Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ»

Альметьевский филиал

Кафедра ЕНДиИТ

Лабораторная работа №6

по теме:

Шифрование данных.

Выполнил

студент группы 24300

Гильметдинов Инсаф Нафисович

Проверил

доцент кафедры ЕНДиИТ

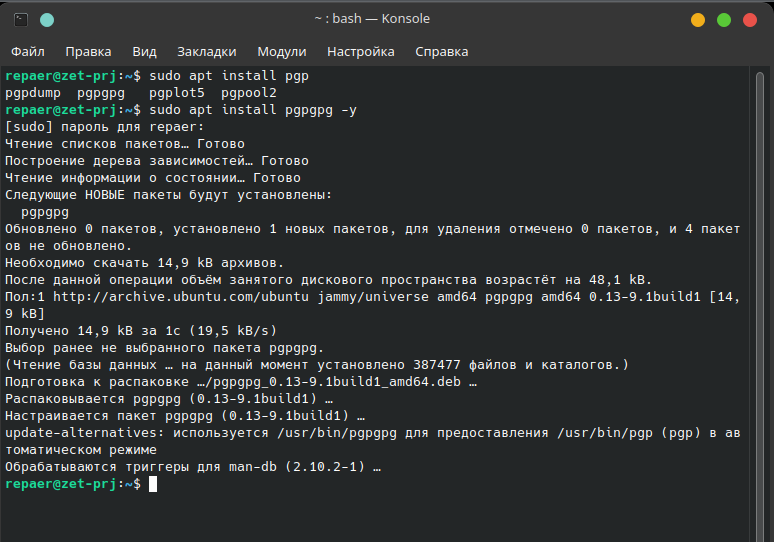
Мисбахов Рустам Шаукатович

Альметьевск 2023

Отчет о выполнении: лабораторной работы:

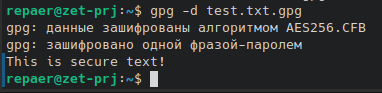
**Задания к лабораторной работе**

Установить PGP, GPG <sudo apt-get install pgpgpg>:

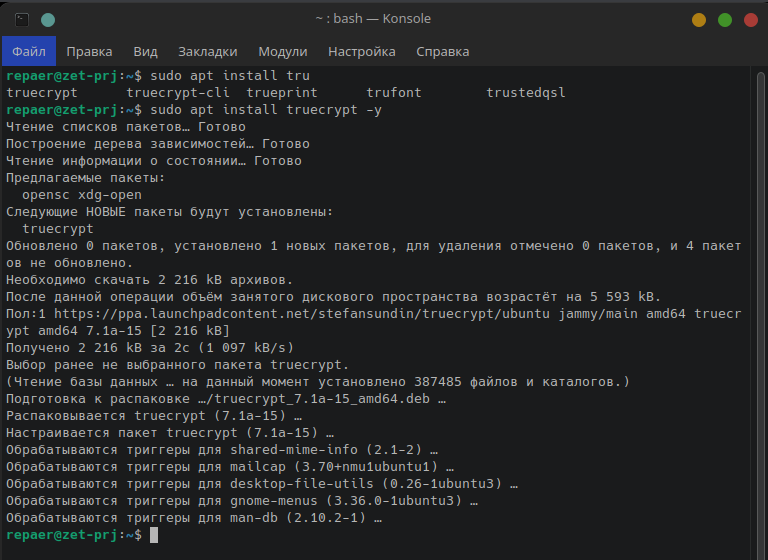


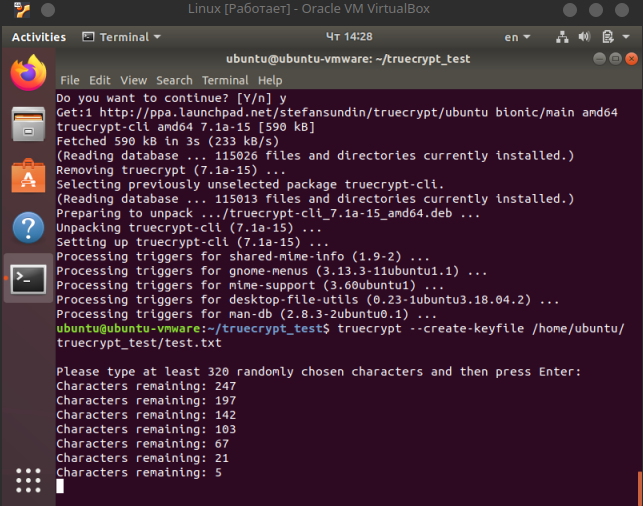
Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду <gpg -c>. Для дешифрования <gpg –decrypt-file> (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте <gpg –decrypt>):



