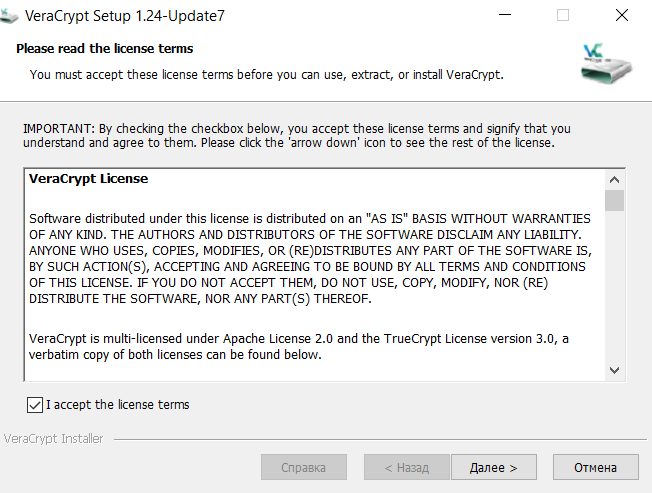
**Бужак Андрій Васильович, 541м**

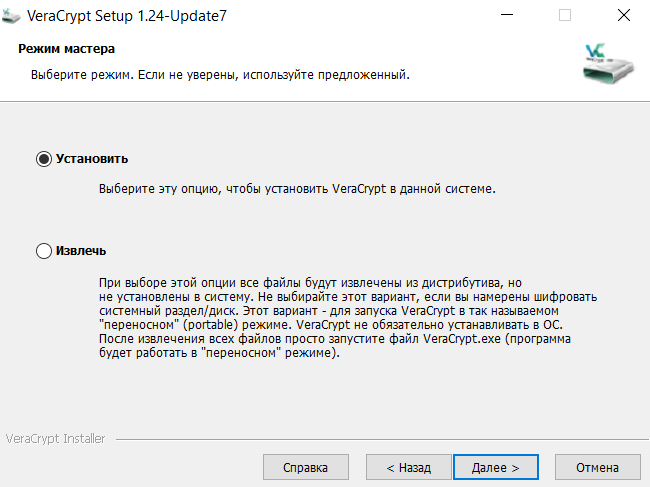
**Лабораторна робота №2**

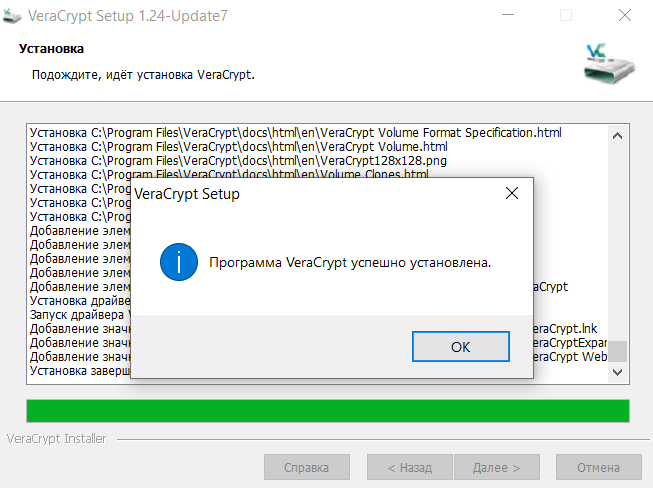
**«Вивчення системи захисту даних VeraCrypt 1.24»**

***Хід роботи***

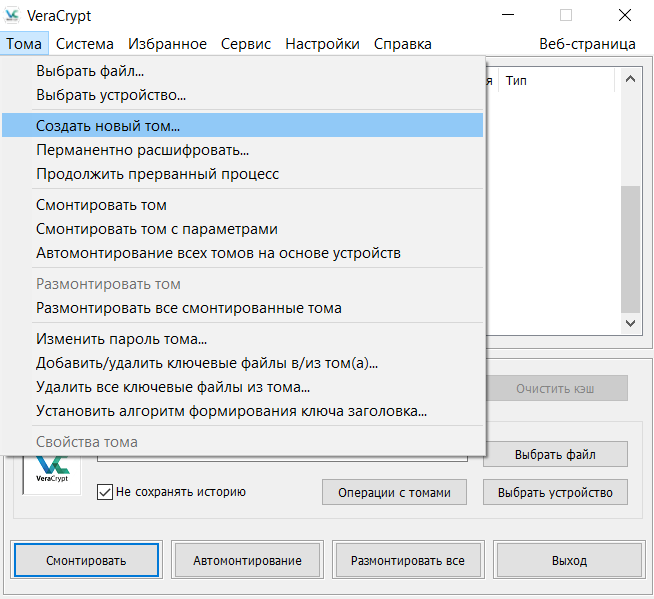
1. Встановимо програму VeraCrypt 1.24 Update 7 на нашому комп’ютері.

