Security Algorithms and Protocols
REEV.US

Professor: Mr. Pablo Rivas

Name: Kavya Reddy Vemula

20076569

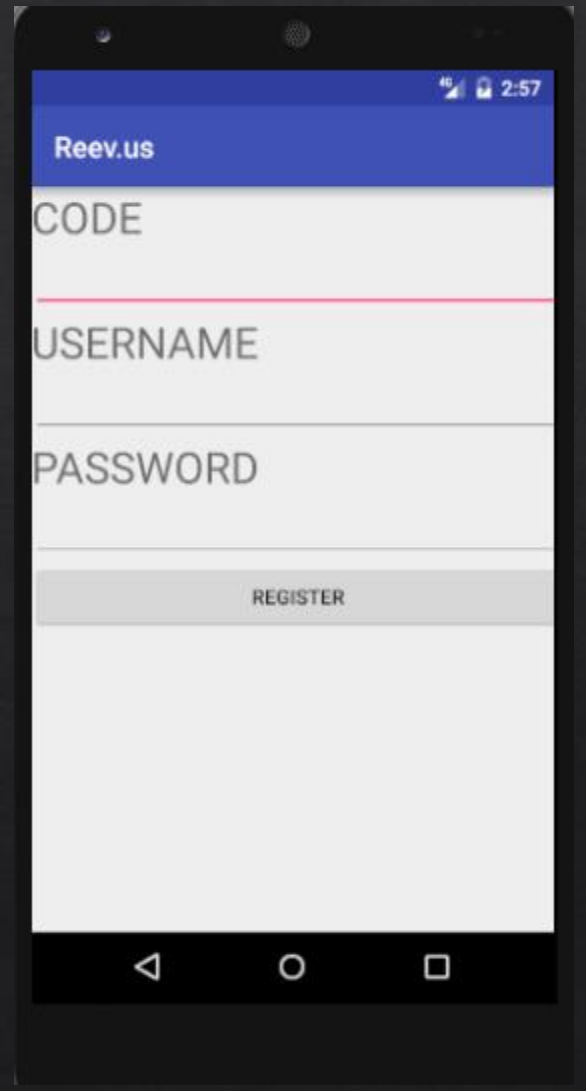
What is Reev.us?

- Reev.us is an attempt to replicate our class website and make an app version of it.
- This makes it easy to access wherever you are.

- This application also has few additional features:
  - Logging in feature
  - FAQ's section
  - Trial and Error Section

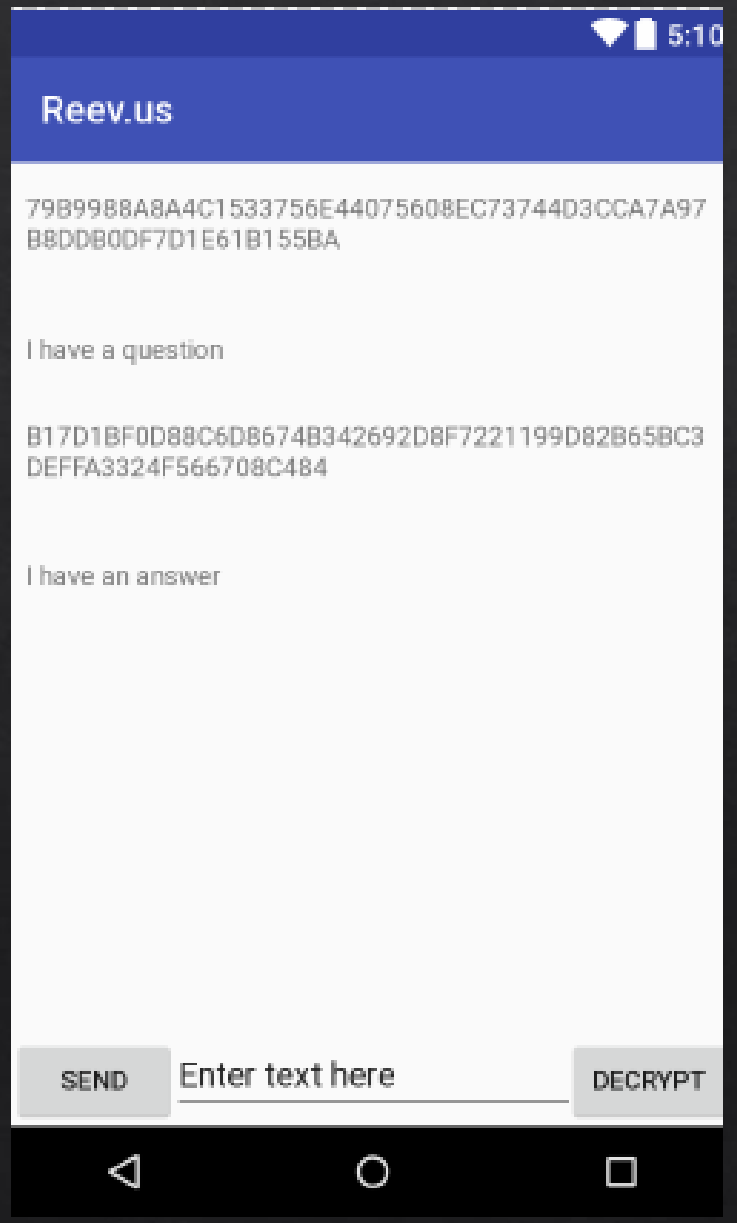
Logging In Section

- Every user can view the introduction page of the app but only registered users can log in and access the schedule and Trial and Error section.
- Log in based on the code
- This section encrypts the login details using SHA-1.
- Java.security.MessageDigest package
- This MessageDigest class provides applications the functionality of a message digest algorithm, such as SHA-1. Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.



