#### **Madhav Institute of Technology and Science, Gwalior**

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

**Department of Information Technology**

**Session: 2020-21**

**A**

**Minor Project Report**

**On**

**Fcrypt**

*In partial fulfillment of the requirement for the award of the degree of*



**SUBMITTED TO**

Prof. Rajeev Kumar Singh

Prof. Shweta Patel

**SUBMITTED BY**

Dheeraj Kushwah (0901IT181023)

Shivansh Shrivastav (0901IT181056)

Abhilekh Bansal (0901IT181003)

|  |  |
| --- | --- |
| C:\Users\100RABH\Desktop\mitsmono.jpg | **Madhav Institute of Technology and Science, Gwalior (M.P.)** |
| (A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal) |
|  | |

**CANDIDATE'S DECLARATION**

I hereby declare that the Project entitled “**Project Title Name”** which is being submitted in the partial fulfillment of the requirement for the award of **Bachelor of Technology** in **Information Technology**.

All information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I have fully cited and referenced all material and results that are not original to this work.

To the best of my knowledge the material presented in this Project has not been submitted elsewhere for the award of any other degree/diploma.

**Date: 4/5/2021**

**Place: MITS Gwalior**

**Dheeraj Kushwah (0901IT181023)**

**Shivansh Shrivastav (0901IT181056)**

**Abhilekh Bansal (0901IT181003)**

**Content**

**Topic Page No.**

## Introduction

## Motivation

## Problem Statement

## Overview

## System Requirement

## System Analysis and Design

## Implementation

## Conclusion and Future Scope

## References

**Chapter - 1**

**Introduction**

* 1. **Motivation**

As privacy and data security has becoming a big concern. Now a days data leaking is becoming so normal even big companies are unable to give proper security yo data and our files that’s give as a motivation to make an Android application through which we can encrypt or imp files by which we can save our data and protect our files.

As Lockdown is increasing and work from home is becoming so easy but work is increasing and to submit that work sometimes we have to convert our work to different formats that’s why we implemented a document converter this features is still in working.

* 1. **Problem Statement**

The underlying respective architecture of most IT systems, including the desktop computer and internet, does not guarantee security. Users with malicious intents have always found a way of exploiting one vulnerability or the other. An attack that affects the confidentiality of information often presents the platform for the integrity of such information to be compromised.

Intercepted information on transit would make little or no sense to an interceptor if he is not able to decipher the content of the information. This explains why it is very necessary to ensure that even when an intruder or unauthorized user successfully obtains access to some information the confidentiality and integrity of the information remain uncompromised.

* 1. **Overview**

Encryption, as a general concept, is the conversion or masking of information to prevent unauthorized parties from accessing it.

The altered information is referred to as ciphertext, which can be thought of as basically “digital gibberish." The information is unintelligible and essentially impossible to use for anyone without the encryption key.

An encryption key is an indicator or identifier used to turn ciphertext into your desired output. Keys are kind of like passwords, but they’re virtually impossible to decipher without expert computational resources and decryption experience.

**Chapter-2**

## **System Requirement**

The security requirement entails the capacity to control user access, manage data and also support the three security concept (e.g. confidentiality, integrity and availability of data). The security requirements of the new data encryption and decryption systems are listed below:

i. The system shall be able to authenticate users.

ii. The system must be able to deny access to illegitimate users to the system.

iii. The system shall be able to verify the sender of a message through authenticating the user’s digital Signature.

iv. The system must be able to retrieve the forgotten keys by asking some security questions in order to verify user’s

authenticity. This is achieved via email matching and secret questions supplied by the user during registration.

## **Chapter-3**

## **System Analysis and Design**

**Cryptography** is the science of writing in secret codes which can be achieved either by using software encrypter or hardware encrypter. This study presents the development of a pair of circuit **system**-**based** (hardware) **cryptographic** processor.

A **cryptographic system** (or a cipher **system**) is a method of hiding data so that only certain people can view it. ... The protected data is called ciphertext. Encryption is a procedure to convert plaintext into ciphertext. Decryption is a procedure to convert ciphertext into plaintext.

