**Project Proposal**

**Encryption of text messages using the same android application.**

Gentjan Gjeci

MSCS 630

Due 2-8-2017

For my application I would like to implement an android application that uses AES-128 bit encryption. This application would send encrypted SMS messages between two parties using the same application. In today’s world protecting personal information is crucial to our wellbeing. Privacy is very important to us all, and I personally believe that being able to have a private conversation with friends and family is without worrying too much that someone will hijack the conversation and use that information to harm us is very important.

Each user application will be able to generate an AES-128 bit key locally and use that key to encrypt the data to be sent over the internet to the destination. The receiving applications at the destination will use the same AES-128 bit key to decrypt the message. Then it can send a reply message back encrypting it with the same AES-128 bit key. The encryption/decryption key will be shared using a private and public key method (This will not be implemented; it is just one way of sharing the key between applications).

Encrypting the messages between two parties ensures that no one can read the plain text message meant to be read only by the receiving party with a valid AES key. If the message is intercepted it will be impossible to read the cipher text without the appropriate key. This prevents the man in the middle attack from happening. This app will not only prevent random hackers from stealing personal and sensitive information from users but also prevents government agencies from sniffing the available data in the public domain without authorization.

We know that in our era protecting our information especially sensitive information is very important. Identity theft can have a big impact on us individually and financially. Sometimes it is almost impossible to recover from the damage done to us with the information stolen from us and used illicitly. For these reasons protecting our information as much as we can is an necessity.