**Лабораторная работа 6.**

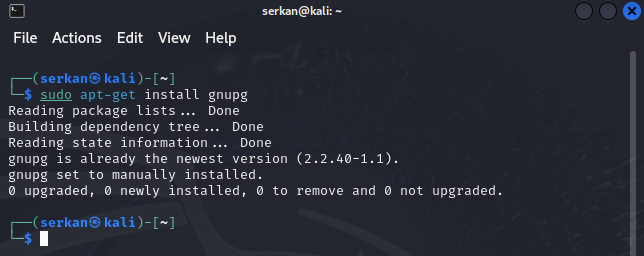
**Шифрование данных**

**Серт Серкан Группа 8**

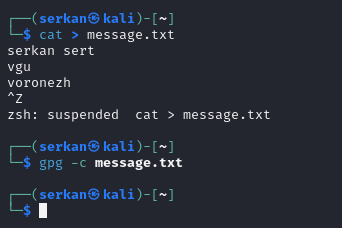
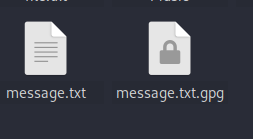
**Цель:** Получение теоретических и практических навыков работы с программными средствами шифрования данных

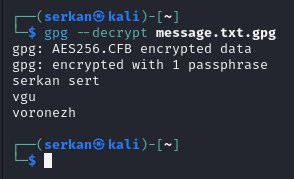
**Задания к лабораторной работе**

Установить PGP, GPG

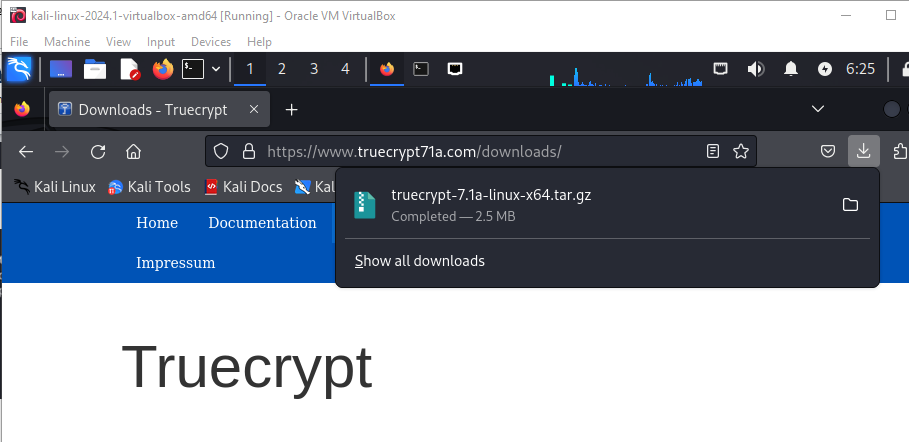


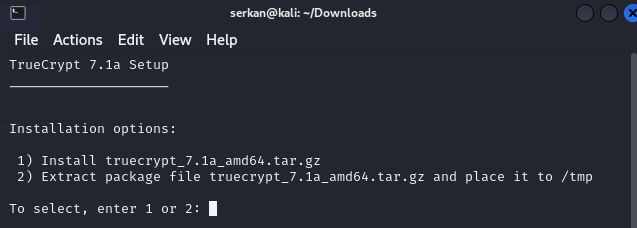
Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду . Для дешифрования (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте )

