CS344 - Final Report

Smart Phone Cryptography

A comparison of techniques for encrypted data communication

Tom Nicholls - 1006007

Discrete Mathematics - Year 3

Marcin Jurdzinski

April 8, 2013

Abstract

Protecting sensitive or secret information has always been an important issue. With the increased popularity and usability of smartphones, tasks from accessing confidential work files or personal bank accounts to communicating with clients and friends, are being completed through applications over mobile or wireless internet connections. In this project the various cryptographic schemes used by popular applications available to Android based smartphones for secure data communication will be researched. Accompanying this will be a study of other cryptographic schemes. These techniques 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. 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. The results of the described implementation and analysis were that the currently used cryptographic techniques are appropriate for the current state of smartphone usage and capabilities. These techniques, however, should be combined to create a new application. A different technique, which has increased security for a smaller resource cost, exists that can easily be used in the event that the requirements of the current cryptographic schemes surpass the available resources of current smartphones.

Keywords: Cryptography, Encryption, Decryption, Smartphone, Android, AES, RSA, ECC

Contents

Chapter 1

Introduction

1.1 Background

To start this project report, all relevant background information will be presented allowing the reader to fully understand all aspects of the project. An overview of basic techniques and topics will be given, with a greater explanation for more specialised areas.

1.1.1 Smartphones

In this section, the basics of the smartphone will be introduced and described. As smartphones are a prominent part of modern culture, and therefore known in some degree to everybody, only an overview will be given. The book by Sarah Allen et al. [1] was used as reference material.

'Mobile' or 'Cell' phones have been available for commercial use since the beginning of the 1980s. The most popular functions of these phones are for telephone calls, text or multi-media message sending or even basic internet access and games. With the development of the smartphone these older devices are considered low-end phones. Higher-end phones, universally named the 'smartphone' provide the same basic features (telephone calls, messaging etc) but with a plethora of added functions such as full internet access, as well as increased computing capabilities through more powerful processors and other hardware. Smartphones also utilise the QWERTY keyboard and a larger, higher-resolution, screen.

Compared to desktop computers, smartphones have a diverse set of operating systems, determined by the manufacturer of the smartphone. Smartphone operating systems include; Apple iPhone iOS [2], Windows Phone [3] and Google Android [4]. Each operating system, unlike that of a desktop, determines which programming language a developer must use if they are to develop an app for a particular smartphone. This leads to a separate application marketplace, a database where users can download and install new applications, for each smartphone operating system. Whilst applications can be developed in a cross-platform manner, through the use of HTML and CSS, this is not yet standard, so the various marketplaces are individual in the applications that are on offer. The Android operating system, developed by Google and mostly found on devices by Samsung, HTC or Google themselves, use the Google Play marketplace

[5] for application distribution with applications being developed using the Java programming language.

The message sending capabilities of smartphones is the feature that is most important for this project, whether it be using the in-built standard messaging service (SMS) or through the use of an installed application. Message sending allows the specification of a recipient and a user entered message for that recipient, with a near instant sending and receiving of that message. On average, the message is of a short length and can be described as an easier, more lightweight form of simple email exchange.

1.1.2 Cryptography

Taken from the book by Richard A. Mollin [6], the meaning of cryptography is 'the study of methods for sending messages in secret (namely, in enciphered or disguised form) so that only the intended recipient can remove the disguise and read the message (or decipher it).' Many keywords are used in the study of cryptography and help to give an introduction to the field;

- Plaintext - The original message, input by the initiating user.
- Ciphertext - The disguised message, created using the plaintext.
- Encryption - The process of transforming the plaintext into the ciphertext.
- Decryption - The process of turning the ciphertext into the original plaintext. Accomplished by the recipient, who has the knowledge to remove the disguise.
- Cipher - The Method for enciphering and deciphering.
- Cryptanalysis - The study of mathematical techniques for attempting to break the cryptographic methods.
- Cryptographic Key - A tool for encryption or decryption

This shows that basic cryptography has the following form:

$$\textbf{Plaintext} \rightarrow \textit{Encryption} \rightsquigarrow \textbf{Ciphertext} \rightsquigarrow \textit{Decryption} \rightarrow \textbf{Plaintext}$$

Two very basic examples of cryptography, which can and have been expanded into many different, more elaborate, techniques, are the substitution and transposition ciphers. Substitution ciphers replace symbols in the plaintext with other symbols, using a given rule (the key), to produce the ciphertext. For example, the key may be; a → q, b → f, c → m, and so on. A transposition cipher, on the other hand, transposes the places in which the plaintext letters are situated. This means that no new letters are introduced. The key for this cipher is a permutation that describes how the letters should be transposed. For a plaintext that consists of 10 letters, the key could be:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 5 & 7 & 6 & 4 & 9 & 10 & 3 & 8 \end{pmatrix}$$

where the symbol in the position number in the top row, is replaced by the symbol in the position number below it (in the second row). Using these techniques as a basis, other more advanced cryptographic schemes can be created and are defined by the cipher (and key) that is used for the particular method.

