EFArmor 標準版使用手冊

Standard Version 1.5.0

目錄

一：軟體介紹

EFArmor 是一款方便易用的加密軟體。它使用了標準高強度加密演算法和安全協議對保存在電腦中視頻，照片等文檔等進行加密保護，以防止他人隨意閱讀，修改和使用它們。

EFArmor 使用 RSA 演算法作為**安全金鑰**。它就像一把鑰匙，您需要設置一個主金鑰口令保護它。軟體會使用金鑰口令**加密該安全金鑰，然後**保存在您本地電腦中。出於安全考慮，EFArmor 不會將保存金鑰口令，**您需要自己妥善的保管該口令。**

軟體使用標準的密碼演算法（比如：RSA, DES, 3DES, AES 等）；預設情況下面使用 AES（Advanced Encryption Standard：高級加密標準）；同時使用類似 PGP 的安全協議實現加密保護。

目前版本（Version 1.5.0）提供如下的功能：

- 檔案 Explorer：一個直觀 Explorer 介面，幫助您快速的尋找檔/資料夾。
- 金鑰管理模組：管理用於加密/解密的安全金鑰。
- 加密/解密控制面板：進行加密/解密檔操作。
- 文檔完整性檢查：計算網路下載/外部設備存儲的檔的校驗和，以確保該文檔未被篡改/損壞。

EFArmor 支援操作平臺：
Windows：Windows Vista 或以上平臺；建議您使用 Windows 10 系統運行本軟體。
Mac 平臺：支持最新版本 – macOS Catalina。
注意：

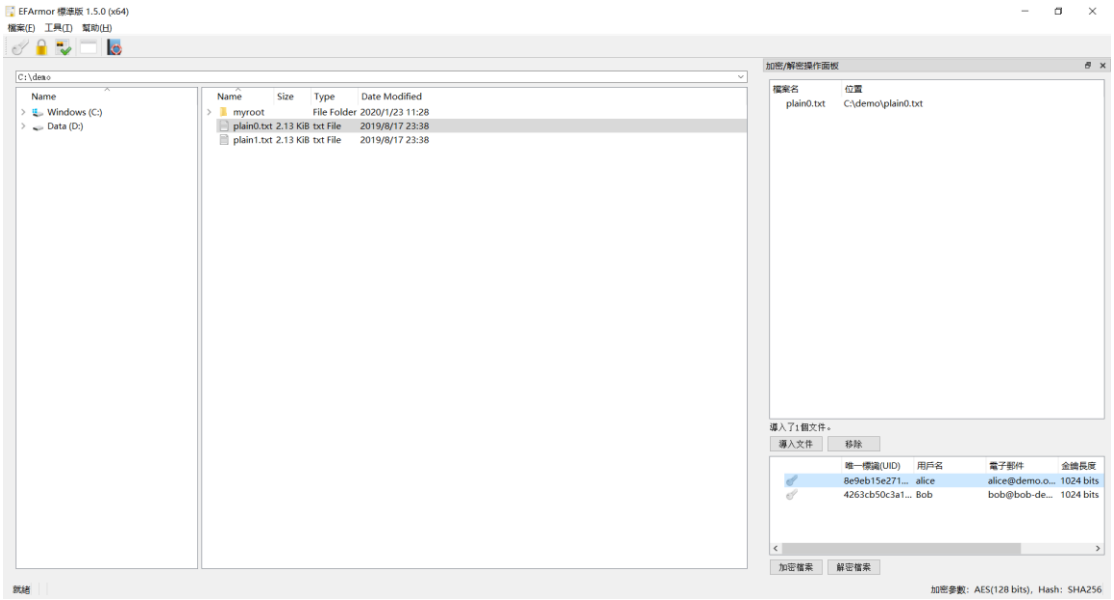
- EFArmor 有 32 位和 64 位兩個版本；它們的功能，特性完全一致。
  - 32 位版本 – 該版本用於 32 位元的 Windows 系統(比如：32 位版本的 Win7)。
  - 64 位版本 – 該版本用於 64 位元的 Windows 系統和 Mac 電腦中。