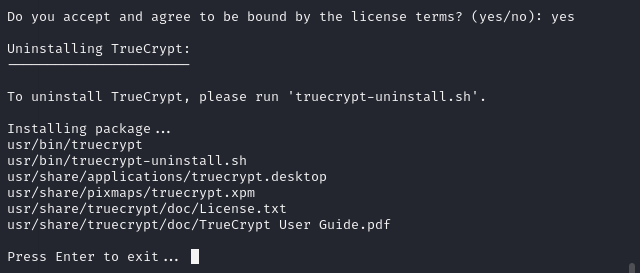


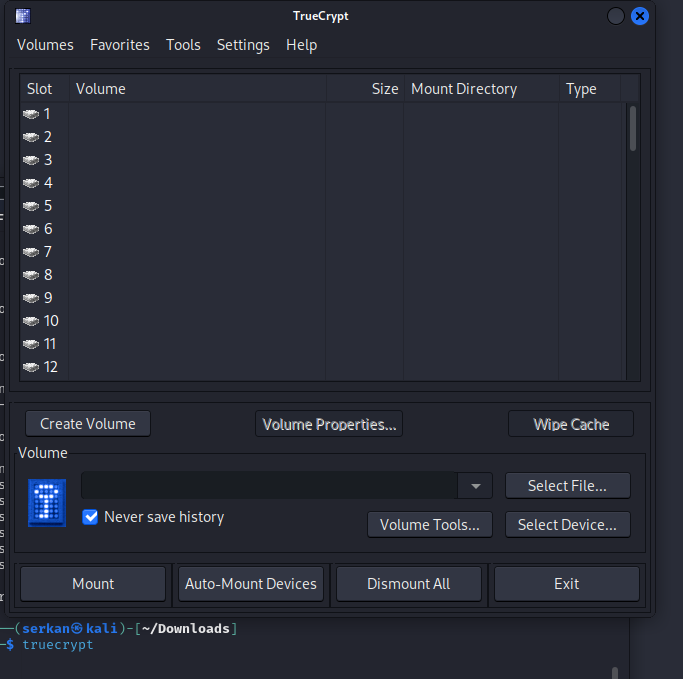


Установить TrueCrypt. Нам потребуется версия 7.1а





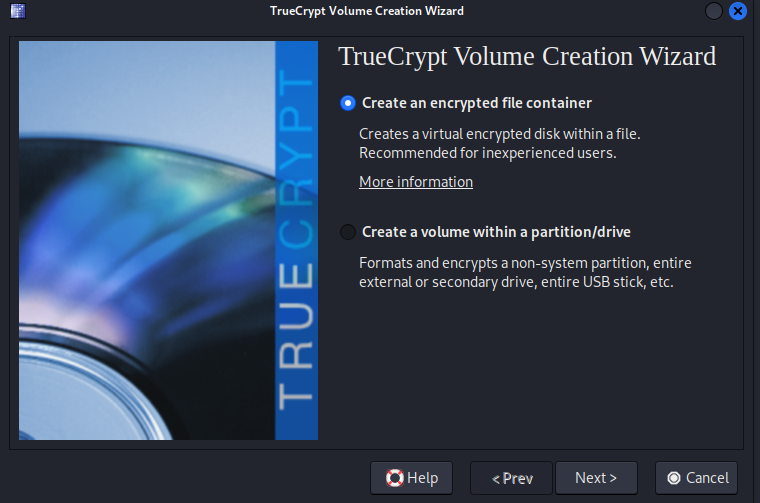




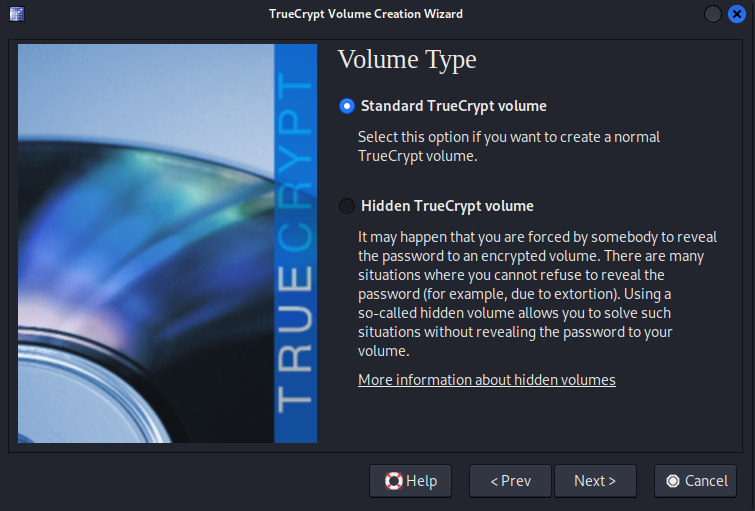
Создать криптоконтейнер, примонтировать его как виртуальный диск.