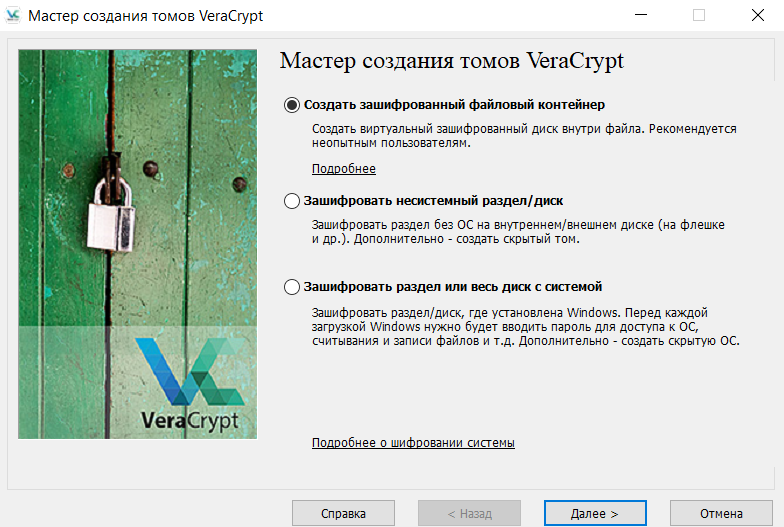




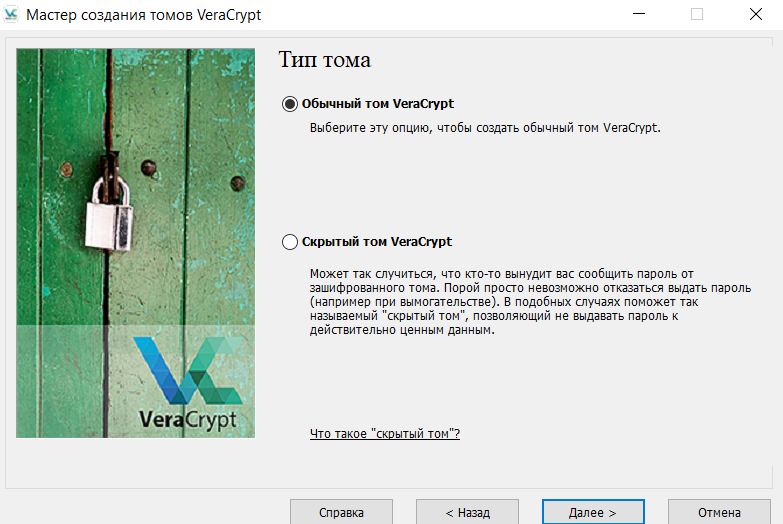


2. Згідно з вказівками теоретичної частини створимо на нашому флеш-носієві захищений диск. Для захисту використаємо пароль та ключовий файл

