Software Requirements Specification

for

Encryption Tool

Version 1.0 approved

Prepared by Mihir Sharma

**20th September 2016**

Table of Contents

Table of Contents ii

Revision History ii

1. Introduction 1

1.1 Purpose 1

1.2 Document Conventions 1

1.3 Intended Audience and Reading Suggestions 1

1.4 Product Scope 1

1.5 Use Case Diagram 2

1.6 References 2

2. Overall Description 3

2.1 Product Perspective 3

2.2 Product Functions 3

2.3 User Classes and Characteristics 3

2.4 Operating Environment 4

2.5 User Documentation 4

3. External Interface Requirements 5

3.1 User Interfaces 5

3.2 Hardware Requirements 5

3.3 Software Requirements 5

4. System Features 6

4.1 Learning Tool 6

4.2 Testing Tool 6

4.3 Encryption/DecryptionTool…………………..……………………………………6

5. Other Nonfunctional Requirements 7

5.1 Safety Requirements 7

5.2 Security Requirements 7

5.3 Software Quality Attributes 7

6. Other Requirements 8

1. **Introduction**
   1. **Purpose**

This system requirement specification document will aim at describing the overall specifications and functionality of our encryption tool. This document will provide a detailed list of the specifications of the encryption tool and the system and design requirements. It will outline the various layers of the software and its features. It will give details of the encryption used in the tool and the learning aspect the tool provides.

* 1. **Document Conventions**

This SRS document is written in the Arial font, with headings in font size 11 and descriptions in font size 12.

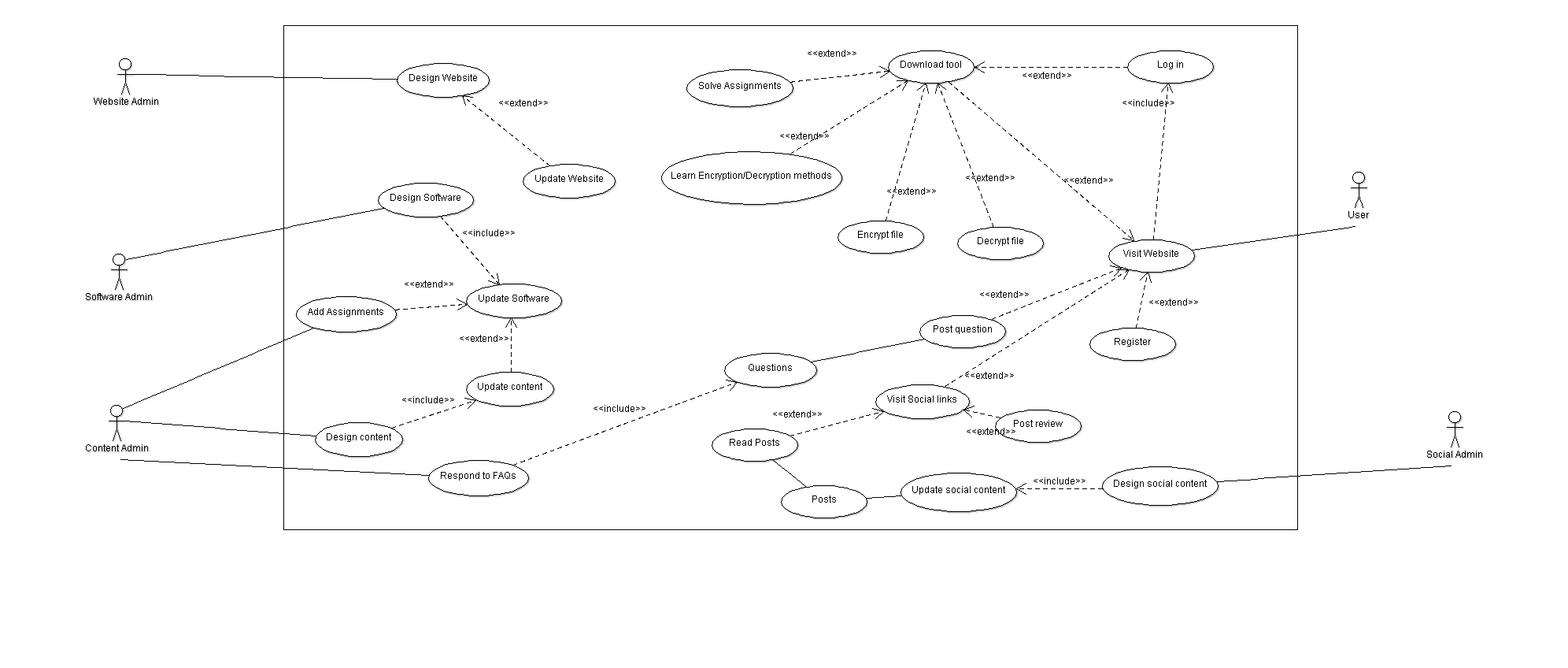
**1.3 Intended Audience and Reading Suggestions**

This project has been designed and implemented by undergraduate engineering students under the guidance of faculty in the software engineering branch. This project is intended for general public and business organizations and facilitates all who wish to use the encryption tool or learn the basics of cryptography in the cyber world.