**Three types of cryptography**: secret-key, public key, and hash function.

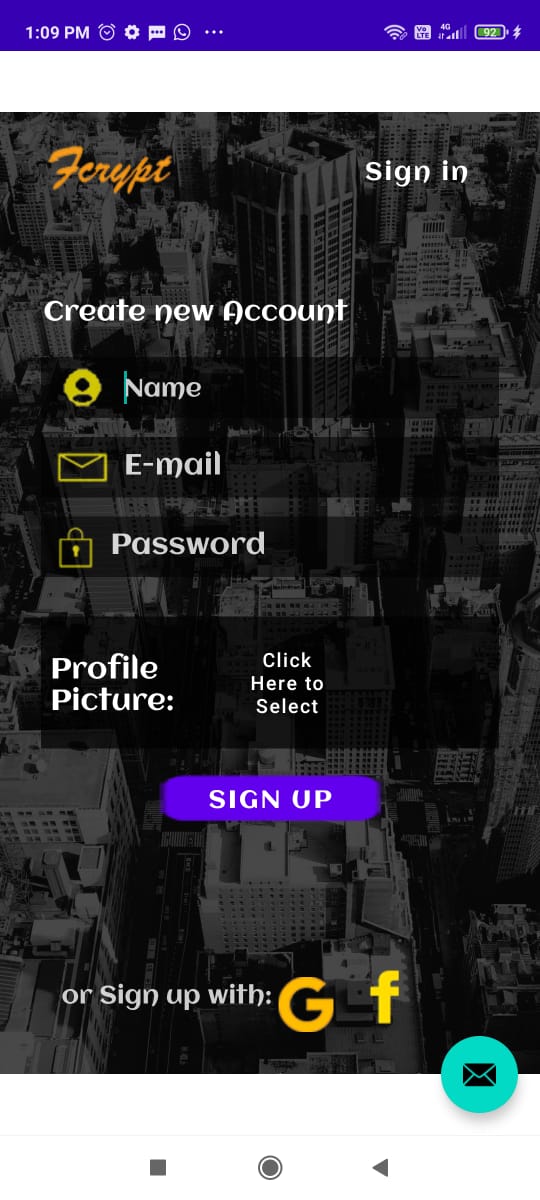
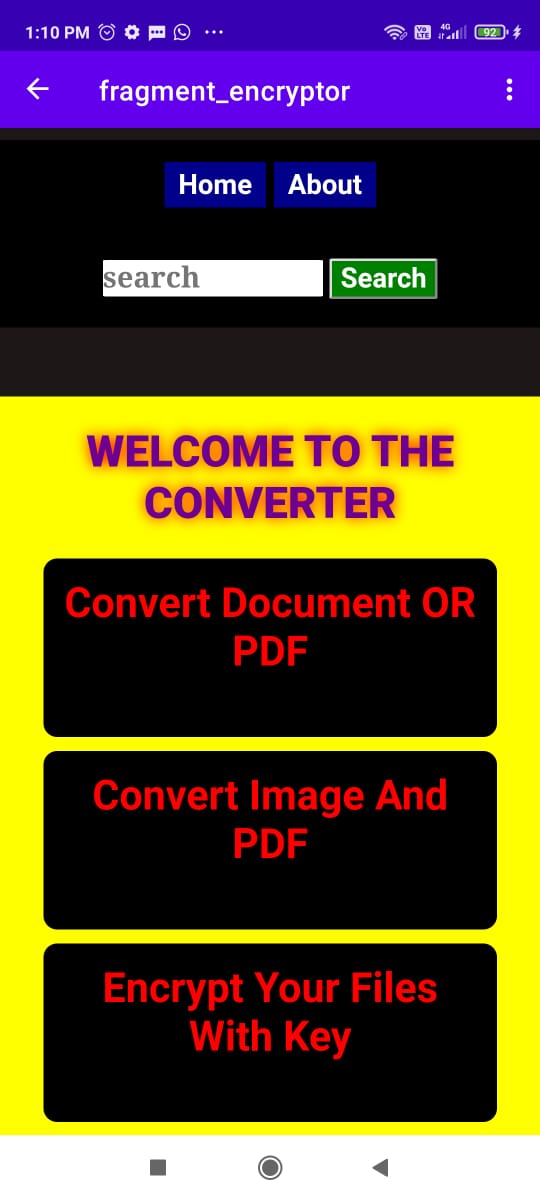
We are using screte-key Cryptography.

