**SAFE KLUTCHER**

**A PROJECT REPORT**

###### ***Submitted by***

##### Adnan Khan (19BCY10051)

**Priya Sharma** (19BCY10077)

**Saloni Gupta** (19BCY10007)

**Vipul Jaiswal** (19BCY10016)

*in partial fulfillment for the award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

*in*

# **COMPUTER SCIENCE AND ENGINEERING**



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

##### NOV 2020

**VIT BHOPAL UNIVERSITY,KOTHRIKALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“SAFE KLUTCHER”** is the bonafide work of “**ADNAN KHAN (19BCY10051), SALONI GUPTA (19BCY10007), PRIYA SHARMA (19BCY10077), VIPUL JAISWAL (19BCY10016)”** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported here does not form part of any other project / research work on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

**PROGRAM CHAIR PROJECT GUIDE**

Dr. Shishir kumar Shandilya Dr. Gaurav Choudhary

School of Computer Science and Engineering School of Computer Science and Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGEMENT**

First and foremost I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. Manas Kumar Mishra, Head of the Department, School of Computer Science for much of his valuable support and encouragement in carrying out this work.

I would like to thank my internal guide Dr. Gaurav Choudhary, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science, who extended directly or indirectly all support.

Last, but not the least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**ABSTRACT**

The world today relies heavily on encryption. Many of our daily mission-critical activities, tasks and jobs require the use of internet and digital platform encryption. From ordinary citizens to businesses, organizations, and government agencies today’s world relies on the power of encryption to make data transfer as confidential and secure as possible. And with the advent of Big Data and the Internet of Things, the need for encryption will only grow exponentially in the years to come.Just by interacting with their devices as they normally would, end users are sending encrypted messages and data every day. Some platforms, of course, have stronger measures than others, and even among the most-protected systems, there may exist flaws. Importantly, we continue to get better at encrypting data, possibly too good, for some and third-party services add an extra layer of security to built-in encryption software.

Thus we want to advance the concept of encryption to integrate it with other forensic tools to take data protection to the next level .

**TABLE OF CONTENTS**

| CHAPTER NO. | TITLE | PAGE NO. |
| --- | --- | --- |
|  | Acknowledgement  Abstract  List of Figures | 2  3  6 |
| 1 | INTRODUCTION 1.1 Introduction 1.2 Motivation for the work  1.3 Problem statement  1.4 Objective of the work  1.5 Summary | 7  8  8  8  8 |
| 2 | LITERATURE SURVEY  2.1 Introduction  2.2 <Core area of the project>  2.3 Existing Algorithms  2.4 Research issues/observations from  literature Survey  2.5 Summary | 9  9  10  12  12 |
| 3 | PROJECT PROCEDURE (Methodology followed)  3.1 Introduction  3.2 Disadvantages/Limitations in the existing system  3.3 Proposed System  3.4 Summary | 13  14  15  16 |
| 4 | WORK DONE  4.1 Introduction  4.2 Module description   1. Photo Capture Module 2. Encryption and Decryption Module 3. Database Module 4. Logs Module   4.3 Module workflow  4.4 System Architecture  4.5 Summary | 17  17  18  18  21  21  22  23  24 |
| 5 | OBSERVATION  5.1 Introduction  5.2 Performance Measures  i. Testing  5.3 Performance Analysis  i. Feedback  5.4 Summary | 25  25  25  27  27  28 |
| 6 | RESULT AND CONCLUSION  6.1 Introduction  6.2 Limitation/Constraints of the System  6.3 Future Enhancements  6.4 Conclusion | 29  29  30  30 |
| 8 | REFERENCES | 31 |
|  |  |  |

