

# EFArmor 标准版使用手册

Standard Version 1.5.0

# 目录

EFArmor 标准版使用手册.....	1
一： 软件介绍 .....	3
二： 快速指南 .....	4
三： EFArmor 支持的密码算法 .....	13
四： 常见问题 .....	14
五： 感谢 .....	14

## 一：软件介绍

EFArmor 是一款方便易用的文件加密软件。它使用了标准高强度加密算法和安全协议对保存在计算机中视频, 照片等文档等进行加密保护, 以防止他人随意阅读, 修改和使用它们。

EFArmor 使用 RSA 算法作为**安全密钥**。它就像一把钥匙, 您需要设置一个主密钥口令保护它。软件会使用密钥口令**加密该密钥**, 然后保存在您本地计算机中。出于安全考虑, EFArmor 不会将保存密钥口令, [您需要自己妥善的保管该口令。](#)

软件使用标准的密码算法 (比如: RSA, DES, 3DES, AES 等); 默认情况下面使用 AES (Advanced Encryption Standard: 高级加密标准) 算法; 同时使用类似 PGP 的安全协议实现文件加密保护。

目前版本 (Version 1.5.0) 提供如下的功能:

- 文件浏览模块: 一个直观的文件浏览界面, 帮助您快速的寻找文件/文件夹。
- 密钥管理模块: 管理用于加密/解密的安全密钥。
- 加密/解密控制面板: 进行加密/解密文件操作。
- 文件完整性检查: 计算网络下载/外部设备存储的文件的校验和, 以确保该文件未被篡改/损坏。

EFArmor 支持操作平台:

Windows: Windows Vista 或以上平台; 建议您使用 Windows 10 系统运行本软件。

Mac 平台: 支持最新版本 – macOS Catalina。

注意:

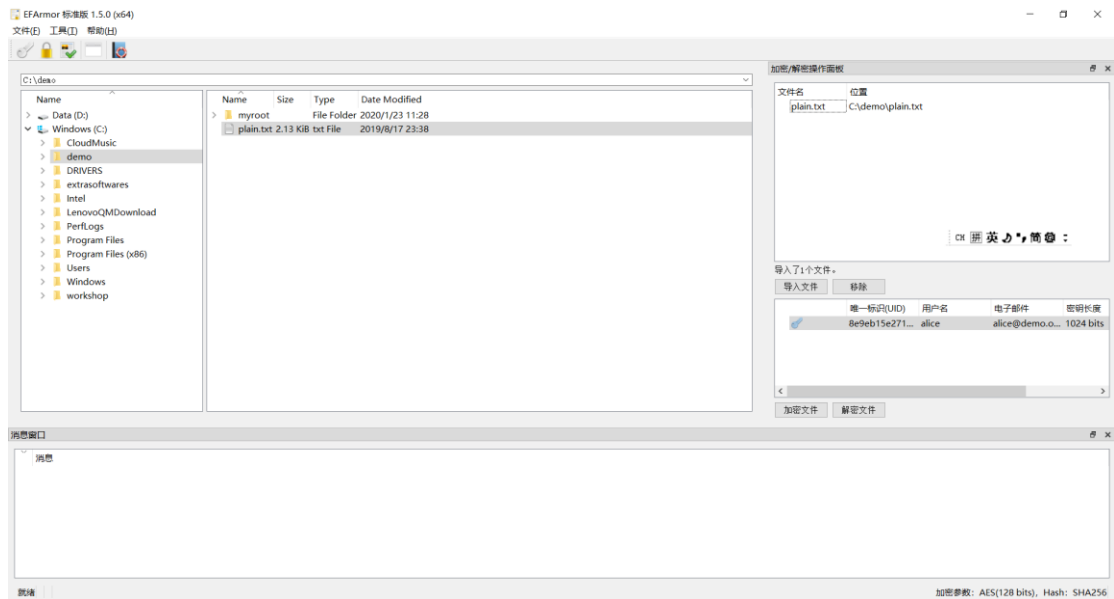
- EFArmor 有 32 位和 64 位两个版本; 它们的功能, 特性完全一致。
  - 32 位版本 – 该版本用于 32 位的 Windows 系统 (比如: 32 位版本的 Win7)。
  - 64 位版本 – 该版本用于 64 位的 Windows 系统和 Mac 计算机中。

## 二：快速指南

使用 EFArmor 加密保护您的文件是非常简单的，实际上只有三步：

- ✓ 设置自己的安全密钥 – 管理安全密钥
- ✓ 导入需要加密/解密的文件 – 导入文件
- ✓ 执行加密/解密操作 – 加密/解密文件

### EFArmor Ver1.5.0 in Windows



插入 Mac 平台下面的截图 - !!!

