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

Tom Nicholls

April 3, 2013

## Contents

# 1 Introduction

In this progress report, details will be given as to how this project has evolved from the description presented in the project specification (Appendix **??**), 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 timetabled plan of how the project will continue over the next term, up to completion.

# 2 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.

## 2.1 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 the various cryptographic schemes used by popular applications available to smart phones running the Android operating system for secure data transmission and communication will be researched. Accompanying this research will be a study and comparison of other schemes which could be used instead of those presented previously. Currently used cryptographic techniques 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.

As can be seen, the project is now centred around the implementation of currently used schemes and an alternative scheme, in a mobile application setting. Tests will then be used to provide a comparison between the schemes, with which a conclusion over which scheme should be encouraged,

can be obtained. The conclusion will be original as no other external results have been found or considered.

## 2.2 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 conclusions 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)

A further breakdown of the objectives can be found by looking at the Gantt chart provided with this document (Appendix **??**).

## 2.3 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. The testing phase for each section of the project can also be completed in parallel to its development, as I will describe later in this document. Furthermore, only minor changes been made to the 'Resources' section; a 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. 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 in case 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 avoidance of the issue viewed in an ethical sense.

# 3 Work Completed

In this section the work that has been completed in this project so far will be presented.

## 3.1 Research

In this project, the first task was to perform research (see Objectives section). An overview of the results of the research performed is described below. The results of this research will be formally presented and described in more detail, including a full explanation of any cryptographic schemes, in the final project report.

1. **Framework Design**

   Research was made into how a system could be set up to facilitate the communication of data messages between any two users of the system. Socket-based communication will allow networking between a central Java based server and P.C client, whereas HTTP Post and broadcast-receiver methods will be used to allow the Android application to transfer and receive data from the server [**?**]. The result of this research, to utilise a multi-client server [**?**], can be found in the design section, where an outline of the system to be created is given.

2. **Cryptographic Methods** Research was completed using books by Wenbo Mao [**?**] and William Stallings [**?**].

   - **AES**

     AES is a symmetric-key algorithm in which the same cryptographic key is used for both encryption and decryption. The AES scheme takes a block of plaintext and the key as inputs and applies several rounds of transformations to produce the ciphertext block. Decryption is done by reversing the process.

   - **RSA**

     RSA is an example of an asymmetric key algorithm, in which a public key and a private key are utilised. The public key is shared and known with everyone and used in the encryption process. The messages encrypted with the public key can only be decrypted using the matching private key. The RSA algorithm is based upon the difficulty of factoring large integers, with encryption and decryption of the form

     $$C = M^e \mathrm{mod}(n)$$

     $$M = C^d mod(n) = (M^e)^d \mathrm{mod}(n) = M^{ed} \mathrm{mod}(n)$$

     where M is the plaintext message and C is the ciphertext.

- **ECC**
  ECC is another approach to public-key cryptography (asymmetric key algorithm) but is based on the algebraic structure of elliptic curves over finite fields. The assumption that finding the discrete logarithm of a random elliptic curve element, with respect to a publicly known base point, is infeasible is the basis for the elliptic curve cryptographic scheme.

3. **Current Applications**

   As a result of searching on the Google application marketplace Google Play, only two different applications currently exist that perform encrypted message communication. These two applications are:

   - RSA Cipher Cat by Miasoft [**?**]
   - Cloak SMS Free by Hamish Medlin [**?**]

   Both applications allow the communication of encrypted messages between two users of the application. RSA Cipher Cat utilises the RSA asymmetric encryption scheme whereas Cloak SMS Free is uses the AES symmetric key encryption scheme.

4. **Mobile device application comparison factors**

   As the third section of this project is concerned with the analysis and comparison of cryptographic schemes, research was performed to discover which factors impact how successful and useful an encryption scheme on a mobile device is. The discovered factors were largely found in a article by Nirav Jobanputra, *et al* [**?**]:

   - Difficulty of techniques required to break encryption
   - Energy Consumption/Battery power required
   - Operation and Processing Time
   - Cryptographic key size
   - Mobile data usage
   - Application size
   - Number/Duration of data connection required

## 3.2 Design

As can be seen from the previous sections in this document, this project includes a software development section. The system is built upon a multi-client server facilitating the communication of data between two clients. This data is encrypted (and decrypted) using different cryptographic schemes.