**LIST OF FIGURES**

| **S.No** | **Figure Number** | **Figure name** | **Page Number** |
| --- | --- | --- | --- |
| 1 | fig 3.3.1 | real time usage | 3.3.1 |
| 2 | fig. 4.2 | Different modules | 4.2 |
| 3 | fig. 4.3 | Workflow of the modules | 4.3 |
| 4 | fig. 4.4 | Architecture of the whole system | 4.4 |
| 5 | fig 5.2(a) | Testing (a) | 5.2 |
| 6 | fig 5.2(b) | Testing (b) | 5.2 |
| **7** | fig 5.2(c) | Testing (c) | 5.2 |
| 8 | fig 5.3 | Feedback | 5.3 |
|  |  |  |  |

**INTRODUCTION**

**1.1 Introduction**

More and more data records are being lost and stolen everyday. As breaches continue to plague in organization and the impact to individual increase,the need to protect such breaches has increased.

If we work on our project we need to work with files that contain privileged information which is stored in our computer disk and the best way to secure those files is by using encryption tools.

As healthcare gets digitized in the Indian context and with millions of digital health records being produced every day in places like public health centers and hospitals, concerns around data privacy are coming up. In the latest data leak related to users in India, over a million medical records and 121 Mn medical images of Indian patients, including X-rays and scans, have been leaked online to be freely accessible by anyone. Given the importance and the possibility of data being used for surveillance or corporate interests, it is critical to establish a robust and sensitive data governance structure among the various stakeholders.

Therefore, the aim of this work is to provide tools that safeguard a firm's integrity.

**1.2Motivation for the work**

Very keen interest in the subject of Cyber security and Digital forensics, as we do not have very strict rules for safe guardian privacy in india thus we wanted to work on technology that could help hospitals ,schools etc to protect the personal data that they have and we came up with idea to build an encryption tool which also provide digital evidence in case of breach .

**1.3 Problem statement**

To create an encryption tool to encrypt data and decrypt data by the user using a private key and also add features that could provide digital evidence in case of breach.

**1.4 Objective of the project**

To successfully encrypt and decrypt files as per users needs and to develop tools which help us to identify possible suspects and provide surveillance data of the time ofdata breaches that happen and capturing images at the time of breach.

**1.5 SUMMARY**

The need for encryption tools have become very important in today’s world. Therefore, our aim of this work is to provide tools that itself is an integration of different forensic tools so that privacy could be enhanced with the help of surveillance.

**2. LITERATURE SURVEY**

**2.1 Introduction**

Encryption technology might serve as a key factor to create a more secure environment by encrypting sensitive digital documents present inside the firm.

[Needham R M](https://en.wikipedia.org/wiki/Roger_Needham) , This paper introduced the basic ideas of cryptographic protocols and showed how both secret key and public key encryption could be used to achieve authentication. Shamir. A[.](https://en.wikipedia.org/wiki/Adi_Shamir) in this paper Shamir tried to explain a safe method for sharing a secret.This report presents a detailed review in the field of encryption technology . Cryptographic technique is one of the principal means to protect information security. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm. This we propose an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm. In addition, the encrypt procedure and code implementation is provided in details with some extra features added to it .

**2.2 Core area of the project**

The core area of the project is Data privacy and digital forensics .

**2.3Existing Algorithms**

There’s a host of different encryption algorithms available today. Here are some of the more secured once -

AES. The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations. Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for very demanding encryption purposes. AES is widely considered invulnerable to all attacks except for brute force. Regardless, many internet security experts believe AES will eventually be regarded as the go-to standard for encrypting data in the private sector.

Triple DES. Triple DES is the successor to the original [Data Encryption Standard (DES) algorithm](http://www.simplilearn.com/what-is-des-article), created in response to hackers who figured out how to breach DES. It’s a symmetric encryption that was once the most widely used symmetric algorithm in the industry, though it’s being gradually phased out. TripleDES applies the DES algorithm three times to every data block and is commonly used to encrypt UNIX passwords and ATM PINs.

RSA. RSA is a public-key encryption asymmetric algorithm and the standard for encrypting information transmitted via the internet. RSA encryption is robust and reliable because it creates a massive bunch of gibberish that frustrates would-be hackers, causing them to expend a lot of time and energy to crack into systems.