### 1. 管理安全密钥：

#### 1.1 创建安全密钥

- 1) 打开菜单项：工具→密钥环

**密钥管理**
?
×

用户名

电子邮件

主密钥口令

确认主密钥口令

密钥类型

密钥长度

8e9eb15e271...

alice

alice@demo.o...

1024 bits

你的<RSA>

新建密钥

删除密钥

关闭

## 2) 按照界面指示

- ✓ 填入：用户名，电子邮件，主密钥口令；选择密钥类型（RSA）和密钥长度。
- ✓ 点击按钮“新建密钥”。

例子：为 Bob 创建安全密钥。

**密钥管理**
?
×

用户名

电子邮件

主密钥口令

确认主密钥口令

密钥类型

密钥长度

8e9eb15e271...

alice

alice@demo.o...

1024 bits

你的<RSA>密...

新建密钥

删除密钥

关闭

密钥管理

?

×

用户名

电子邮件

主密钥口令

确认主密钥口令

密钥类型

RSA

▼

密钥长度

1024

▼

	唯一标识(UUID)	用户名	电子邮件	密钥长度	描述
	8e9eb15e271...	alice	alice@demo.o...	1024 bits	你的<RSA>密钥...
	4263cb50c3a1...	Bob	bob@bob-de...	1024 bits	你的<RSA>密钥...

新建密钥

删除密钥

关闭

注意：

- 安全密钥是根据：用户名和电子邮件来识别。
- 用户唯一标识符（UUID）是根据用户名和电子邮件生成的，它是唯一的。
- 您可以生成多把安全密钥；但是需要使用不同的用户名+电子邮件的组合。
- 关于密钥口令：

密钥口令是您自己输入的字符串。[切记：请您牢记这个密钥口令。](#)软件本身不会保存口令。一旦遗失了该口令，使用该口令和安全密钥加密的文件将会无法被解密。

## 1.2 删除密钥

打开菜单项：工具→密钥环

密钥管理

?

×

用户名

电子邮件

主密钥口令

确认主密钥口令

密钥类型

RSA

▼

密钥长度

1024

▼

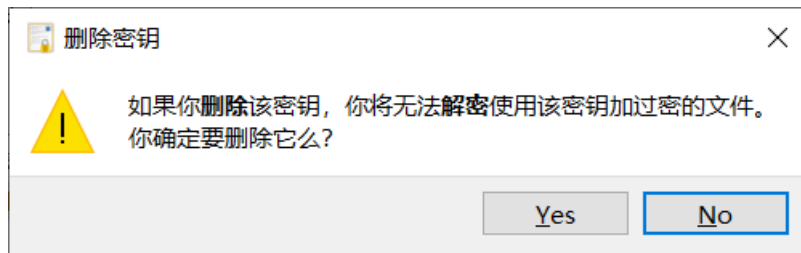
	唯一标识(UUID)	用户名	电子邮件	密钥长度	描述
	8e9eb15e271...	alice	alice@demo.o...	1024 bits	你的<RSA>密钥...
	4263cb50c3a1...	Bob	bob@bob-de...	1024 bits	你的<RSA>密钥...

新建密钥

删除密钥

关闭

- ✓ 选中待删除的密钥。
- ✓ 点击按钮“删除密钥”，在执行删除动作之前，密钥管理界面会弹出一个确认对话框，让您确认。当您选择了“确定”之后，那个选中的密钥会从密钥库中删除。