二：快速指南

使用 EFArmor 加密保護您的文檔是非常簡單的，實際上只有三步：

- ✓ 設置自己的安全金鑰 – 管理安全金鑰
- ✓ 導入需要加密/解密的文檔– 導入文檔
- ✓ 執行加密/解密操作 – 加密/解密文檔

EFArmor Ver1.5.0 in Windows

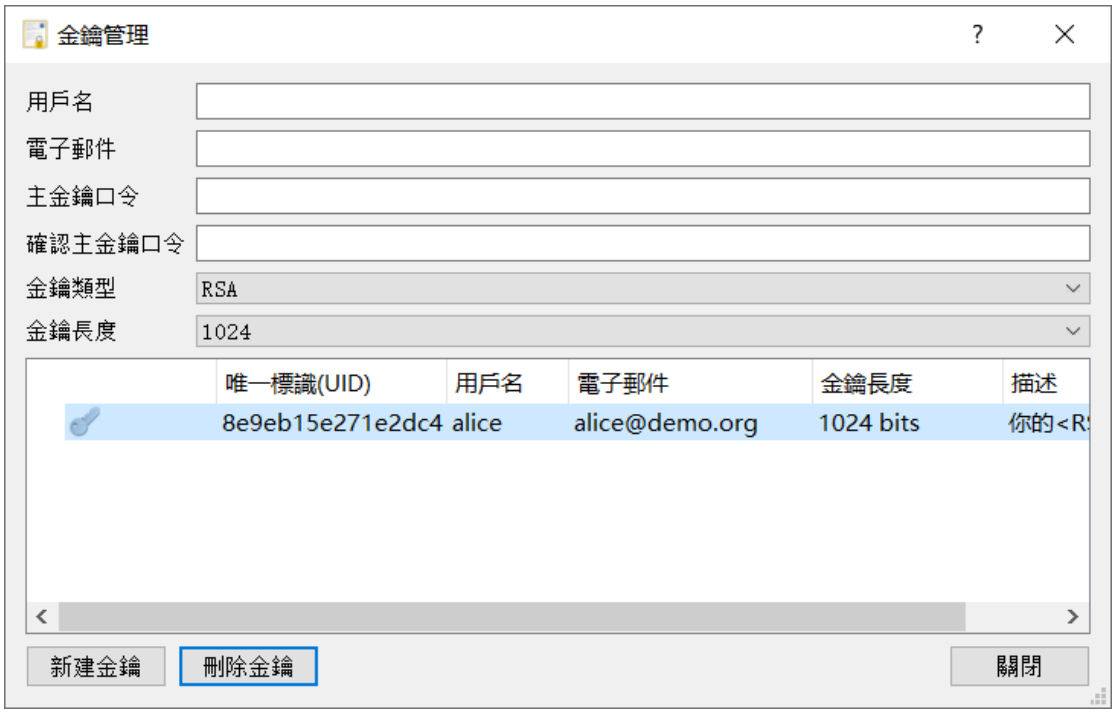


插入 Mac 平臺下麵的截圖 - ！！！

1. 管理安全金鑰：

1.1 創建安全金鑰

1) 打開 Menu 項：工具→金鑰環

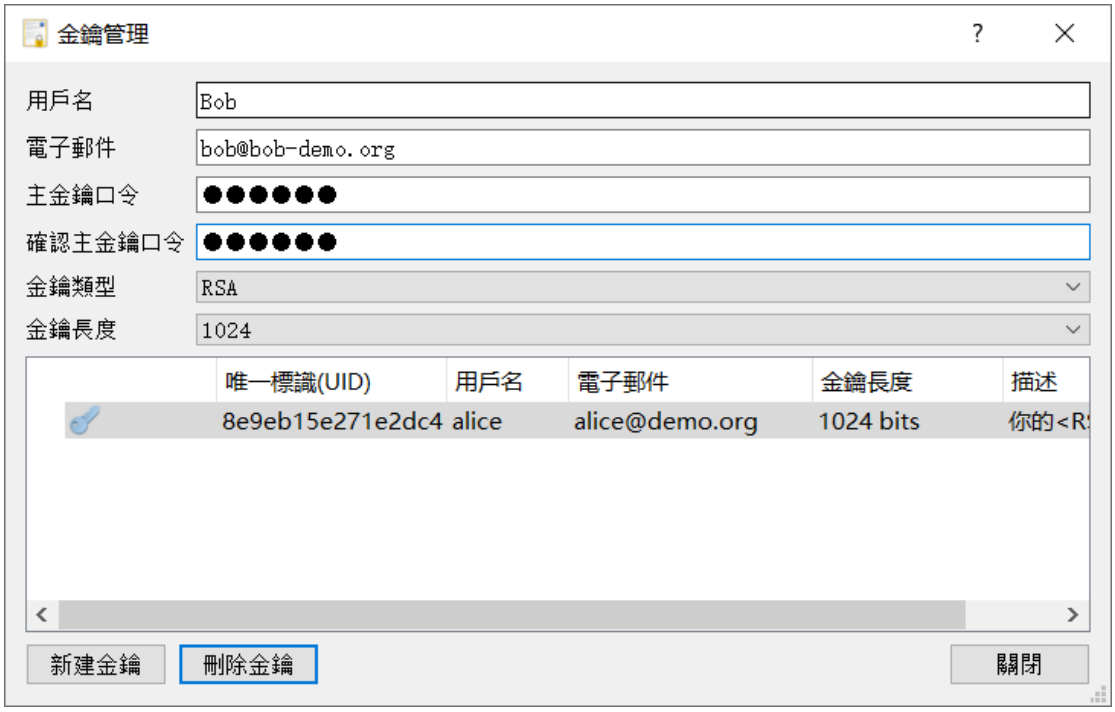


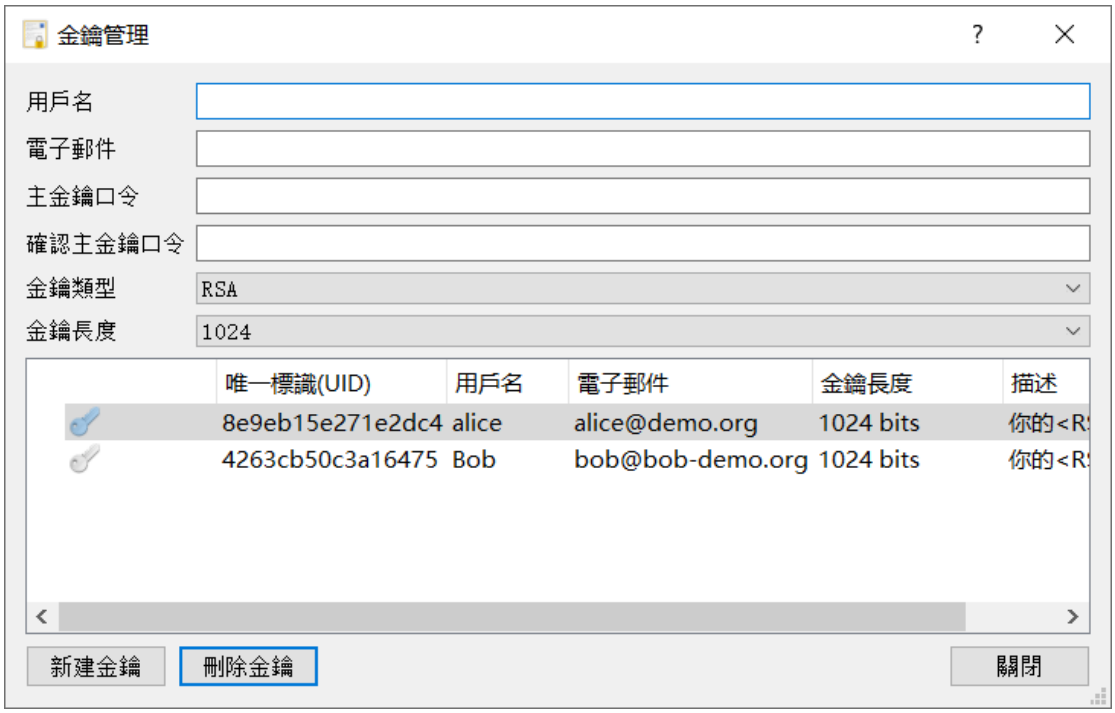