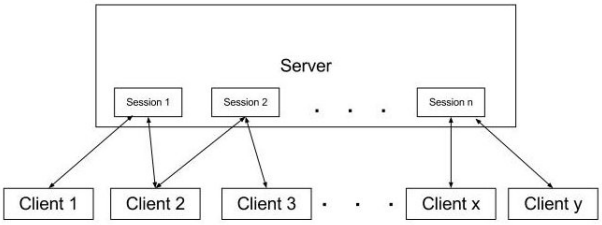



Figure 1: The server can create many communication sessions from a collection of clients

The server creates a session between two clients that wish to communicate. Clients initiate sessions with any other client with which they have shared their identification code (ID number). Each session is a new thread within the server. This allows the server to establish any number of sessions, to allow for multiple communication links between any two clients. As can be seen in Figure **??**, any client can have more than one communication session at any one time, with any other client in the client base.

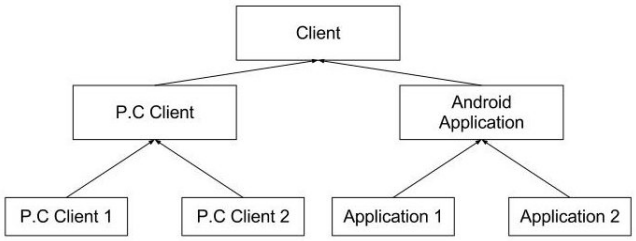



Figure 2: Basic inheritance hierarchy of the clients

The Client class contains the methods which allow it to connect to the server and send data to another client in the client base through the server. The P.C client and Android application inherits these abilities from the client but are more specific, so are implemented according to its own rules (e.g. sockets or HTTP methods). Hence, a P.C client can send a message (unencrypted), via the server, to another P.C client or an application. This can also be achieved by an application client. Compatibility between the clients will be ensured through the use of the XML file structure. P.C client 1 (and 2) are more specific versions of the P.C client class. P.C client 1 has all the capabilities of the P.C client, with an added encryption method. Similarly for P.C client 2, but a different encryption scheme will be implemented. For example, if two cryptographic schemes are implemented; Application 1 and P.C client 1 will utilise scheme 1 and Application 2 and P.C client 2 will utilise scheme 2. P.C clients are required in this project to simulate the process of a user sending an encrypted message to a company, for example,

their account details to their bank, via their mobile application.

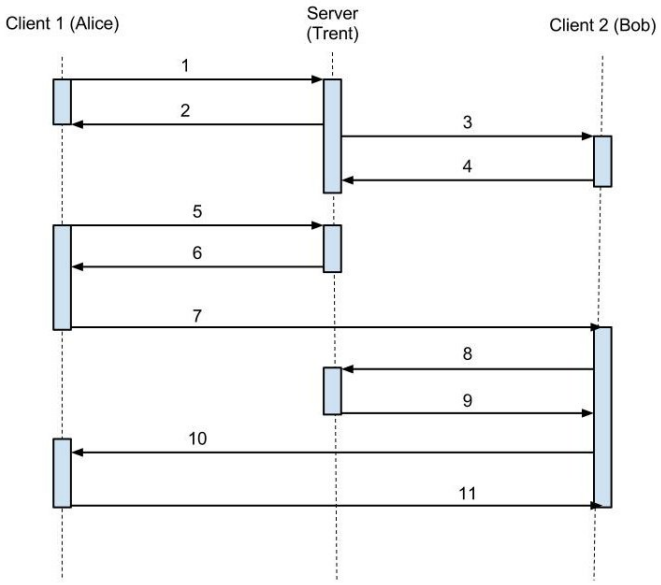



Figure 3: Sequence diagram showing distribution of public keys

The encryption schemes used within this project all require the sharing of public keys. Figure **??** shows how this will be achieved as described by Wenbo Mao [**?**]. The place-holder names Alice (User A), Bob (User B) and Trent (Trusted third-party server) have been used in keeping with tradition set out by Bruce Schneier [**?**].