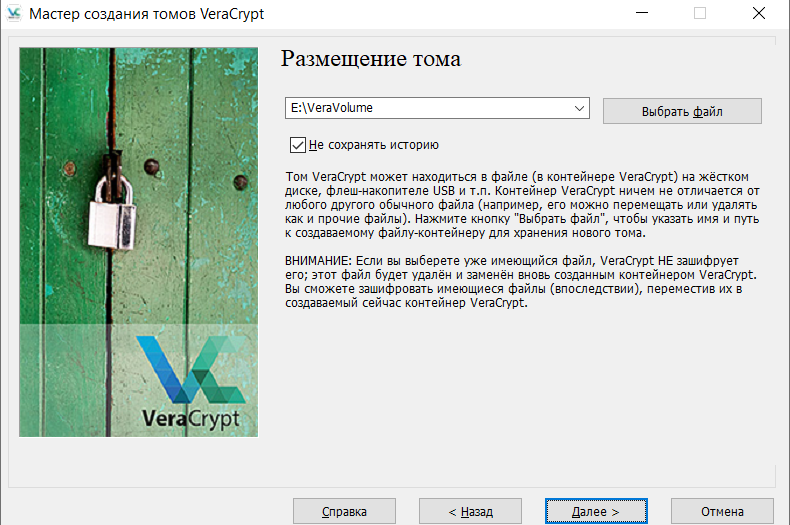




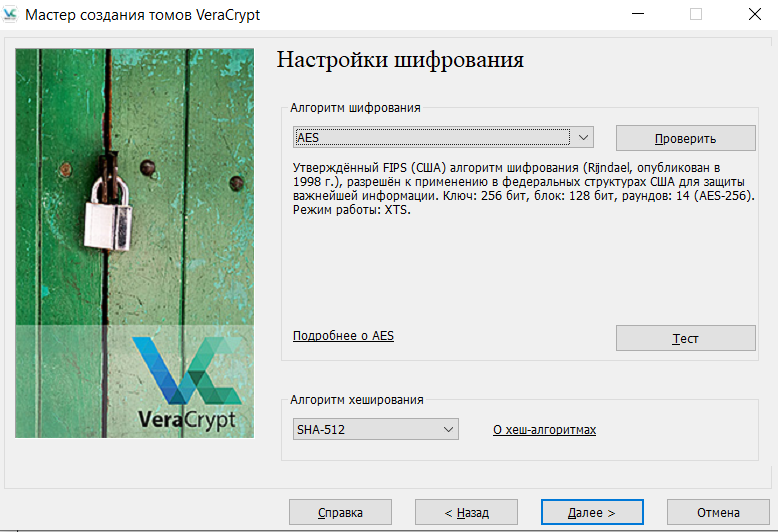
Наступним кроком буде вибір типу зашифрованого диска. Виберемо «Обычный том VeraCrypt»



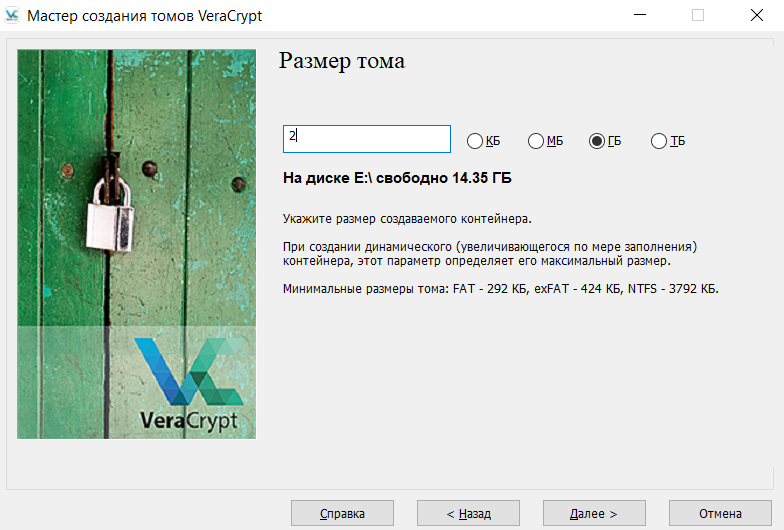
Виберемо місцем розміщення захищеного диска флешку.



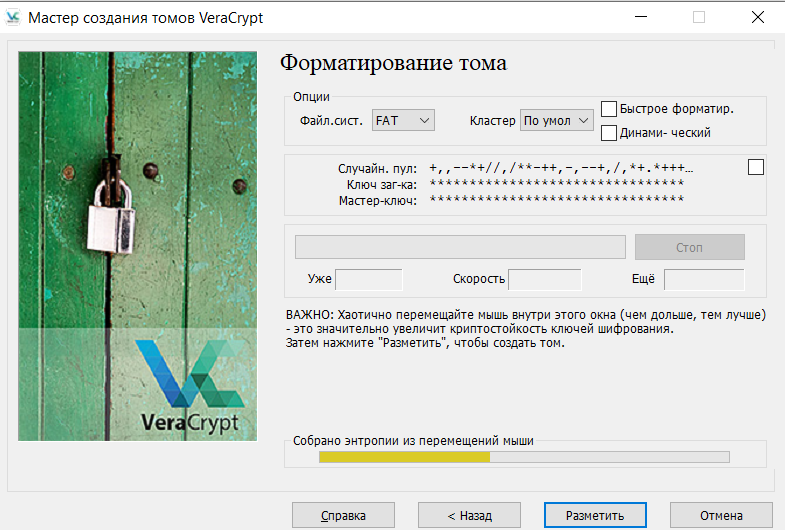
Виберемо алгоритм шифрування та задамо потрібні параметри