Начнем с создания криптоконтейнера. Запускаем TrueCrypt и в главном окне жмем на кнопку Create Volume.

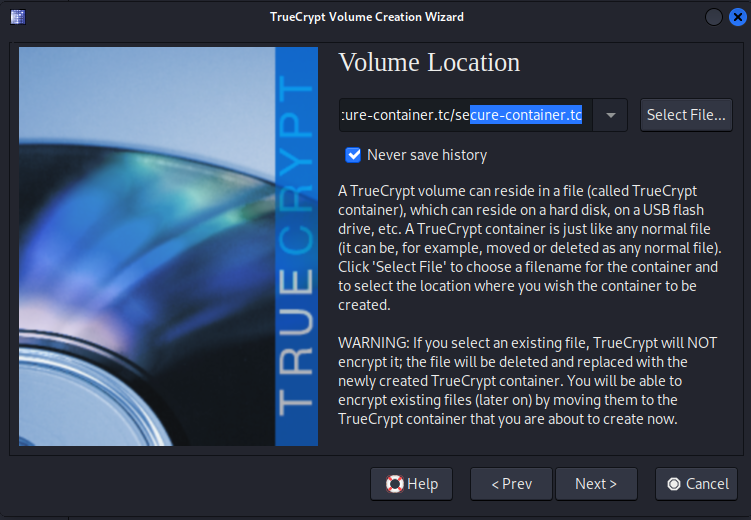
*Create an encrypted file container* – создать обычный криптоконтейнер. Нам нужен именно он.



На следующем шаге программа уточнит у вас, какой тип криптоконтейнера вы хотите создать: стандартный или скрытый. В этом курсе мы научим вас создавать скрытые криптоконтейнеры, а сейчас выберите стандартный криптоконтейнер - Standard TrueCrypt volume.



Переходим к окну выбора имени криптоконтейнера и его расположения. Жмем Select File…

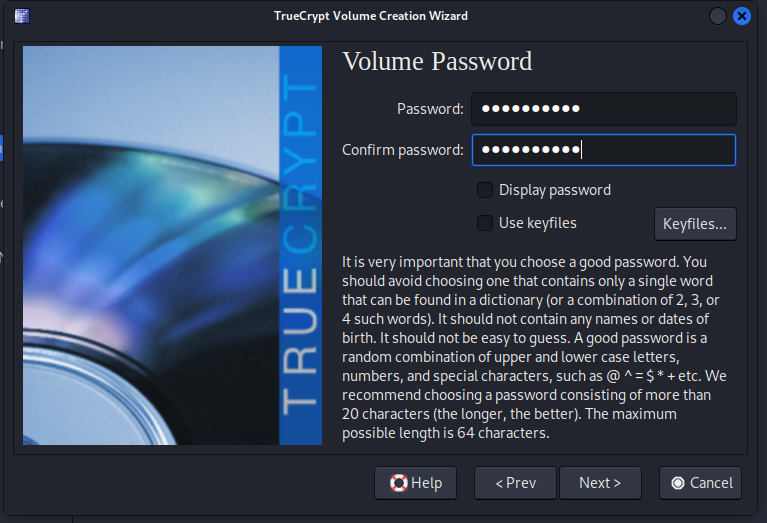


затем нажмите "Next".

