**Шифрование данных.**

**Основные теоретические сведения**

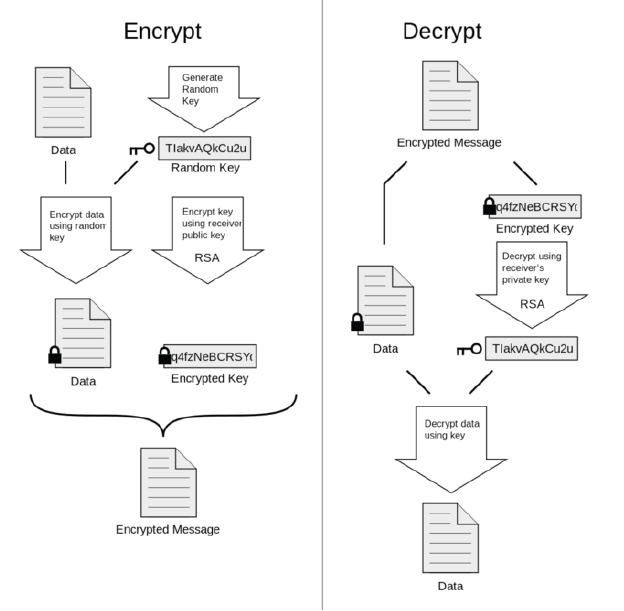
**Цель:** Получение теоретических и практических навыков работы с программными средствами шифрования данных.

**Консольные команды:**

* **gpg** <параметры> - инструмент для шифрования и цифровой подписи.
* **cryptsetup** <параметры> - программа для управления шифрованными дисковыми разделами, работающая на основе модуля ядра dm-crypt.
* **truecrypt** <параметры> - программа для управления шифрованными дисковыми разделами, при помощи truecrypt.
* **fallocate** <параметры> - команда, позволяющая вручную выделять блоки для файлов.

**PGP**

**PGP** (Pretty Good Privacy) — компьютерная программа, которая позволяет выполнять операции шифрования/дешифрования и цифровой подписи файлов или сообщений, а также другой информации, представленной в электронном виде, в том числе шифрование данных на запоминающих устройствах.



Процесс шифрования в PGP проходит в несколько этапов: хеширование, сжатие данных, шифрование с симметричным ключом, и, наконец, шифрованием с открытым ключом. Причём каждый этап может использовать разные алгоритмы. Так симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, Blowfish, 3DES, CAST5, IDEA,Twofish, Camellia) на сеансовом ключе. Сеансовый ключ в свою очередь генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Он зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal (в зависимости от исходного открытого ключа получателя).

Изначально PGP разрабатывалась для защиты электронной почты на стороне клиента, но начиная с 2002 года также включает в себя шифрование жёстких дисков, директорий, файлов, сессий программ мгновенного обмена сообщениям, защиту файлов и директорий в сетевых хранилищах, пакетной передачи файлов, а в новых версиях — шифрование HTTP-запросов и ответов на стороне сервера и клиента.

**TrueCrypt**

**TrueCrypt** — одна из самых известных программ для шифрования данных «на лету». Позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде особого файла - криптоконтейнера. С помощью TrueCrypt также можно полностью зашифровать раздел жёсткого диска или любого другого носителя информации, например, USB диск.

В процессе работы данная утилита создает на компьютере специальную защищенную область. Операционная система в свою очередь воспринимает эту область как файл или диск. Отличие между защищенным пространством TrueCrypt и обычным диском, в том, что на обычном диске данные обычно никак не защищены, а TrueCrypt шифрует данные «на лету», абсолютно незаметно для пользователей, и тем самым обеспечивает надежную защиту информации без специальных манипуляций с ней. Кроме того, в защищенной области TrueCrypt умеет размещать данные, которые будут не просто зашифрованы, но и скрыты от посторонних глаз.

TrueCrypt может создавать зашифрованный виртуальный диск:

* В файловом контейнере, что позволит легко работать с ним — копировать, переносить (в том числе на внешние устройства в виде файла), переименовывать или удалять;
* В виде зашифрованного раздела диска, что сделает работу более удобной и производительной, начиная с версии 5.0 появилась возможность шифровать системный раздел;
* Путём полного шифрования содержимого устройства, такого как USB диск (флоппи-диски перестали поддерживаться с версии 7.0).

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

Для того, чтобы получит доступ к зашифрованным данным применяется пароль (ключевая фраза), ключевой файл (один или несколько), а также их комбинации. В качестве ключевых файлов можно использовать любые доступные файлы на локальных, съёмных, сетевых дисках (при этом будут использоваться первые 1,048,576 байт) или генерировать свои собственные ключевые файлы.

