# S-DES 接口文档

## 1.encryptionwidget.cpp

1.1 函数名称：

void EncryptWidget::encrypt()

1.2 参数：

无参数

1.3 功能：

该函数用于在用户界面中执行加密操作，将用户输入的明文使用 S-DES 算法进行加密，并将加密后的密文显示在界面上。

1.4 输入：

m_plainTextEdit: 明文输入框，用户在该输入框中输入待加密的明文。

m_keyEdit: 密钥输入框，用户在该输入框中输入用于加密的密钥。

1.5 输出：

m_cipherLabel: 显示加密后的密文的标签，密文将在该标签中显示。

1.6 行为:

（1）获取用户在明文输入框（m_plainTextEdit）中输入的明文。

（2）获取用户在密钥输入框（m_keyEdit）中输入的密钥。

（3）进行输入验证：

检查明文和密钥是否为空，如果为空，则显示消息框提示用户输入。

检查密钥是否为 10 位的二进制数字,如果不是,显示消息框提示用户输入正确的密钥。

检查输入是否为 ASCII 编码字符串或二进制字符串，如果不是，显示相应的错误消息。

（4）根据输入的类型进行加密：

如果输入的是 8 位二进制数，直接使用 S-DES 算法进行加密。

如果输入的是 ASCII 编码字符串，将每个字符转换为 8 位二进制数，再进行加密。

（5）将加密后的结果显示在界面上：

如果加密后得到的是二进制字符串，直接显示在界面上。

如果加密后得到的是 ASCII 编码字符，将其转换为 QChar 对象，然后拼接到 encryptedText 字符串中。

设置界面上显示的密文，并设置允许用户通过鼠标选择文本。

1.7 异常处理:

如果用户输入不符合要求（如输入为空、密钥不是 10 位二进制、明文不是合法的 ASCII 编码或二进制字符串），将显示相应的错误消息框。

1.8 注意事项:

该函数假定在其他部分已经实现了 S-DES 算法的加密函数，且该函数在 m_sdes.encrypt()处被调用。

该函数使用了 Qt 框架中的一些类和函数，如 QString、QMessageBox、QChar 等，因此需要确保 Qt 库正确引入和配置。

函数的功能是对用户输入的明文和密钥进行加密，所以在使用之前，需要确保 m_plainTextEdit、m_keyEdit 和 m_cipherLabel 等相关界面元素已经正确初始化和连接到函数中。

开发者需要根据具体的需求和 S-DES 算法的实现细节来进一步完善和测试该函数。

## 2. decryptWidget.cpp

2.1 函数名称：

void DecryptWidget::decrypt()

2.2 参数：

无参数

2.3 功能：

该函数用于在用户界面中执行解密操作，将用户输入的密文使用 S-DES 算法进行解密，并将解密后的明文显示在界面上。

2.4 输入：

m_cipherTextEdit: 密文输入框，用户在该输入框中输入待解密的密文。

m_keyEdit: 密钥输入框，用户在该输入框中输入用于解密的密钥。

2.5 输出：

m_decryptedLabel: 显示解密后的明文的标签，明文将在该标签中显示。

2.6 行为：

（1）获取用户在密文输入框（m_cipherTextEdit）中输入的密文。

（2）获取用户在密钥输入框（m_keyEdit）中输入的密钥。

（3）进行输入验证：

检查密文和密钥是否为空，如果为空，则显示消息框提示用户输入。

检查密钥是否为 10 位的二进制数字,如果不是,显示消息框提示用户输入正确的密钥。

检查输入是否为 ASCII 编码字符串或二进制字符串，如果不是，显示相应的错误消息。

（4）根据输入的类型进行解密：

如果输入的是 8 位二进制数，直接使用 S-DES 算法进行解密。

如果输入的是 ASCII 编码字符串，将每个字符转换为 8 位二进制数，再进行解密。

（5）将解密后的结果显示在界面上：

如果解密后得到的是二进制字符串，直接显示在界面上。

如果解密后得到的是 ASCII 编码字符，将其转换为 QChar 对象，然后拼接到 decryptedText 字符串中。

设置界面上显示的明文，并设置允许用户通过鼠标选择文本。

2.7 异常处理：

如果用户输入不符合要求（如输入为空、密钥不是 10 位二进制、密文不是合法的 ASCII 编码或二进制字符串），将显示相应的错误消息框。

2.8 注意事项：

该函数假定在其他部分已经实现了 S-DES 算法的解密函数，且该函数在 m_sdes.decrypt()处被调用。

该函数使用了 Qt 框架中的一些类和函数，如 QString、QMessageBox、QChar 等，因此需要确保 Qt 库正确引入和配置。

函数的功能是对用户输入的密文和密钥进行解密，所以在使用之前，需要确保 m_cipherTextEdit、m_keyEdit 和 m_decryptedLabel 等相关界面元素已经正确初始化和连接到函数中。

开发者需要根据具体的需求和 S-DES 算法的实现细节来进一步完善和测试该函数。

## 3. decryptWidget.cpp

3.1 函数名称：

void Crackwidget::crack ()

3.2 参数：

无参数

3.3 功能：

该函数用于在用户界面中执行暴力破解攻击操作,尝试找到能够将明文加密为已知密文的密钥，并将破解的密钥以及破解的时间显示在界面上。

3.4 输入：

m_plainTextEdit：已知的明文字符串。

m_cipherTextEdit：已知的密文字符串。

3.5 输出：

m_timeLabel：显示破解后的密文的标签，密文将在该标签中显示

m_keyEdit：显示破解后的符合条件的所有密钥

3.6 行为：

（1）获取用户在明文输入框（m_plainTextEdit）中输入的密文。

（2）获取用户在密文输入框（m_cipherTextEdit）中输入的密钥。

（3）进行输入验证：

检查明文和密文是否为空，如果为空，则显示消息框提示用户输入。

检查明文和密文的大小是否一致，如果数量不一致，则显示消息框提示用户输入正确的明密文对。

检查输入是否为 ASCII 编码字符串或二进制字符串，如果不是，显示相应的错误消息。

（4）根据输入的类型进行解密：

如果输入的是 8 位二进制数，直接使用进行遍历破解。

如果输入的是 ASCII 编码字符串，将每个字符转换为 8 位二进制数，再进行破解。

（5）计算破解时间

通过 QElapsedTimer，记录从运行开始到结束的时间，并通过 nsecsElapsed 函数精确具体时间到微秒。

（6）将破解后的结果显示在界面上：

如果未找到对应的密钥，则显示消息框提示未能找到该明密文对的密钥

如果找到对应的密钥，则将找到的正确的密钥拼接在 allkey 字符串中，并统一输出到 m_keyEdit，另外将破解的时间显示在 m_ timeLabel 上。

3.7 异常处理：

如果用户输入不符合要求（如输入为空、明密文数量不一致、明密文不是合法的 ASCII 编码或二进制字符串），将显示相应的错误消息框。

1.8 注意事项:

该函数假定在其他部分已经实现了 S-DES 算法的加密函数，且该函数在 m_sdes.encrypt()处被调用。

该函数使用了 Qt 框架中的一些类和函数，如 QString、QMessageBox、QChar 等，因此需要确保 Qt 库正确引入和配置。

函数的功能是对用户输入的明文和密钥进行加密，所以在使用之前，需要确保 m_plainTextEdit、m_cipherTextEdit 、m_keyEdit 和 m_timeLabel 等相关界面元素已经正确初始化和连接到函数中。

开发者需要根据具体的需求和 S-DES 算法的实现细节来进一步完善和测试该函数。