**Project Proposal**

**Encryption of chat messages on messenger app for android**

Mitin Sharma

MSCS 630

Due 2-8-2017

For Security algorithm project i would like to implement AES 128 bit encryption on chat messenger app that work on android platform. The manifest of this application would be to provide 2 way security by implementing encryption on both ends. Sender will send encrypted message over http protocol and receiver will receive encrypted message that is need to decrypt at this end. The requirement of this application would be android operating system minimum version Jelly Bean and up to latest one. This app should be installed on both users to have private and secured conversation.

In today’s era of technology and networking. People get connected so fast over internet but they don't insure security and their important conversation get leak. In this application each user will generate AES 128 encryption key, with this key messages will encrypt and send to destination. At destination receiver will use shared public/private key to decrypt the ciphertext and reply back to sender by encrypting information with his own key.

This app will assure both parties that the information they are sharing with each other will be secure. Nobody can read messages without correct key. This app will also prevent organisations to steal information from public source. Today hiding identity is very important because hackers can impact your private information as well can hurt you financially. Identity theft can impact you personally and socially. There are very less number of such applications that provide you 2 way encryption over internet.

For these reasons i decided to develop an application that would secure our information on the network using Encryption AES-128 bit.