FAQ section

- In this section, students can ask any question.
- The question will be visible in encrypted form.
- Every user on registering gets a “key” that they will be using to decrypt this question
- On entering the correct key, the question will be decrypted and anyone who knows the answer can reply. This will be encrypted as well.
- All the messages in this section are in encrypted form and can be decrypted by entering the right key.
- AES- 128 bits for the encryption.



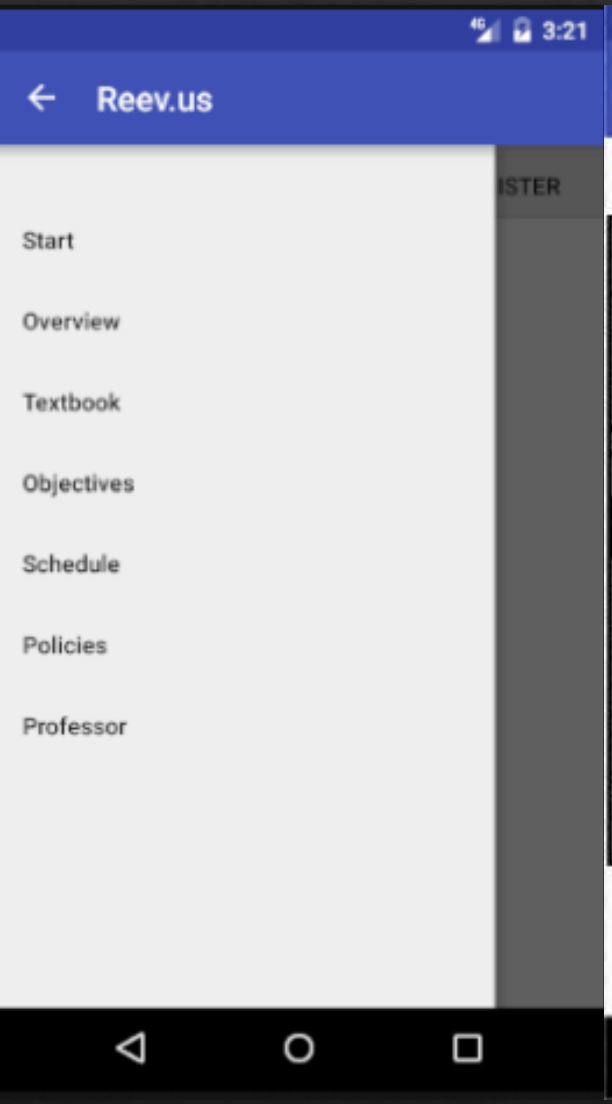
Trial and Error Section

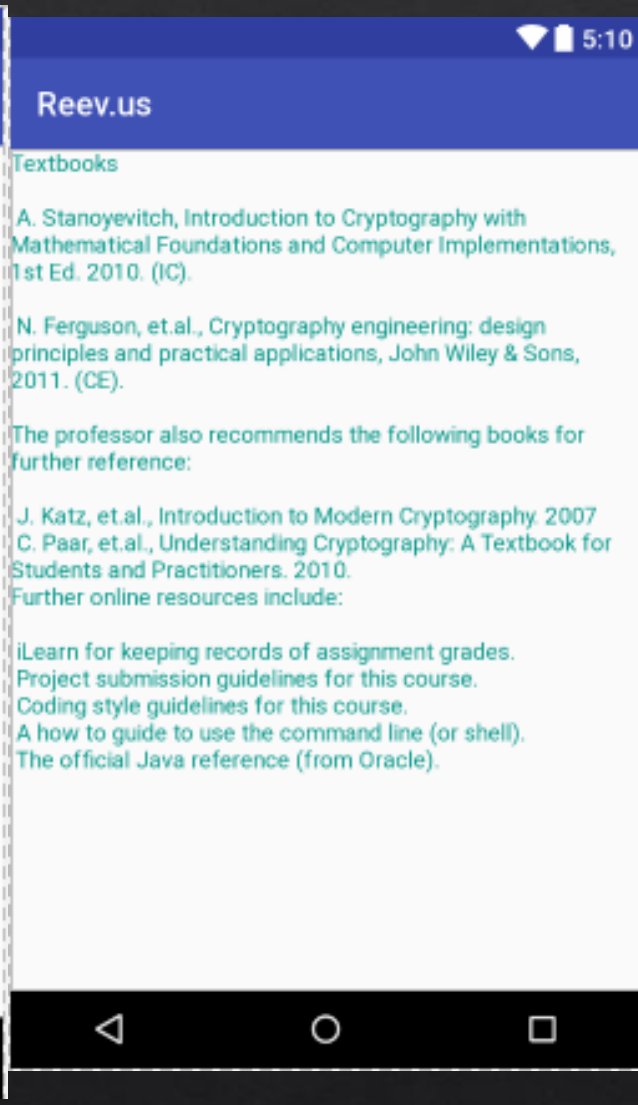
- This section consists of list of ciphers.
- When clicked on a cipher, you will be able to try different inputs and see their outputs after encryption.
- The selected cipher will be used to encrypt the input and the output is an encrypted text.
- This section is mainly intended to try and explore different encryption algorithms and have a better understanding.

