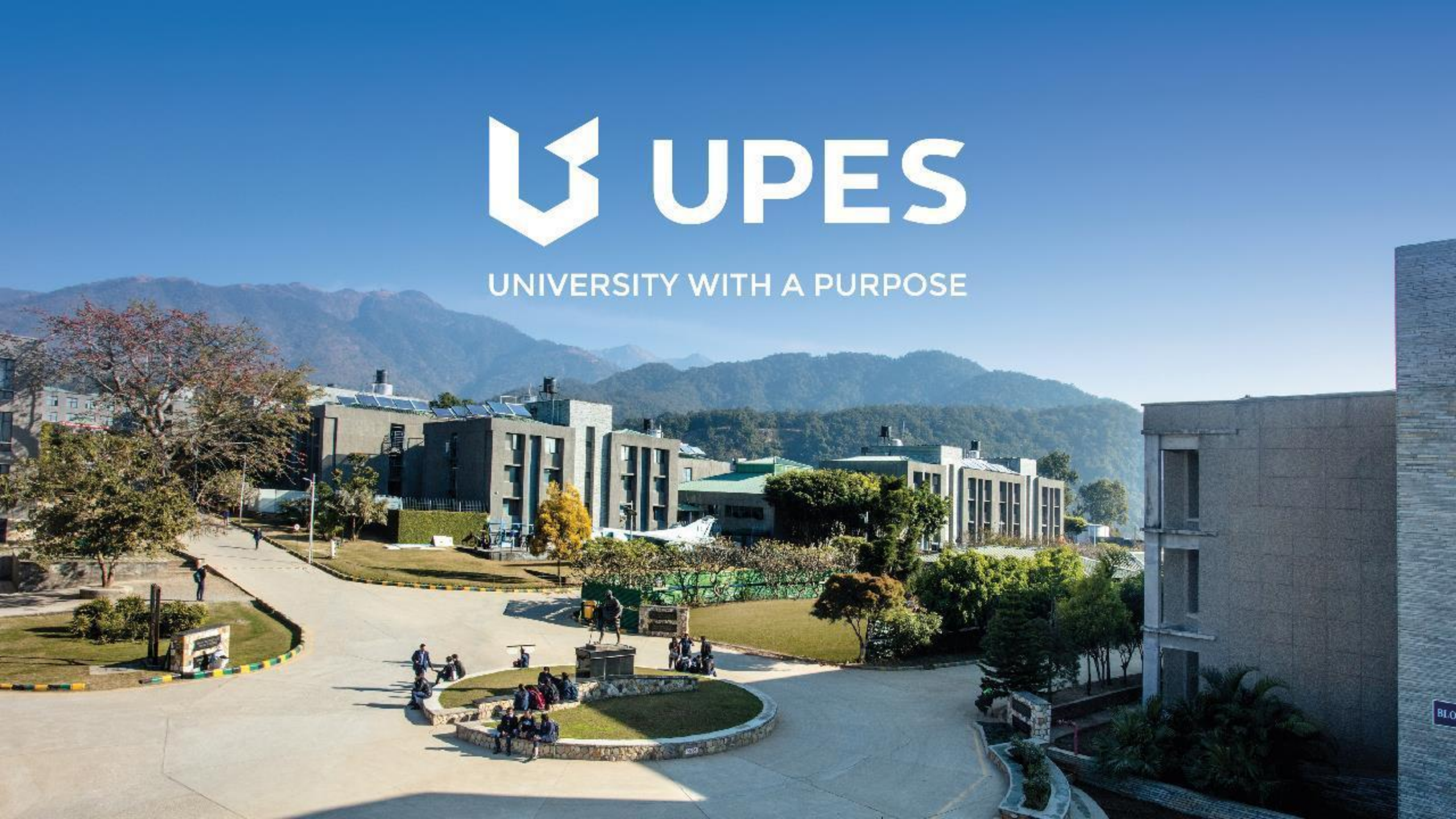

UPES
UNIVERSITY WITH A PURPOSE

UPES
UNIVERSITY WITH A PURPOSE

Enigma

A File Security System based on Standard Cryptographic Algorithms using structured programming approach.