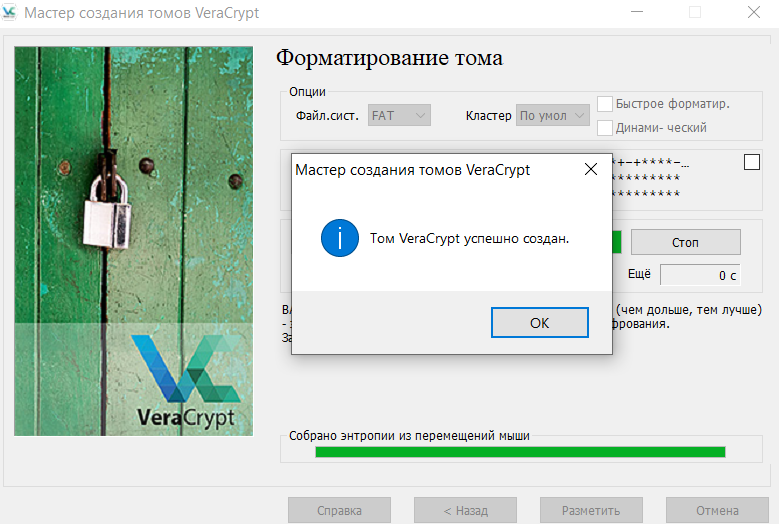


Встановимо розмір захищеного диску



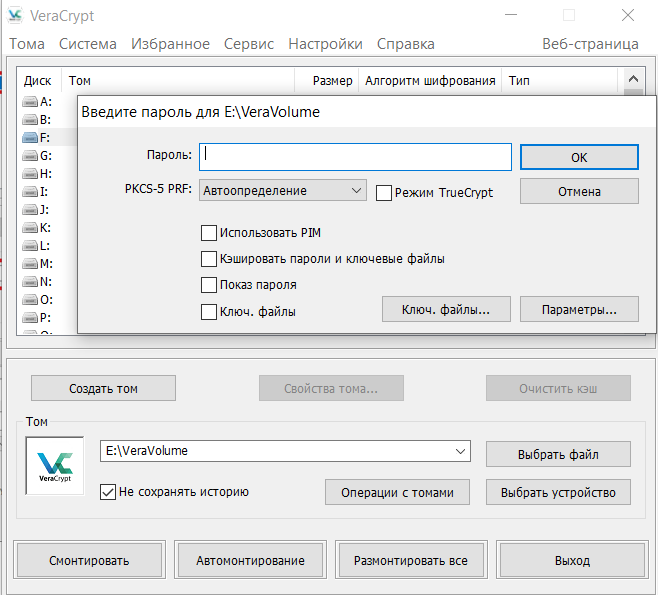
Встановимо пароль та перейдемо до розмітки тому





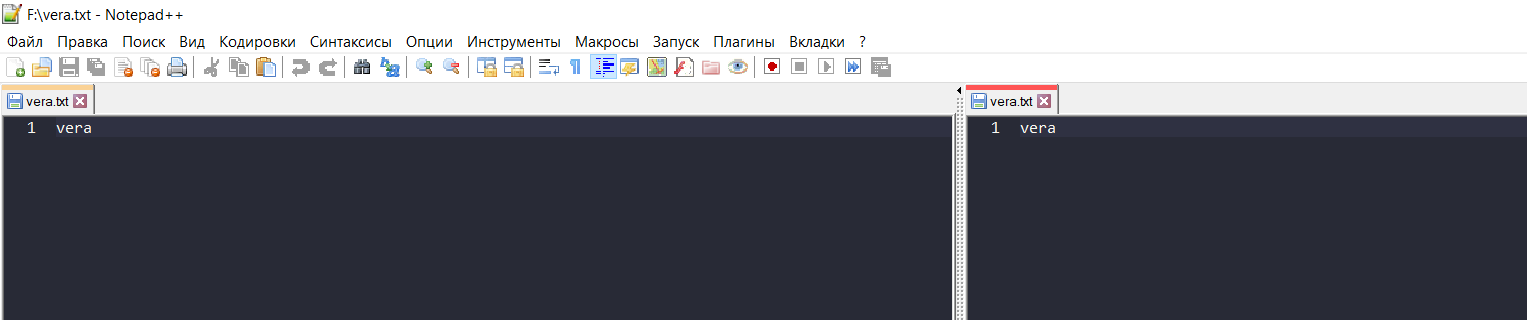
3. Змонтуємо захищений диск, користуючись паролем та ключовим файлом

Для цього виберемо вільний слот для подальшого монтування та виберемо підготовлений на попередньому кроці файл.



