## 1.需求分析

目标：设计一个基于加密搜索的可靠在线文件管理系统

### 1.1功能需求

1.客户端对于指定的文件可以进行用对称加密的技术进行加密和解密，通过给定的安全系数可以生成指定秘钥，加密解密的秘钥由客户端进行管理。

2.客户端与服务端之间可以采用UDP方式进行可靠文件传输，文件在传输过程中是经过加密处理。

3.服务端存储上传的加密文件，对于用户的数据具有简单的版本控制功能，用户可以对其文件进行搜索并且搜索过程是经过加密的。

### 1.2性能需求

1.加密与解密的速度在本地能达到100Mb/s（机械硬盘7200转情况下）。

2.传输速度在100M宽带下达到20Mb/s。

3.对文件的版本控制长达一年。

4.运行在windows PC端64位系统下

## 2.模块设计

### 2.1客户端模块架构设计

#### 2.1.1加密模块

1.给与指定安全系数生成秘钥。

2.给定的文件加密和解密。

3.对于指定的信息进行加密和解密。

4基于指定信息生成关键字

#### 2.1.2传输模块

1.工具模块 对文件的完整性进行检查，对文件缺少的部分信息进行统计，对文件发送时装配文件头部信息。

2.通讯部分