Under the guidance of
Dr. Mrinal Goswami
Assistant Professor

Aman Bhardwaj	***500067105***	***R164218009***
Aviral Kumar Srivastava	***500068442***	***R164218020***
Keshav Garg	***500069767***	***R164218035***
Meghna Barthwal	***500067369***	***R164218045***

Introduction

- A **file security system** is used for securely storing our data in files which are encrypted using certain cryptographic algorithms.
- The file security system implemented in our project, offers data security and encryption to user data so when the user uploads a file, which they want to encrypt, the system uses the **standard cryptographic algorithm** and encrypts it. This **generates an encrypted file** which is then sent to the user along with a security code which is used to **decrypt the file** and reveal its contents, as and when needed. Therefore this security code basically acts as a password for the encrypted file.
- Moreover, the proposed system will also allow the user to decide their own password as per their convenience. Furthermore, to enhance security, the encryption algorithm used is kept as secret and once a file is encrypted it can only be restored by our system after entering correct security code.

Enigma

A File Security System based on Standard Cryptographic Algorithms using structured programming approach.

Introduction to Enigma

Domain

- Domain of this project lies within the bracket of Cryptography and the study of standard cryptographic algorithms and their applications.
- By this project, we aim to cover the domain of File Security Systems and create a console based program that is capable of manipulating files and provide secure encryption and decryption to it.

Motivation

- In these times the security & privacy of data, that is stored or transferred, has become increasingly essential for each user.
- Spurred by the growing development in the field of cryptography and security algorithms, we decided to create a File Security System.

Purpose

- Understand the working of cryptographic algorithms and their uses.
- Apply the concepts learnt in order to create a File Security System that encrypts and decrypts files that are stored on a system.
- Try to provide an optimal approach towards creation of a File Security System and the use of Cryptographic Algorithms.

Problem Statement

There exists a need for a dedicated console based program that provides small cypher blocks while encrypting large files.

Moreover, there is a need for a user authentication system that secures the channel for encryption and decryption to take place while storing and accessing files.

Solution and Objectives

Main Objective:
To create a console based program that will encrypt the user files and protect it from any unauthorized access and also to provide a way of decryption for the same.