Blowfish. Blowfish is another algorithm that was designed to replace DES. This symmetric tool breaks messages into 64-bit blocks and encrypts them individually. Blowfish has established a reputation for speed, flexibility, and being unbreakable. It’s in the public domain, so that makes it free, adding even more to its appeal. Blowfish is commonly found on e-commerce platforms, securing payments, and in password management tools.

Twofish. Twofish is Blowfish’s successor. It’s a license-free, symmetric encryption that deciphers 128-bit data blocks. Additionally, Twofish always encrypts data in 16 rounds, no matter what the key size. Twofish is perfect for both software and hardware environments and is considered one of the fastest of its type. Many of today’s file and folder encryption software solutions use this method.

Rivest-Shamir-Adleman (RSA). Rivest-Shamir-Adleman is an asymmetric encryption algorithm that works off the factorization of the product of two large prime numbers. Only a user with knowledge of these two numbers can decode the message successfully. Digital signatures commonly use RSA, but the algorithm slows down when it encrypts large volumes of data.

**2.4 Research issues/observations from literature Survey**

The security of any encryption algorithm should never depend upon the secrecy of the algorithm itself. Rather, the algorithm should be publicly disclosed and open to the cryptographic community for analysis. The true security of the algorithm should always lie in the security of the keys used to decrypt messages.The most important thing to keep in mind when choosing an encryption algorithm is that you should select an algorithm that is widely used and accepted by the security community. Unless you are a highly skilled and well-trained mathematician, you should *never* try to write your own encryption algorithm. It's simply far too difficult to create an algorithm that is not inherently flawed. Think of it as building your own pacemaker: It's simply not worth the risk.While making this tool implementation speed increased rapidly because of adding different features to it thus we identified features which were taking too much time to implement. We, either removed them or tried to make them more efficient .Being a multifunctional tool it is difficult to make the whole tool in one go thus we divided the whole project in sub projects and then integrate it at the last.Finding bugs in the code was a challenging task , we made many mistakes to give proper input to the program so that it can run .

**2.5 Summary**

The encryption tool we are making uses a very secure RSA algorithm for encryption where a specific file is selected and replaces the original data with encrypted data . We evaluated the RSA algorithm on several security factors before choosing the algorithm we use for our tool encryption tool .

**3. PROJECT PROCEDURE**

**3.1 Introduction**

1. We aimed at securing a file using a hybrid RSA cryptographic technique and collecting important digital forensic evidence to save time in case of emergencies.

2. We decided to go with PYTHON, as it has many in-built libraries. Firstly we did half code in C++, but it started becoming difficult as we proceeded with C++ due to individual installation of each new library.

3. We conducted a survey before starting building our program to know the reaction of people to such a project.

4. We divided the project into modules for the ease of working and debugged them individually.

5. After completing all the modules we combined them and run the code as one.

6. We conducted a final testing survey to see if the requirements and expectations of users are fulfilled and to which extent.

**3.2. Disadvantages/Limitations in the existing system**

1. Forgetting Passwords may lead to lost data.
2. RSA algorithms restrict us in many ways like it makes it difficult to add different features to the algorithm to make a full fledged tool.
3. Adding features was making the algorithm vulnerable.

Few of the challenges we faced were,

* how to increase the implementation speed.
* Since we are trying to make a multi featured project it was difficult to make it in one go as a whole so for that we divided the project into subprojects and then later combined it all together.
* Now finding bugs and fixing them was the most time consuming task of all .

## 

## 

## 

## 

## 

## 

## 

## 

## 3.3. Proposed System

## 3.3.1. Real time Usage

fig. 3.3.1 real time usage

Now how will the user interaction be in real time while using the program,

Firstly as soon as they run the program the user will see a prompt asking for whether they want to encrypt a file or open a protected file and if they choose to encrypt a file they will be asked again to give the files path and password they want to set for it.