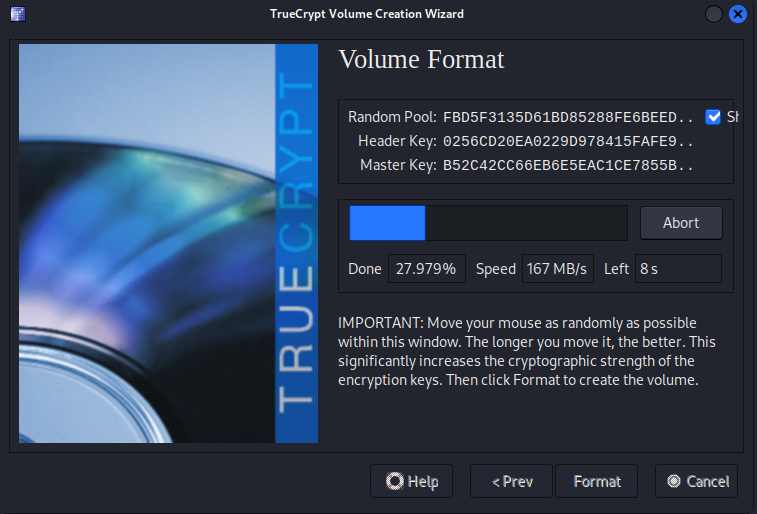
Далее система предложит вам указать объем памяти создаваемого криптоконтейнера



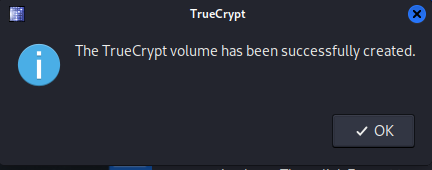
После выбора выделяемого объема памяти нам необходимо будет создать пароль для дешифрования криптоконтейнера.



затем нажмите "Next".



После настройки параметров контейнера, нажмите "Format" для создания зашифрованного контейнера.

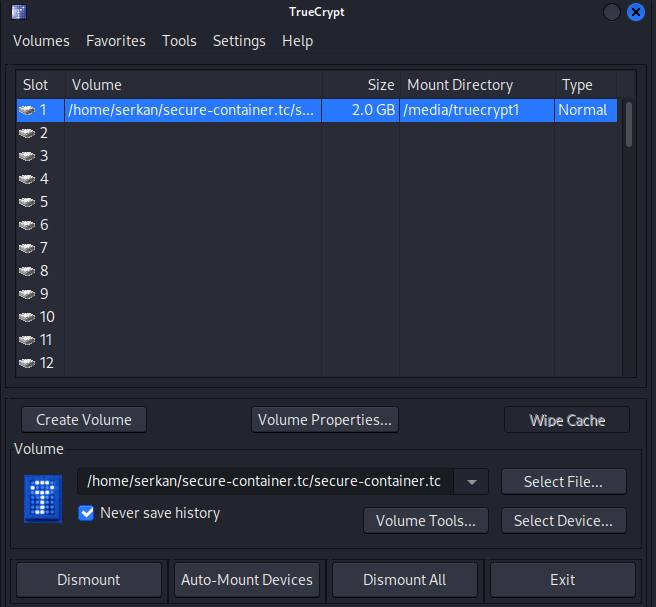


Монтируем криптоконтейнер как виртуальный диск

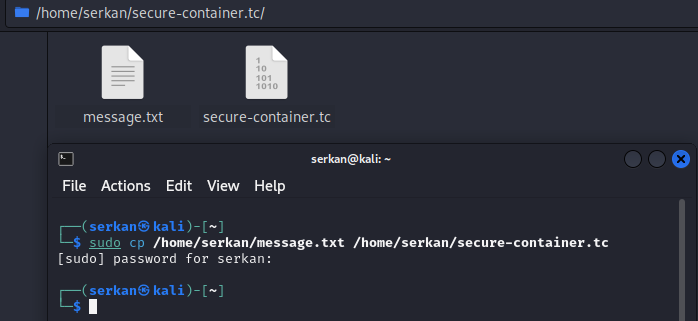
В главном окне TrueCrypt нажмите "Select File" и выберите созданный криптоконтейнер.

Нажмите "Mount" для монтирования контейнера.

Введите пароль для контейнера и нажмите "OK".