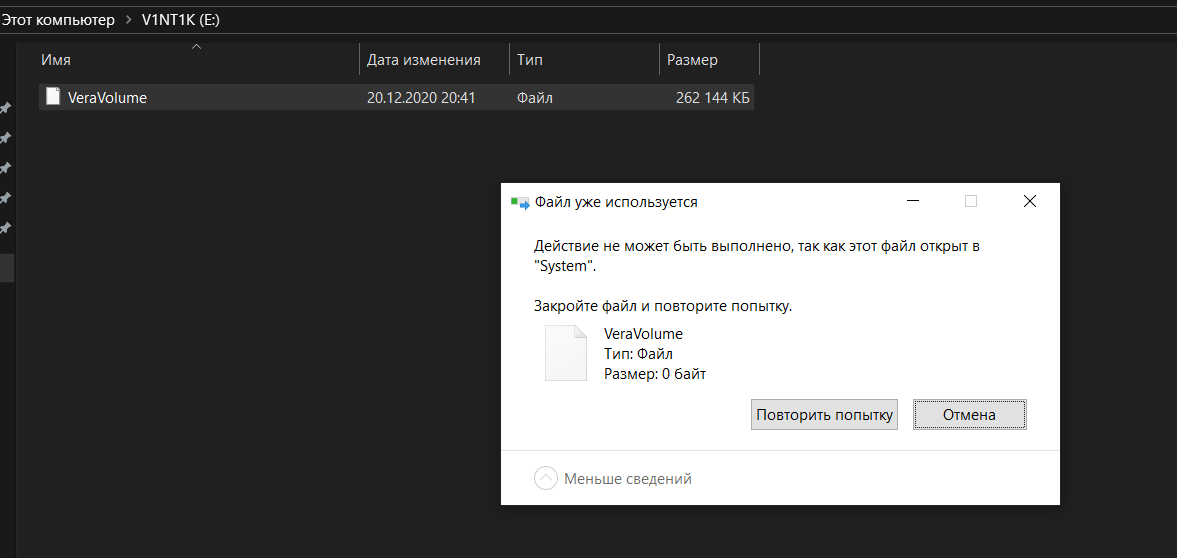


4. Створіть текстовий файл у MicrosoftWord(наприклад, звіт з лабораторної роботи) та збережіть його на захищеному диску. Копію файлу збережіть на відкритому диску. Відкрийте файли за допомогою TextView(HEX-mode) у FAR, порівняйте їх вміст та зробіть відповідний висновок. Чому отримано такий результат?



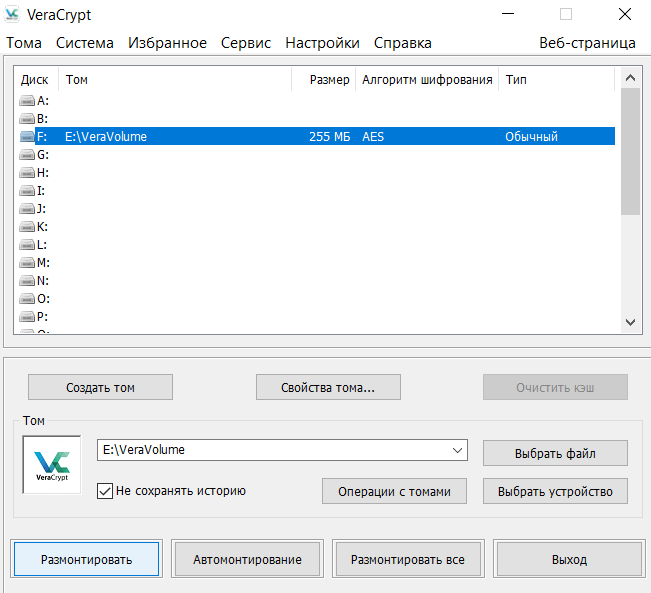
Доки захищений том змонтований – ми маємо доступ до запису і читання зашифрованих файлів у ньому. Тому можемо прочитати однаковий вміст вайлів.

