**INSTRUCTION MANUAL**

**FOR**

**SECRET MESSENGER**

**TEAM MEMBERS:**

AKASH KUMAR

RAJESH

SAHIBJOT SINGH

VIKAS KUMAR

**TABLE OF CONTENTS:**

|  |  |  |
| --- | --- | --- |
| **SR. NO.** | **DESCRIPTION** | **PAGE NO.** |
| 1 | General Information | 3 |
| 2 | Description | 3 |
| 3 | System Overview | 3 |
| 3.1 | System Configuration | 3 |
| 3.2 | User Access Levels | 3 |
| 3.3 | Contingencies | 3 |
| 4 | First Things First | 3-4 |
| 5 | Getting Started | 4-7 |
| 6 | Features | 8 |
| 7 | Benefits | 8 |

1. **GENERAL INFORMATION**

Secret Messenger software is intended to encrypt confidential messages that one can send though mail. This software uses a single key for both encryption and decryption which is one of the basic techniques of cryptography. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext.

1. **DESCRIPTION**

Cryptography is an indispensable tool for protecting information in computer systems. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Keeping this thing in mind, Secret Messenger has been developed to cater these requirements. The sender can send confidential message in encrypted form to receiver through e-mail using internet. As we know, the cyber threats are shooting up; therefore the need to protect information becomes a paramount concern. The receiver, on the other hand, can decipher the message/code using the same software only if he is provided with correct decryption key.

1. **SYSTEM OVERVIEW**

**3.1 SYSTEM CONFIGURATION**

Secret Messenger software can operate on any computer having Windows XP and above. It is compatible only with Python 3.6.3 IDE. The application requires connection to Internet in order to send and receive encrypted messages. After installing Python 3.6.3 IDLE on the computer, Secret Messenger can be used immediately without any further configuration.

**3.2 USER ACCESS LEVELS**

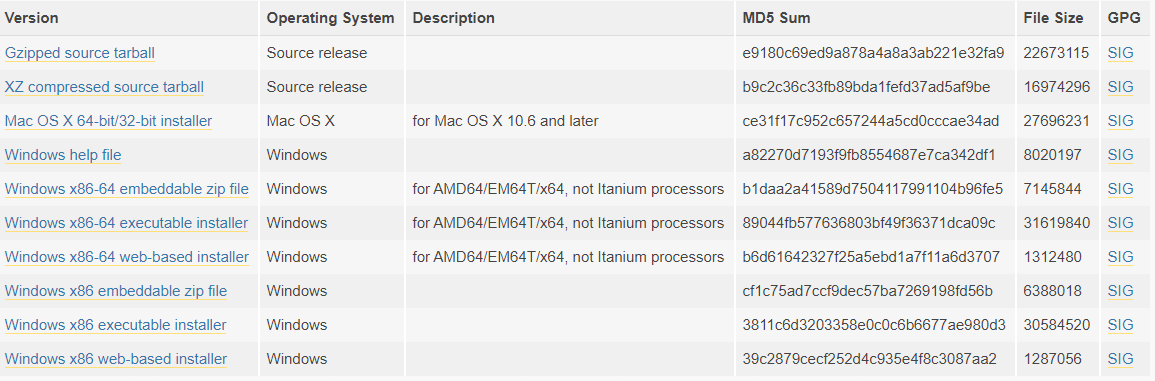
Only the sender and receiver, who have this software installed in their PCs, can use this application.

**3.3 CONTINGENCIES**

In case there is no Internet connection, the sender can’t send the encrypted message and the receiver can’t receive it.

1. **FIRST THINGS FIRST**

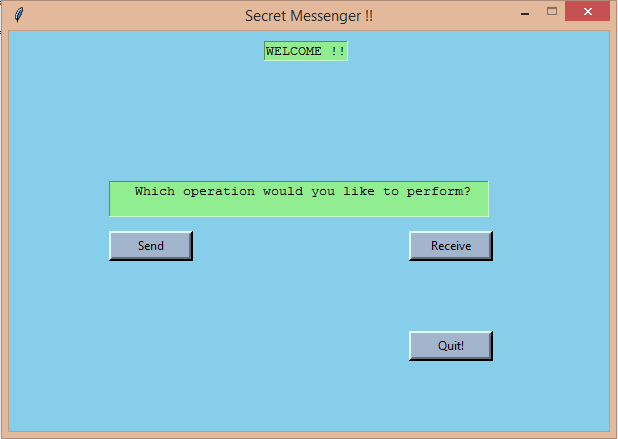
In order to run this application, one must first install Python 3.6.3 IDLE. To install it, go to <https://www.python.org/downloads/release/python-363/> and move to the following section to download the recent version compatible to your computer. Click on [Windows x86-64 executable installer](https://www.python.org/ftp/python/3.6.3/python-3.6.3-amd64.exe) to quickly install the IDLE.



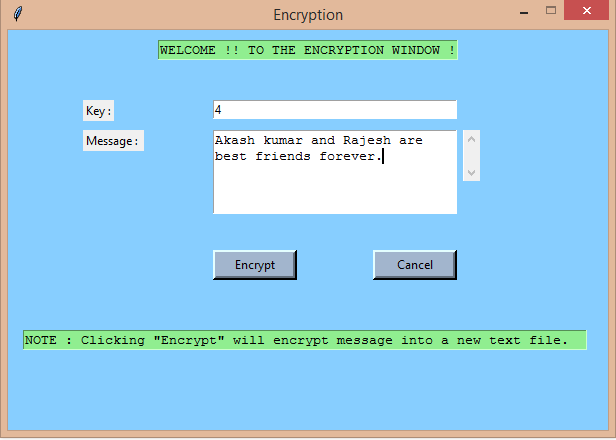
1. **GETTING STARTED**

* After the successful installation of IDLE, open the source code in it and go to Run🡪 Run the module. When you’ll execute the software, home page will be displayed to you first, this will ask you to choose one of the three operations available.