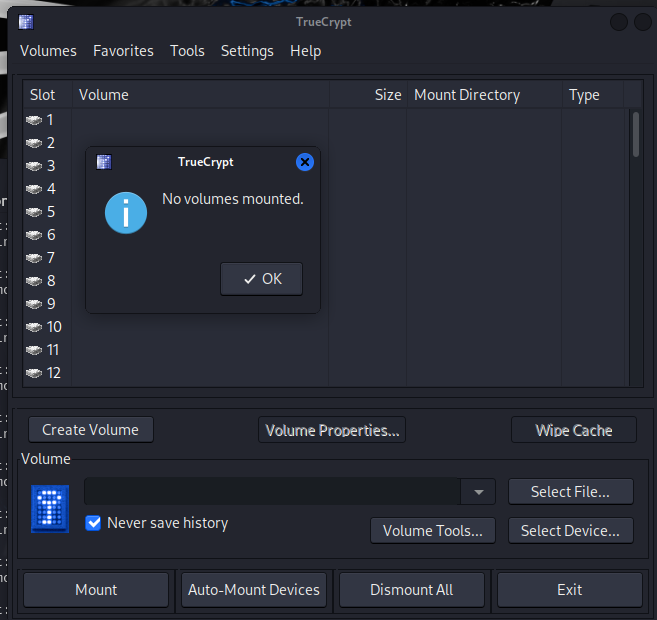


Поместить в криптоконтейнер какую-то информацию.

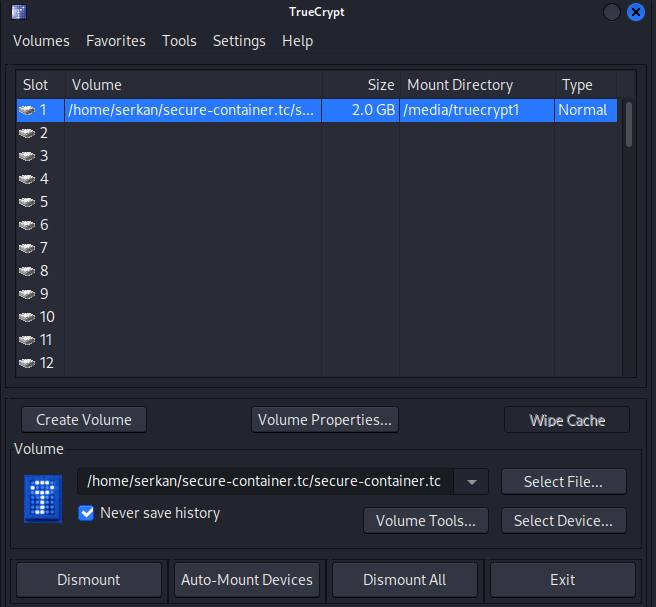


Отмонтировать диск и переместить криптоконтейнер

Открыл TrueCrypt затем Нашел примонтированный криптоконтейнер в списке. Выбрал его и нажмимал "Dismount". После этого криптоконтейнер будет отмонтирован.

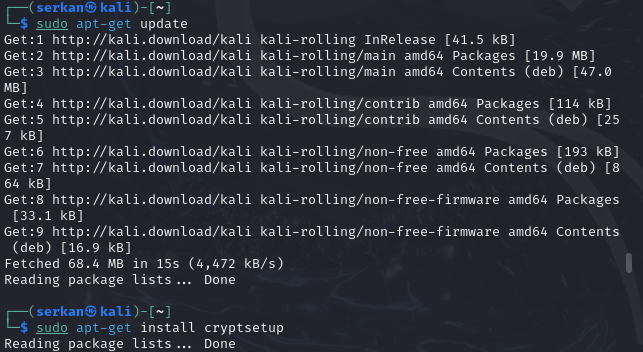


Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что криптоконтейнер может передаваться и использоваться независимо.



Установить LUKS/dm-crypt <sudo apt-get update>, <sudo apt-get install cryptsetup>.

