**ABSTRACT**

This final year project is focused on the use of encryption methods for mobile text messaging application and develop SMS security mechanism on android enabled mobile. The fulfilled objectives are to study and identify the appropriate encryption/decryption algorithm for mobile application; study and identify the appropriate security technique for end-to-end text message security; design the architecture of secure text message using android studio; develop a prototype for secure text messaging application which enables the user to send and receive confidential information using any android enabled mobile phone; and evaluate the performance and quality of service after implementation of the secure system.

In this mobile application solution, Blowfish is used for encrypting the original SMS messages and Elliptic Curve Cryptography (ECC) is used in this system as a secure channel to transfer the onetime key which is used to encrypt the message. The onetime key is encrypted by ECC and sent to the receiver together with the message at a time.

The deliverable of this project is a mobile application that writes and reads encrypted text messages. For an encrypted message, the key is generated at the point of creation of the text message. At the recipient’s end, the key is extracted from the content and used to decrypt the main body of the message and it is displayed to the user. When the “Create New Message” is clicked, a screen is brought forward and a prompt for the use to input the destination phone number and a message content. There is also a button at the bottom of the screen to encrypt the message. When the button is clicked a key is generated using ECC encryption and the key is used to encrypt the message using blowfish encryption algorithm and then encoded in base 64 so as to pass over the network and the encrypted message is sent over the mobile network. On every run of the app, the user has to input the security pin created so as to be able to access the application software.