扩散加密机需求说明书

## 业务需求

实现最高级别和最快速度的加密、解密需要；

支持文件、文本的加密、解密需求；

并可以在多种终端实现加密及解密（非PC机上只支持文本）。

## 领域知识

* 1. 加密

使用某种方法，将明文在密匙的影响下改变为密文，使得在没有提供密匙的情况无法还原为明文。

* 1. 解密

使用某种方法，将密文在密匙的影响下还原为明文。

* 1. 明文

指没有经过加密的原始信息（包括数字、字符串等）。

* 1. 密文

指经过加密后的信息（包括数字、字符串等）。

* 1. 密匙

指用于加密或加密的密码。

* 1. 加密算法

用于进行加密的运算方法。

* 1. 解密算法

用于进行解密的运算方法，通常与加密算法互逆。

* 1. 对称加密技术

是指加密和解密都使用同样密码的一种加密方法。

* 1. 文件

是指存储在存储材质中的信息集合（包括文本文件、图像文件、视频文件等）。

* 1. 数据

在计算机中，数据是指由0、1组成的信息集合。

## 用户需求

### 3.1文件加密

用户选择要加密的文件或目录，并设置加密参数，然后执行加密。

用户可选择是否重命名加密后的文件，或加密文件名；

用户可选择直接对文件加密或者另建文件；

用户可选择加密完成后是否删除源文件。

### 3.2文件解密

用户选择要解密的文件或目录，并设置解密参数，然后执行解密。

用户可选择直接对文件加密或者另建文件；

用户可选择加密完成后是否删除源文件。

### 3.3文本加密

用户输入要加密的文本，并设置加密参数，然后执行加密。

用户可对输入和输出格式进行选择。

### 3.4文本解密

用户输入要解密的文本，并设置解密参数，然后执行解密。

用户可对输入和输出格式进行选择。

## 系统需求

## 质量约束

* 1. 高性能

加密速度要快。

* 1. 可恢复性

当加密文件的过程中被意外中断时，软件能够恢复到终端钱的过程，并能继续未完成的任务。

* 1. 可伸缩性

软件能完成超大文件和超大量文件的加密/解密。

* 1. 完整性

软件必须保证数据能能被正确加密/解密，不能丢失或损坏数据。

* 1. 可移植性

软件能够在Windows、Linux或其他平台上工作。

* 1. 可修改性

软件是能够被易于修改和扩展的。