сначала я проверил update потом установил cryptsetup



**Создаем файл, где будем хранить зашифрованные данные. Самый простой способ <fallocate -l 512M /root/test1>, где /root - директория хранения файла, test1 - имя файла. Так же для создания этого файла можно использовать команду dd. <dd if=/dev/zero of=/root/test2 bs=1M count=512>. Третий способ - использовать команду dd и заполнить файл случайными данными. <dd if=/dev/urandom of=/root/test3 bs=1M count=512>.**

**Команда fallocate быстро создает файл нужного размера, выделяя место на диске, но не записывая данные.**

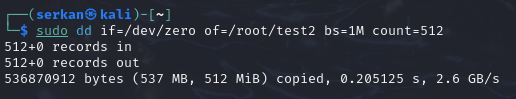
sudo fallocate -l 512M /root/test1

* **/root - директория, где будет храниться файл.**
* **test1 - имя файла.**
* **-l 512M - размер файла (512 МБ).**



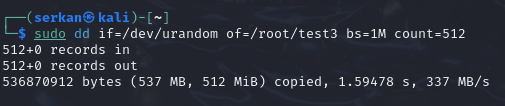
**Использование dd с заполнением нулями**

* **if=/dev/zero - входной файл, состоящий из нулевых байтов.**
* **of=/root/test2 - путь и имя создаваемого файла.**
* **bs=1M - размер блока (1 МБ).**
* **count=512 - количество блоков (512 МБ).**



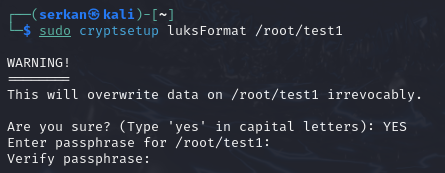
**Использование dd с заполнением случайными данными**

* **if=/dev/urandom - входной файл с генерацией случайных данных.**
* **of=/root/test3 - путь и имя создаваемого файла.**
* **bs=1M - размер блока (1 МБ).**
* **count=512 - количество блоков (512 МБ).**



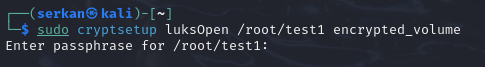
**Шаги для использования зашифрованного файла с LUKS**

**После создания файла вы можете использовать его для создания зашифрованного тома с LUKS.**

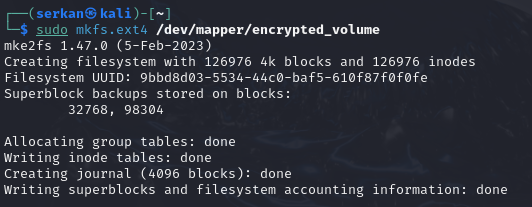


**Заменим /root/test1 на путь к нашему файлу (test2 или test3). Введим YES, чтобы подтвердить создание зашифрованного тома, и установите пароль.**

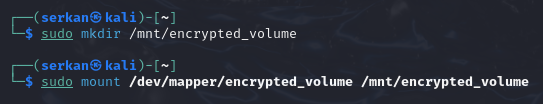
**Открываем наш файл с помощью cryptsetup luksOpen.**



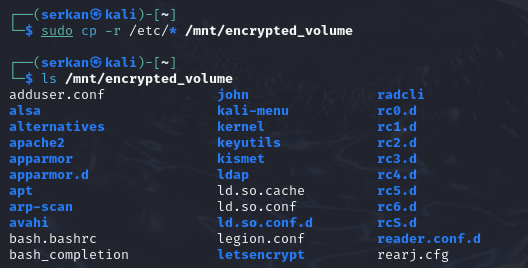
**Создаем файловую систему на зашифрованном томе**



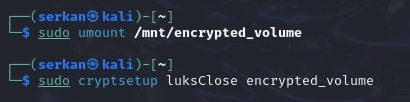
**Смонтируем зашифрованный том**



Теперь перенесем какие\_ниибудь файлы в криптоконтейнер. Например, скопируем папку /etc .



**После того как мы убедились, что файлы успешно скопированы, отмонтируйте и закроем зашифрованный том:**



**Вопросы к лабораторной работе**

1. Какие алгоритмы шифрования входят в комплект TrueCrypt?

В список поддерживаемых TrueCrypt алгоритмов шифрования входят AES, Twofish и Serpent.

1. Какие алгоритмы шифрования входят в комплект PGP, GPG?

