CIPHERBOOK

USER MANUAL

Authors:

Vikas Nandanam

Vikram Patil

Description:

Cipherbook is an android application created by Vikas Nandanam and Vikram Patil. The application follows AES 128 bit encryption and decryption technique. The AES(Advanced Encryption Standard) one of the robust encryption technique most frequently used in military communications. The cipherbook application follows this encryption standard. This is a single user application which encrypts and decrypts the text. The application cipherbook helps to protect the confidential data by saving them in the in file. In android, the file that has the confidential data is stored in the internal memory. The file saved in the internal memory is used by the application when required. The saved file cannot be found explicitly.
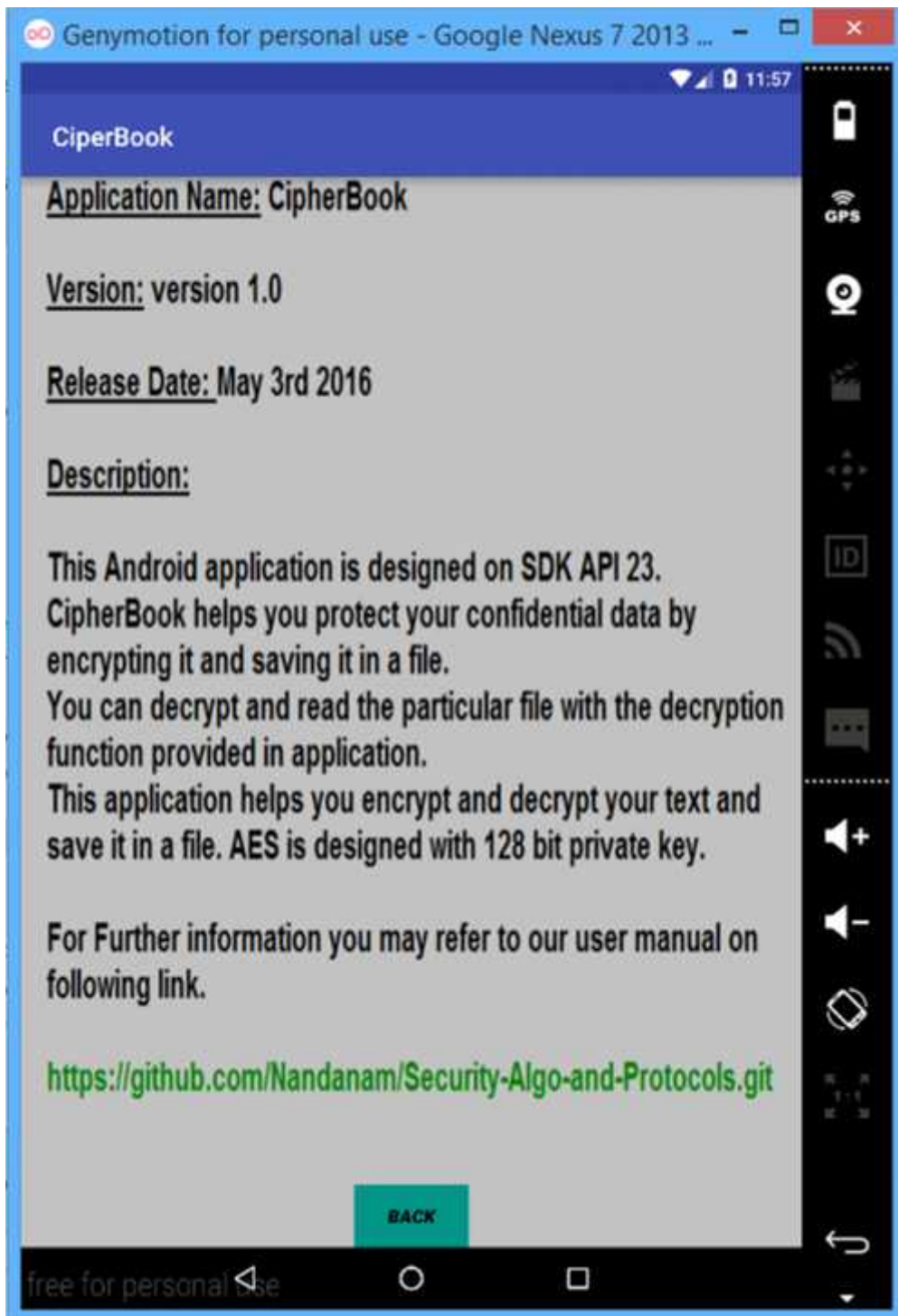
The application has text fields for entering the text and key for encryption. The generated results are shown on text view on the button click.