2) 按照軟體介面指示

✓ 填入：用戶名，電子郵件，主金鑰口令；選擇金鑰類型（RSA）和金鑰長度。

✓ 點擊按鈕“新建金鑰”。

例子：為 Bob 創建安全金鑰。





注意：

a) 安全金鑰是根據用戶名和電子郵件來識別。

b) 使用者唯一識別碼（UID）是根據用戶名和電子郵件生成的。

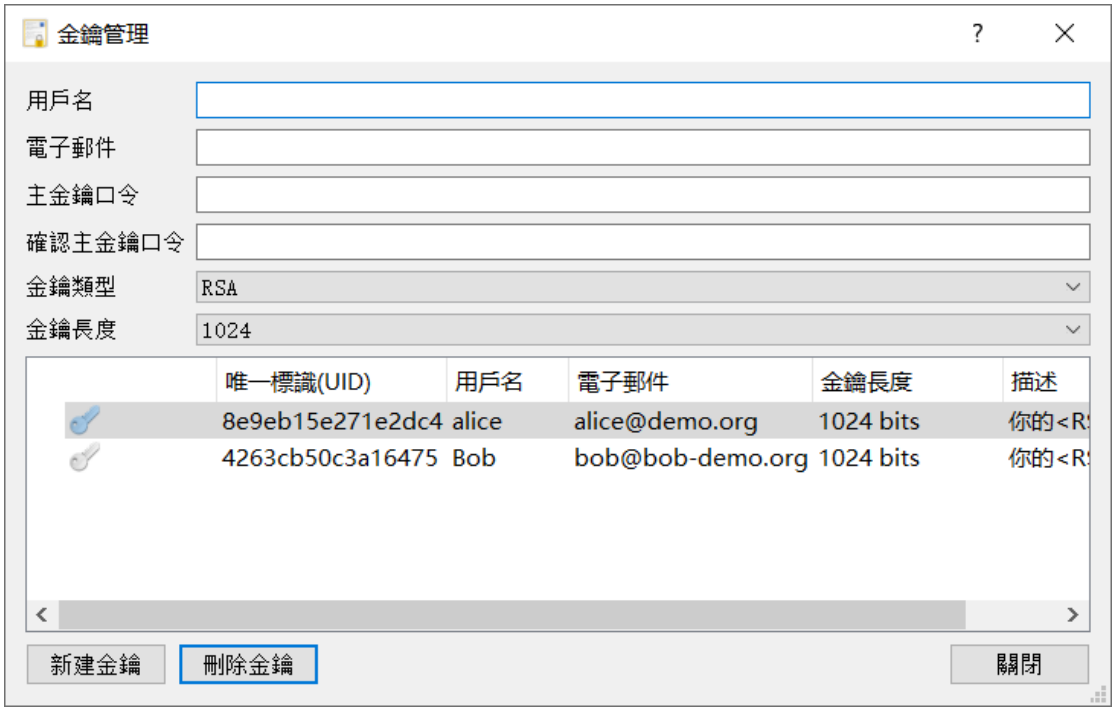
c) 您可以生成多把安全金鑰；但是需要使用不同的用戶名+電子郵件的組合。

d) 關於金鑰口令：

金鑰口令是您自己輸入的字串。切記：請您牢記這個金鑰口令。軟體本身不會保存口令。**一旦遺失了該口令，使用該口令和安全金鑰加密的檔將會無法被解密。**

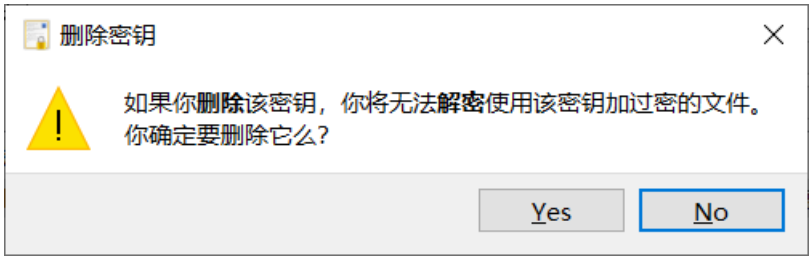