1. Alice registers her public key $K_A$ with Trent
2. Trent sends his public key $K_T$ to Alice
3. Bob registers his public key $K_B$ with Trent
4. Trent sends his public key $K_T$ to Bob
5. Alice sends to Trent: $Alice, Bob, Timestamp1$
6. Trent sends to Alice: $\{K_B, Bob, Timestamp1\}K_T^{-1}$
7. Alice checks Trent's signature on "$K_B, Bob$" and the timestamp, creates her nonce $N_A$ at random and sends to Bob: $\{N_A, Alice\}K_B$
8. Bob decrypts the message, checks Alice's ID and sends to Trent: $Bob, Alice, Timestamp2$
9. Trent sends to Bob: $\{K_A, Alice, Timestamp1\}K_T^{-1}$

10. Bob checks Trent's signature on "$K_A, Alice$" and the timestamp, creates his nonce $N_B$ at random and sends it to Alice: $\{N_A, N_B, Bob\}K_A$

11. Alice decrypts and sends to Bob $\{N_B\}K_B$

(Steps 7, 10 and 11 passed through server and directed straight to client) Note: $\{M\}K_x^{-1}$ represents the encryption of message $M$ with the private key of client $x$, whilst $\{M\}K_x$ represents the encryption of message $M$ with the public key of $x$.

Once this protocol has been completed, each client has the other client's public key and the communication of encrypted data can commence. Steps 1 to 4 registers the public keys of the clients with the server, which are only required when a connection is made between two clients that are new to the system or have not yet made a connection to the server. Therefore, these steps will not be required for each new session initialisation. However, for various reasons, a user may wish to generate a new key-pair, which will need to be registered with the server and hence the protocol completed in full when they wish to set up a session with another client. This feature will be fully implemented and available in the final product.

# 4 Project Management

As described in the project specification, various methods will be adopted to ensure that the project files (code, documentation etc.) are constantly backed up and that version control is maintained. The free services of Dropbox[**?**] and Git/Github[**?**] have been set up and can be accessed from any computer or workstation that is used in this project, allowing a constant back up. In addition to this an external flash drive has been dedicated to the task of providing a back up of data, as well as the Department of Computer Science machines. Bash scripts have been written to make the back up of data to all of these services less time consuming.

For documentation, the document preparation system LaTeX will be used. This is because LaTeX allows the inclusion of mathematics into a document in a simple and easy to use way with high typographical quality, which will be extremely beneficial in this project.

As for the software development section of this project, the technique of test driven development in a plan-driven setting will be employed as described by Ian Sommerville [**?**]. Plan-driven development is clearly the best choice due to the nature of this project. The other option, agile development, is best suited for a project with a dedicated customer, such that constant communication can be maintained. It also encourages the constant evolution of a system due to changing ideas or specifications and restricts the amount of documentation created. Plan-driven development, on the other

hand, has a set plan for development which it follows to produce the end product and a firm set of documentation.

Test-driven development combines testing and development. Code is developed incrementally, along with a set of tests for that increment. The next increment is not started until the previous increment is fully tested and completed. In the context of this project, the implementation of the cryptographic schemes will not be started until the multi-client server is set up and can transfer data, for example.

