**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії***

**ЛАБОРАТОРНА РОБОТА № 14**

з курсу

***«Безпека програм та даних»***

**ТЕМА: Криптографічні та стеганографічні програмні засоби.**

**Студент : Трембіцький Нікіта**

**Група : 41ІПЗ**

**Факультет : Інформатики**

**Викладач : Галицький О.В.**

**Київ 2019**

**1. За допомогою пошукової системи глобальної мережі Інтернет знайти та дослідити програмні засоби для шифрування даних.**

**1) Kruptos 2 Professional**, v3.0.27,Steve Beckett, Kruptos 2 Software.



2) Ліцензія - пропрієтарний програмний засіб. Платна.

3) Операційна система - Windows XP / Vista / 7, 15мб. вільного дискового простору.

4) Програма включає просте меню керування, має декілька кнопок для шифрування та дешифрування файлів. Всі результати корстувач спостерігає в діалоговому вікні програми, яке відкивається після завершення операції.

5) Наявність інтернет підтримки існує.

6) Мова інтерфейсу англійська(опціонально - російська)

7) Керування здійснюється мишкою або клавіатурою.

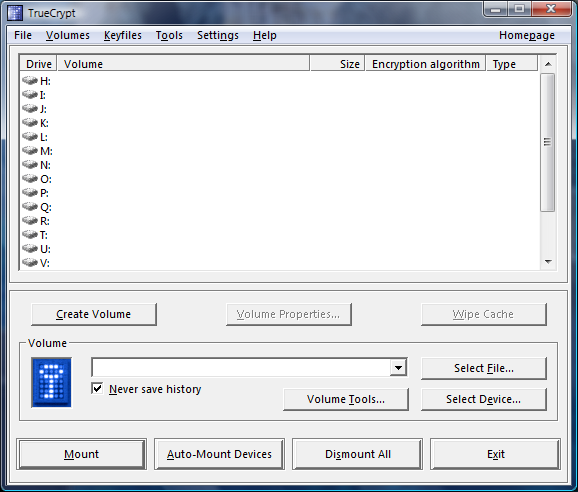
8)

* 128-бітова система шифрування використовує алгоритм Blowfish;
* програма зашифровує будь-яку кількість файлів і папок, а також всі відомі формати файлів;
* потужна і легка у використанні утиліта, яка використовує провідник;
* немає прихованого доступу, прихованих ключів або якогось іншого методу декодування зашифрованих даних без правильного пароля;
* підтримує плагін Windows Explorer, який дозволить Вам зашифрувати / декодувати / роздрібнити файли, використовуючи функції звичайного Microsoft Windows Explorer. Програма інтегрується в Windows Explorer і вона дозволяє працювати з важливими файлами використовуючи контекстне меню Explorer;
* ви можете декодувати файл, потім автоматично відкрити програму Kruptos 2 і повторно зашифрувати файл відразу після завершення його редагування, і все це можна зробити за допомогою натискання всього однієї кнопки;
* програма створює саморозпаковуються зашифровані файли (EXEs), які містять як захищену інформацію, так і необхідне програмне забезпечення для розпакування її змісту. Користувачі можуть розпаковувати зміст саморозпаковуються файлів просто запустивши цю програму, як будь-яку другу звичайну програму. Все що необхідно для запуску - це правильний пароль;
* програма ретельно і безпечно видаляє файли і їх сліди з Вашого комп'ютера за допомогою інструменту видалення, після чого ці файли не можуть бути відновлені за допомогою звичайного інструмента "скасувати видалення";

9) Не знайдено.

10) Застосовується для шифрування та дешифрування файлів, каталогів. В різних офісних структурах, банківських установах.Або інших закладах, де потребується особливий рівень безпеки деякої інформації, чи даних.

**2) TrueCrypt Foundation.**



2)Ліцензія - TrueCrypt Collective License(безкоштовна)

3) Операційна система - Microsoft Windows NT 5+, Linux, Mac OS X, 4мб вільного дискового простору.

4) Програма працює і без встановлення на операційну систему. Має просте меню, та кнопки керування. Працює по принципу створення віртуальних зашифрованих логічних дисків. Вони зберігаються у вигляді файлу, і можуть бути легко розпаковані цією ж програмою по вимозі.

5) Інтернет підтримка відсутня.

6) Мова інтерфейсу англійська (опціонально російська).

7) Керування відбувається мишкою та клавіатурою. Командний рядок в нових версія не підтримується більше.

8) TrueCrypt вміє створювати зашифрований віртуальний диск:

у файловому контейнері, що дозволяє легко працювати з ним - переносити, копіювати (у тому числі на зовнішні пристрої у вигляді файлу), перейменовувати або видаляти;

у вигляді зашифрованого розділу диска, що робить роботу більш продуктивною і зручною, у версії 5.0 додалася можливість шифрувати системний розділ;

шляхом повного шифрування вмісту пристрою, такого як USB флеш-пам'ять (пристрої флоппі-диск не підтримується з версії 7.0).

Створення зашифрованого віртуального диска у файловому контейнері, у вигляді зашифрованого розділу диска, а також шляхом повного шифрування вмісту пристрою.

- Зміна паролів та ключових файлів для томи без втрати зашифрованих даних.

- У список підтримуваних TrueCrypt алгоритмів шифрування входять AES, Serpent і Twofish. Можливе використання каскадного шифрування різними шифрами, наприклад: AES + Twofish + Serpent.

- Всі алгоритми шифрування використовують режим XTS.

- TrueCrypt дозволяє вибрати одну з трьох хеш-функцій: HMAC-RIPEMD-160, HMAC-Whirlpool, HMAC-SHA-512 для генерації ключів шифрування, солі і ключа заголовка.