The application cipherbook is developed on android studio and displayed virtually on emulator (GenyMotion).
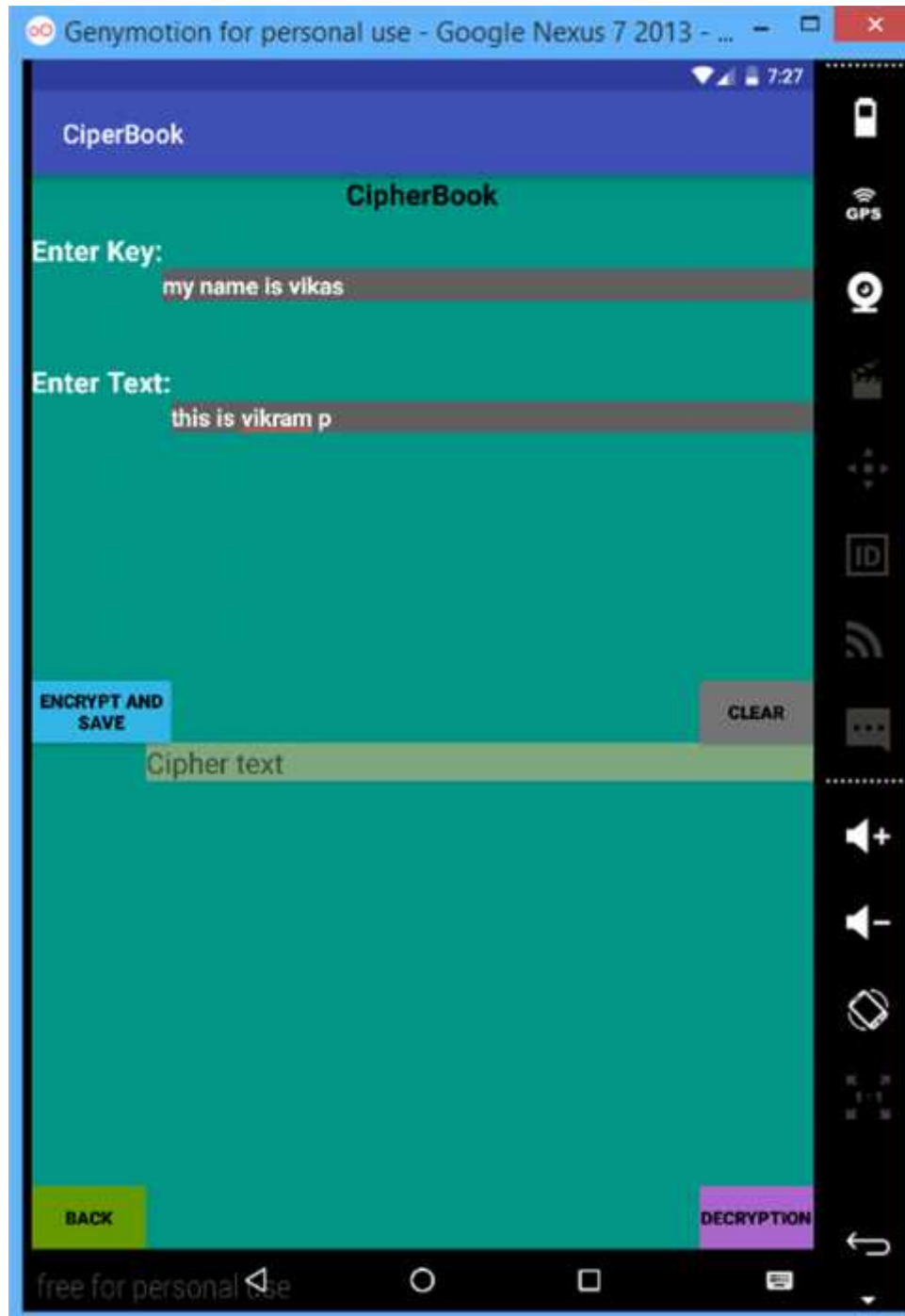
HOW TO USE THE APPLICATION