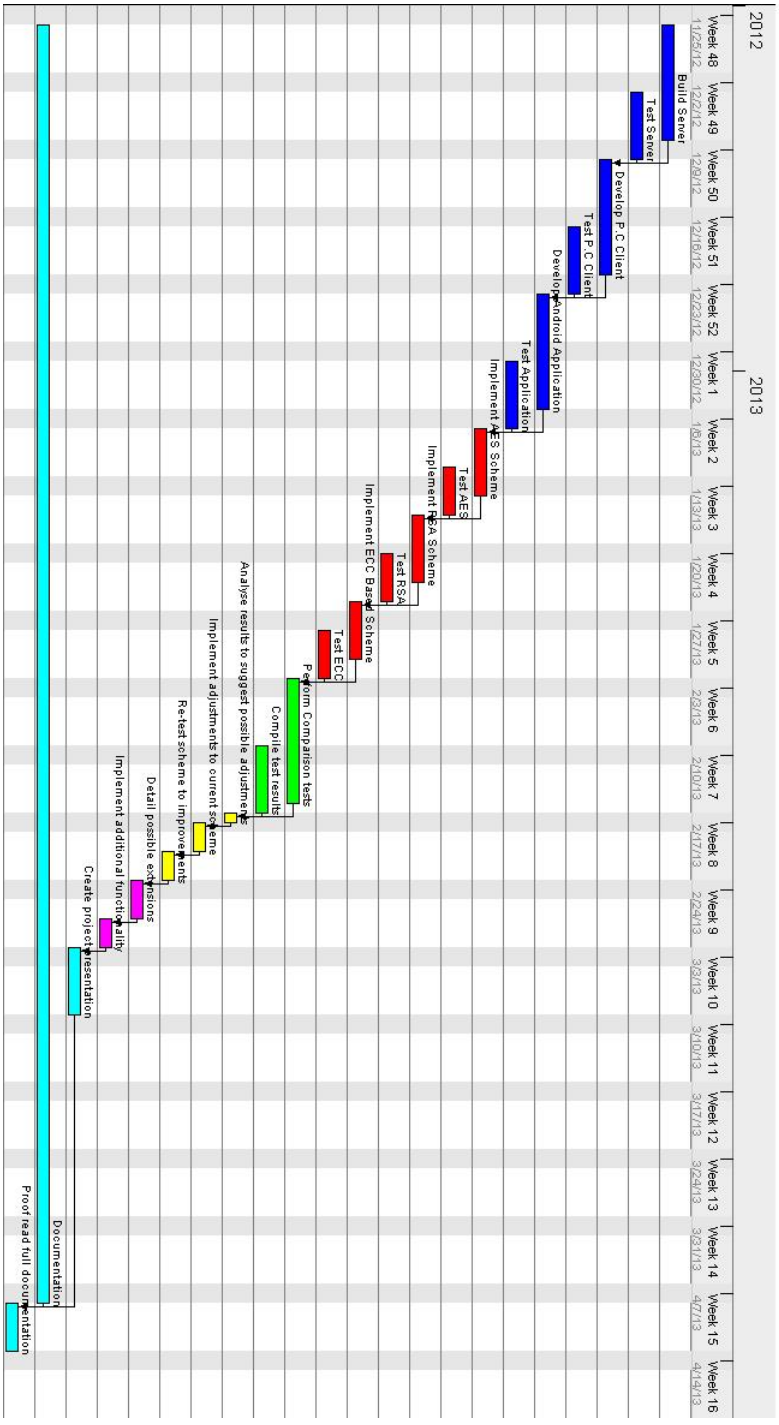
# 5 Project Continuation Plan

A timetable showing the completion dates of main events and milestones in this project, starting from the hand in date of this document, is presented below. Please refer to Appendix **??** for a Gantt chart showing a more detailed plan.

| Date | Task |
|---|---|
| **Monday Week 9 - Term 1** | **Submit Progress Report** |
| Week 10 - Term 1 | Server Implementation completed |
| Christmas Break - Week 1 | |
| Christmas Break - Week 2 | P.C Client completed |
| Christmas Break - Week 3 | |
| Christmas Break - Week 4 | Android Application completed |
| Week 1 - Term 2 | Complete framework finished |
| Week 2 - Term 2 | |
| Week 3 - Term 2 | |
| Week 4 - Term 2 | Implementation finished |
| Week 5 - Term 2 | |
| Week 6 - Term 2 | Analysis completed |
| Week 7 - Term 2 | Conclusion completed |
| Week 8 - Term 2 | Further work finished |
| Week 9 - Term 2 | Presentation finished |
| Week 10 - Term 2 | |
| **Week 9 and Week 10 - Term 2** | **Project Presentations** |
| Easter Break - Week 1 | |
| Easter Break - Week 2 | |
| Easter Break - Week 3 | |
| Easter Break - Week 4 | Project Report finished |
| Easter Break - Week 5 | |
| **Thursday Week 1 - Term 3** | **Submit Project Report** |

Table 1: Timetable of completion dates of main objectives

# A Gantt Chart



# B Project Specification

# A study and implementation of Cryptographic and Cryptanalytic methods

## Project Specification

**Problem**

The privacy of sensitive information has always been an important issue. With the development of computer networks and the internet, the secrecy of data is ensured through the use of different techniques of cryptography. Cryptanalysis uses mathematical techniques to 'break' the cryptographic methods used. Both cryptography and cryptanalysis are ever increasing and developing fields of computer science and mathematics, both within research and in industry.

In this project I will research the various techniques used in the current state of cryptography and cryptanalysis. Using this research I will analyse, compare and implement some existing encryption methods, which can be complemented by the development of a new original method, if my analysis shows the need and means for it. I will also develop a unique form of cryptanalysis in an attempt to break the encryption.