And if they decide to open an encrypted file they'll be asked to give the files the correct path and the password they set earlier to unlock it. if they type the password correctly they can access the file otherwise they'll get 3 attempts after that the file will be locked for 2 min. to before he/she can reattempt . This 2minutes of cooldown/ waiting time can be increased accordingly later on up to any amount of time.

**3.4. Summary**

In the project procedure, we discussed the methodology or we can say what were the methods we did at the time of completion of the project, what was our idea and how we implemented it. We also presented our idea using a workflow chart.

**4. WORK DONE**

## 4.1. Introduction

We divided our project into 4 main modules i.e. the photo capture module which helps to take the photo, encryption & decryption module for encrypting and decrypting the files, database module to store the necessary data and logs module which helps record the logs of every login.

**4.2. Module Description**

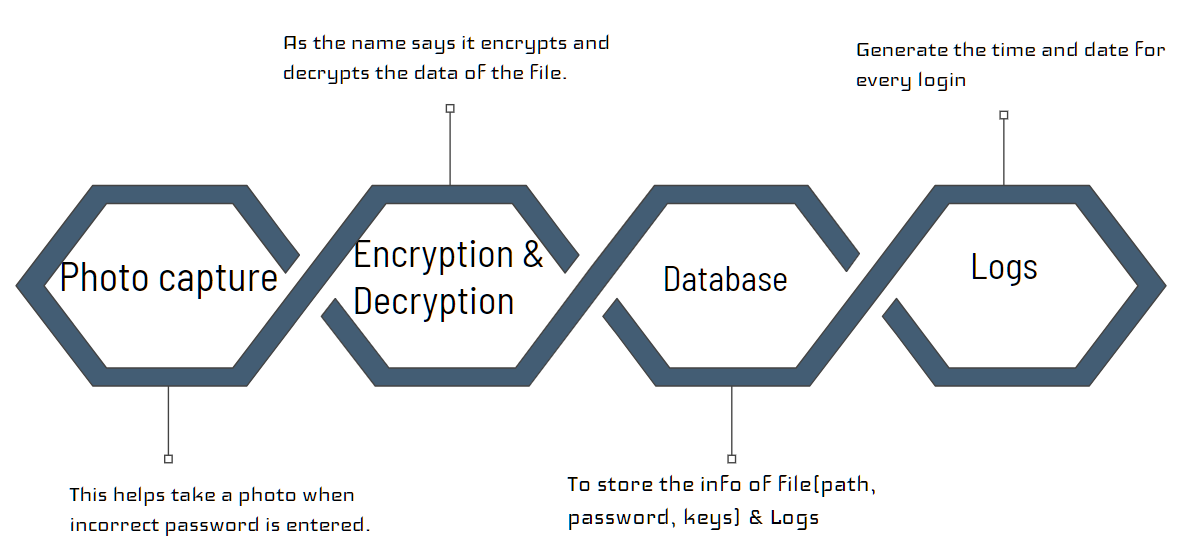


fig. 4.2 Different modules

1. **Photo Capture Module**

We imported the “opencv” library and used its some of the functions for capturing photographs.

camera\_port = 0

camera = cv2.VideoCapture(camera\_port, cv2.CAP\_DSHOW)

time.sleep(0.1) # If you don't wait, the image will be dark

return\_value, image = camera.read()

img\_name = f"safe\_klutcher{str(date.today())}\_\_{dt\_string}.jpeg"

cv2.imwrite(img\_name, image)

del (camera)

1. **Encryption and Decryption Module**

In the encryption module, we firstly took the path of the file as input and then the user’s choice password for encryption of file. Then we simply generated the encryption key , decryption key, public key. After this we read the content of the file that we took as input. Then we sent the content of the file to the encrypt function with encryption and public key so that file can be encrypted and stored in the encrypted code in the enc variable. And in the end we sent the credentials to the database.

keysize = 32

e, d, N = generateKeys(keysize)

msg = file\_in()

enc = encrypt(e, N, msg)

# dec = decrypt(d, N, enc)

print(f"Message: {msg}")

print(f"e: {e}")

print(f"d: {d}")

print(f"N: {N}")

print(f"enc: {enc}")

file2 = open(path, 'w')

file2.truncate()

file2.write(enc)

sql = ("INSERT INTO SAFE\_KLUTCHER" "(File\_name,d,N, password)" "values(%s,%s,%s,%s)")

val = (path, d, N, pswd)

mycursor.execute(sql, val)

mydb.commit()

In the decryption module, we took the path of the file from the user as input and also password for decryption of file and then we access the database to match credentials whether the user entered the correct credentials or not.