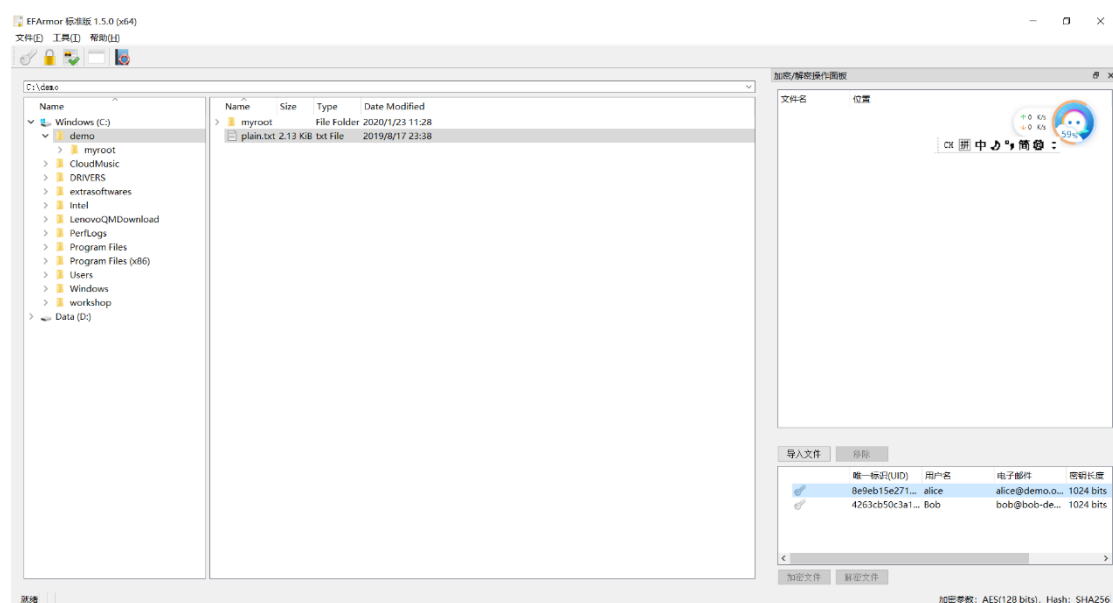


注意：

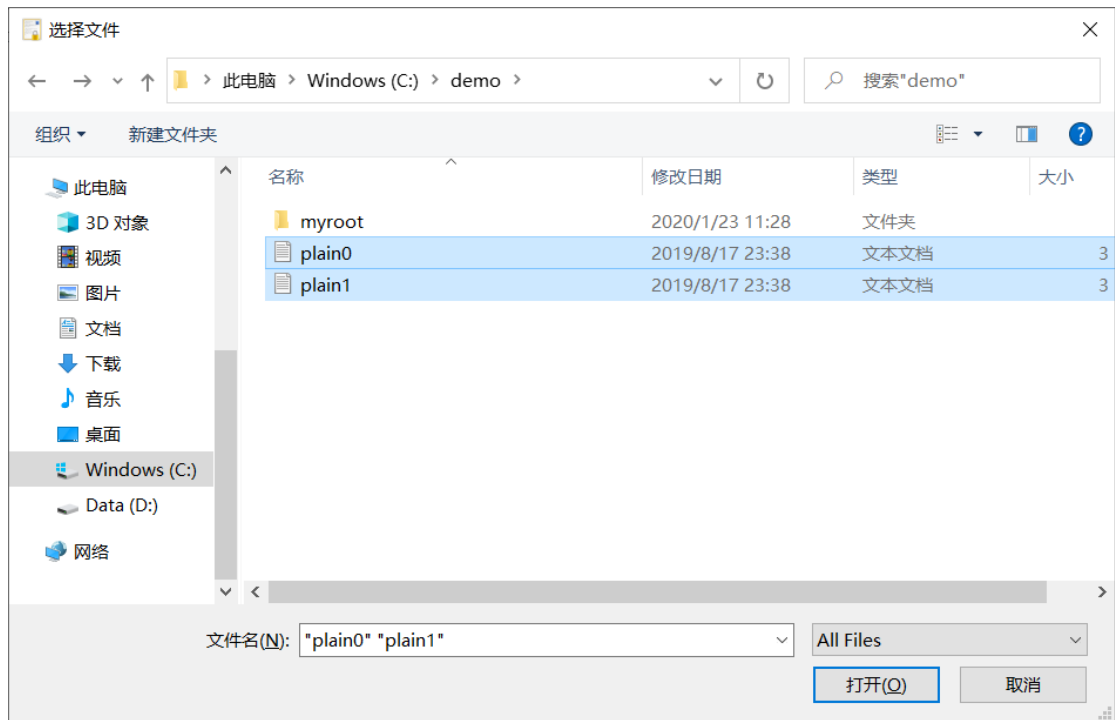
- a) 删除密钥的操作是不可逆转的：一旦密钥被删除，是无法恢复的。**执行删除密钥操作之前，请务必谨慎。**
- b) 密钥被删除（比如：删除了属于 Alice 的密钥 - [alice@demo.org](mailto:alice@demo.org)），那么使用该密钥加密的文件就无法在解密了。

