

软件需求规格说明

李嘉博

目录

1	引言	2
1.1	目的	2
1.2	范围	2
1.3	定义、简写和缩略语	2
1.4	引用文件	2
1.5	综述	2
2	总体描述	2
2.1	产品描述	2
2.1.1	系统接口	2
2.1.2	用户界面	2
2.1.3	硬件接口	2
2.1.4	软件接口	2
2.1.5	通信接口	2
2.1.6	内存	2
2.1.7	运行	3
2.1.8	现场适应性需求	3
2.2	产品功能	3
2.3	用户特点	3
2.4	约束	3
2.5	假设和依赖关系	3
2.6	需求分配	3
3	具体需求	3
3.1	外部接口需求	3
3.2	功能需求	3
3.2.1	加密算法演示功能	3
3.2.2	设置功能	3
3.3	性能需求	3
3.4	设计约束	4
3.5	软件系统属性	4
3.5.1	可靠性	4
3.5.2	可用性	4
3.5.3	可维护性	4
3.5.4	可移植性	4

1 引言

1.1 目的

本文档旨在说明CryptoDemoZero项目的需求，为软件开发打下基础，指导软件开发的过程。本文档的预期读者为软件系统相关人员及系统用户。

1.2 范围

本软件的名称为CryptoDemoZero，是一个密码学算法演示程序，旨在为密码学算法的教学、学习工作提供帮助。

1.3 定义、简写和缩略语

1.SRS：软件需求规格说明（Software Requirements Specification）的缩写。

2.本软件：指CryptoDemoZero软件。

1.4 引用文件

[1]GB/T 9385-2008, 计算机软件需求规格说明规范[S].

1.5 综述

接下来的第2部分对需求进行了总体描述，第3部分进行了详细描述。

2 总体描述

2.1 产品描述

2.1.1 系统接口

本系统没有外部接口。

2.1.2 用户界面

用户界面采用自上而下、“瀑布”组织形式，其中主界面采用二级列表的形式。

2.1.3 硬件接口

本系统没有硬件接口。

2.1.4 软件接口

本系统没有软件接口。

2.1.5 通信接口

本系统没有通信接口。

2.1.6 内存

本系统没有特定的主存、辅存约束。

2.1.7 运行

用户通过触摸的方式与本软件进行交互。

2.1.8 现场适应性需求

本系统需要在移动操作系统中运行。

2.2 产品功能

产品具有演示简单替换加密算法、对称加密算法、公钥加密算法的功能，以及替换壁纸的功能。

2.3 用户特点

本软件假设用户对密码学算法已经有了初步的了解。

2.4 约束

本软件没有特别的约束。

2.5 假设和依赖关系

本软件没有特别的假设和依赖关系。

2.6 需求分配

本软件的公钥加密算法中的验签功能需要在未来版本中实现。

3 具体需求

3.1 外部接口需求

本软件没有外部接口需求。

3.2 功能需求

3.2.1 加密算法演示功能

- 1.简单替换密码
- 2.对称密码
- 3.公钥密码

3.2.2 设置功能

能够满足用户基本的设置，如更换壁纸等。

3.3 性能需求

本软件应在1s内处理完毕用户的操作请求。

3.4 设计约束

本软件需要符合界面较为美观的要求。

3.5 软件系统属性

3.5.1 可靠性

本软件需要正确地求出加密算法的结果。

3.5.2 可用性

本软件需要保存用户的设置。

3.5.3 可维护性

本软件需要在将来能较为简单地维护。

3.5.4 可移植性

由于是HTML5应用，本软件需要满足很好的可移植性。