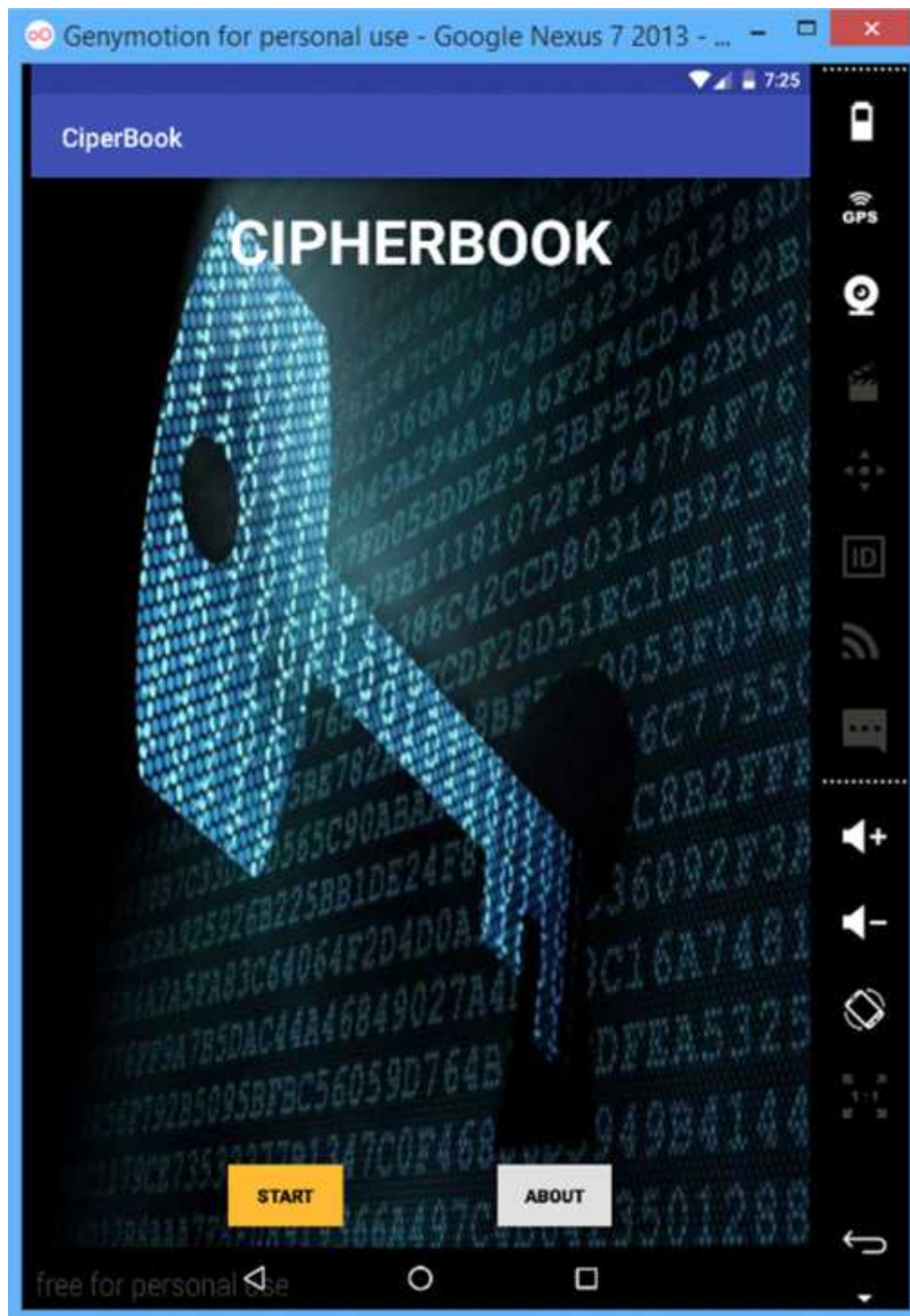
This is the main screen of the application. The Start button starts the application and the about button gives the description about the application.