5. Спробуйте прочитати файл, який „символізує” захищений диск, спробуйте його витерти або змінити. Поясніть отриманий результат.



Прочитати файл захищеного диску, змінити чи витерти його неможливо до моменту поки диск не буде відмонтований

6. Відмонтуємо диск, після чого зможемо змінити чи видалити файл захищеного диску



***Відповіді на контрольні запитання***

1. Для чого призначена програма VeraCrypt 1.24?

VeraCrypt – це програмне забезпечення для встановлення та підтримання зашифрованого on-the-fly обсягу (пристрій зберігання даних). On-the-fly означає, що дані автоматично шифруються безпосередньо перед тим, як їх зберігати і дешифрують відразу після їх завантаження, без будь-якого втручання користувача.

1. Які основні можливості програми VeraCrypt 1.24?

Жодні дані, що зберігаються на зашифрованому томі, не можуть бути прочитані (розшифровані) без використання правильних паролів / файлів ключів або правильних ключів шифрування. Зашифрована вся файлова система (наприклад, імена файлів, імена папок, вміст кожного файлу, вільний простір, метадані тощо).

Файли можна копіювати на прикріплений том VeraCrypt та з нього, як і на будь-який звичайний диск (наприклад, простими операціями перетягування та перетягування). Файли автоматично дешифруються автоматично на льоту (в пам'яті / оперативній пам'яті) під час їх читання або копіювання із зашифрованого тома VeraCrypt. Подібним чином, файли, які записуються або копіюються на том VeraCrypt, автоматично шифруються на льоту (безпосередньо перед тим, як їх записати на диск) в оперативній пам'яті. Зауважте, що це не означає, що весь файл, який потрібно зашифрувати / розшифрувати, повинен зберігатися в оперативній пам'яті, перш ніж його можна зашифрувати / розшифрувати. Для VeraCrypt не вимагається додаткової пам'яті (ОЗУ).

1. Які способи захисту інформації у програмі?

*Алгоритми*

VeraCrypt може використовувати наступні алгоритми шифрування: AES, Serpent, та Twofish. Додатково доступні 5 комбінацій цих алгоритмів: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES і Twofish-Serpent. Втілені криптографічні хеш-функції: RIPEMD-160, SHA-256, SHA-512 та Whirlpool.

*Режими шифрування*

VeraCrypt використовує режим шифрування XTS

*Ключі*

Ключ заголовка і вторинний ключ заголовка для режиму XTS генеруються за допомогою алгоритму PBKDF2 з використанням 512-бітної криптографічної солі, число ітерацій становить від 327,661 до 655,331, залежно від використовуваної хеш-функції.

1. Які способи захисту доступу до захищеного диску?

* Хеш-алгоритм
* Алгоритм шифирування
* Швидкий доступ

1. Які Ви бачите недоліки програми?

Станом на серпень 2015, не опубліковані відомості про явні вразливості VeraCrypt. VeraCrypt схильний до ряду потенційних атак, до яких чутливе і інше програмне забезпечення шифрування дисків, наприклад BitLocker. Для пом'якшення цієї небезпеки, розробники VeraCrypt дали користувачам ряд профілактичних рекомендацій.

Деякі з цих проблем перелічено нижче:

*Ключі шифрування, які зберігаються в оперативній пам'яті*

VeraCrypt зберігає ключі в оперативній пам'яті у відкритому вигляді. Теоретично, зловмисник може отримати доступ до її вмісту за допомогою так званої атаки методом холодного перезавантаження — при якій зловмисник отримує фізичний доступ до вмісту модулів оперативної пам'яті комп'ютера після його виключення і за допомогою спеціального програмного забезпечення або обладнання відновлює їх старий вміст. Подібна атака була успішно застосована до розділів диску, зашифрованих за допомогою TrueCrypt[16].

*Фізична безпека*

VeraCrypt не забезпечує безпеки даних на комп'ютері, до якого зловмисник має фізичний доступ, як правило, таємний, в процесі роботи з зашифрованими даними. Ця вразливість відноситься не у випадку втрачених, конфіскованих або викрадених комп'ютерів, а у випадку, коли зловмисники мають можливість встановити на комп'ютер той чи інший вид троянського апаратного забезпечення — апаратний Keylogger, bus-master пристрій, що володіє прямим доступом до оперативної пам'яті або якийсь інший пристрій, призначений для рішення подібних задач.