If the user has entered the correct credentials then logs for each login attempt will be saved and then the file will be decrypted using the decrypt function and then we will show the content of the file on the screen .

If in case the user enters the wrong password, then we will check for 3 attempts. For every wrong attempt the PC will capture the user’s photo with ‘date and time’ as the name of the file who is trying to access the file . And also after 3 attempts, the file will be blocked for some specific time.

1. **Database Module**

We imported the mysql.connector module to make use of mysql database. So, below are some steps for the connection of the database to our program.

import mysql.connector

mydb = mysql.connector.connect(

host="localhost",

user="root",

password="Priya@12345"

)

mycursor = mydb.cursor()

mycursor.execute("use SAFE\_KLUTCHER")

1. **Logs Module**

We created a table named ‘logs’ within the database we attached to our program.

mycursor.execute("CREATE TABLE LOGS(Date varchar(255), Time varchar(255))")

**4.3. Module Workflow**

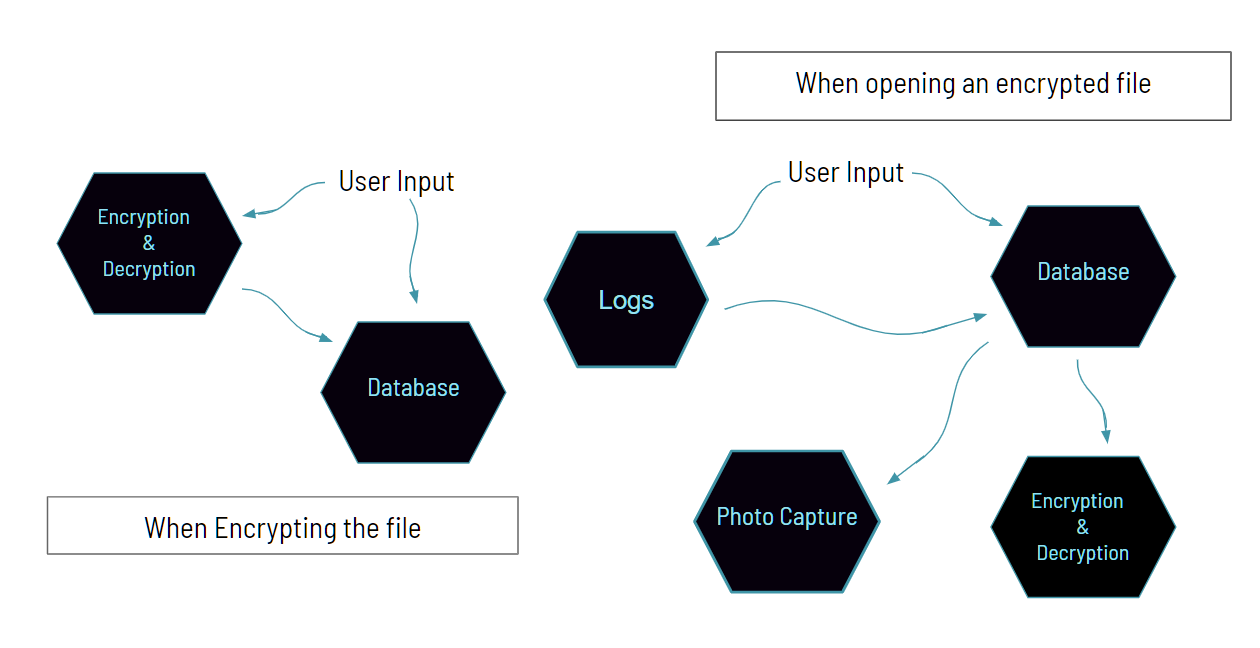


fig. 4.3 Workflow of the modules

The module have been used in two different task :

1. Encrypting the file.
2. Opening the file.

This is explained in more detail in chapter 4.4.

