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.

References

Data Protection Act 1998. Chapter 29. Part IV. Section 36. (1998) London: Stationery Office.

Jeremy Kirk. 2007. *UK Data Encryption Disclosure Law Takes Effect*. Available at: http://www.pcworld.com/article/137881/article.html