## 2. 导入文件或文件夹

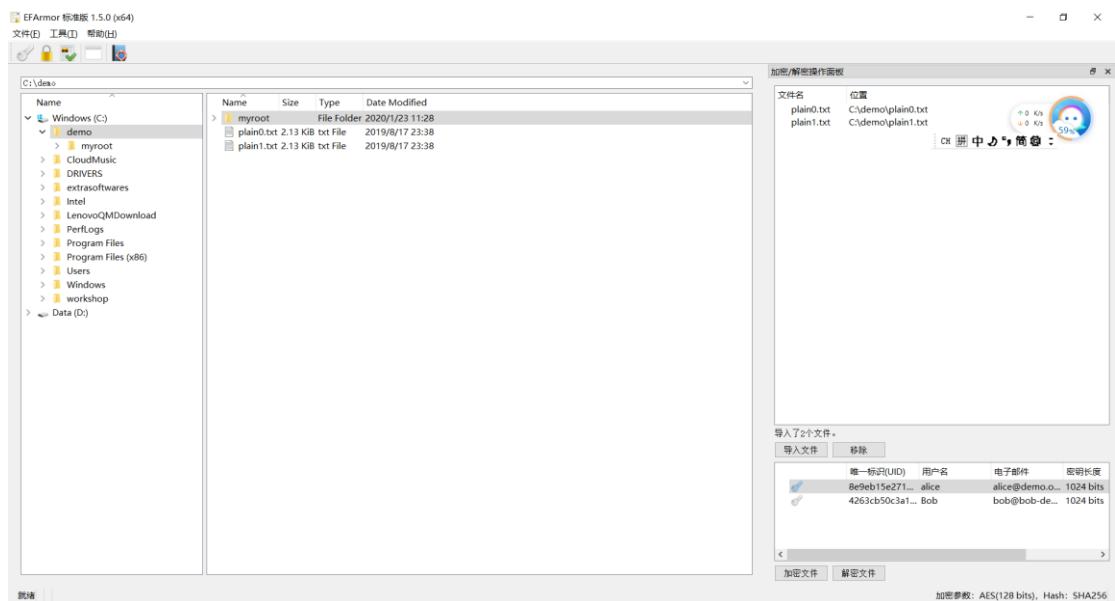
### 2.1 打开菜单项：工具→加密/解密操作面板



#### 2.1.1 点击“导入文件”按钮，选择文件导入



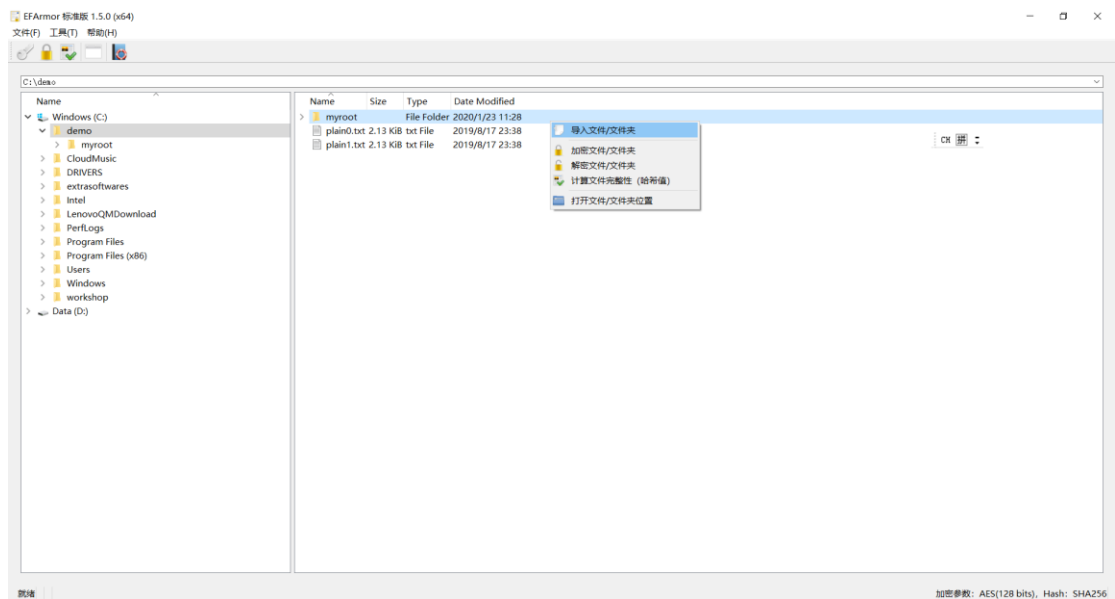
点击“打开”按钮后，会导入文件“plain0”和“plain1”：



