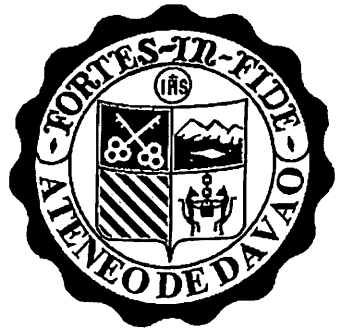
Designing and Developing a Hybrid Cryptography for Google Android



By

$\sum R^{o}P^{i}C^{a}$

CANCERAN, CITADEL DONNA E.
PIEDRAVERDE, RINGO RAY H.
ROSETE, VINCENT JUDE D.

ATENEO DE DAVAO UNIVERSITY

COMPUTER STUDIES DIVISION

DAVAO CITY

MARCH 2010

Designing and Developing a Hybrid Cryptography for Google Android

A Mini-Thesis

Presented to the

Undergraduate Faculty of the

Computer Studies Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

By

$\sum R^{o}P^{i}C^{a}$

CANCERAN, CITADEL DONNA E.
PIEDRAVERDE, RINGO RAY H.
ROSETE, VINCENT JUDE D.

ATENEO DE DAVAO UNIVERSITY

COMPUTER STUDIES DIVISION

MARCH 2010

TABLE OF CONTENTS

ABSTRACT

The use of mobile phones nowadays has grown rapidly in markets and industries. In line with this, the rapid consumer adoption of mobile OS is a marked increase in the level of mobile search activity. This increasing demand in cell phone applications also requires higher level of security. As mobile networks expand their bandwidth, mobile phones, as with any other Internet device, become substantially exposed to Internet security vulnerabilities. Since the high technology mobile applications are derived from the computer application, the security of mobile phones may also be derived from computers. Nowadays, the most efficient procedure in making the system secured is by using Cryptography algorithms, specifically asymmetric cryptography. However, this method requires much memory in which mobile phones are limited. This study aims to design a hybrid cryptography for mobile applications especially on google android.

Keywords:

<Google Android, Asymmetric Cryptography, Hybrid Cryptography >

Chapter 1

INTRODUCTION

1.1 Background of the Study

Android is a software platform and operating system for mobile devices based on the Linux kernel and developed by Google and later the Open Handset Alliance. It allows developers to write managed code in the Java language, controlling the device via Google-developed Java libraries (Wikipedia, 2009). The release of Android platform enables the developers to build applications for Google phones

Asymmetric cryptography is a method for secret communication between two parties without requiring an initial exchange of secret keys. It can also be used to create digital signatures. Public key cryptography is a fundamental and widely used technology around the world, and enables secure transmission of information on the Internet.

Asymmetric cryptography requires much space since it produces two keys. There is a difficulty implementing it on mobile phones since mobile memory is limited. On the contrary, symmetric key which produces only the public key works faster than the asymmetric cryptography. However, there is less security in symmetric key since it uses only one key for encrypting and decrypting. The proponents decided to create a cryptography that uses two keys, public key and the private key, and generate the keys like Symmetric Key does. More so, the proponents also designed a new way on how to exchange keys efficiently. By this,

an application which uses cryptography can be used not only on computers but also on mobile.

1.2 Statement of the Problem

The study seeks to answer the following general problem: How can we design a Hybrid Cryptography Application for Google Android?

The proponent also seeks to answer the following sub-problem:

- What components of Symmetric and Asymmetric cryptography are useful for creating efficient hybrid method?
- What are the existing designs for exchanging the public key of two parties?
- How can the Hybrid method be implemented on google android?

1.3 Objectives of the Study

The general objective of this research is to develop a Hybrid Cryptography and design a way on how to exchange keys on a network.

The specific objectives of the study are the followings:

- To implement a prototype application to protect text messages using the Hybrid Cryptography.

- To prevent Google Android from security threats in the mobile environment.
- To initiate innovations on mobile phone security.

1.4 Significance of the Study

This innovation on mobile phone security serves as the first way on how to secure not only the messages but also the exchanging of public keys. This study is significant to all mobile users especially to the GPhone users. More so, this also helps the government security agencies in sending secret messages to the other party. This study also gives idea to the developers on how to improve the security of mobile phones.

1.5 Scope and Limitations of the Study

The study will focus on implementing a Prototype application using the hybrid cryptography on the phone. This design shall be implemented for Google Android phone to secure its messaging. The final output which is the designed cryptography and the method on how to exchange keys will be tested using short messages application.

An Android emulator shall be used to examine and evaluate the created application to the phone and will be limited on the said area.

1.6 Definition of Terms

- **Google Android** – is a software platform and operating system for mobile devices based on Linux kernel, developed by Google and late the Open Handset Alliance
- **Asymmetric Cryptography** – this will be used as the method of security by encrypting and decrypting messages which consist of public key and private key.
- **Symmetric Cryptography** – this is a cryptography that uses only one key in encrypting and decrypting message. It's advantage which is fast key generation will be used for the hybrid.
- **RSA Algorithm** – a specific kind of asymmetric cryptography in which the computation of private and public key will be derived.
- **Public Key** – in this paper, it is used as a recipient's key which is used for encrypting messages.
- **Private Key** - it will be associated with the public key at the same time it is used to decrypt the encrypted messages.