Software Engineering Project

Group Members:

1. Muhammad Shahryar Khan Bscs14001
2. Usama Sadiq Bscs14006
3. Farrukh Zaib Bscs14065
4. Umer Saleem Bscs14067

Project Title: **Encryptify**

Project Description:

Our idea is to make a text messaging android app based on 256-bit AES encryption technique. There will be two keys, one will be user based and one will be app based key. User based key will be different for each contact key. Both these keys will be combined to make a new key which will be used to encrypt the message. It will enable the encryuption service such that no third party, even the telecom companies will not be able to read the messages. Encryption based messaging can only be used if our application is installed on both ends, otherwise simple message will be shown to the user without any encryption or decryption. We are interested in doing this project because currently no such application is present on play store.

Questions:

***Q1*. Do you think you need mathematical verification of correctness of your system or a part of your system? Why?**

***Ans*:**

Yes, since our project is based on encryption of text messages. So we'll need to verify that our encryption is strong enough that it can't be decrypted with simple brute force technique or any other normal techniques.

***Q2*. Can you separate various concerns of your project from functional and quality perspectives? Highlight the concerns and describe how can you handle concerns separately?**

Ans:

Yes, our project can be seperated in various concerns. The functional perspective deals with the development of project on moduler basis. How modules will be added in the software on incremental basis and how project will be made accessible to people. Quality perspective concerns the security of our encryption technique. It deals with the

issue that how much strong our encryption technique is?

Some of the functional concerns are to make the text messaging fully functional before adding encryption to it and then provide fully functional encryption based text messaging. This issue can be solved by making the project in incremental model.

Quality concerns are to have a strong enough encryption technique. We will use 246-bit AES encryption technique, which is so far the strongest technique of encryption and it can only be breakable by the use of quantum computers or very high resources. Using the built in libraries for this encryption will deal with the security issue. One more layer of security will be to have a combination of two keys, user based key and application key. The message can only be decrypted if both the keys and the operation to combine those keys is known.

***Q3*. Identify some functional modules in your system. Discuss coupling and cohesion aspects.**

Ans:

Our project will be divided in two major parts i.e. Messaging and Encryption. Both of these modules are cohesive enough to exist independent of each other. In this project we will combine both of these projects with minimum coupling to make a new software which will have features of both of these modules.

***Q4*. Identify the potential future changes in your system. Pick one potential change and discuss how would you address it in your system?**

Ans:

Some of the potential changes in our system can be following:

- To make the encryption more secure by applying a randomized key generation process on both application and user level.
- To provide network based messaging (like Whatsapp) along with the standard SMS feature.

To include the network based messaging in our system, we will use Google Firebase storage to store, send and retrieve messages on cloud. User will be provided an option on whether to send message through cloud services or by standard sms service.

***Q5*. Which increments would your suggest if you are asked to build your system**

incrementally?

Ans:

Our main aim is to build our project on incremental basis, and the stpes will be following

i. Simple text messaging application

ii. Text messaging application with application based key encryption

iii. Text messagin application with both application and user keys based encryption