# Smart Phone Cryptography: A comparison of techniques for encrypted data communication Progress Report

Tom Nicholls

November 22, 2012

In this progress report document details will be given as to how this project has evolved from the description presented in the project specification, outlining and justifying any changes made. The state in which the project is currently in will be shown, including a presentation of the work completed up to this point. This will included any design and project choices that have been made. The document will be finished with a detailed plan of how the project will continue over the next term, up to completion.

## 1 Project Alterations

Since the project specification document, this project has undergone a few changes in order to ensure that it is both an interesting project and also that it includes sufficient original work and accomplishments to current areas of Computer Science. This section details the adjustments made to the project.

### 1.1 The Problem Definition

The main alterations in this project can be best described through a statement of the new problem definition:

The privacy of sensitive information has always been an important issue. With the increased popularity and usability of smart phones, tasks from accessing confidential work files or personal bank accounts to communicating with clients and friends, are being completed through applications over mobile, wireless internet connections.

In this project I will research the various cryptographic schemes used by popular applications available to smart phones running the Android operating system for secure data transmission and communication. Accompanying this research will be a study and comparison of other schemes which could be used instead of those presented previously. A currently used cryptographic technique and an alternative technique will be implemented through a data

transmission application. Tests will be carried out to analyse various important factors that need to be considered for a successful encrypted data transmission application, such as mobile data usage or cryptanalytic methods required to break the data encryption. An original conclusion will then be drawn as to whether the current techniques of cryptography available are appropriate or if a new scheme should be encouraged. How this conclusion can be extended to encompass functions other than text transmission will then be presented, for instance secure secret sharing.

## 1.2 Objectives

To further explain the adjustments made, the new objectives of the project will be presented.

### Main Objectives

1. Research
    - Framework design
    - Cryptographic Techniques
    - Currently Available Applications
    - Relevant factors that can be used to compare schemes implemented on a mobile device
2. Implementation
    - Framework
        - Design Data Communication framework
            - Server
            - Mobile Application
            - P.C Client
        - Build, test and document framework
    - Encrypted Data Communication
        - Design and implement cryptographic techniques, justifying choices
        - Test and document implementation
3. Analysis
    - Perform tests from research
    - Collect and present results
4. Conclusion

- Present and justify the findings and conlusions that can be made form the completed tests
- Show possible adjustments to the implemented schemes which would increase their usability

5. Further Work
    - Detail possible extensions that can be made to the systems to include other possible functions
6. Documentation
    - Design documentation layout
    - Complete and proof read full documentation

**Secondary Objectives**

1. Design, create and justify an industry acceptable and marketable user interface for the finished product
2. Implement functionality described in the further work objective (Objective 5)

## 1.3 Additional Changes

Aside from the adjustments made in the problem definition and objectives sections detailed above, only minimal changes have been made to the rest of the project specification. For example in the 'Methods' section the research phase can still be completed in parallel to the framework development phase, with all other objectives requiring the objective before it to be completed before it can be started. Furthermore, only minor changes been made to the 'Resources' section; re-wording of the project components to account for the changes mentioned above and the addition of the Google application market place 'Google Play' to the list of resources. This is available through the internet which I have full access to.

A final addition to the specification that should be noted is the inclusion of another legal issue surrounding the project. As the resulting product of this project facilitates the secure and secret communication of messages which, in the wrong hands, could be used to aid a number of illegal operations such as crime organisation or terrorism. To avoid this issue in a legal sense I will not publish the final application to the Google market place and I will also present a legal disclaimer attached to this product incase someone does obtain a copy of the application. The issue could also be viewed as an ethical issue, but the actions taken to escape the legal issue should ensure the avoidence of the issue viewed in an ethical sense.

## 2 Work Completed