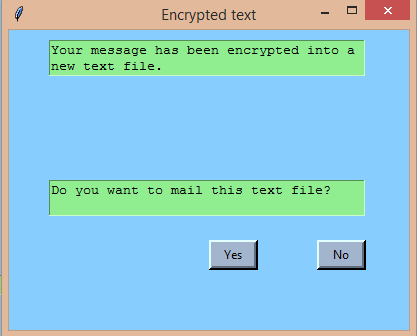
1. Send
2. Receive
3. Quit



* If you’ll click on **‘Send’** button, the following Encryption Window will appear on screen.

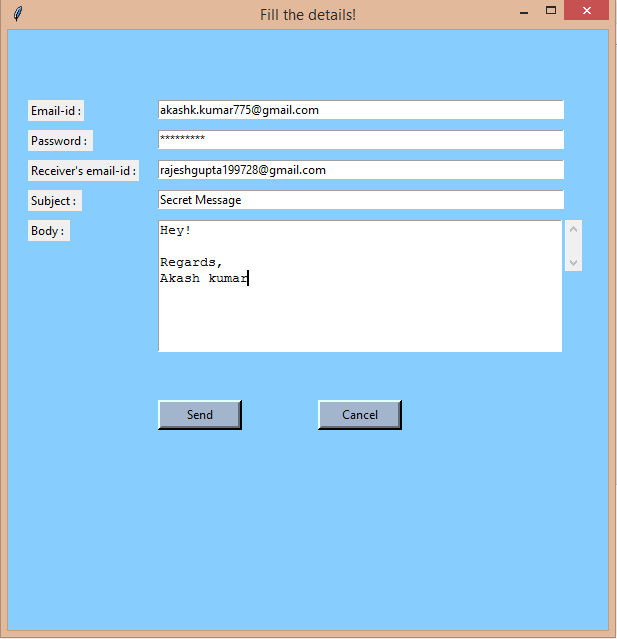


* Input the encryption key in **‘Key’** Text Field, using which you want to encrypt your confidential message.
* Type in the message in **‘Message’** Text Field.
* Click on **‘Encrypt’** Button to encrypt the message into a new text file named **‘encrypted\_file’** which will be saved on sender’s computer and following dialog box will pop up.

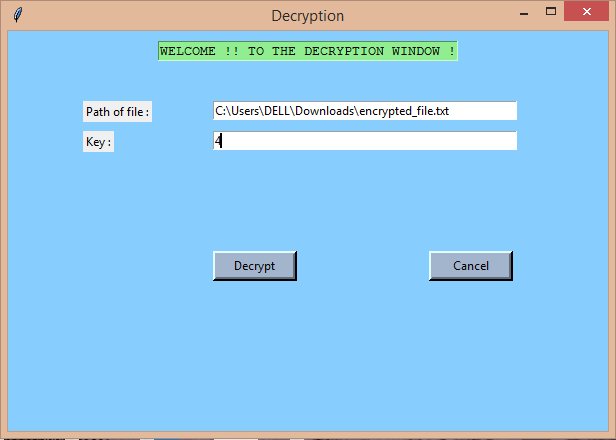


* Click on **‘Yes’** to send the encrypted message through mail.
* A new window will appear on screen which will ask you to fill out the following details:

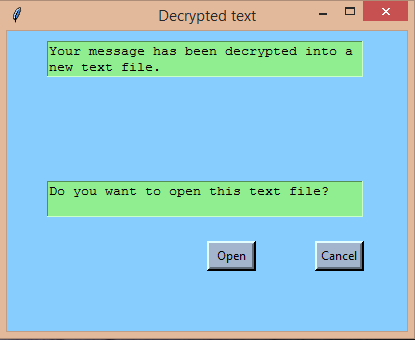
1. Sender’s Email-id
2. Sender’s Password
3. Receiver’s Email-id
4. Subject of the mail
5. Body of the mail



* Click ‘Send’ button to send the encrypted message to receiver.
* Receiver would also open the software to decrypt the message after downloading the encrypted message file into his computer.
* Click on **‘Receive’** button to perform decryption.
* Receiver would enter the correct path of encrypted file in **‘Path of file’** text field followed by correct decryption key in **‘Key’** text field to decrypt the message.



* Click on **‘Decrypt’** button to decrypt the encrypted message.
* The following window will appear on screen giving you confirmation about the new text file in which decrypted (original) message is saved.



* To open the text file, click on **‘Open’** button. The decrypted message will be saved in new file named **‘decrypted\_file’** on receiver’s computer.

1. **FEATURES:**

* The source code is written in Python Language which is easy to understand and implement. All we need is Python 3.6.3 IDLE which is compatible with given source code.
* The interface for this application is designed using Tkinter module which is user-friendly.
* With secret key cryptography, both communicating parties use the same key to encrypt and decrypt the messages.
* The amount of efforts or time required to learn how to use the software is less. This makes the software user-friendly even for IT-illiterate people.
* The software supports extensibility, that is, it is easy to add more functions in it to increase its flexibility.
* It can be run on different platforms such as Windows and Mac.

1. **BENEFITS:**

* **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
* **Authentication**: the sender and receiver can confirm each other’s identity and the origin/destination of the information
* **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.
* **Non-repudiation**: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information