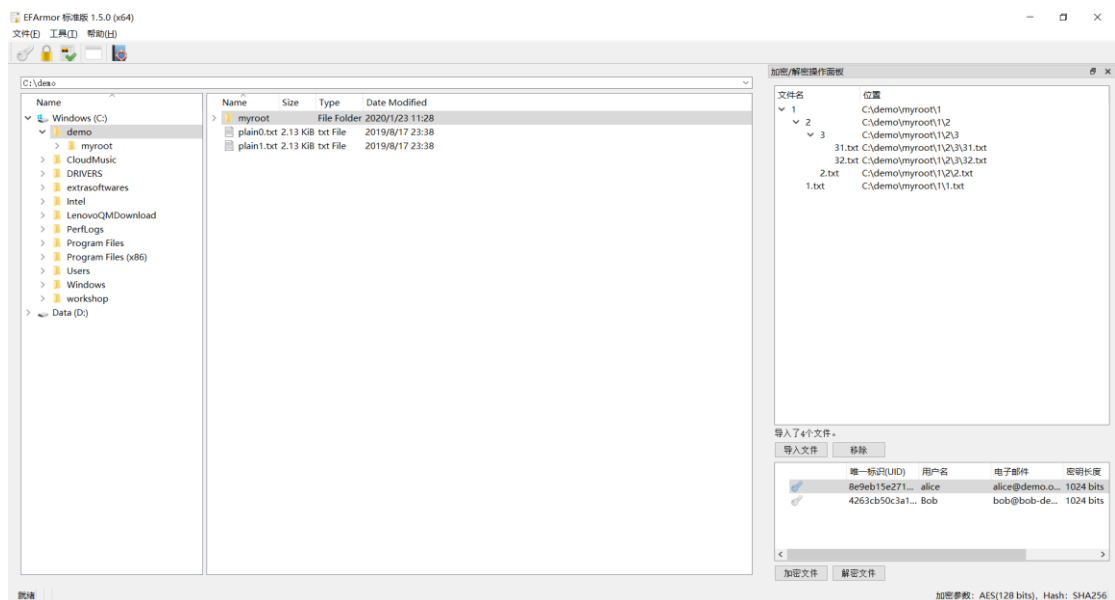
## 2.2 使用右键菜单--导入文件/文件夹

在文件选择区域，选中文件/文件夹，点击右键菜单—导入文件/文件夹。





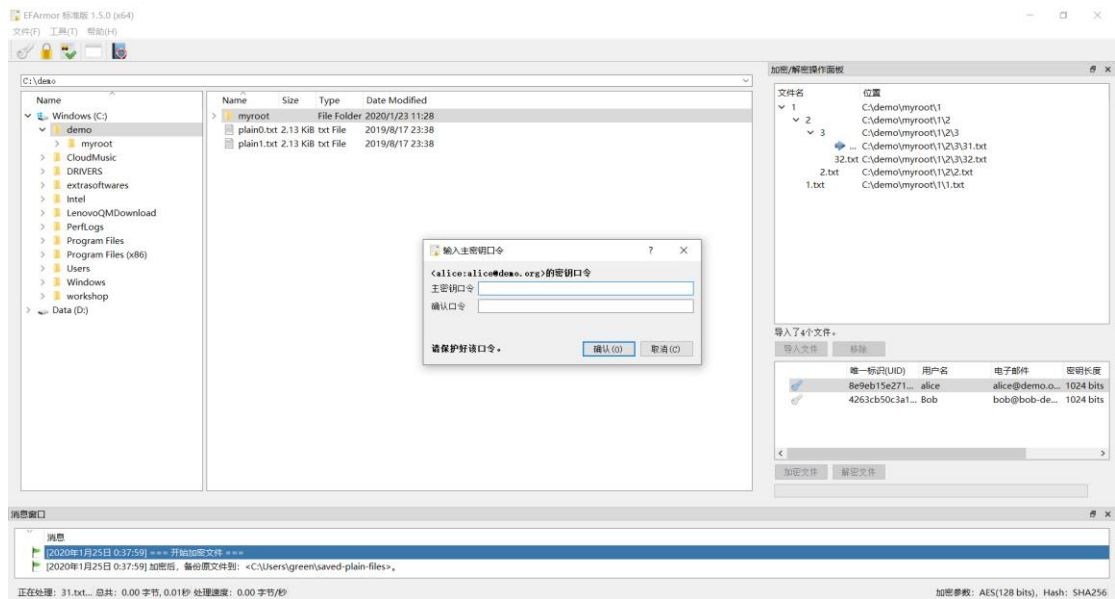
按照上述步骤完成导入操作后，导入的文件会排列在列表区域。如下图所示：



