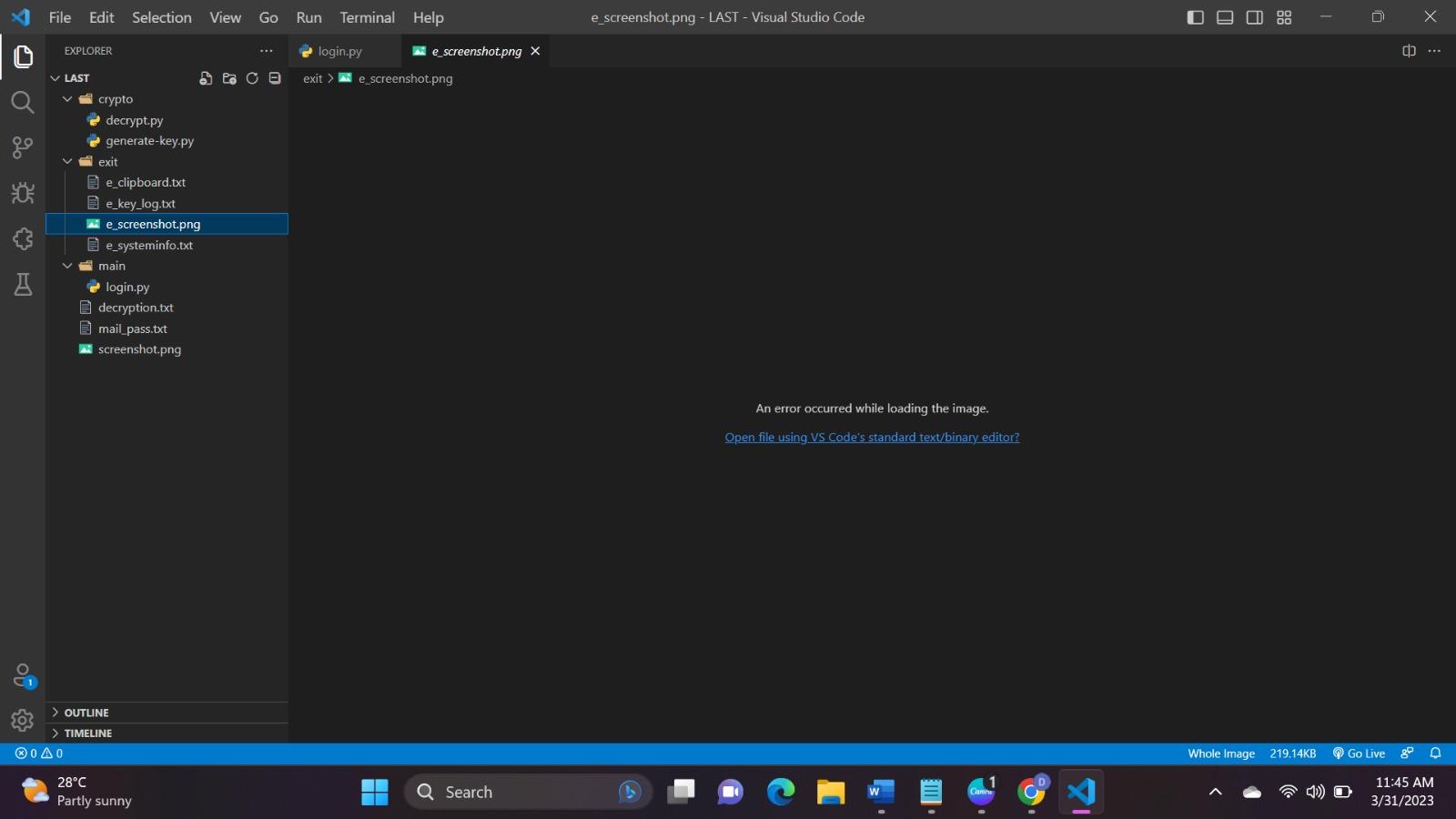
* Hard Disk: 20 GB

**3.4 Implementation:**

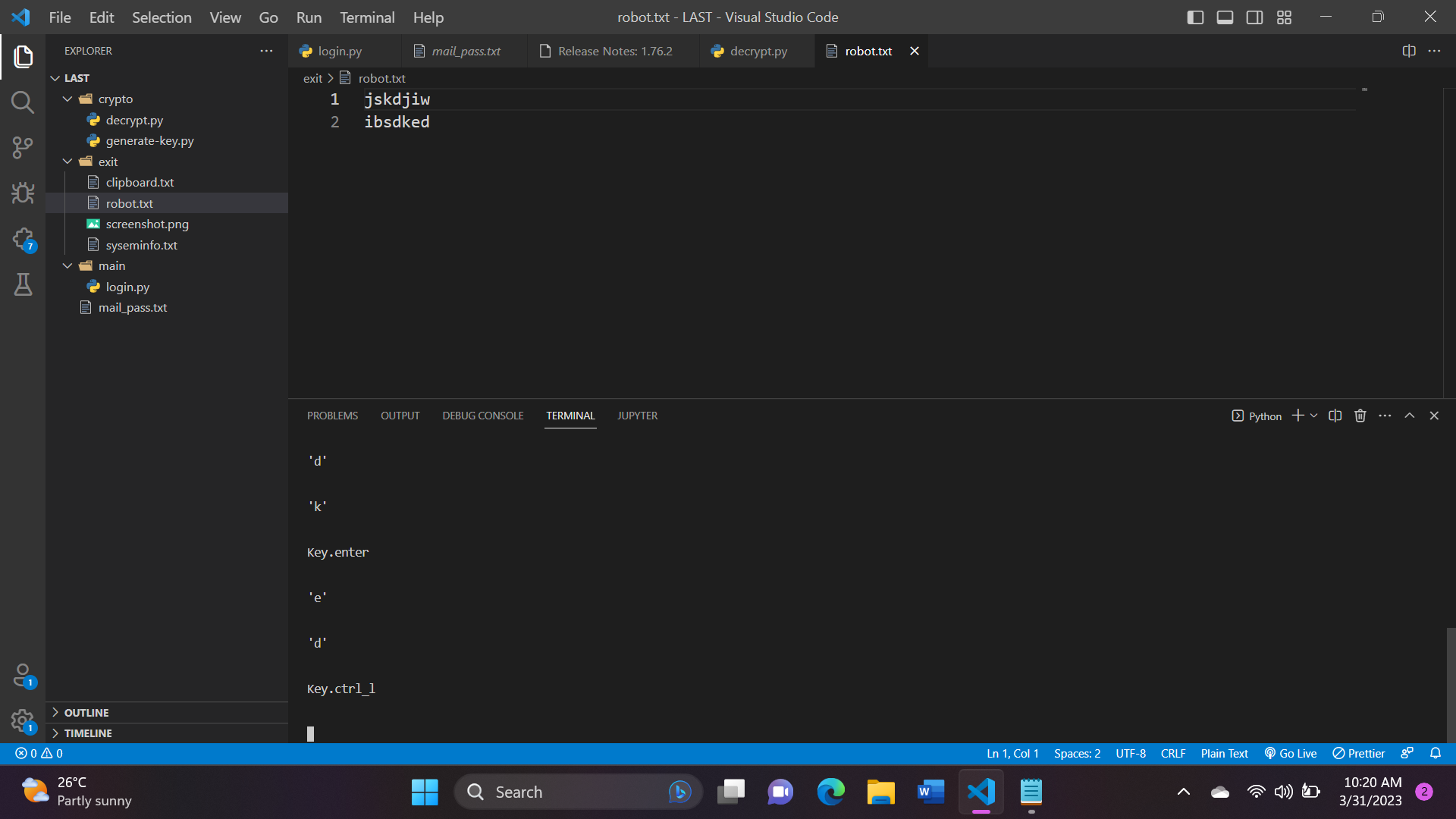
* **ENCRYPTED**





****

* **DECRYPTED**

****

**3.5 Security:**

The password entered by the user is concatenated with a random generated salt as well as a static salt. The concatenated string is passed as the input of the hashing function. The result obtained is stored in the database. Dynamic salt is required to be stored in the database since it is different for different users. When the user is to be authenticated, first the value of dynamic salt for that user is fetched from the database, it is concatenated with user supplied input and the static salt. The result is compared with the hash stored in the database.

If the database is compromised the hacker will not only get your password hashes but also the dynamic salt used. You might be wondering then what is the advantage of dynamic salt over static salt if attacker has dynamic salt? Even if the attacker has dynamic salt he needs to create a new hash-table (or rainbow table) for each and every user present in the database (as per dynamic salt). This is a lot more expensive operation than creating just one table for all the users.

**3.6 Future Work and Conclusion:**

* The model is created by taking security purposed under condition, for major organization
* As the model is build on software terms, in future it will be able to install in operating system using hardware tearms
* We can also be able to convert .py file to .exe using auto-py-to-exe library.

**REFERENCES:**

* 1. Nyang, DaeHun; Mohaisen, Aziz; Kang, Jeonil . ["Keylogging-Resistant Visual Authentication Protocols"](https://ieeexplore.ieee.org/document/6746187). *IEEE Transactions on Mobile Computing*.(2014-11-01)
* 2. Conijn, Rianne; Cook, Christine; van Zaanen, Menno; Van Waes, Luuk  ["Early prediction of writing quality using keystroke logging"](https://doi.org/10.1007%2Fs40593-021-00268-w). *International Journal of Artificial Intelligence in Education*.(2021-08-24).
* 3. [Use of legal software products for computer monitoring](https://www.keylogger.org/keylogger.html#h_8), keylogger.org
* 4. [Keyloggers: How they work and how to detect them (Part 1)](https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/), *Secure List*, "Today, keyloggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new keylogger Trojans for this very purpose.