1.2 刪除金鑰

打開 Menu 項：工具→金鑰環



✓ 選中待刪除的金鑰。

✓ 點擊按鈕“刪除金鑰”，在執行刪除動作之前，金鑰管理介面會彈出一個確認對話方塊，讓您確認。當您選擇了“確定”之後，那個選中的金鑰會從金鑰庫中刪除。



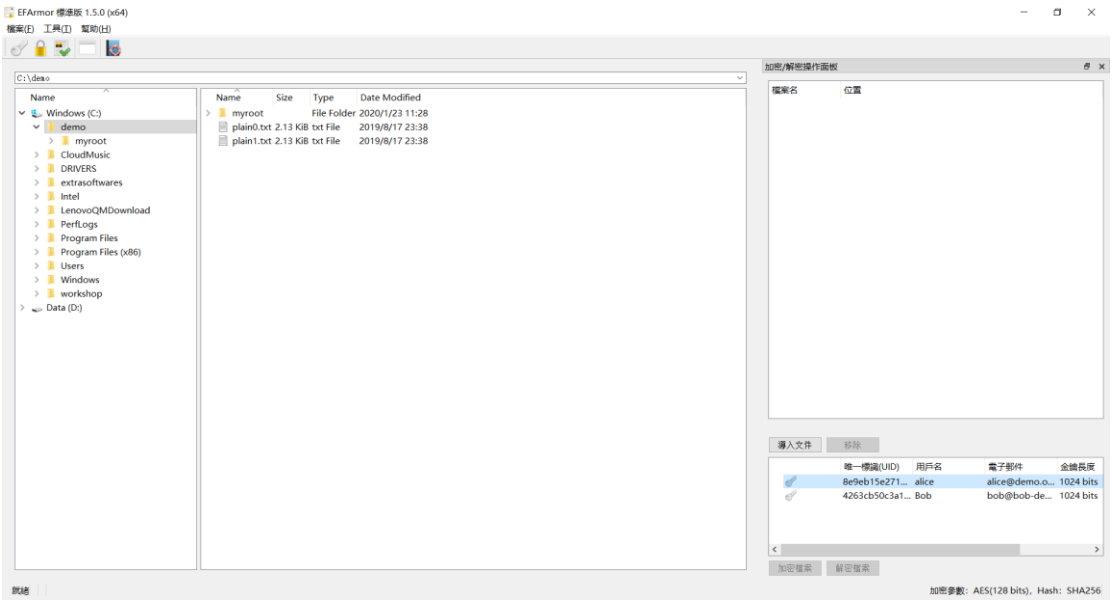
注意：

a) 刪除金鑰的操作是不可逆轉的：一旦金鑰被刪除，是無法恢復的。**執行刪除金鑰操作之前，請務必謹慎。**

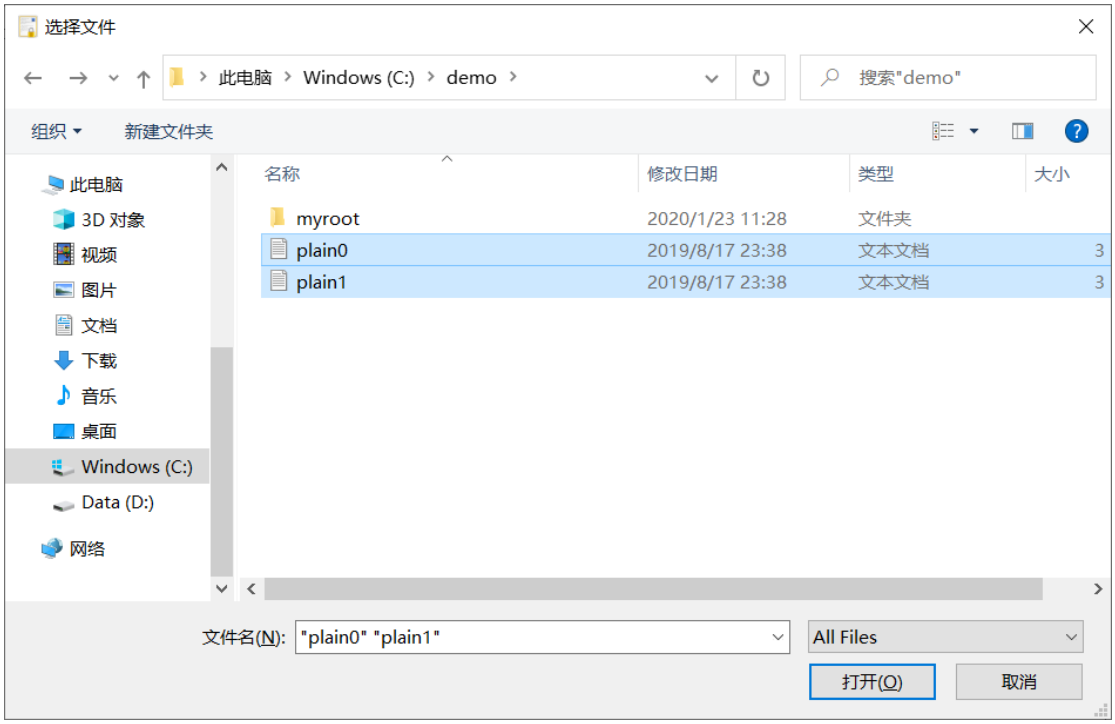
b) 金鑰被刪除（比如：刪除了屬於 Alice 的金鑰 - alice@demo.org），那麼使用該金鑰加密的檔就無法在解密了。