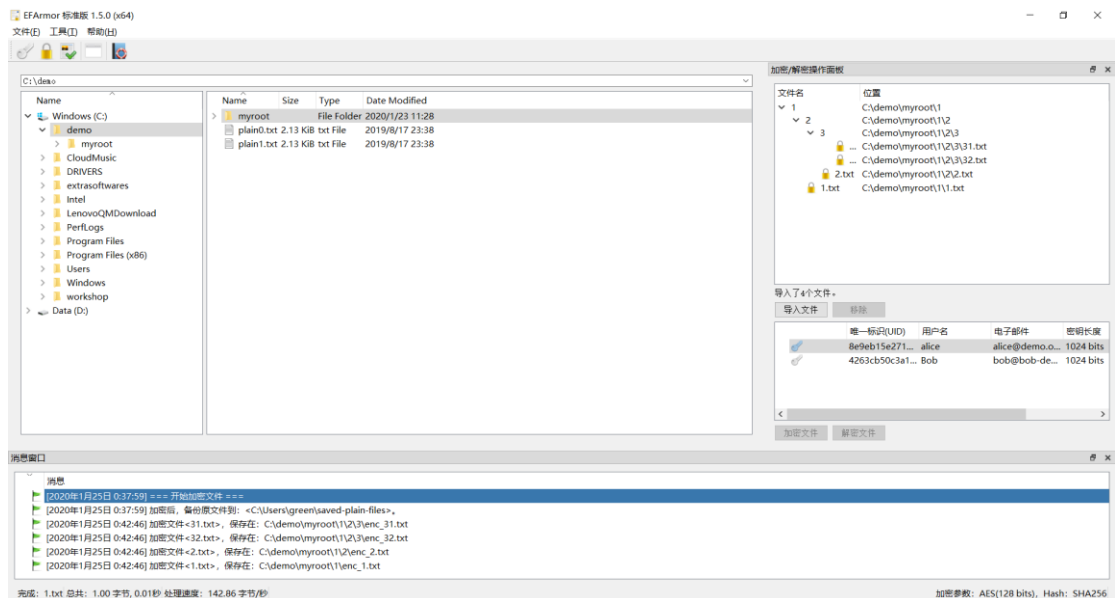
### 3. 加密和解密

完成导入文件操作后，然后点击“加密文件”或“解密文件”按钮：开始执行对应的操作。

软件会首先弹出一个对话框：输入“主密钥口令”；一旦输入了正确的密钥口令，软件就加密或解密先前导入的所有文件。