What I achieved and what needs to be done

- I was able to understand the concepts of android app development, implementing AES algorithm, java cryptography packages.
- I was able to replicate our class website into an android app.
- I was able to implement logging in feature that stores user details in database.
- I was able to implement FAQ section.
- I need to implement Trial and Error Section

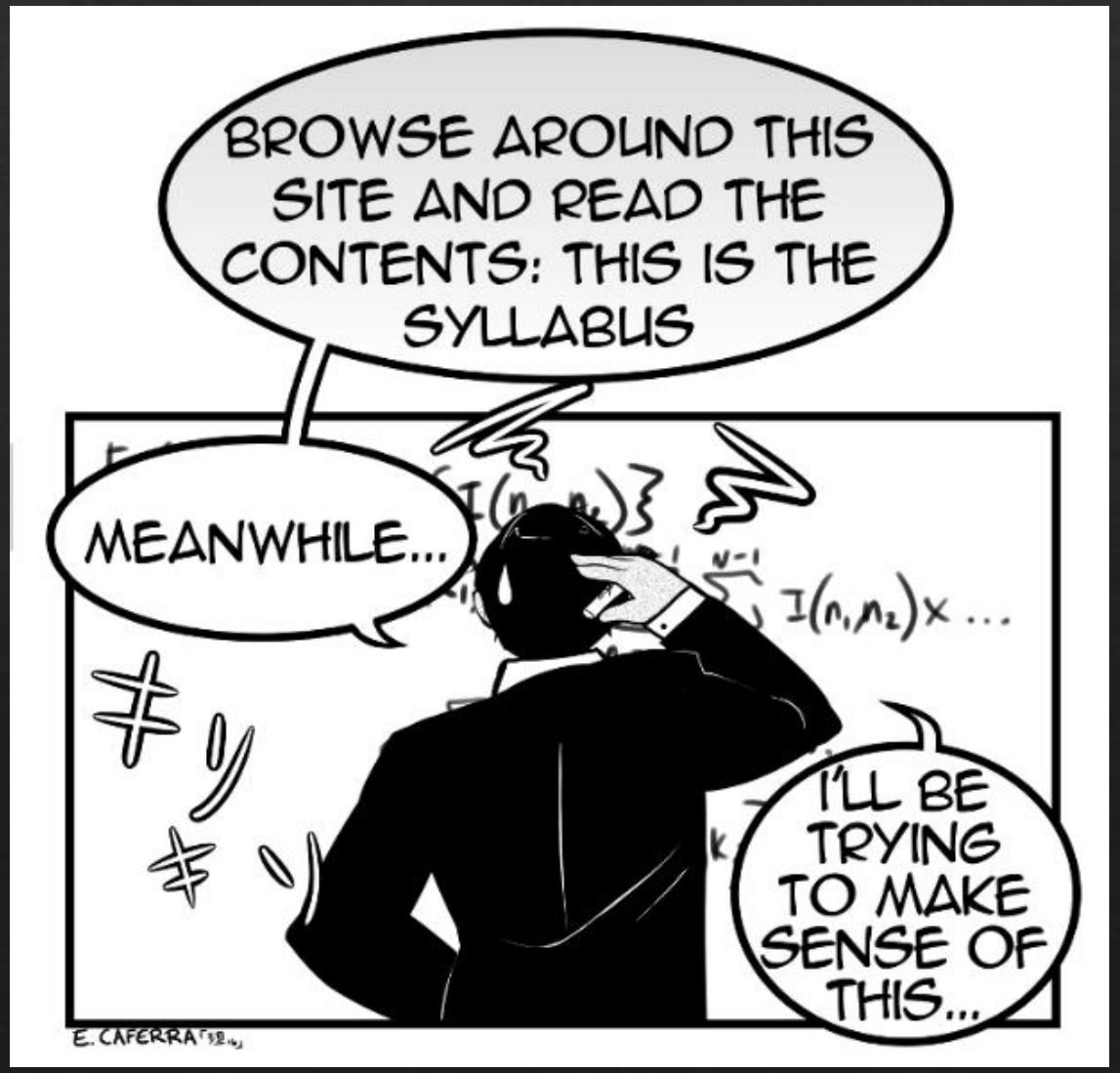
Screenshots





Future Enhancements

- User Interface -> Improved Look and feel
- Notification Function for the app whenever a question is posted
- Few additional functionalities like announcements, puzzles that incorporate cryptography.
- Extend it as an IOS app.



Thank you!!