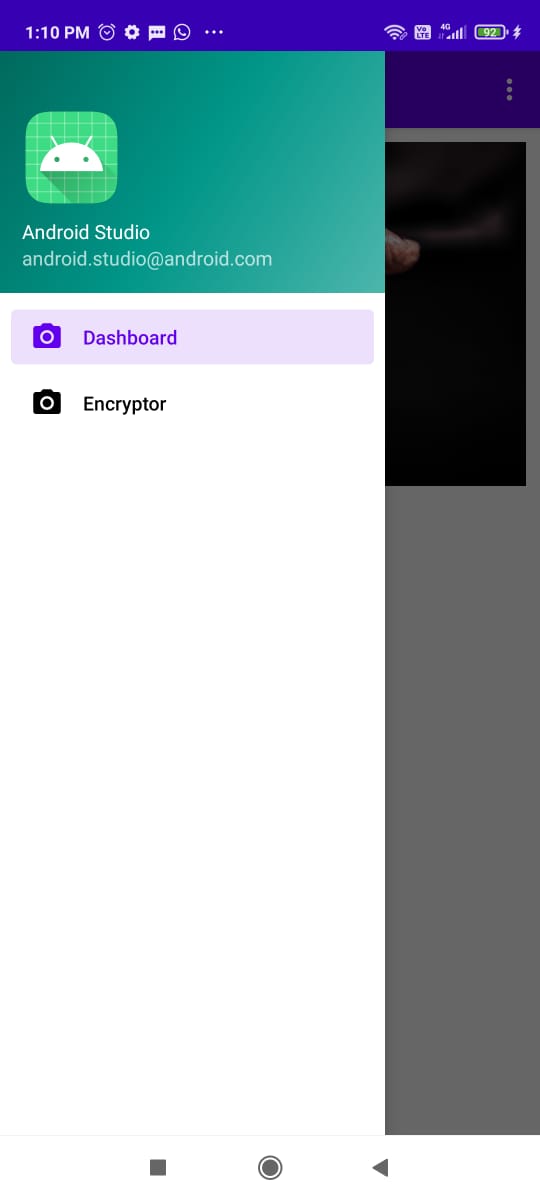
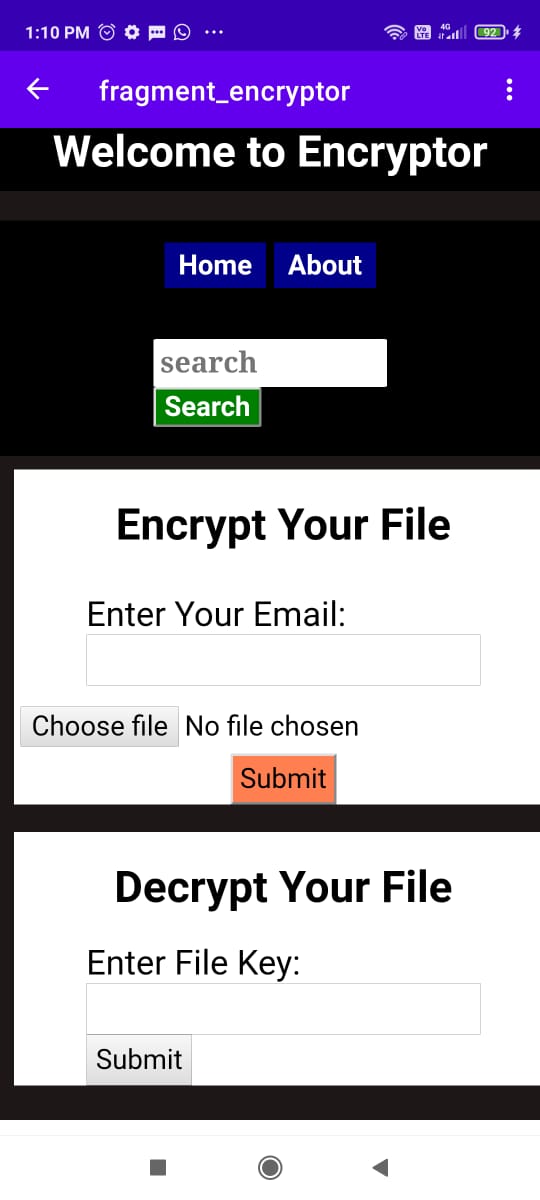
All cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over some kind of secure channel. Many key agreement methods have been developed, with different security requirements for the secure channel. Various defenses against MITM attacks use authentication techniques that include:

certificates authority. Similarly VPNs do mutual authentication before sending data over the created secure tunnel.

**Design :-**



** **

**Chapter-4**

**Implementation**

The app is divided into two activity and four fragments. Each activity contains two fragments.

One activity is for singup which handles the fragments designed for sign up and autnetication of the user. This contains NavCotroller for navigating the user between signin and signup fragment.

When the user logins then he/she will be redirected to the nav\_hom activity which again handles two fragments with name EncryptorFragment and Dashboard Fragment and the navigation between them is handled by the different nav controller. When user is on Dashboard then there the user have option to go in EncrytionFragment and when he goes to that fragment, there user can encrypt and decrypt file.

The EcryptorFragment using the webview for showing itself on the app. It makes the post request to the server with file and username and then server in turns respond with the JsonResponse which contains key which user can use to decrypt the file. The file is encrypting using standard AES algorithm which reads the binary data of the file and then server generates a key using a library of cryptography which is available in python. And that key is used to encrypt the binary data of the file and that’s why we are able to manage and encrypt any kind of file irrespective of its type because we are reading binary data and encrypting that data. Once that data encrypted server returns the key which it has used to encrypt the file and user receives that key. Now only the user which have the key can able to decrypt the file no matter who has that file. In this way we encrypted the data using cryptography.

## **Chapter-5**

## **Conclusion and Future Scope**

The main Conclusion of this project is to encrypt the important files of the user so that even when he/she has been hacked by someone then attacker cannot read the content inside it. We have used the key encryption so only the user which have the key can able to decrypt the file.

You may have used secret messages or languages to communicate with friends or siblings, and you have likely observed the use of cryptography in various aspects of our society – maintaining the confidentiality of personal, consumer, corporate, and government data. However, on top of this, cryptography’s status as an indispensable building block in digital infrastructure continues to grow with the perpetual increase in online connectivity – securing online transactions, authentication, and access to resources.

Cryptographic systems are often built on the premise that certain math problems are, computationally, very hard to solve. Many of these problems, such as factoring certain types of large numbers, have been studied by mathematicians anywhere from decades to centuries. In fact, mathematicians often estimate the projected security of such systems by plotting the evolution in ‘running time’ of the best-known attacks. These predictions work well, but only in the absence of major disruptions; new algorithms or technologies drastically improve the expected running time of attacks.

**Chapter-6**

**References**

1. Stack overflow
2. Youtube
3. GeeksforGeeks