

Security Algorithms and Protocols

Project: Write-up

REPO

Aishwarya Pagalla

Deeksha Sudini

Abstract:

The project Repo is an Android Application with encryption system used to encrypt any text inside a file. Repo is File sharing App, which allows to share the files from one's own system to application in an encrypted format. Only the owner of the file can see the content in the file and others can view the file but the contents of the file will be in encrypted format. The Content of shared files are encrypted using RSA algorithm. This generates a cipher, upon which the data in the chosen file is encrypted using RSA algorithm, which provides security to the user to store the data without thinking about any intrusion.

Introduction:

We are in a world where information is everything and privacy is a myth. Sharing any data on internet, just as it is without any additional security measures might lead to a privacy breach. So using an encryption standard to protect the data from a third person is very much necessary. RSA is a perfect way to protect the data from unauthorized access. RSA is hugely popular as its advantage speaks for themselves, For instance this encryption standard is freely usable, incurs no license fees and is not subject to patent restrictions. Added to this come relatively low storage and hardware requirements. The encryption algorithm is uncomplicated and elegant in programming, and is simple to implement.

Background:

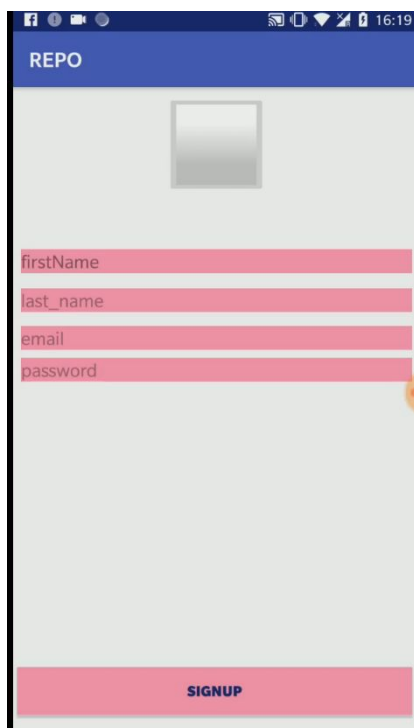
The Repo word is taken from the repository of GitHub but the difference is the files are encrypted when others wanted to see the content of your files. It also provides security to the files which are stored in it. It lets the user encrypt the data in a file, others can only view the encrypted contents of the files shared.

Experiments:

- 1) Text encryption java file - which encrypts the contents of the file in the local system.
- 2) Android Studio - Created File sharing Android Application
- 3) FireBase - Is an inbuilt database in Android Studio which stores the files in cloud in an encrypted format.
- 4) Eclipse IDE- Used for encryption algorithm.

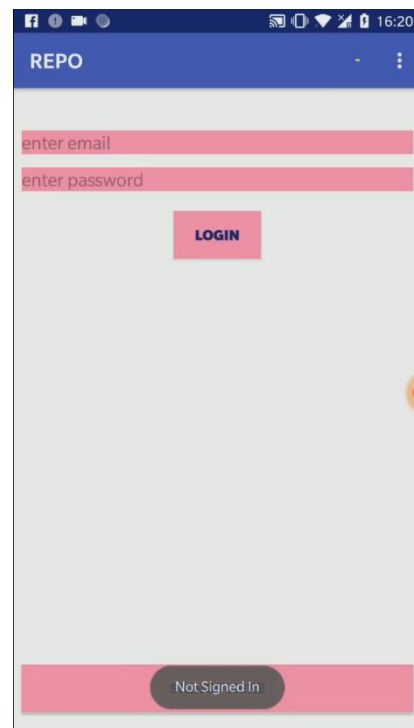
Screens:

Sign-Up



The Sign-Up screen features a blue header with the text "REPO". Below the header is a grey square placeholder for a profile picture. Underneath the placeholder are four pink input fields labeled "firstName", "last_name", "email", and "password". At the bottom of the screen is a pink button labeled "SIGNUP". The status bar at the top shows the time as 16:19.

Login



The Login screen features a blue header with the text "REPO". Below the header are two pink input fields labeled "enter email" and "enter password". A pink button labeled "LOGIN" is positioned below the input fields. At the bottom of the screen is a pink button labeled "Not Signed In". The status bar at the top shows the time as 16:20.

File Posting

REPO

File name

enter Text

SUBMIT_TEXT

File Sharing

REPO

repo1

May 1, 2018

deek.aish@gmail.com

Contents

REPO

Project Title:Encryptor

Abstract:The project Encryptor is an encryption system used to encrypt any text inside a file. It allows the user to select a file in a particular file location on his system and allows him to encrypt the data(text) in the file using RSA Algorithm.

The system generates a set of keys(public and private), upon which the data in the chosen file is encrypted using RSA algorithm, which provides security to the user to send the data without thinking about any intrusion.

Introduction: We are in a world where information is

Contents(Encrypted)

REPO

51b870eb4f3e45bcd1d4300796bf1c4136569d4ab3df3ca
a332eb9f8e673f9240d0cc3c4562e54e9c46900377c1b780
5634c248a543bcb17f0e38d6ec42ac2d3a7d18845eb2828
c25d61152a0b90075e15d1bf19b36f868957dbc921d8cfc
39279fb74dcfb7f7ee8707534651654baf1620e8682bc039
bdbb5943b1d535b6379d3eefa7acb9de2a651e4d7f39503
bddb3c8e48ddfd903233ac99bbb11fc4597a8de084163fb
d0e33b2bc2a10d133aae637ec03e2e09ce98fc3bd5db231
d9e7ef23798c696b3811424a67b2d7065dfa2843609bc97
0ec357753564c24aa381642770722c764e6b149029165b6
66baf9e679c932c29009c6ffc5fc456f7136d91150864f0f16
001c7b33d66fe8e15c9a26d17cbd0d2de0219a5488649c7
5a4ab3b8df2a14f69788a02b3e9f4543ce4bbf28b7ec2546
de61229a38a758319e145f9bd26ed564649787dd0802d2
27abcb94097a5e7a262c3bff6b05cbab5543323f62a95d16
2878a27e9d0a9350082ffdedc9942916d4bf347c97918ade
adc63e3de0c06af08b9a0e513ab1e5ffc65fbee5a2baf8d9e

Future Scope:

With the global applicability, this project can be implemented worldwide, in various ecosystem like IOS, web and many more. Enhancements like secure file sharing, social hub, and team productivity modules can be added.

Conclusion:

This application provides security for the files which are shared by using RSA Algorithm with authentication.

Requirements:

- Android Studio
- Eclipse IDE JAVA

References:

<https://stackoverflow.com/questions/6077507/java-rsa-encryption>
<https://www.udemy.com/complete-android-developer-course/>
<https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>
<https://developer.android.com/guide/index.html>