**Objectives**

Main objectives:

1. Research
    a. Research cryptographic techniques
        a.i. Perform research
        a.ii. Compile research into a usable, useful form
        a.iii. Compare and contrast various techniques
    b. Research cryptanalytic methods
        b.i. Perform research
        b.ii. Compile research into a usable, useful form
        b.iii. Compare and contrast various techniques
2. Implementation
    a. Framework
        a.i. Design data communication framework
        a.ii. Build framework
        a.iii. Test framework
        a.iv. Document framework
        a.v. Document testing
    b. Cryptography
        b.i. Design implementation of cryptographic techniques, justifying choices
        b.ii. Implement cryptographic techniques
        b.iii. Test cryptographic techniques
        b.iv. Document implementation
        b.v. Document testing
        b.vi. Perform an evaluation of implemented cryptographic techniques
    c. Cryptanalysis
        c.i. Design implementation of cryptanalytic methods, justifying choices

c.ii. Implement cryptanalytic methods
c.iii. Test cryptanalytic methods
c.iv. Document implementation
c.v. Document testing
c.vi. Perform an evaluation of implemented cryptanalytic methods

3. Original Work
    a. Cryptography
        a.i. Decide and describe the need and motivation for an original cryptographic method
        a.ii. Design, implement and test original method if required
    b. Cryptanalysis
        b.i. Describe unique form of cryptanalysis
        b.ii. Design unique cryptanalytic method
        b.iii. Implement unique cryptanalytic method
        b.iv. Test unique method
        b.v. Document implementation
        b.vi. Document testing
        b.vii. Perform an evaluation of the implemented unique cryptanalytic method
4. Documentation
    a. Design basic documentation layout
    b. Complete full documentation
    c. Proof read documentation

Secondary objectives:

1. Cross platform communication functionality
2. Design and create an industry acceptable user interface

**Methods**

The two objectives listed first in the previous section can be achieved in parallel. This is because building the implementation framework does not rely on any cryptographic or cryptanalytic techniques from the research stage. However, the objectives following this all require the research and framework to be completed. Furthermore, most of the objectives after the framework implementation are dependent on the objective before it being completed. This applies to all the objectives except for those involving testing after implementation, as this can, to some extent, be achieved in parallel. The testing sections can be achieved in parallel due to the fact that the ‘incremental build model’ method of software development model will be used. Although it cannot be completed in parallel to another task, progress can be made on the documentation objective once a previous objective has been completed. For example, the compiled cryptography research can be included into the documentation, whilst the cryptanalysis research is being started.

At the very start of this project, a day will be set aside to research software development and project management techniques and practices, other than those mentioned previously, which will be used to improve this project, if the research shows that it would be appropriate to do so.

**Timetable**

Timetable of the main events and milestones

| Date | | Task |
|---|---|---|
| **10/11/2012** | **Thursday Week 2 - Term 1** | **Submit Project Specification** |
| 11/16/2012 | Week 7 - Term 1 | Framework Finished |
| 11/23/2012 | Week 8 - Term 1 | Progress Report Finished |
| **11/26/2012** | **Monday Week 9 - Term 1** | **Submit Progress Report** |
| 12/7/2012 | Week 10 - Term 1 | Research Finished |
| 1/11/2013 | Friday Week 1 - Term 2 | Feedback returned: Make appropriate notes or changes to current work |
| 1/18/2013 | Week 2 - Term 2 | Implementation Finished |
| 3/1/2013 | Week 8 - Term 2 | Original Work Finished |
| 3/5/2013 | Week 9 - Term 2 | Presentation Finished |
| **07-15/03/2013** | **Week 9 and Week 10 - Term 2** | **Project Presentations** |
| 4/12/2013 | Easter Break - Week 4 | Report Finished |
| **4/25/2013** | **Thursday Week 1 - Term 3** | **Submit Project Report** |

**Resources**

As can be seen above, this project has three components; research, implementation and original development.

For the research component, the resources that will be needed are books and published papers or journals. These can be found and obtained within the University library, which I have complete access to or through the internet, which I can easily access within the Department of Computer Science or from my own personal laptop.

The implementation component requires the following resources: computer(s), programming language and documentation, development environment and back-up/version control facilities. Computer access will always be available as my own personal laptop and netbook will be used. Using the Java programming language, which is freely available, ensures there is a plethora of supporting documentation available in books and on the internet. Eclipse will be the software development environment that will be used, which is available to download and install for free. For back-up and version control the free services of 'Dropbox' and 'Git' will be used, in conjunction with constant back-ups to a personal flash drive.

For the original development component a combination of the resources detailed above will be used, with no additional access or resources required.

**Issues**

Legal issues are the only issues that need to be considered in this project. With a large portion of this project being research, it needs to be ensured that all materials used are correctly and appropriately referenced. Furthermore, as this project is centred on the issues of computer security in the form of cryptography and cryptanalysis, the current legal framework needs to be followed. As long as any material that is encrypted is legal in its own rights and that only data that is solely owned by myself is used in the cryptographic and cryptanalytic processes, then any legal issues will be avoided.