**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії та освітніх вимірювань***

**ЛАБОРАТОРНА РОБОТА №13**

## ТЕМА: Асиметричні і гібридні криптосистеми.

з курсу

***«Безпека даних та програм»***

Студент Коваль О.М.

Група 42-ІПЗ

Факультет Інформатики

Викладач: професор Франчук В.М.

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



Ліцензія - пропрієтарний програмний засіб. Платна.

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

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.

Наявність інтернет підтримки існує.

Мова інтерфейсу англійська(опціонально - російська)

Керування здійснюється мишкою або клавіатурою.

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;

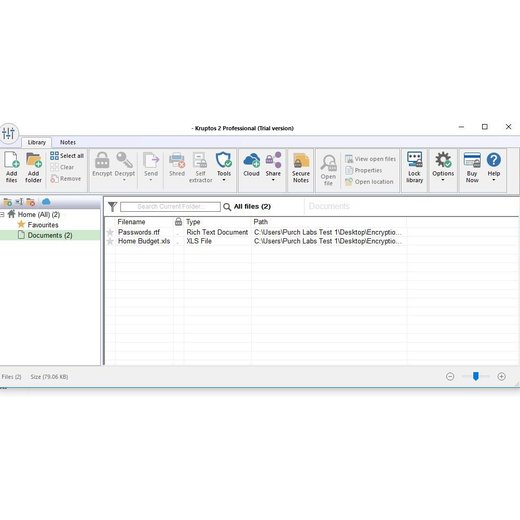
ви можете декодувати файл, потім автоматично відкрити програму Kruptos 2 і повторно зашифрувати файл відразу після завершення його редагування, і все це можна зробити за допомогою натискання всього однієї кнопки;

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";

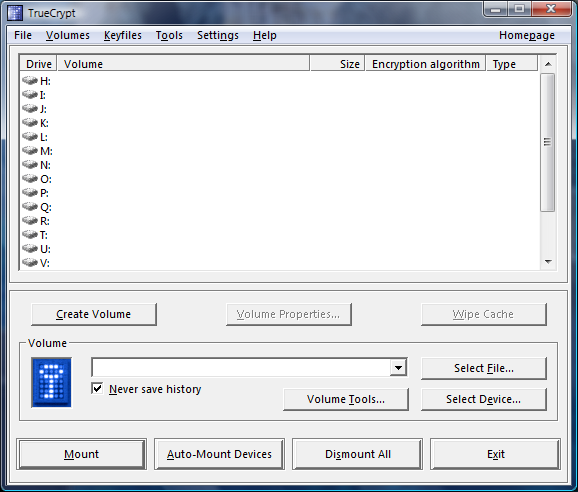
Не знайдено.

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.



*За допомогою пошукової системи глобальної мережі Інтернет знайти, встановити (встановлювати програмні засоби слід на віртуальну машину) та дослідити програмні засоби для стеганографічного захисту даних. Описати 2-3 програмних засоби за схемою поданою у 3-му завданні.*

**TrueCrypt Foundation.**



Ліцензія - TrueCrypt Collective License(безкоштовна)

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

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.

Інтернет підтримка відсутня.

Мова інтерфейсу англійська (опціонально російська).

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

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.

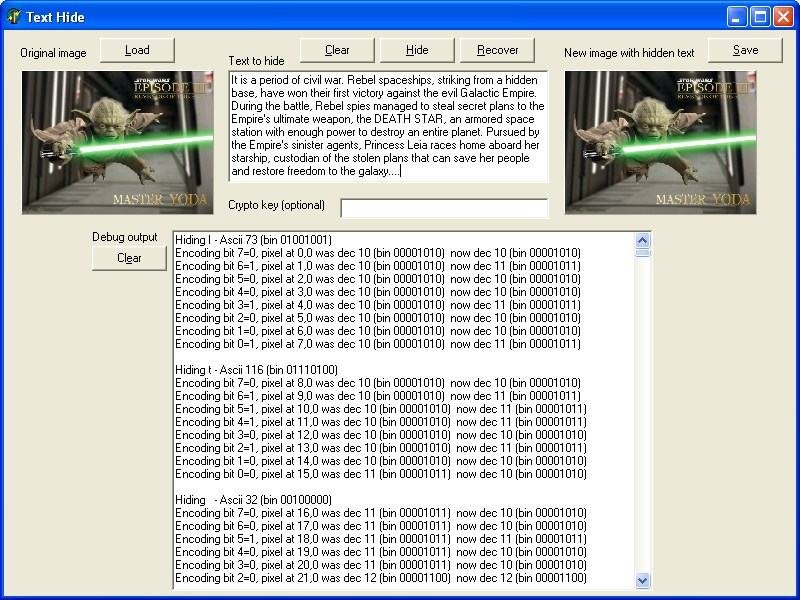
- Підтримка створення зашифрованого динамічного файлу на дисках NTFS. Такі томи TrueCrypt збільшуються в розмірі в міру накопичення нових даних аж до зазначеного максимального розміру.

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

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

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

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



Безкоштовна.

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

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

Інтернет підтримка відсутня.

Мова інтерфейсу - англійська.

Управління програмою здійснюєтсья за допомогою мишки та клавіатури.

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

Незнайдено.

Застосовуєтсья тільки в обробці текстових файлів.