Так симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, Blowfish, 3DES, CAST5, IDEA,Twofish, Camellia) на сеансовом ключе

1. Что такое «криптоконтейнер»?

Позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде особого файла - криптоконтейнера

1. Каковы основные достоинства и недостатки рассмотренных программных продуктов?

**PGP (Pretty Good Privacy)**

Достоинства:

* Шифрование уровня файла и сообщения: PGP позволяет шифровать отдельные файлы и электронные сообщения, обеспечивая высокий уровень безопасности.
* Цифровые подписи: Поддержка создания и проверки цифровых подписей, что обеспечивает целостность и подлинность данных.
* Переносимость: Шифрованные файлы можно легко передавать и использовать на различных платформах.
* Широкая поддержка: Поддерживается множеством почтовых клиентов и программ для шифрования файлов.

Недостатки:

* Сложность в использовании: Настройка и использование PGP может быть сложной для неподготовленных пользователей.
* Менеджмент ключей: Управление ключами и их безопасное хранение требуют значительных усилий и внимания.
* Совместимость: Возможны проблемы с совместимостью между различными реализациями PGP.

**TrueCrypt**

Достоинства:

* Простота использования: Дружелюбный интерфейс и легкость в создании и монтировании зашифрованных томов.
* Кроссплатформенность: Поддержка Windows, macOS и Linux.
* Множественные алгоритмы шифрования: Поддержка различных алгоритмов шифрования, таких как AES, Serpent и Twofish.
* Скрытые тома: Возможность создания скрытых томов для обеспечения дополнительного уровня безопасности.

Недостатки:

* Окончание поддержки: Разработка TrueCrypt была прекращена, и он не получает обновлений безопасности, что делает его потенциально уязвимым.
* Сложности с установкой: Установка и настройка TrueCrypt может быть сложной на современных системах из-за устаревших зависимостей.

**LUKS (Linux Unified Key Setup)**

Достоинства:

* Интеграция с ядром Linux: LUKS является стандартом для шифрования дисков в Linux и имеет хорошую интеграцию с системой.
* Надежность: Высокий уровень безопасности и стабильности благодаря активной поддержке и обновлениям.
* Управление ключами: Поддержка множественных ключей и их управления, что упрощает процесс изменения паролей.
* Производительность: Высокая производительность шифрования благодаря оптимизации для Linux.

Недостатки:

* Ограничение платформы: LUKS доступен только для Linux, что ограничивает его использование в многоплатформенных средах.
* Отсутствие графического интерфейса: Управление LUKS в основном осуществляется через командную строку, что может быть сложным для неподготовленных пользователей.
* Шифрование всего диска: LUKS предназначен для шифрования всего диска или раздела, что может быть избыточным для некоторых задач, требующих шифрования отдельных файлов.

**Резюме**

* PGP подходит для шифрования отдельных файлов и сообщений, особенно для пересылки данных между пользователями.
* TrueCrypt удобен для создания и использования зашифрованных томов, но его использование не рекомендуется из-за прекращения поддержки.
* LUKS является надежным решением для шифрования дисков и разделов на системах Linux, обеспечивая высокий уровень безопасности и производительности.

1. Какие алгоритмы шифрования, используемые в рассмотренных программных продуктах, наиболее надежны и почему?

AES является наиболее надежным и широко используемым алгоритмом шифрования в PGP, TrueCrypt и LUKS благодаря своей устойчивости к атакам, высокой производительности и универсальной поддержке. Twofish и Serpent также считаются надежными и используются как альтернативы, обеспечивающие высокую безопасность. RSA используется в PGP для асимметричного шифрования и также считается надежным при использовании достаточной длины ключа.

1. В каких случаях рекомендуется применять шифрование данных?

**Шифрование данных рекомендуется в любых случаях, когда необходимо защитить конфиденциальную информацию от несанкционированного доступа, утечки или кражи. Это важный инструмент для обеспечения безопасности данных как для личного использования, так и для бизнеса, государственных учреждений и других организаций.**