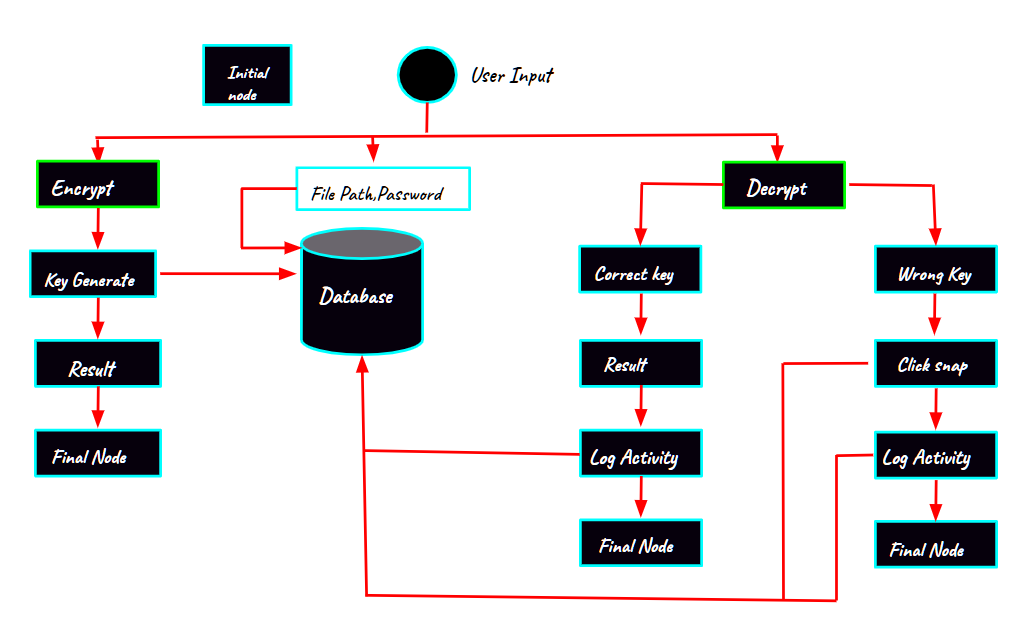
**4.4. System Architecture** 

fig. 4.4 Architecture of the whole system

The leftmost part of the diagram is represents the encryption of file where the 1st user input will be taken(i.e. file path and password) and this will be stored in the database to be used later when trying to open the file and the given file will be encrypted and the keys generated will also be stored in the database.

The rightmost part where the user wants to open a file, here the program will ask the user for the file's path and its password which needs to be opened. Then the program will compare the user input with the ones in the database and check if the password is correct or not.

If the password is correct then the associated keys which were stored in the database with that file's path and password are fetched and the file is then decrypted and the contents of the file are available to the user.

But if the password entered is incorrect then the login activity is stored in a separate database and a photo of the person inputting the password is taken and stored in a specific folder. The user will only get a maximum of three attempts before the file is locked for a given amount of time which can be changed accordingly.

**4.5. Summary**

All these modules , from Encryption and Decryption, to database to Logs and finally the Photo Capture module are all these have been initially made separately and then finally interpreted and combined all together which now works seemingly well specially after all that bugs that came along the way.

**5. OBSERVATIONS**

**5.1. Introduction**

Information related to the experience and reliability of the user and their needs .