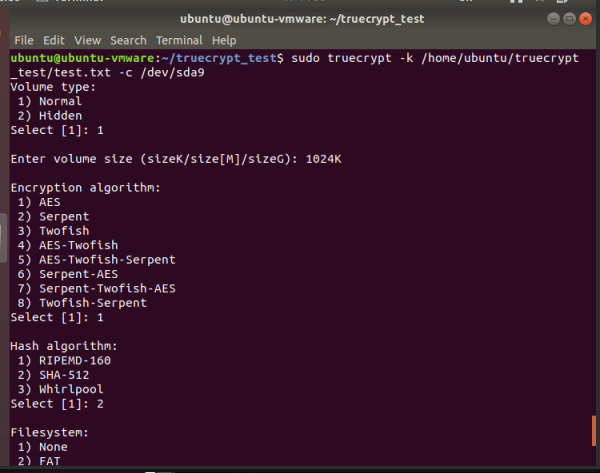


Установить TrueCrypt. Нам потребуется версия 7.1а. Скачать её можно здесь или здесь.

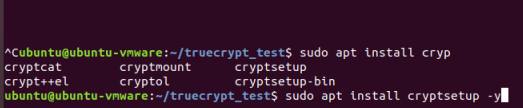




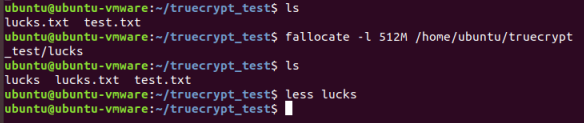




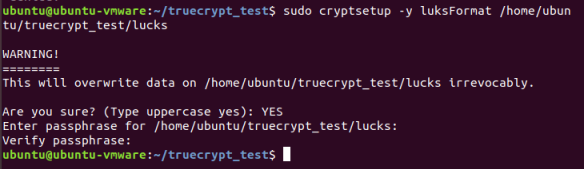
Установить LUKS/dm-crypt <sudo apt-get update>, <sudo apt-get install cryptsetup>:



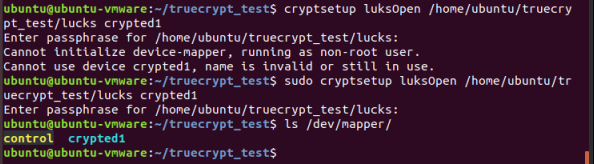
Создаем файл, где будем хранить зашифрованные данные. Самый простой способ <fallocate -l 512M /root/test1>, где /root - директория хранения файла, test1 - имя файла. Так же для создания этого файла можно использовать команду dd. <dd if=/dev/zero of=/root/test2 bs=1M count=512>. Третий способ - использовать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



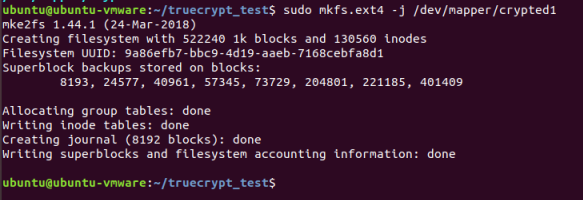
Создать криптоконтейнер. <cryptsetup -y luksFormat /root/test1> (нужно будет согласиться переписать данные и задать пароль):



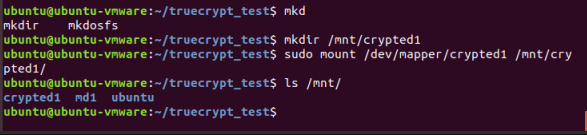
Открыть контейнер. <cryptsetup luksOpen /root/test1 crypted1>. (crypted1 - имя контейнера, его мы задаем этой командой). При этом будет создан файл /dev/mapper/crypted1:



Создать в нем файловую систему <mkfs.ext4 -j /dev/mapper/crypted1>:



Создать папку для монтирования <mkdir /mnt/files>. Монтировать <mount /dev/mapper/crypted1 /mnt/files>:



Теперь перенесем какие-нибудь файлы в криптоконтейнер. Например, скопируем папку /etc <cp -r /etc/\* /mnt/crypted1>:



Размонтировать <umount /mnt/crypted1>:



Теперь закрываем volume1. <cryptsetup luksClose crypted1>. После этого наши данные зашифрованы:



Чтобы открыть их выполним <cryptsetup luksOpen /root/lucks crypted1> и <mount /dev/mapper/crypted1 /mnt/crypted1>:

