****

**JARAMOGI OGINGA ODINGA UNIVERSITY****OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**PROJECT TITLE: MESSAGE ENCRYPTION APPLICATION FOR ANDROID.**

A project submitted in Partial Fulfillment of the Requirements for the award of the

DEGREE OF

**BACHELOR OF SCIENCE**

In

**COMPUTER SECURITY AND FORENSICS**

*Authors:*

**JOHN MWANGI NJUGUNA -**I132/**0865**/2013

**LILIAN MWENDE MUTHUI -**I132/**0870**/2013

*Under the guidance of*

**JOSHUA AGOLA**

# **ABSTRACT**

The emergence of Short Messaging services (SMS) has extensively transformed the nature of communication and information sharing. Billions of text messages are sent daily in the worlds in plain text format and hence user privacy and security is not assured. With the increasing number of software crackers available for free in the internet, SMS continues to suffer from security vulnerabilities and loopholes. Information security has long been thought to be inclusive of only personal computers and networks. However, with the technological trend shifting from computers to mobile devices, malicious attackers are now targeting mobile devices and their users.

The aim of this project is to develop a secure messaging platform for android phones to reduce these vulnerabilities and loopholes. To implement the Advanced Encryption Standard (AES) and applied symmetric encryption concepts. The experimental results revealed that the system was able to encrypt, decrypt, send and receive text messages without adding changing the size of the packets.

The decision to use AES was based on the status of AES as the currently accepted standard for data encryption, and its nearly ubiquitous use in encryption-offering software (and hardware). It is a thoroughly analyzed and accepted algorithm, offering powerful encryption with a small key size. More so, android phones comes with advanced encryption standard classes that can be applied during the development of mobile applications therefore AES is easier to implement in Java platforms as compared to DES which is much slower-depending on the size of the key.