

软件概要设计说明书

（ 14 / 15 学年 第 二 学期）

|  |  |
| --- | --- |
| **项目名称** | 信息RSA加密与解密 |
| **制作小组** | 2101 |
| **小组成员** | 戴为 杨静 许寒玲 李皞 杨徐峰 马箐宇 |
|  |  |
| **指导单位** | 计算机学院软件工程系 |
| **指导教师** | 陈云芳 |

[1引言 2](#_Toc521464958)

[1.1编写目的 2](#_Toc521464959)

[1.2背景 2](#_Toc521464960)

[1.3定义 2](#_Toc521464961)

[1.4参考资料 2](#_Toc521464962)

[2总体设计 2](#_Toc521464963)

[2.1需求规定 2](#_Toc521464964)

[2.2运行环境 2](#_Toc521464965)

[2.3基本设计概念和处理流程 3](#_Toc521464966)

[2.4结构 3](#_Toc521464967)

[2.5功能器求与程序的关系 3](#_Toc521464968)

[2.6人工处理过程 3](#_Toc521464969)

[2.7尚未问决的问题 3](#_Toc521464970)

[3接口设计 3](#_Toc521464971)

[3.1用户接口 3](#_Toc521464972)

[3.2外部接口 3](#_Toc521464973)

[3.3内部接口 4](#_Toc521464974)

[4运行设计 4](#_Toc521464975)

[4.1运行模块组合 4](#_Toc521464976)

[4.2运行控制 4](#_Toc521464977)

[4.3运行时间 4](#_Toc521464978)

[5系统数据结构设计 4](#_Toc521464979)

[5.1逻辑结构设计要点 4](#_Toc521464980)

[5.2物理结构设计要点 4](#_Toc521464981)

[5.3数据结构与程序的关系 4](#_Toc521464982)

[6系统出错处理设计 5](#_Toc521464983)

[6.1出错信息 5](#_Toc521464984)

[6.2补救措施 5](#_Toc521464985)

[6.3系统维护设计 5](#_Toc521464986)

**概要设计说明书**

# 1引言

## 1.1编写目的

为了加强网络通信安全，防止网络数据被第三方劫持。

## 1.2背景

1. 网络安全防护；
2. 提出者：2101所有组员；

开发者：2101组员；

用户：面向广大的上网用户；

计算机站：DO数据中心；

## 1.3定义

客户机：客户端浏览器插件；

服务器：处理用户客户端数据加密，解密的服务器；

VPS：虚拟网络计算机（云服务器）

Chrome内核：谷歌开源的浏览器内核

## 1.4参考资料

《代码大全》：出版社---电子工业 ISBN：978712120

《深入理解计算机系统》：出版社：机械工业出版社 ISBN：9787111321330

# 2总体设计

## 2.1需求规定

|  |  |  |  |
| --- | --- | --- | --- |
| 输入 | 输出 | 处理 | 返回 |
| 用户输入字符（请求） | 加密的级别 | 服务器处理用户请求 | 返回加密的文件数据包 |

## 2.2运行环境

本软件主要是建立在基于谷歌最新的chrome内核（canary版），因为调用其中某个借口的原因，所以在低于此版本的情况下会出现功能的异常，处理用户请求数据出错，从而引起网站不能被正常打开，或者排版出错！

## 2.3基本设计概念和处理流程

## 2.4结构

## 2.5功能器求与程序的关系

本条用一张如下的矩阵图说明各项功能需求的实现同各块程序的分配关系：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 用户处理模块 | 加密发送模块 | 异常处理模块 | 解密数据模块 |
| 处理用户请求 | √ |  |  |  |
| 加密 |  | √ |  |  |
| 解密 |  |  |  | √ |
| 错误处理 |  |  | √ |  |
| 发送 |  | √ | √ |  |

## 2.6人工处理过程

人工处理仅仅对于服务器的修复，以及软件的更新，在出现错误的时候软件自动重启，并且提示用户重启浏览器，清除浏览器的换缓存！

## 2.7尚未问决的问题

尚未解决在基于https加密的网站上再次加密会出现部分网站排版异常，以及网站打开速度过慢问题。

# 3接口设计

## 3.1用户接口

用户发出网络请求的时候会对用户数据做出判断，以及对404,502等错误页面进行劫持，保证用户请求的合法性！

## 3.2外部接口

本软件需要chrome的最新内核，在本地建立浏览器代理，以及有广告拦截的功能，所占用的本地计算机数据端口为8081，服务器的端口为1007

## 3.3内部接口

本软件与服务器建立联系和数据请求的端口为1007，所以保持外网1007端口以及内网1080端口的通畅

# 4运行设计

## 4.1运行模块组合

用户浏览时将会触发软件的用户请求模块

用户请求模块再触发加密模块

加密后发送给服务器

服务器发送数据，根据数据包head，触发接收解密文件

## 4.2运行控制

用户浏览时将会让数据自动经过软件加密

加密后发送给服务器

服务器发送数据，根据数据包head，接收解密文件

最后将数据呈现给用户

## 4.3运行时间

数据加密将会占用0.1ms的时间

数据发送，服务器处理会占用2-3ms时间，具体与网速有关

客户端解密会占用1ms时间，具体与数据包大小有关

# 5系统数据结构设计

## 5.1逻辑结构设计要点

## 5.2物理结构设计要点

占用计算机的物理内存，会导致浏览器的内存占用变大！

## 5.3数据结构与程序的关系

说明各个数据结构与访问这些数据结构的形式:

用户发出请求与加密模块相关联

用户接收与解密相关联

# 6系统出错处理设计

## 6.1出错信息

|  |  |
| --- | --- |
| 404 | 源网站404错误 |
| 503 | 源网站503错误 |
| Error get | 服务器反向代理错误 |
| Error send | 服务器发送错误 |

。

## 6.2补救措施

服务器发生宕机会自动重启服务器

软件崩溃会提示用户重启浏览器

## 6.3系统维护设计

软件发生异常，会提示用户做出相应的处理，及时解决问题，并且会发送错误数据到网站工程师，及时处理！