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. 对称分组流加密

在对称分组加密的基础上，对每一组明文都采用不同的密匙。

* 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。

1.11

## 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

本软件采用的加密算法为：扩散加密算法，加密形式包括：分组加密和分组流加密。

为满足速度要求，本软件将使用多核处理和GPU加速（由用户选择）。

* 1. 文件加密（版本：1.0，级别：高）

提供对文件的加密功能。

用户提供以下信息以执行加密功能：

文件或者目录：当用户选择目录时，需提供是否递归提取子目录的选项。如果是递归提取的，则所加密的文件为用户选择的所有文件加目录及其子目录，否则提取的文件只包含用户所选择目录下的文件，不包含子目录中的文件；

密码：参见6.2；

分组长度：参见6.3；

加密级别：参见6.4；

多核处理：可选的Boolean值，如果加密模式不支持该选项，则忽略；

GPU加速：可选的Boolean值（待定）；

当用户选定参数并执行加密后，需要在用户界面（GUI或CMD）显示加密进度（D1）：

GUI：显示目前需要处理的所有文件列表，每个文件项需要显示如下信息：

文件名称、所在目录、大小、进度、状态、已用时间。

CMD：显示当前文件的完整名称（目录+文件名）、进度、已用时间。

当处理出现错误时：

GUI\CMD：提示用户错误信息，并让用户选择是否继续执行，可选的操作包括：

忽略当前文件的错误，并继续执行；

忽略所有错误，并不在提示；

放弃所有任务。

将产生错误的文件进行标记。

当所有任务处理完成时，提示用户。

* 1. 文件解密（版本：1.0，优先级：高）

提供对文件的解密功能。

用户提供以下信息以执行解密功能。

文件或目录：当用户选择目录时，需提供是否递归提取子目录的选项。如果是递归提取的，则所加密的文件为用户选择的所有文件加目录及其子目录，否则提取的文件只包含用户所选择目录下的文件，不包含子目录中的文件；

密码：字符串或文件形式，如果是字符串，则需要将字符串转换为字节(byte)；

多核处理：可选的Boolean值，如果加密模式不支持该选项，则忽略；

GPU加速：可选的Boolean值（优先级：中）；

当用户选定参数并执行解密后，参见4.1（D1）的处理方式。

* 1. 文本加密（版本：1.0，优先级：高）

提供对任意文本的加密功能。

用户提供以下信息以执行文本加密：

明文：参见6.1；

密码：参见6.2；

分组长度：参见6.3；

加密级别：参见6.4；

用户设定参数，执行文本加密后，显示密文。

如果出现错误，则通知用户错误信息。

需要保存、清除用户的加密记录。

* 1. 文本解密（版本：1.0，优先级：高）

提供对任意文本的解密功能。

用户提供以下信息以执行文本解密：

密文：参见6.1；

密码：参见6.2；

用户设定参数，执行文本解密后，显示明文。

如果出现错误，则通知用户错误信息。

需要保存、清除用户的解密记录。

* 1. 追加或删除文件（版本：1.0，优先级：高）

在GUI环境中，用户在执行加密/解密的过程中，可以继续追加文件或者暂停/删除列表中的文件（包括正在处理或等待处理的文件）。删除文件之前，需用户确认！

* 1. 文件信息格式

定义写入文件中的加密信息格式。

1-6：固定DC3.14

7:信息头版本号

8:

## 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。

## 约束

* 1. 明文/密文

用于加密/解密的明文/密文，只能是字符串形式其格式由用户指定，其长度无限制（具体与软件环境有关）。

可以同时解密多组密文，每一组用换行符分开。

* 1. 密码

密码可以是字符串或文件，密码的长度无限制，但实际有效长度与分组长度有关，当密码过短时（文本少于30个字符，文件少于(log2(N/8)+1)\*(N/8)时，N=分组长度），须提示用户。

* 1. 分组长度

分组长度（单位bit）只能是数字，而且必须是2的N（N为正整数）次方，范围：512~524288。

* 1. 加密级别

只能是数字，目前提供两种加密级别：

1：分组加密；

2：分组流加密；