**1.4 Product Scope**

The software is intended for people of varying backgrounds and with no prior knowledge of cryptography. This software helps people delve into the world of cryptography and learn its working at the same time providing them with a software that puts to use the very concepts they learn. The software employs the RSA encryption algorithm to provide secure transmission of data over public channels. It also teaches people about RSA and many other encryption methodologies. Companies can use the software to encrypt and send sensitive information, whereas the general public can use it to learn about the world of cryptography.

**1.5 Use Case Diagram**

****

**1.6 References**

1. **Overall Description**
   1. **Product Perspective**

This SRS document contains the details of the product perspective. It provides the detailed functions of our software along with constraints, assumptions and dependencies.

**2.2 Product Functions**

This software serves the following functions:

* Teaching the user the basics of cryptography and various encryption techniques.
* Allowing users to take assignments and quizzes to assess their current proficiency w.r.t. what they have learnt.
* Users can encrypt and decrypt textual data and files received from any source using the software.

**2.3 User Classes and Characteristics**

The users will be able to view information based on their individual requirements and learn about the various cryptographic techniques at their desired pace and convenience. They will also be able to encrypt and decrypt files simply by dragging and dropping the file into the software.

The user should be familiar with the Windows UI and basic use of a search engine (Google, Bing, etc.). The user can view any and all information pertaining to any topic related to cryptography by searching for the keyword in the provided search bar.

**2.4 Operating Environment**

For the system to run properly the buyer must ensure that on the machines there is the **Java Runtime Environment installed**, preferably the latest version so that all updates are included. ***Version 7 Update 25*** may be downloaded from this website: <http://java.com/en/download/index.jsp>.

The advantage of using java and its runtime environment is that it enables the system to run on any platform, whether it is Windows, Mac OS, Linux or Solaris. Makes it more portable and platform independent.

The user should also have a web-browser that can run the latest version of HTML and JavaScript (preferably Google Chrome or Firefox).

**2.5 User Documentation**

All user documentation including user manual will be available online on the website. Any queries can be posted on the forum available on the website and will be addressed by the developers.

1. **External Interface Requirements**

**3.1 User Interface**

The UI will be designed using front end languages which will require a web-browser to interpret.

Client-side technologies used are:

* HTML5
* JavaScript
* JQuery
* CSS

Server-side technologies include:

* Java
* PHP
* Python

**3.2 Hardware Requirements**

**Microsoft Windows XP Professional SP3/Vista SP1/Windows 7 Professional:**

o Processor: 800MHz Intel Pentium III or equivalent

o Memory: 512 MB

o Disk space: 1GB of free disk space

**Ubuntu 9.10:**

o Processor: 800MHz Intel Pentium III or equivalent

o Memory: 512 MB

o Disk space: 1GBof free disk space

**3.3 Software Requirements**

* Java Runtime Environment
* Web Browser supporting HTML5, CSS, JavaScript

1. **System Features**
   1. **Learning tool**

The software gives textual information to teach the user the basics or cryptography and various methods of encryption and decryption. This allows the user to tailor-make the course, to suit their learning speed and convenience.

* 1. **Testing tool**

The software allows users to check how much they have learnt by taking online tests and solving assignments to facilitate their understanding of the subject. These assignments are entirely voluntary and can be taken by the user at any point during the course. They offer varied difficulty and suggest areas for improvement.

* 1. **Encryption/Decryption tool**

The software allows users to encrypt files and send them to a recipient. The recipient can decrypt the file using the same software. The software uses RSA methodology to encrypt and decrypt the data securely.

1. **Other Non-Functional Requirements**
   1. **Safety Requirements**

The tool does not cause any damage to your system or data. We still recommend using an Anti-Virus software to make your download safer.

* 1. **Security Requirements**

The user may to permit the developers to collect anonymous usage data and other stats. The user must also register on the website to download the tool and log-in to use the website and tool.

* 1. **Software Quality Attributes**

The Admins and developers will be available to answer the queries of the user and in answering the question the admins assure least possible delay.

The tool and website will be updated if any error is discovered or the user finds it difficult to use.

The users can report any problems on the website and all anonymous usage stats will also be used to find any hidden errors.

1. **Other Requirements**

The software has no other requirements besides the ones mentioned above.