**5.2. Performance Measures**

**i. Testing**

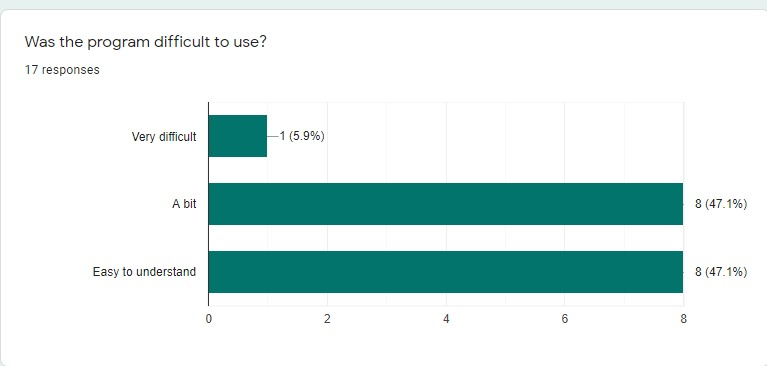
****

fig. 5.2 Testing (a)

* Most people find it an easy program to run as you just have to write the path of the original file to be encrypted and which operation the user wants the program to execute.

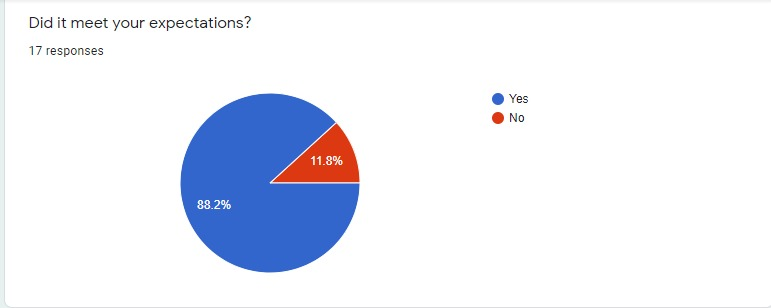
****

fig. 5.2 Testing (b)

* We conducted a survey in the beginning to know the needs and expectations of people. So here we asked them whether we have fulfilled their expectations.

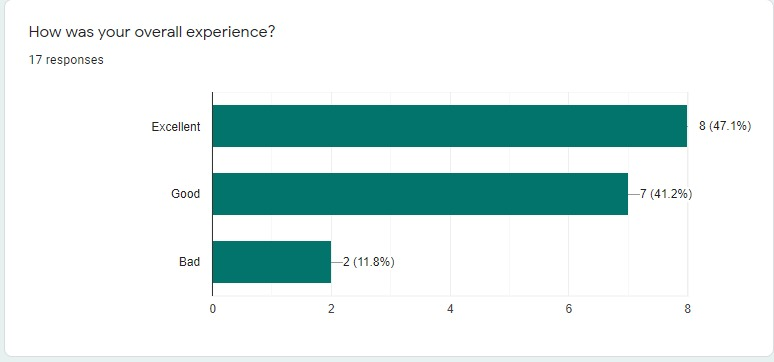
****

fig. 5.2 Testing (a)

* 11.8% of people found it difficult to interact with the program.