## 加密后

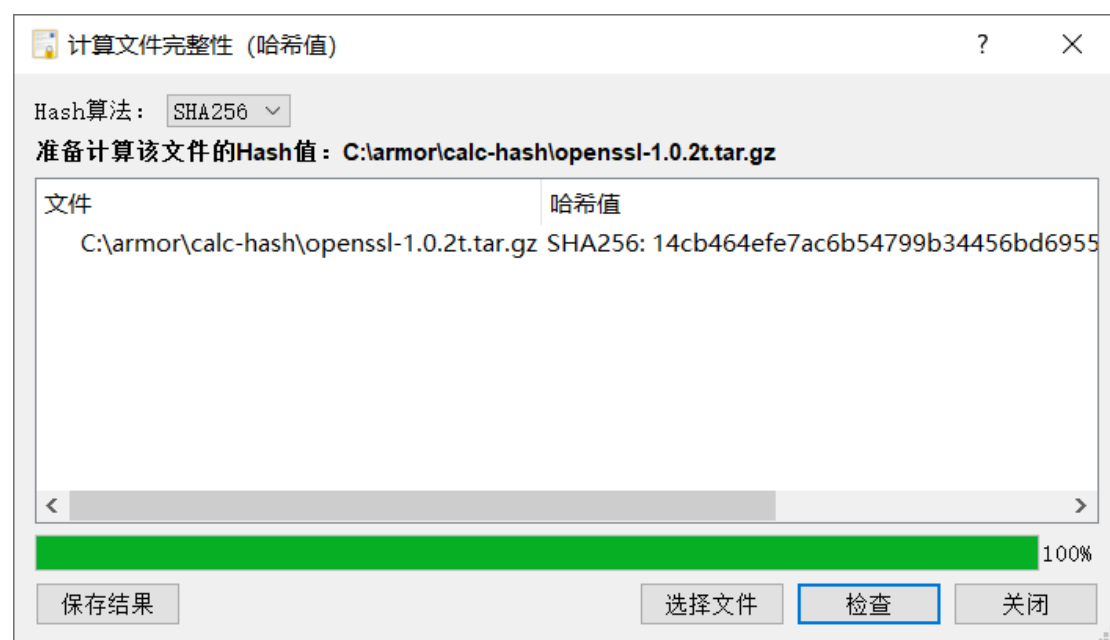


注意：

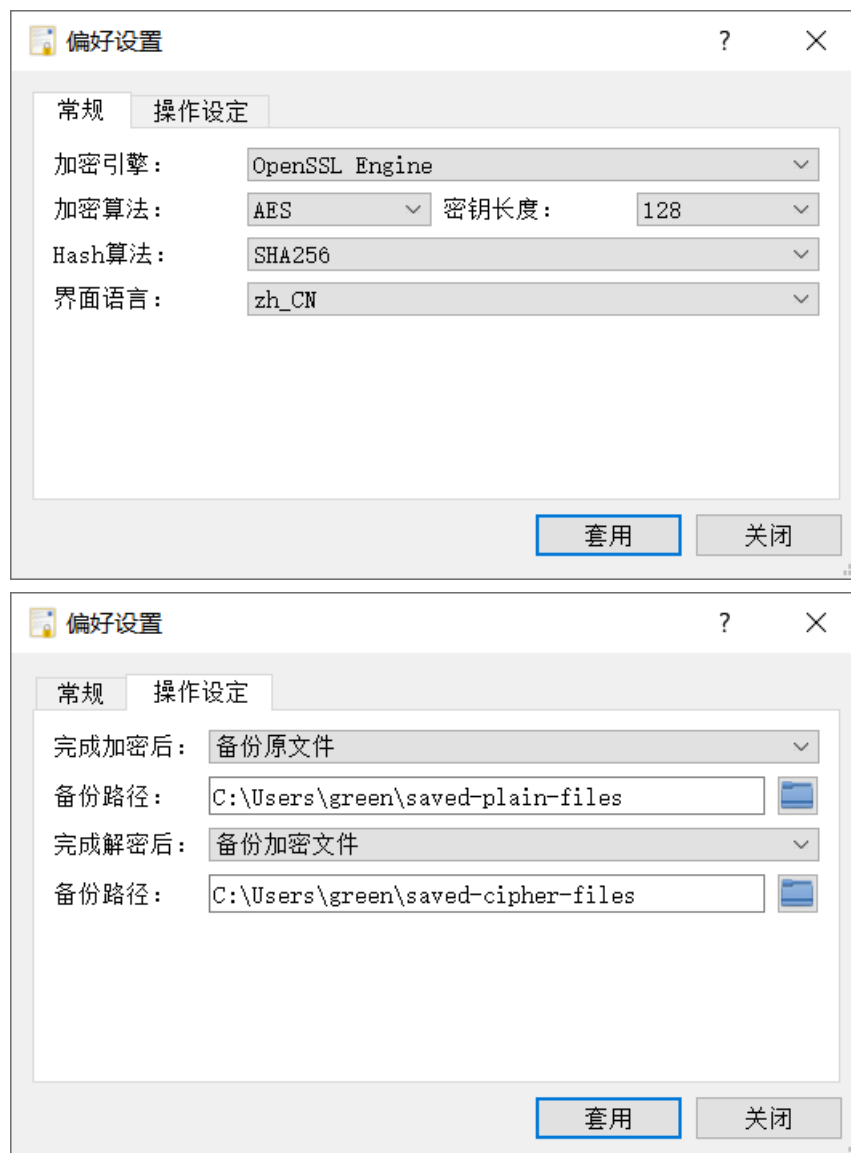
- 如果有多个安全密钥，那么您可以选择不同的密钥进行加密：  
在上面的加密示例，选择了“alice”的密钥进行加密。
- 解密文件的时候，您只需要输入对应的密钥口令；软件会自动的完成解密操作。