Одна из интересных возможностей TrueCrypt — обеспечение двух уровней отрицания наличия зашифрованных данных, необходимого в случае вынужденного раскрытия пароля пользователем:

* Создание скрытого тома, что позволяет задать еще один пароль (или набор ключевых файлов) к обычному тому. Доступ к этим данным невозможно получить доступ с основным паролем, при этом скрытый том может иметь свою файловую систему, а располагается он в свободном пространстве основного тома.
* Ни один из томов TrueCrypt не может быть определен (тома TrueCrypt невозможно отличить от случайного набора данных, поэтому файл нельзя связать с TrueCrypt или с программой его создавшей, ни в какой форме и рамках).

У TrueCrypt есть графический интерфейс для Linux, но можно управлять шифрованием и из консоли.

* Создать файл ключа <truecrypt –create-keyfile /home/user/test/file> , где file - название файла-ключа. Учтите, что директория /home/user/test должна существовать.
* Создать криптоконтейнер <sudo truecrypt -k /home/user/test/file -c /dev/sda9>.
* Примонтировать <sudo mount /dev/mapper/truecrypt0 /mnt/crypto> Директория для монтирования (здесь /mnt/crypto) уже должна существовать.
* Размонтировать <truecrypt -d>.
* Чтобы снова получить доступ к информации, подключим контейнер <truecrypt -k /home/user/test/file /dev/sda9 /mnt/crypto>.

**LUCKS/dm-crypt**

**LUKS (Linux Unified Key Setup)** — спецификация шифрования диска (или блочного устройства), изначально предложенная для Linux, но сейчас поддерживаемая и в ряде других операционных систем. Основана на стандартной подсистеме шифрования Linux-ядра под названием dm-crypt и следующая рекомендациям TKS1/TKS2.

Особенности:

* В качестве «контейнера» используется файл. Его размер фиксирован. Возможно изменение размера.
* «Внутри» контейнера создается файловая система, любого удобного вам формата.
* При использовании - монтируется, как обычный раздел.
* Данные сохраняются по блокам, как в обычном файле/файловой системе. То есть :
  + модификация файла внутри контейнера приводит к перезаписи блоков, занимаемых этим файлом, но не всего контейнера;
  + «потеря/порча» одного блока приводит к потере информации «того-что-было-в-этом-блоке», и не более того.
  + при синхронизации контейнера «в облако» - как правило, перезаписывается не весь файл, а «модифицированная часть», что требует малого объема трафика.

В отличие от Truecrypt:

* как правило, выше скорость обработки данных (зависит от алгоритма/размера ключа);
* проще работа с ключами;
* нет механизма «двойного дна»;
* возможны проблемы при попытке использования контейнера «из другой ОС»

**Задания к практическому экзамену**

* 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](https://www.truecrypt71a.com/downloads/) или [здесь.](https://truecrypt.ch/downloads/)
* Создать криптоконтейнер, примонтировать его как виртуальный диск.
* Поместить в криптоконтейнер какую-то информацию.
* Отмонтировать диск и переместить криптоконтейнер.
* 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>.
* 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 volume1>. (volume1 - имя контейнера, его мы задаем этой командой). При этом будет создан файл /dev/mapper/volume1.
* Создать в нем файловую систему <mkfs.ext4 -j /dev/mapper/volume1>.
* Создать папку для монтирования <mkdir /mnt/files>. Монтировать <mount /dev/mapper/volume1 /mnt/files>
* Теперь перенесем какие\_ниибудь файлы в криптоконтейнер. Например, скопируем папку /etc <cp -r /etc/\* /mnt/files>.
* Размонтировать <umount /mnt/files>.
* Теперь закрываем volume1. <cryptsetup luksClose volume1>. После этого наши данные зашифрованы.
* Чтобы открыть их выполним <cryptsetup luksOpen /root/test1 volume1> и <mount /dev/mapper/volume1 /mnt/files>

**Контрольные вопросы**

1. Какие алгоритмы шифрования входят в комплект TrueCrypt?
2. Какие алгоритмы шифрования входят в комплект PGP, GPG?
3. Что такое «криптоконтейнер»?
4. Каковы основные достоинства и недостатки рассмотренных программных продуктов?
5. Какие алгоритмы шифрования, используемые в рассмотренных программных продуктах, наиболее надежны и почему?
6. В каких случаях рекомендуется применять шифрование данных?