Cryptography has been used in some form or another to exchange secret message throughout history. For example, the first use of of cryptography in a military setting was by the Spartans in 475 B.C. In the modern age, cryptography is most commonly used when sending or storing data using a computer system, such as sending an email across a network, or saving a file on a company server.

1.2 Motivation

Protecting important and secret information is big issue, particularly when data such as bank accounts details or private work related conversations are taking place or being exchanged. When new devices or computer systems are developed and deployed, the security of that system is always considered and studied. Smartphones, on the other hand, have a substantial amount of user-input in the form of publicly developed applications. With smartphones becoming the most popular tool for communicating and completing other tasks with the transfer of sensitive information combined with the fact that there are a vast number of tools for completing such tasks, the study of the strength and current state of security of smartphones is an ever evolving field. This creates a number of questions, the answers to which form the basis of this project:

- Do applications that facilitate the secure transfer of messages exist?
- What are the cryptographic techniques behind these applications?
- Are there other techniques which could also be used for this purpose?
- What is the performance of these styles applications?
- Can these applications or methods be improved upon?
- Can a conclusion be made about the current state of secure message communication and its future?

The results of this project will contribute an original conclusion to the field of cryptography within smartphones. Preliminary research showed that the questions set out to be answered in this project have not been answered before for the current, present-day state of smartphones. This is important because even in the last few years significant improvements and developments have been made concerning the design and processing power of smartphones which has had a tremendous affect on smartphone usability, for example the more advanced and widely available use of GPS in direction planning.

1.3 Scope and Limitations

It is important to set out in the introduction to this project report what the scope of the project is and to describe any limitations that have been placed on the project.

Firstly, as will be detailed later in this report, the choice was made that any developed software will be in the Java programming language and that the Android operating system will be the focus of study and application development. This is so that the project can be accomplished within the given time frame, to the standard required and with the hardware that is more easily available. It also ensures that the project does to try to encompass an area that is so huge that any conclusion loses focus and therefore its value.

This project also focuses on the use of cryptography in sending secure messages between users as opposed to other issues regarding smartphone security. A few examples of other forms of security related to smartphones could be a study of stored data protection, techniques to retrieve data from a smartphone wirelessly and protecting a smartphone from attacks or viruses. The reasons that this project is focused on one particular aspect of security with smartphones is much that same as the reasons given for the previous point. Furthermore, narrowing the scope of the project in this way means that a full solution and conclusion can be found for this particular aspect, as opposed to giving brief or vague conclusions for a number of aspects. Cryptography, particularly in this setting, also allows for a project that encompasses both computer science and mathematics and therefore is appropriate for a Discrete Mathematics student.

Lastly, this goal of this project is not to design and develop a product (application) that meets industry and user requires and can be sold or released to the general public. A project of that type would focus more on human-computer interactions, product design and marketing, as opposed to focusing on the mathematically based computer science areas of smartphones and cryptography. Therefore, the project can be categorised as a combination of both a research based and software development based project, each emphasising and reinforcing the other.

1.4 Issues

Every project is faced with issues regarding the projects final goals and outcomes, or the techniques or methods used to reach these outcomes. This section will discuss the issues faced or considered with this project.

1.4.1 Legal

Legal issues are the main issues that need to be considered with this project. As a large section of this project is research based, 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, legal issues need to be discussed [7] [8]. 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 processes, then any legal issues will be avoided in this case. Also, the resulting product facilitates the secure communication of messages which, in the wrong hands, could be used to aid a number of illegal operations. To avoid the direct use of the final application for illegal purposes, it will not be published to the Google Play application marketplace and will therefore not be available to the public. This also means that a disclaimer or end-user license agreement (EULA) will not be required, which would included the consultation of a professional lawyer. If the software created in this project was obtained by a malicious user, then any data required by the police could and would be given to break the illegal encryption by the author.

1.4.2 Ethical

In almost all modern technical advances, ethical issues can be found, posing unique problems depending on the perception or views of the topic by various groups or persons. For this topic, the legal issues presented above can also be viewed as ethical issues. Should an application be developed, or a field be advanced, that could be used to facilitate illegal operations? This question, and many like it, could and are constantly discussed and argued by professionals and amateurs alike, from almost all academic backgrounds. Because of this, a universally agreed upon set of ethics will never be concretely reached. However, through the actions taken to escape any legal issues, the avoidance of any major ethical issues are avoided.

As no interviews, questionnaires or experiments will be taken place in this project, other ethical issues regarding this do not need to be considered.