## 4. 计算文件完整性

- 在文件的选择区域，用鼠标选中文件或文件夹。
- 打开主界面的菜单，选择：工具→文件完整性
  - ✓ 选择 Hash 算法。
  - ✓ 点击“检查”按钮。



## 5. 偏好设置 (Preference)



您可以在偏好设置中对软件行为进行调整：

- A. “常规” - 调整加密参数
  - a) 调整加密算法和密钥长度。
  - b) 调整 Hash 检验算法。
- B. “操作设定” - 调整加密/解密后的操作
  - a) 加密后，对原文件的操作：
    - ✓ 不移动/删除原明文文件：完成加密后，原文件和密文保存在同样的位置。
    - ✓ 只保留加密后的文件：完成加密后，删除原文件。如果加密失败的话，不会删除原文件。
    - ✓ 备份原文件：完成加密后，软件会把原文件移动到您设定的磁盘位置。
  - b) 解密后，对密文的操作。
    - ✓ 不移动/删除加密文件：完成解密后，解密后的文件和密文保存在同样的位置。
    - ✓ 只保留解密文件：完成解密后，删除加密文件。但是解密失败的话，不会

删除加密文件。

✓ 备份加密文件: 完成解密后, 软件会把加密文件移动到您设定的磁盘位置。

C. 调整软件界面语言

a) en\_US: 英文

b) zh\_CN: 简体中文

c) zh\_TW: 繁体中文

注意: 修改界面的语言设定后, 您需要重新启动软件才能让这个设置生效。

### 三: EFArmor 支持的密码算法

EFArmor 1.5.0 使用 OpenSSL (<https://www.openssl.org/>) 作为加密引擎。

这样就让 EFArmor 具有统一的跨平台能力: 无论您使用 Windows 或 Mac, 您都可以运行 EFArmor 来加密保护您的计算机文档。

EFArmor v1.5.0 支持的密码算法表

算法名称	用途	备注
RSA	非对称算法, 用于安全密钥中。	安全密钥的默认长度是 1024 比特。您也可以选择 2048 比特。
RC2	对称加密算法, 可以用于数据文件的加密。	密钥长度: 40/64/128 比特。
RC4		密钥长度: 40/128 比特。
AES	高级加密标准	默认的数据加密算法, 默认密钥长度为 128 比特。您也可以选择 192 或 256 比特。
DES	数据加密标准	密钥长度: 56 比特。
DESX	DES 的一种变种算法, 旨在提高计算复杂度以对抗暴力破解。	密钥长度: 184 比特。
BLOWFISH	对称加密块算法。	密钥长度: 128 比特
CAST5	对称加密块算法。	密钥长度: 128 比特
IDEA	对称加密块算法。	密钥长度: 128 比特
3DES	三重 DES 算法, DES 一种	密钥长度: 168 比特。
RNG	随机数算法。	遵守的标准: FIPS 186-2, FIPS 140-2, NIST SP 800-90
MD2	MD2 信息摘要算法。 注意: 该算法仅用在计算文件校验和中。	数字摘要长度: 128 比特。
MD4	MD4 信息摘要算法。	
MD5	MD5 信息摘要算法。	
SHA1	Secure Hash Algorithm	数字摘要长度: 160 比特。
SHA2	Secure Hash Algorithm 2	数字摘要长度: 256/384/512 比特。

## 四：常见问题

1. 在 Windows 中，为什么我加密 U 盘中文件，有时候会无法成功？  
请把文件复制到您的计算机中的硬盘中，然后重新执行加密操作。
2. EFArmor 1.5.0 的版本可以运行在什么平台下面？  
EFArmor 1.5.0 可以运行在 32 位和 64 位 Windows 平台以及 Mac 中；它支持最新的 macOS 版本。
3. EFArmor 有什么特色？  
首先它使用类 PGP 协议以及高强度的加密算法来保护您的计算机文档；其次，它可以运行在 Windows 平台和 Mac 平台 – 所有的功能和操作方式都一样。  
最重要的是：它操作方便：仅仅需要设定一个口令和密钥就可有效的加密保护您的文件了。
4. EFArmor 未来会怎样发展？  
请访问 EFArmor 项目网站来了解项目未来的发展方向和产品路线：  
<https://github.com/EFArmorSupport/EFArmor>

## 五：感谢

本软件使用如下的第三方组件，非常感谢他们的辛勤劳动和贡献。

1. zlib 1.2.11: zlib 压缩库。
  2. Qt5.13.0: Qt 跨平台库。
  3. The oxygen-icons 和 KDE 开发组(<https://kde.org/>): 程序使用的图标库。
  4. OpenSSL 1.1.1d: 广泛使用的高强度密码库。
- 请参考安装目录中的 3RDLicenses 参看详细信息。