Genymotion for personal use - Google Nexus 7 2013 ...

▼◢ 🔋 11:57

CiperBook

<u>Application Name:</u> CipherBook

<u>Version:</u> version 1.0

<u>Release Date:</u> May 3rd 2016

<u>Description:</u>

This Android application is designed on SDK API 23.
CipherBook helps you protect your confidential data by encrypting it and saving it in a file.
You can decrypt and read the particular file with the decryption function provided in application.
This application helps you encrypt and decrypt your text and save it in a file. AES is designed with 128 bit private key.

For Further information you may refer to our user manual on following link.

https://github.com/Nandanam/Security-Algo-and-Protocols.git

BACK

free for personal use

ABOUT PAGE

The about page is opened on clicking the about button on the main screen.
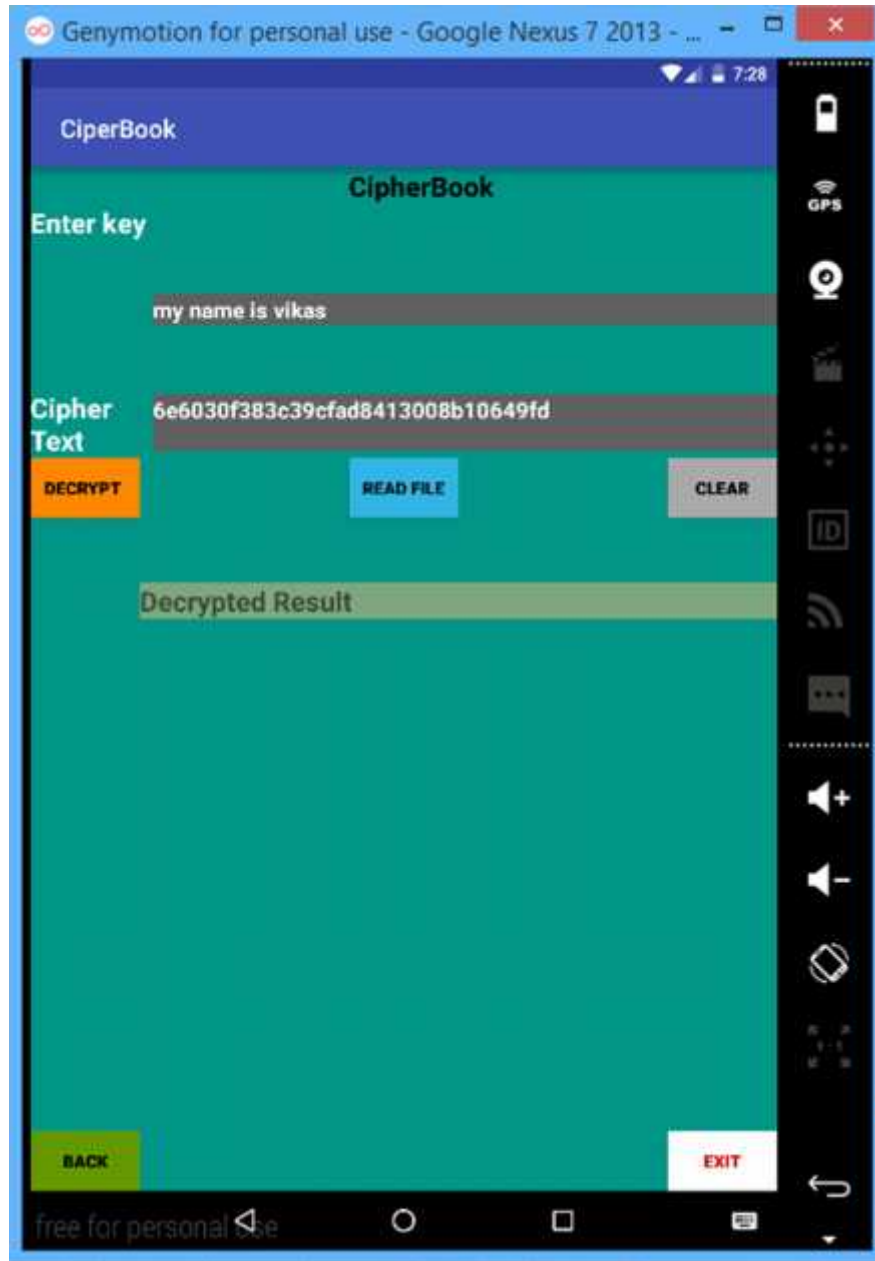
ENCRYPTION