2. 導入文件或資料夾

2.1 打開 Menu 項目：工具→加密/解密操作面板



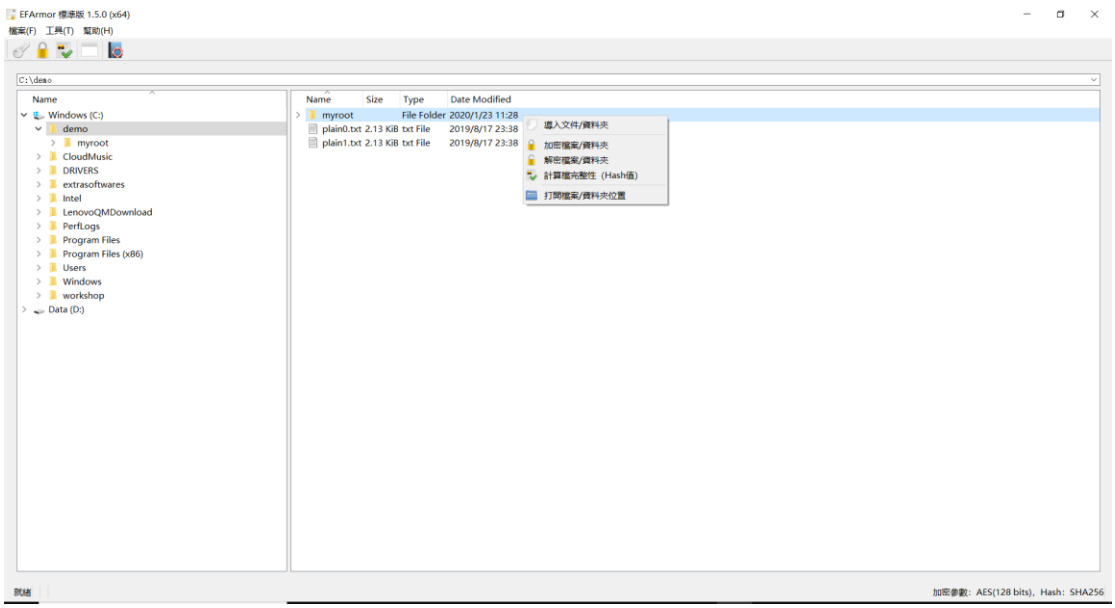
2.1.1 點擊“導入文件”按鈕，選擇檔案導入



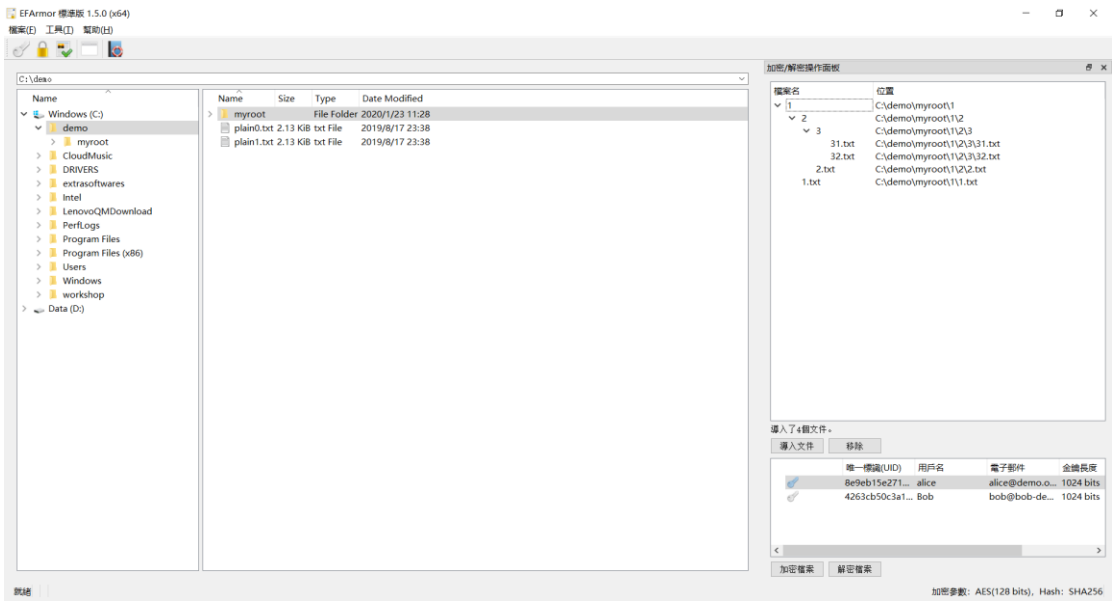
點擊“打開”按鈕後，會導入文件“plan0”和“plan1”：

2.2 使用右鍵功能表--導入文件/資料夾

在檔選擇區域，選中檔/資料夾，點擊右鍵菜單—導入文件/資料夾。



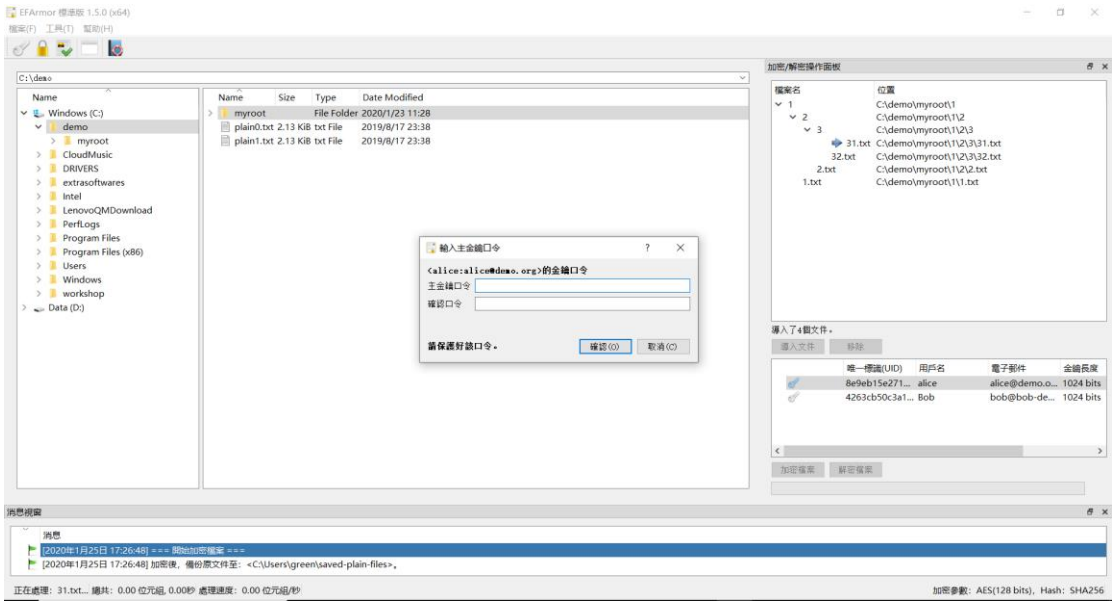
按照上述步驟完成導入操作後，導入的文件會排列在右側區域中。如下圖所示：