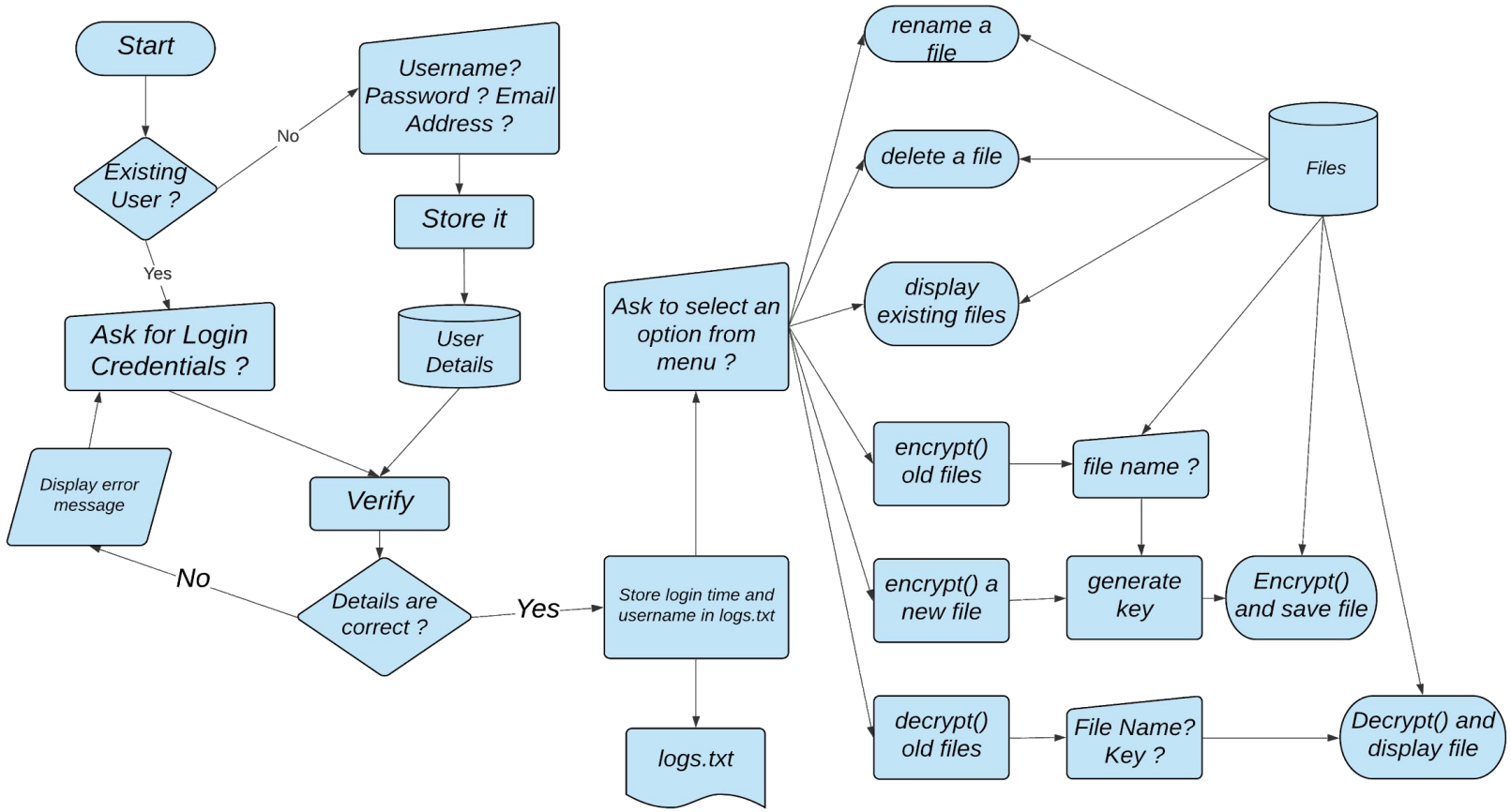
Sub-Objectives :
To provide a good interface to the user so that they can easily save their files in encrypted format.
No loss of information during the whole process.
To take the file size and encrypt the data using the optimal algorithm of encryption.
Further strengthen the algorithms by using a shuffled approach.
Comparison of various algorithms based on the user data on the basis of various parameters.
Proper authentication system for the user data.

Design of Experiment

Flowchart

Enigma

A File Security System based on Standard Cryptographic Algorithms using structured programming approach.