- Для доступу до зашифрованих даних можна застосовувати пароль (ключову фразу), ключові файли (один або декілька) або їх комбінації.

- Забезпечення двох рівнів правдоподібного заперечення наявності зашифрованих даних, необхідного в разі вимушеного відкриття пароля користувачем.

- Підтримка створення зашифрованого динамічного файлу на дисках NTFS. Такі томи TrueCrypt збільшуються в розмірі в міру накопичення нових даних аж до зазначеного максимального розміру.

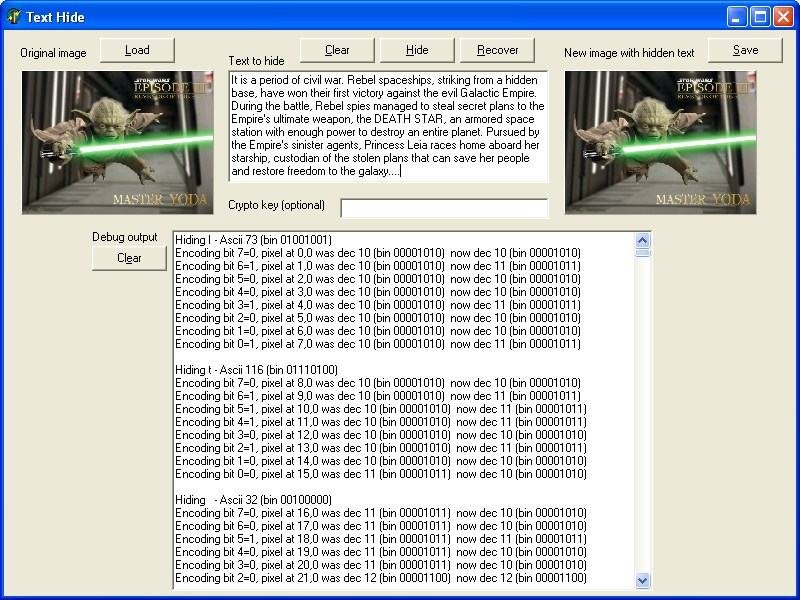
- Змонтований том в TrueCrypt подібний до звичайного логічного диску, тому з ним можна працювати за допомогою звичайних утиліт перевірки та дефрагментації файлової системи.

9) По-перше, це орієнтованість на Windows-системи - багато функціональні можливості, як було зазначено вище, працюють тільки в ОС Windows. По-друге, немає можливості зміни розміру контейнера, до того ж операція дешифрування несистемного розділу далеко не тривіальна і вимагає деяких маніпуляцій з файлами. По-третє, програма не має вбудованого генератора паролів і допускає використання користувачем простих паролів. По-четверте, при зберіганні даних у контейнерах TrueCrypt існує ймовірність повної втрати даних внаслідок видалення файлу-контейнера. Ну і, по-п'яте, зазначу одну особливість,яка комусь може послужити на користь, а кому навпаки. Справа в тому, що в багатокористувацької середовищі (термінальний режим) змонтований тому TrueCrypt буде видно і доступний для всіх користувачів без винятку, уникнути доступу до нього можна використанням дозволів NTFS. Та ж ситуація повториться при зміні користувача на системах Windows, починаючи з версії Windows XP

10) Використовується для шифрування даних, створення цілих розділів локальних дисків з каталогами та файлами які повністю шифруються.

**2) За допомогою пошукової системи глобальної мережі Інтернет знайти, встановити та дослідити програмні засоби для стеганографічного захисту даних.**

**1) Text Hide 2.0,** The\_Krypto\_Anarkist.



2) Безкоштовна.

3) Windows 98\Xp\Vista\7\8. 2мб вільного місця на HDD.

4) Програма має 1 блок управління, та 4 кнопки управління проесом шифрування.

5) Інтернет підтримка відсутня.

6) Мова інтерфейсу - англійська.

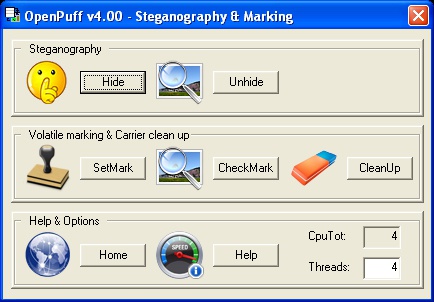
7) Управління програмою здійснюєтсья за допомогою мишки та клавіатури.

8) Дозволяє заховати в текстовому файлі будь бінарний файл. Є можливість 32-бітної шифровки інформації, що приховується з паролем.

9) Не знайдено.

10) Застосовуєтсья тільки в обробці текстових файлів.

**2) OpenPuff**



2) Безкоштовно (Freeware)

3) Windows XP, Vista, 7, 8, 10

4) Програма не вимагає установки (портативна) і легка у використанні.

5) Наявність інтернет підтримки існує.

6) Мова інтерфейсу - англійська.

7) Управління програмою здійснюєтсья за допомогою мишки та клавіатури.

8) Використовуючи цей безкоштовний додаток ви можете приховати конфіденційну інформацію в звичайні файли - зображення, відео або аудіо. Файли зашифровані способом стеганографії можна безпечно зберігати і передавати по електронній пошті друзям або діловим партнерам, не викликаючи підозр в прихованому змісті у користувачів які випадково отримали до них доступ.

Підтримувані формати файлів:

* зображення - JPG, PNG, BMP, PCX, TGA
* відео - MP4, 3GP, MPG, VOB
* аудіо файли - MP3, WAV, AIFF, NEXT/SUN
* Flash-Adobe - FLV, SWF, PDF

9) Не знайдено.

10) Програма для шифрування і приховування даних за допомогою стеганографії.