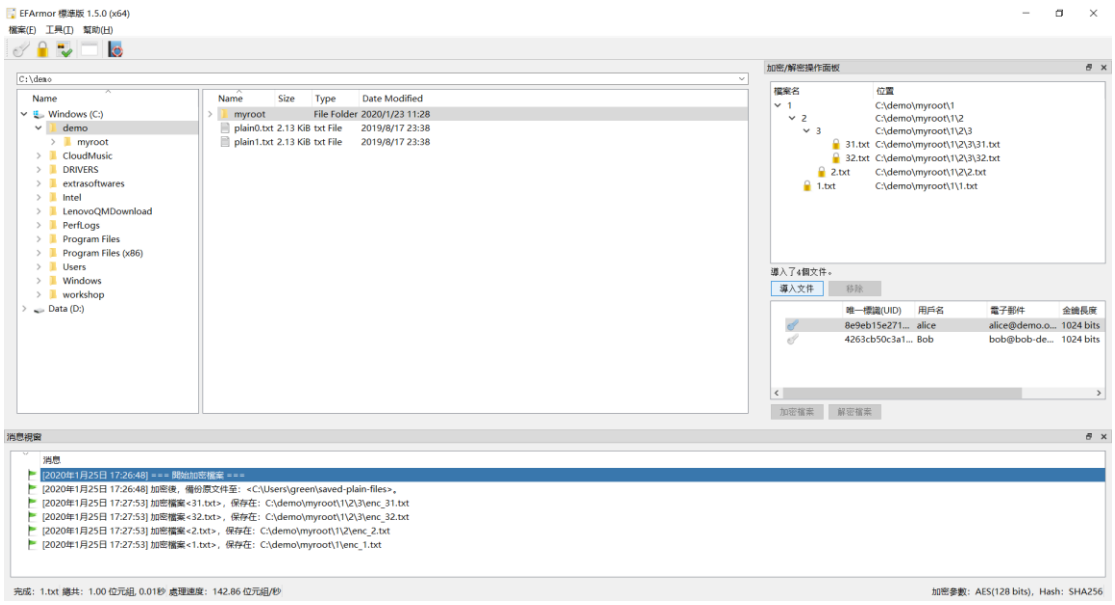
3. 加密和解密

完成導入操作後，然後點擊“加密檔案”或“解密檔案”按鈕：開始執行對應的操作。

軟體會首先彈出一個對話方塊：輸入“主金鑰口令”；一旦輸入了正確的金鑰口令，軟體就加密或解密先前導入的所有文件。



加密後



注意：

a) 如果有多個安全金鑰，那麼您可以選擇不同的金鑰進行加密：
在上面的加密示例，選擇了“alice”的金鑰進行加密。

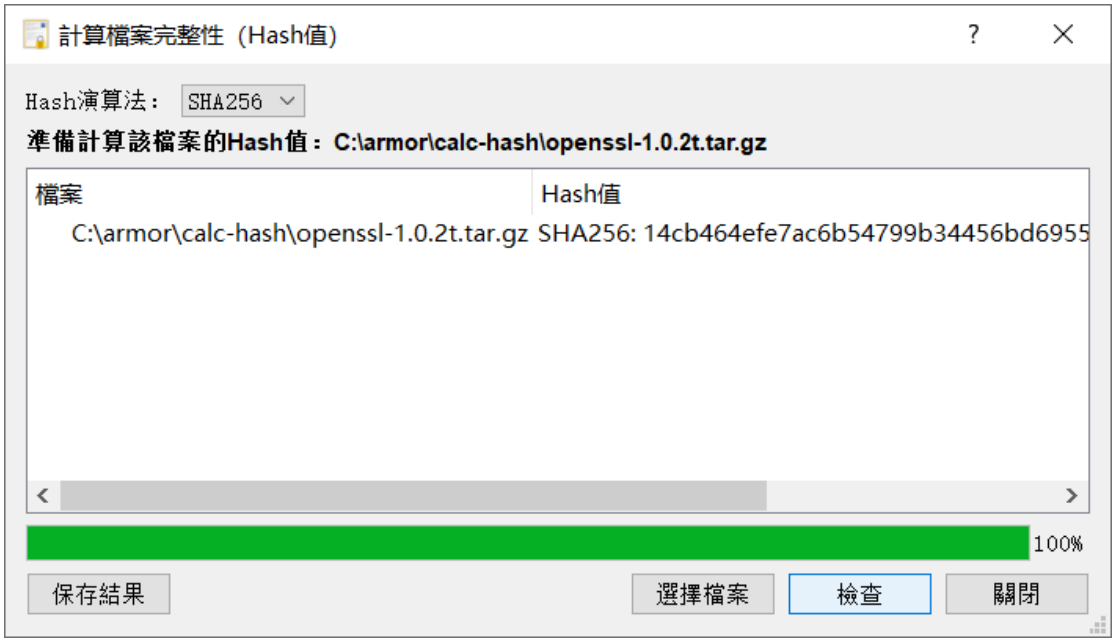
b) 解密檔案的時候，您只需要輸入對應的金鑰口令；軟體會自動的完成解密操作。

4. 計算檔完整性