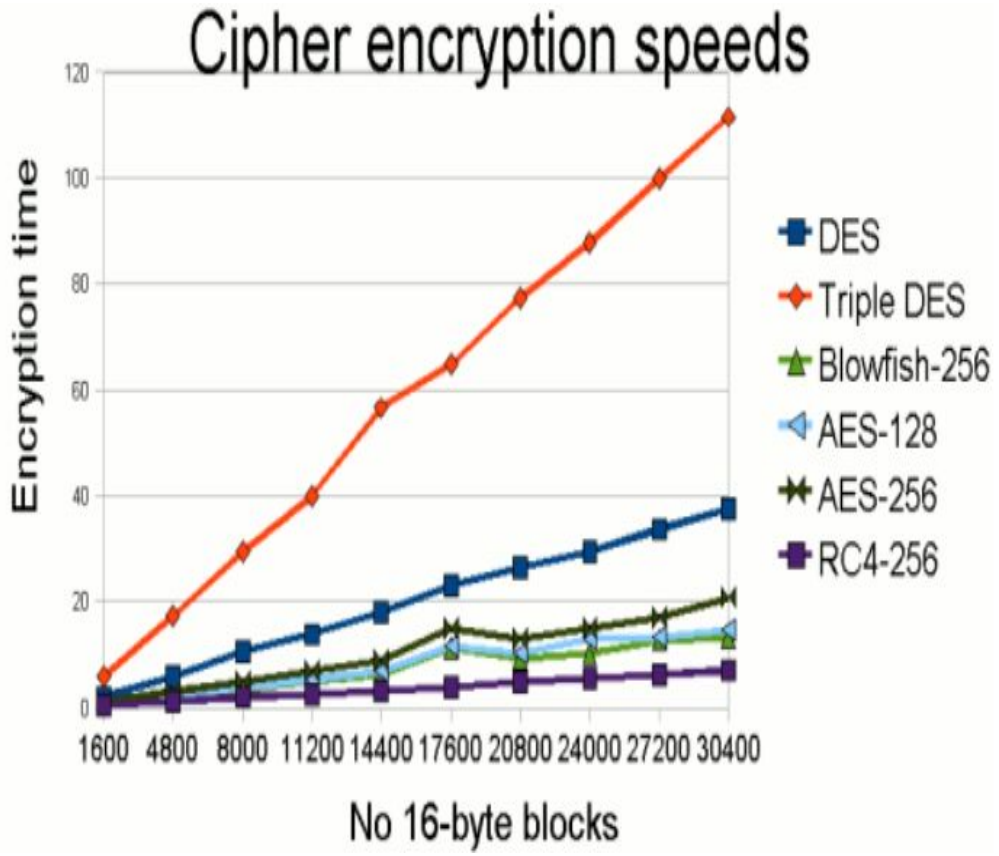
UPES
UNIVERSITY WITH A PURPOSE

Modelling and Simulation

Analysis & Interpretation

The implemented File Security System has the following modules:

- **Authentication for different users:** This is responsible for the authentication of existing as well as registration for new users.
- **Login page:** This module deals with login and verification of user details.
- **Encryption for New Files:** This module is the most important one as it deals with encryption of plain text to ciphertext.
- **Update Files:** This module is responsible for storing information in the new file. This can be encrypted message or simply input message.
- **Delete Files:** This module is responsible for deleting the files in the system.
- **View Files:** This module is used to display the directory for the stored files as it gives a list of files.