**5.3. Performance Analysis**

**5.3.i. Feedback**

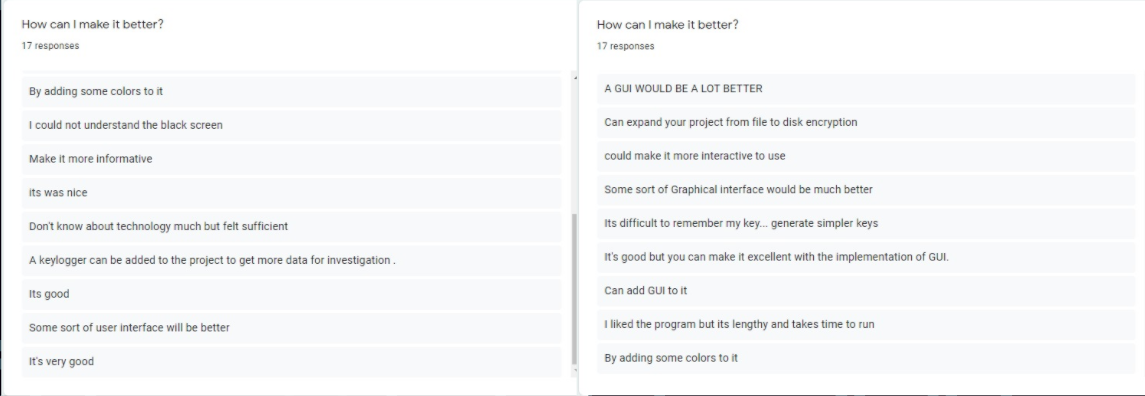
****

fig. 5.2 Feedback

* Improvement is a must in life, for that we asked our users how can we further improve our program. Despite having a huge positive response we wanted to know the followed up requirements of users.
* Most of the people found it difficult to cope with the black screen. Most of the suggestions were to add a proper GUI to the program.
* Another interesting suggestion that we can think about in future was adding a keylogger to our program. We can definitely think about this in future.
* One suggestion that we got was to generate simpler keys as the existing keys are difficult to remember (but they are this way due to security reasons). For that we can plan some designs in the future.

**5.4. Summary**

As per the performance analysis we can see possibilities for improvement which help us make our tool more efficient ,easy to use ,reliable and product based .

**RESULTS AND CONCLUSION**

**6.1 Introduction**

Today,We live in an era of ever-increasing cyber security threats and data breaches. As security professionals we know that it is not whether our systems have been compromised as much as it is when we will find they have been and to what extent.This problem is not one of security for securities sake, the fear of a data breach impacts trust in our ability to protect an individual’s assets, privacy, and ability to operate their business functions. It is more important than ever to stay connected and well informed on all topics related to cyber security, information risk management, and privacy concerns.It would be funny to say a common man will know all the privacy related issues that could harm him thus our tool is made to help such people to take care of their school, hospitals,businesses etc.

**6.2 Limitation/Constraints of the System**

The project we made is very fast to encrypt and decrypt for 0-300 words then the function slows down as the time complexity is o(n^2).As per survey , implementing code for a non-technical user is a bit difficult . our tool is made to be run only on devices where python is installed thus we can not use this tool on phones .

**6.3 Future Enhancements**

Based on our observation of the limitations there is a lot of scope for improvement . Once this project gets approved, we’ve planned to enhance our project . Firstly , as the complexity is o(n^2) we can improve this by more efficient and safe algorithm .As out tool is limited to desktop we are planning to made this tool using python for Android smart phones and for desktop we will build GUI to improve our tools usability and make it easy to use for non-technical people .

**6.4 Conclusion**

The project will have a tracking system which would record the timestamp of every login and logout . if someone tries to gain access by hit and trial methods, the file will get locked for 60 minutes after 3 wrong attempts within 15 minutes of time. The file if once formatted will not be accessible even with the recovery tools available in the digital market.So all these features seem to be very powerful and useful to cops if there is some data breach. To be added.

**8. REFERENCES**

1. 1. Abdelhalim, M. B., El-Mahallawy, M., Ayyad, M. and Elhennawy, A. (2012). Design & Implementation of an Encryption Algorithm for use in RFID System. International Journal of RFID Security and Cryptography (IJRFIDSC), Vol. 1, Issues 1-4, pp. 51 57.
2. Adesanya, O. (2002). The impact of information technology on information dissemination. In Madu, E.C. and Dirisu, M.B. (Eds.), Information science and technology for library schools in Africa (pp.10-24). Ibadan, Nigeria: Evi-Coleman.
3. Henry, D. (n.d.) RSA: Asymmetric Cryptography and Algorithm Analysis for a Secure Computing Environment. Retrieved from www.dwhenry.com/files/RSA.pdf .
4. Madji, A. and Lin, Y. H. (2007). Simple Encryption/Decryption Application. International Journal of Computer Science and Security, Vol. 1, Issue (1), pp. 33 40.
5. Stallings, W. (2011). Cryptography and Network Security: Principles and Practice (5th ed.). NY, US: Prentice Hall.