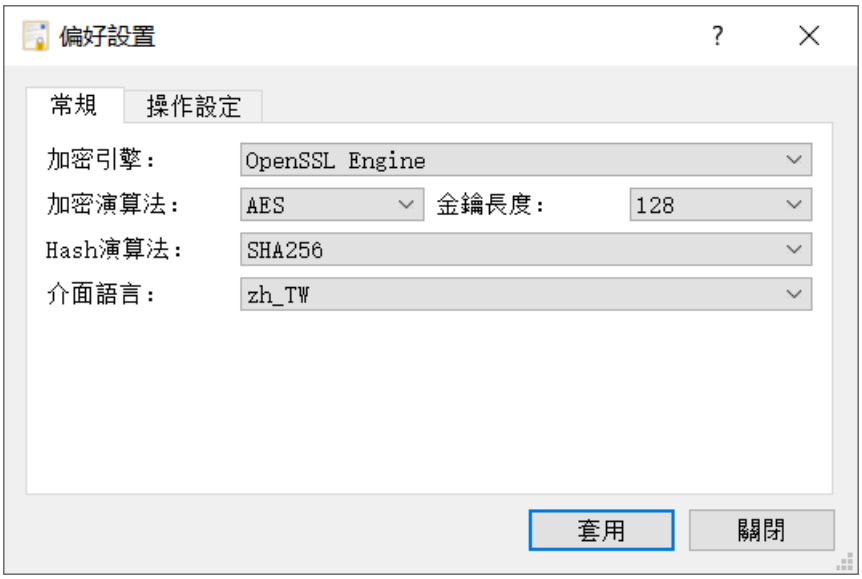
4.1 在檔的選擇區域，用滑鼠選中檔或資料夾。

4.2 打開主介面的功能表，選擇：工具→檔完整性

- ✓ 選擇 Hash 演算法。
- ✓ 點擊“檢查”按鈕。


計算檔案完整性（Hash值）
Hash演算法：
SHA256
準備計算該檔案的Hash值：C:\armor\calc-hash\openssl-1.0.2t.tar.gz
檔案
Hash值
C:\armor\calc-hash\openssl-1.0.2t.tar.gz
SHA256: 14cb464efe7ac6b54799b34456bd6955
100%
保存結果
選擇檔案
檢查
關閉