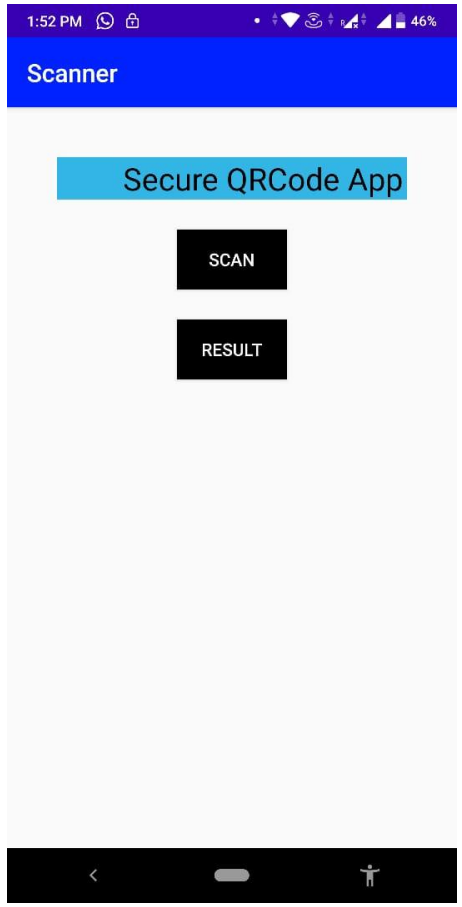


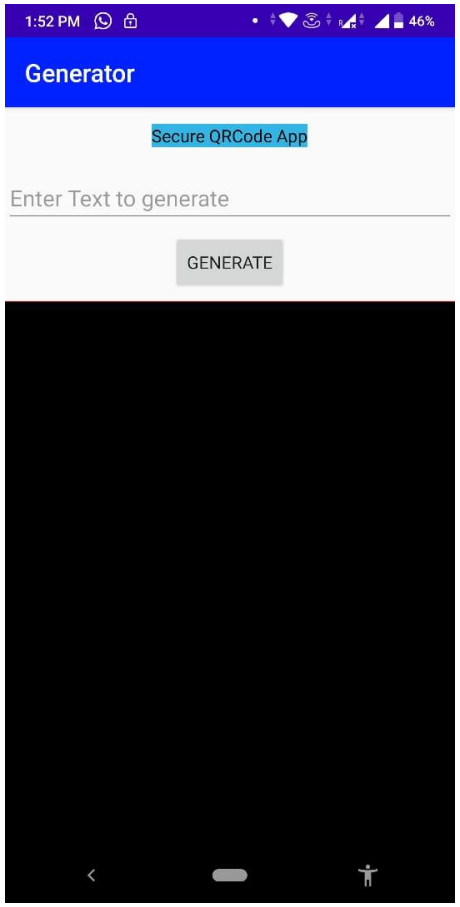
Further Work

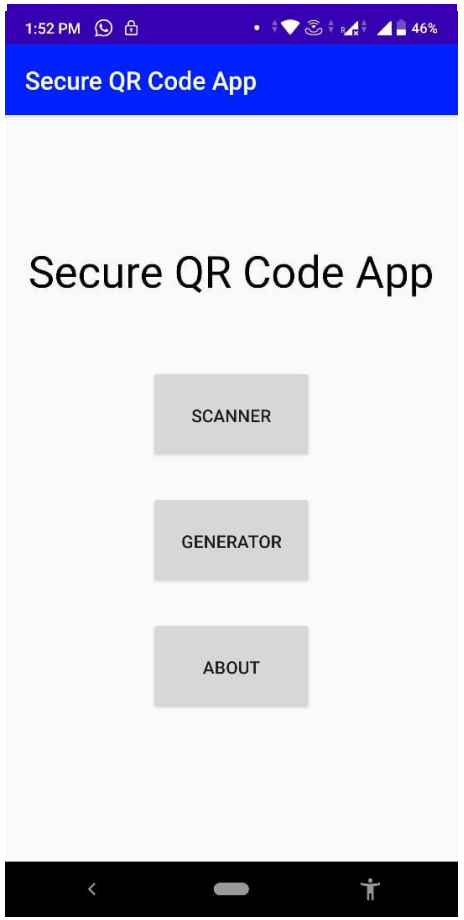
- **To provide a good interface to the user as a web app or a mobile app so that they can easily save their files in encrypted format and retrieve them easily.**
- **The process can be made in such a way that we can have a GUI version for this.**
- **Some real world applications of such a system can be found in IoT security, Electronic Money , Disk Encryption, Authentication/Digital Signatures etc.**

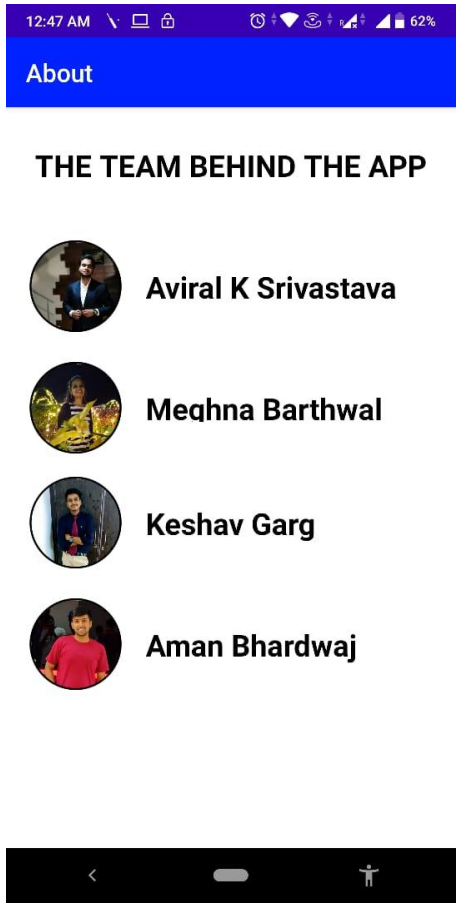
Further Work

Our team set out to find one such application in the field of data security, and found that companies need to protect sensitive information of their installed equipments in such a way that any third party couldn't read it but there is also a tool to maintain its integrity and authenticity and therefore we applied Enigma to solve this problem.









UPES
UNIVERSITY WITH A PURPOSE

THANK YOU