1.4.3 Social and Professional

With smartphones and text messaging services already being a central part of society, this project does not face any social issues.

1.5 Report Structure

The structure of the report from this point onwards will be as follows:

Objectives A discussion of the objectives and goals of the project.

Research Presentation and thorough explanation of all research completed.

Design Full system design, outlining and explaining choices made and tools used.

Development Implementation and software development aspect of the project presented, including the testing phase.

Results Analysis of the developed system accompanied with all conclusions and results found.

Further Work All further work completed for this project and a suggestion and discussion of any improvements that could be made.

Project Conclusion A conclusion of the project as a whole, including self-assessment.

Acknowledgements A list of acknowledgements relating to this project.

References All reference material used through the project.

Theorems, proofs, code snippets, diagrams and screen shots will be used throughout, as required, to improve understanding and to help explain various sections of this report.

Chapter 2

Objectives

In order to answer the questions described previously, certain goals and objectives must be met. The main objectives of this project where:

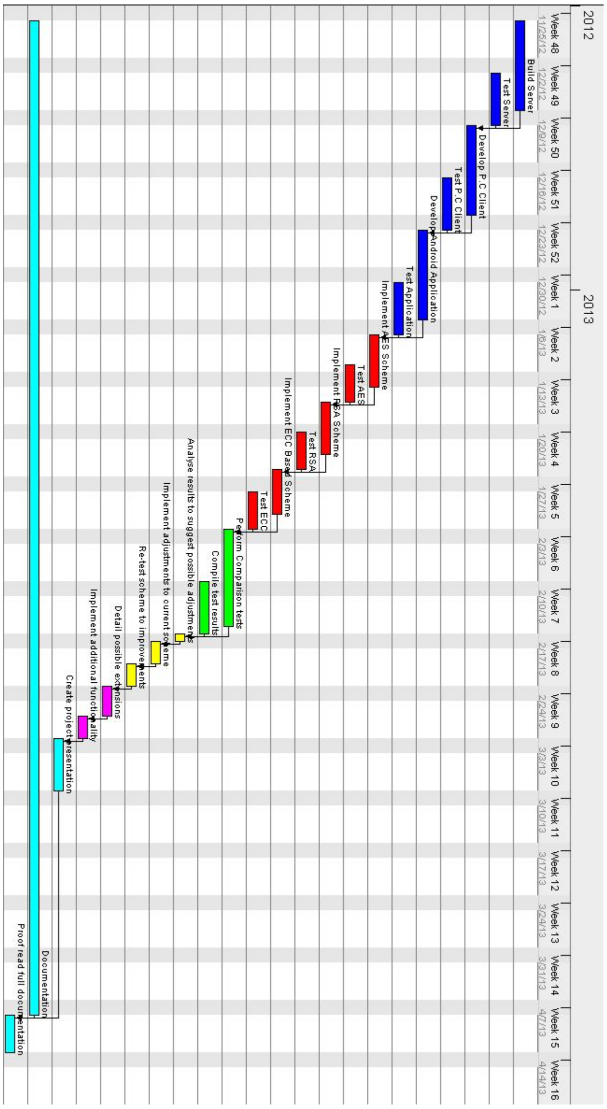
1. Research
    - Framework design
    - Cryptographic Techniques
    - Currently Available Applications
    - Relevant factors that can be used to compare schemes implemented on a mobile device
2. Development
    - Framework
        - Design Data Communication framework
            - Server
            - Mobile Application
            - P.C Client
    - Encrypted Data Communication
        - Design and implement cryptographic techniques
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

All aspects of software development are accompanied by thorough testing and are completed using a test driven development technique in a plan-driven setting, as de- scribed by Ian Sommerville [9]. A further breakdown of the objectives, together with a thorough project task timetable, can be found in the form of a Gantt chart in Appendix A.

Appendix A

Gantt Chart



Bibliography

[1] Allen, S [et al]. Pro Smartphone Cross-Platform Development: iPhone, Blackberry, Windows Mobile and Android Development and Distribution. Apress; 2010.

[2] Apple Inc . Apple iPhone iOS;. [Online](URL `http://www.apple.com/uk/ios/`).

[3] Microsoft Coporation. Windows Phone 8;. [Online](URL `http://www.windowsphone.com/en-gb`).

[4] Google Inc . Android;. [Online](URL `http://www.android.com/`).

[5] Google Inc . Google Play Store;. [Online](URL `https://play.google.com/store`).

[6] Mollin RA. An Introduction to Cryptography. 2nd ed. Chapman & Hall; 2007.

[7] Data Protection Act 1998. London: Stationery Office; 1998.

[8] Rowland, D [et al]. Information Technology Law. Taylor and Francis; 2011.

[9] Sommerville I. Software Engineering. Ninth ed. Pearson; 2011.