5. 偏好設置（Preference）



您可以在偏好設置中對軟體行為進行調整：

A. “常規” - 調整加密參數
   a) 調整加密演算法和金鑰長度。
   b) 調整 Hash 演算法。

B. “操作設定” - 調整加密/解密後的操作
   a) 加密後，對原文件的操作：
      ✓ 不移動/刪除原檔：完成加密後，原文件和密文保存在同樣位置。
      ✓ 只保留加密後的檔：完成加密後，刪除原文件。如果加密失敗的話，不會刪除原文件。
      ✓ 備份原檔：完成加密後，軟體會把原文件移動到您設定的磁片位置。
   b) 解密後，對密文的操作。
      ✓ 不移動/刪除加密檔：完成解密後，解密後的檔和密文保存在同樣的位置。
      ✓ 只保留解密檔：完成解密後，刪除加密檔。但是解密失敗的話，不會刪除加密檔。

✓ 備份加密檔：完成解密後，軟體會把加密檔移動到您設定的磁片位置。

C. 調整軟體介面語言

a) en_US：英文

b) zh_CN：簡體中文

c) zh_TW：繁體中文

注意：修改介面的語言設定後，您需要重新開機軟體才能讓這個設置生效。

三：EFArmor 支援的密碼演算法

EFArmor 1.5.0 使用 OpenSSL（https://www.openssl.org/）作為加密引擎。這樣就讓軟體具有統一的跨平臺能力：無論您使用 Windows 或 Mac，您都可以運行 EFArmor 來加密保護您的電腦文檔。

EFArmor v1.5.0 支援的密碼演算法表

演算法名稱	用途	備註
RSA	非對稱演算法，用於安全金鑰中。	安全金鑰的默認長度是 1024 比特。您也可以選擇 2048 比特。
RC2	對稱加密演算法，可以用於資料檔案的加密。	金鑰長度：40/64/128 比特。
RC4		金鑰長度：40/128 比特。
AES	高級加密標準	預設的資料加密演算法，預設金鑰長度為 128 比特。您也可以選擇 192 或 256 比特。
DES	資料加密標準	金鑰長度：56 比特。
DESX	DES 的一種變種演算法，旨在提高計算複雜度以對抗暴力破解。	金鑰長度：184 比特。
BLOWFISH	對稱加密塊演算法。	金鑰長度：128 比特
CAST5	對稱加密塊演算法。	金鑰長度：128 比特
IDEA	對稱加密塊演算法。	金鑰長度：128 比特
3DES	三重 DES 演算法，DES 一種	金鑰長度：168 比特。
RNG	亂數演算法。	遵守的標準：FIPS 186-2, FIPS 140-2, NIST SP 800-90
MD2	MD2 資訊摘要演算法。 注意： 該演算法僅用在計算檔校驗和中。	數字摘要長度：128 比特。
MD4	MD4 資訊摘要演算法。	
MD5	MD5 資訊摘要演算法。	
SHA1	Secure Hash Algorithm	數字摘要長度：160 比特。
SHA2	Secure Hash Algorithm 2	數字摘要長度：256/384/512 比特。

四：常見問題

1. 在 Windows 中，為什麼我加密 U 盤中檔，有時候會無法成功？
   請把檔複製到您的電腦中的硬碟中，然後重新執行加密操作。
2. EFArmor 1.5.0 的版本可以運行在什麼平臺下面？
   EFArmor 1.5.0 可以運行在 32 位和 64 位 Windows 平臺以及 Mac 中；它支持最新的 macOS 版本。
3. EFArmor 有什麼特色？
   首先它使用類 PGP 協定以及高強度的加密演算法來保護您的電腦文檔；其次，它可以運行在 Windows 平臺和 Mac 平臺 – 所有的功能和操作方式都一樣。
   最重要的是：它操作方便：僅僅需要設定一個口令和金鑰就可有效的加密保護您的檔了。
4. EFArmor 未來會怎樣發展？
   請訪問 EFArmor 專案網站來瞭解專案未來的發展方向和產品路線：
   https://github.com/EFArmorSupport/EFArmor

五：感謝

本軟體使用如下的第三方軟體組件，非常感謝他們的辛勤勞動和貢獻。

1. zlib 1.2.11：zlib 壓縮庫。
2. Qt5.13.0：Qt 跨平臺庫。
3. The oxygen-icons 和 KDE 開發組(https://kde.org/)：程式使用的圖示庫。
4. OpenSSL 1.1.1d：廣泛使用的高強度密碼庫。

請參考安裝目錄中的 3RDLicenses 參看詳細資訊。