*Malware*

VeraCrypt не забезпечує безпеку даних на комп'ютері з встановленим malware. Багато шкідливих програм цього типу містять в собі keylogger та можуть, зокрема, зчитувати паролі, що вводяться з клавіатури, і передавати їх зловмисникам.

*Trusted Platform Module*

VeraCrypt не підтримує взаємодію з TPM, так як, на думку розробників, TPM не повинен використовуватись для вирішення задач інформаційної безпеки[19], оскільки TPM не забезпечує ніякого захисту комп'ютера від зловмисника, який отримав фізичний доступ до комп'ютера і, наприклад, встановив апаратний keylogger.

6. Що таке прихований том та які його способи захисту та властивості?

Принцип полягає в тому, що том VeraCrypt створюється в іншому томі VeraCrypt (у межах вільного місця на тому). Навіть коли зовнішній том встановлений, не повинно бути можливо довести, чи є в ньому прихований том чи ні, оскільки вільний простір на будь-якому томі VeraCrypt завжди заповнюється випадковими даними при створенні тому і жодна частина (демонтований) прихований том можна відрізнити від випадкових даних. Зауважте, що VeraCrypt жодним чином не змінює файлову систему (інформацію про вільний простір тощо) у зовнішньому томі.

7. Які особливості шифрування системного диска?

VeraCrypt може на льоту шифрувати системний розділ або весь системний диск, тобто розділ або диск, де встановлена Windows і з якої вона завантажується.

Системне шифрування забезпечує найвищий рівень безпеки та конфіденційності, оскільки всі файли, включаючи будь-які тимчасові файли, які Windows та програми створюють на системному розділі (як правило, без вашого відома чи згоди), файли сплячого режиму, файли обміну тощо тощо завжди є постійно зашифровані (навіть коли раптово переривається подача електроенергії). Windows також реєструє великі обсяги потенційно конфіденційних даних, таких як імена та розташування відкритих файлів, програми, які ви запускаєте тощо. Усі подібні файли журналів та записи реєстру також постійно зашифровані.

8. Що таке прихована операційна система?

Прихована операційна система - це система (наприклад, Windows 7 або Windows XP), яка встановлюється у прихованому томі VeraCrypt. Неможливо довести, що існує прихований том VeraCrypt, а отже, неможливо довести, що існує прихована операційна система.

9. Охарактеризуйте алгоритми шифрування, що використовуються у програмі?

VeraCrypt може використовувати наступні алгоритми шифрування: AES, Serpent, та Twofish. Додатково доступні 5 комбінацій цих алгоритмів: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES і Twofish-Serpent. Втілені криптографічні хеш-функції: RIPEMD-160, SHA-256, SHA-512 та Whirlpool.

10. Охарактеризуйте алгоритми хешування, що використовуються у програмі? Охарактеризуйте їх призначення?

У Майстрі створення томів, у діалоговому вікні зміни пароля та у діалоговому вікні Генератор ключових файлів ви можете вибрати алгоритм хешування. Вибраний користувачем алгоритм хешування використовується Генератором випадкових чисел VeraCrypt як псевдовипадковою функцією "змішування" та функцією виведення ключа заголовка (HMAC на основі хеш-функції, як зазначено в PKCS # 5 v2.0) як псевдовипадково функція.

На даний момент VeraCrypt підтримує такі алгоритми хешування:

* RIPEMD-160
* SHA-256
* SHA-512
* Whirlpool
* Streebog

11. Для чого використовується ключовий файл?

Ключовий файл - це файл, вміст якого поєднується з паролем (інформацію про метод, що використовується для поєднання ключового файлу з паролем.

Використання ключових файлів має деякі переваги:

* може покращити захист від атак грубої сили (суттєво, особливо якщо пароль тома не дуже надійний).
* дозволяє використовувати маркери безпеки та смарт-карти (див. нижче).
* дозволяє кільком користувачам монтувати один том, використовуючи різні паролі або pin-коди користувачів. просто надайте кожному користувачеві маркер безпеки або смарт-карту, що містить той самий файл ключів veracrypt, і дозвольте їм вибрати свій особистий пароль або pin-код, який захистить його маркер безпеки або смарт-карту.
* дозволяє керувати спільним доступом для кількох користувачів (усі власники файлів ключів повинні представити свої файли ключів, перш ніж можна буде підключити том).