On clicking the start button on the main screen the encryption screen is opened. The user should enter the key and text in the text fields for encrypting the text.
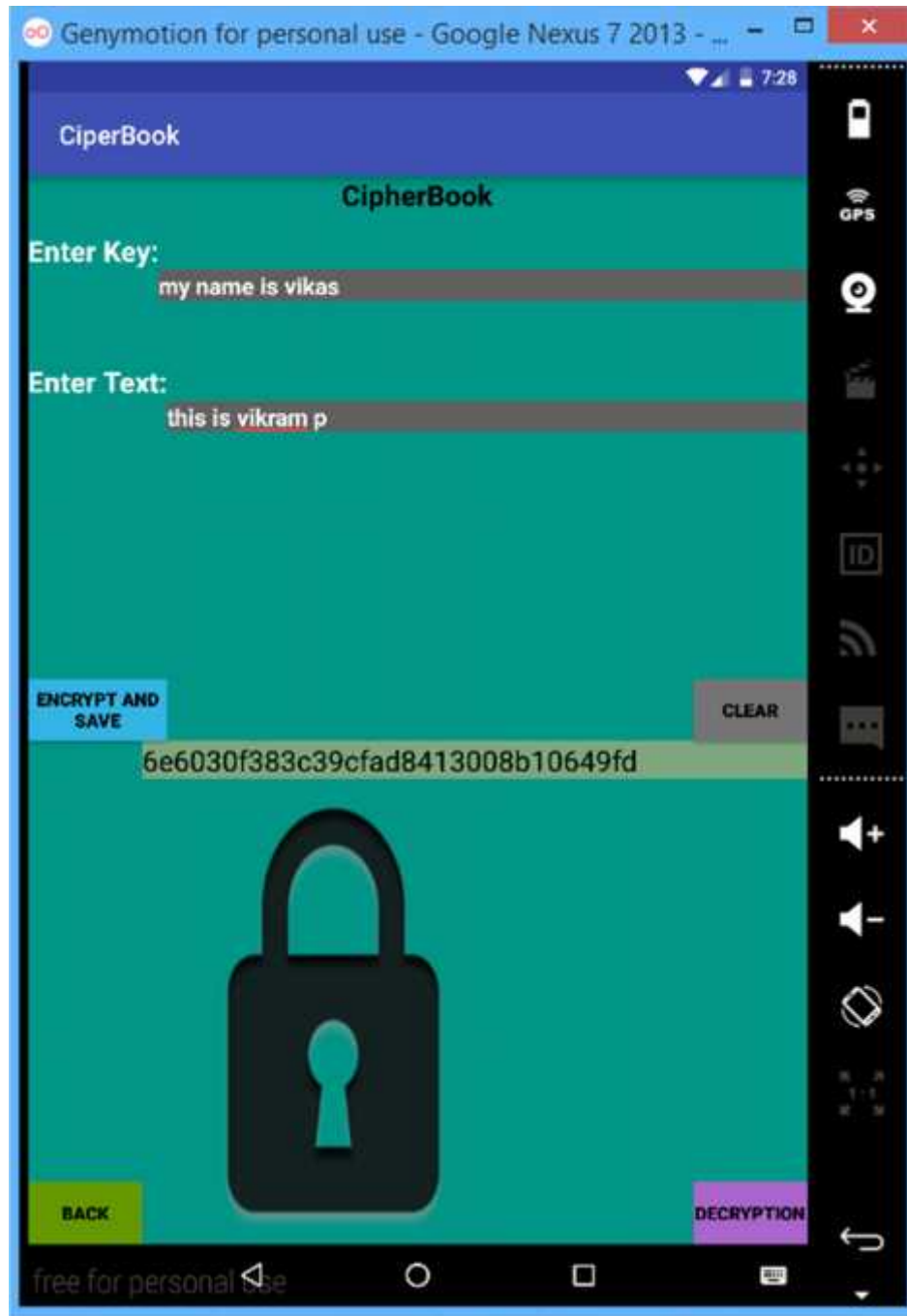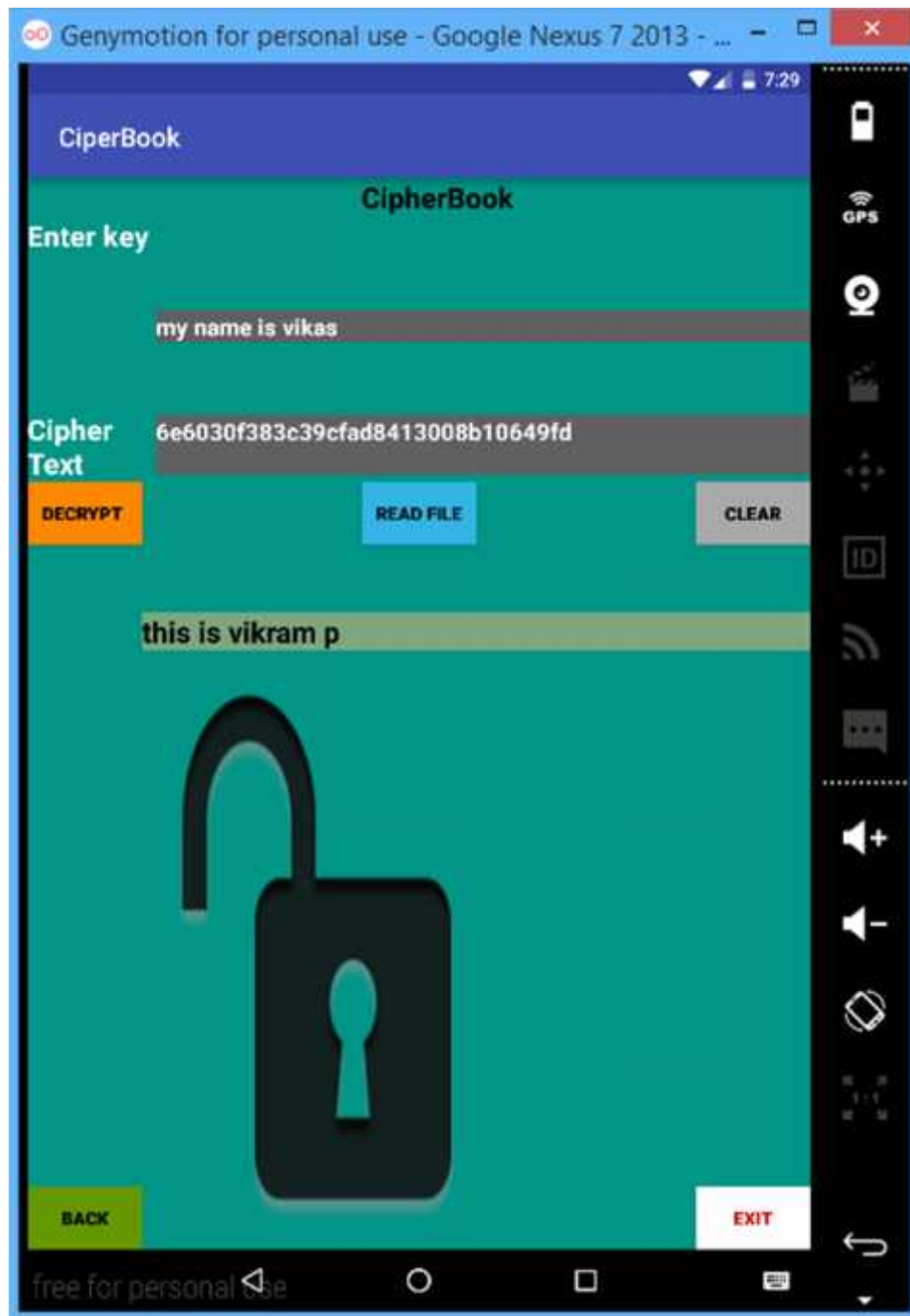
On clicking the encrypt and save button the plain text entered is encrypted and displayed on the text view. This also saves the encrypted text into a file. It displays a message as file saved. The clear button clears all the text fields. On clicking the button decryption the application displays the screen for decrypting.

DECRYPTION

This is the decryption screen of the application. Here the two fields, the key which must be entered manually and for the cipher text field just click the read file button. This displays the encrypted text on the cipher text field.

The key entered should be the same key entered for encrypting the text. On clicking decrypt button the plain text is displayed on the text view. The exit button closes the application.

Key points for using this application:

- The application cipherbook uses AES 128 bit encryption and decryption techniques.

- The key and the plain text to be entered for the encryption and decryption is strictly limited to 16 characters (mandatory).

- At the encryption process the cipher text generated is stored into a file as soon as the text is encrypted.

- In decryption, the key used and the cipher text generated in the encryption process should only be used for decrypting.

- For decryption process the cipher text need not be typed manually instead just click the read button on the screen. The cipher text generated at the encryption process is displayed on the text field.

Future Enhancement:

The application cipherbook is a basic version for encryption and decryption using AES 128 bit technique. The current application is a single user application, where encryption and decryption is processed on the same device. In future, the application will be enhanced for AES 192 and 256 bit encryption and decryption techniques. The other versions of the application will be for multi users and even authentication will also be enabled.

There is also a scope for introducing authentication in the application.