Лабораторная работа №4

Устанавливаем LUKS (cryptsetup)

```
root@l4zzur-VirtualBox:/home/l4zzur# apt install cryptsetup
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```

Создаём 2048-битный ключ

```
root@l4zzur-VirtualBox:/home/l4zzur# dd if=/dev/urandom of=key.sdb1 bs=1024 cou
nt=2
2+0 records in
2+0 records out
2048 bytes (2,0 kB, 2,0 KiB) copied, 0,000355227 s, 5,8 MB/s
```

Делаем доступ только владельцу

```
root@l4zzur-VirtualBox:/home/l4zzur# chmod 0400 key.sdb1
```

Создаём LUKS-раздел используя внешний файл с ключом

```
root@l4zzur-VirtualBox:/home/l4zzur# cryptsetup luksFormat /dev/sdb1 key.sdb1

WARNING!
========
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
```

Связываем ключ с разделом и создаём устройство ввода-вывода для взаимодействия с разделом

```
root@l4zzur-VirtualBox:/home/l4zzur# cryptsetup luksAddKey /dev/sdb1 key.sdb1 -
-key-file=key.sdb1
root@l4zzur-VirtualBox:/home/l4zzur# cryptsetup luksOpen /dev/sdb1 secret --key
-file=key.sdb1
```

```
sdb           8:16   0     2G  0 disk
├─sdb1        8:17   0   500M  0 part
│ └─secret 253:0    0   484M  0 crypt
```

```
root@l4zzur-VirtualBox:/home/l4zzur# ls /dev/mapper/
control  secret
```

Устанавливаем eCryptfs

```
root@l4zzur-VirtualBox:/home/l4zzur# apt install ecryptfs-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  keyutils libecryptfs1
Suggested packages:
```

Создаём пустой каталог и шифруем его

```
root@l4zzur-VirtualBox:/home/l4zzur# mkdir /mnt/ecryptfs-demo
root@l4zzur-VirtualBox:/home/l4zzur# mount -t ecryptfs /mnt/ecryptfs-demo/ /mnt
/ecryptfs-demo/
Passphrase:
Select cipher:
 1) aes: blocksize = 16; min keysize = 16; max keysize = 32
 2) blowfish: blocksize = 8; min keysize = 16; max keysize = 56
 3) des3_ede: blocksize = 8; min keysize = 24; max keysize = 24
 4) twofish: blocksize = 16; min keysize = 16; max keysize = 32
 5) cast6: blocksize = 16; min keysize = 16; max keysize = 32
 6) cast5: blocksize = 8; min keysize = 5; max keysize = 16
Selection [aes]:
Select key bytes:
 1) 16
 2) 32
 3) 24
Selection [16]:
Enable plaintext passthrough (y/n) [n]:
Enable filename encryption (y/n) [n]:
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=0a18885753008ddb
Mounted eCryptfs
```

```
 /mnt/ecryptfs-demo on /mnt/ecryptfs-demo type ecryptfs (rw,relatime,ecryptfs_si
 g=0a18885753008ddb,ecryptfs_cipher=aes,ecryptfs_key_bytes=16,ecryptfs_unlink_si
 gs)
```

Создаём файл и меняем содержимое

```
root@l4zzur-VirtualBox:/home/l4zzur# touch /mnt/ecryptfs-demo/file1.txt
root@l4zzur-VirtualBox:/home/l4zzur# nano /mnt/ecryptfs-demo/file1.txt
```

```
  GNU nano 4.8                 /mnt/ecryptfs-demo/file1.txt
Sample Text
```

При попытке открыть копирования и чтения файла после перезагрузки получаем следующее

```
root@l4zzur-VirtualBox:/home/l4zzur# cat /mnt/ecryptfs-demo/file1.txt > file
root@l4zzur-VirtualBox:/home/l4zzur# cat file

hU◆◆<K◆"3DUfw`◆]1        ◆◆◆◆     NF◆_CONSOLE
◆WS◆◆◆◆&◆◆{?◆◆Ft◆,◆B◆J[aWA◆◆I[◆◆[g◆◆◆◆◆1V◆◆◆gG◆◆◆◆◆◆6V◆◆◆2◆wO4ξ}e◆◆Q◆◆◆]Ipl◆◆◆F
◆l˜$◆0v◆l◆◆◆s◆~◆'◆M◆I◆L&}◆◆◆◆F◆%◆F5◆◆◆$+◆&
                                        5◆◆*◆}◆$Sx◆◆◆q◆        }◆◆◆◆e~H◆◆◆◆6◆◆
◆4◆◆(◆◆◆◆6F1j◆◆ME6◆◆*:!◆,◆◆◆◆!e2◆t◆"◆◆◆D◆◆◆◆◆q◆◆◆◆Pb◆u$=q◆
                                                        ◆◆◆◆◆◆◆◆*◆s6◆;◆yy◆g◆
◆0o◆S◆z◆◆◆◆◆B◆j
              ◆c◆◆.◆◆-◆◆◆◆◆<◆;◆^=◆
                                p◆jd◆◆
                                      ◆◆wni9◆◆7◆h4-◆>◆<◆-◆◆◆◆B◆◆3f◆¼◆◆=ov◆◆T
◆◆◆D
◆8◆7◆ShH◆◆)◆f◆O◆◆◆(◆1-◆f◆◆ن{CsXz2◆◆}◆n;◆0◆8_◆◆◆◆◆◆◆◆?G@◆F◆◆◆
                                                      ◆◆O)◆◆
                                                           ◆T◆h◆◆◆◆8◆$
◆!◆h◆Cm◆n◆◆◆RBV̇K◆◆◆H<y◆2◆nW◆y◆lh◆◆◆5◆T◆◆◆◆◆◆y◆F◆◆=Y◆-P◆◆4◆◆◆X◆◆◆◆◆j◆◆a◆h◆DI`◆È
}$:P_̃Q◆8◆◆◆     1◆◆B◆W◆◆◆"◆◆2◆◆◆◆0◆◆R◆◆◆'◆{'
```

Запоминаем подпись

```
  GNU nano 4.8              /root/.ecryptfs/sig-cache.txt
0a18885753008ddb
```

Создаём файл с паролем

```
  GNU nano 4.8                        password.txt
```

Создаём файл для хранения всех необходимых данных для монтирования зашифрованного каталога

```
  GNU nano 4.8                      /root/.ecryptfsrc
key=passphrase:passphrase_passwd_file=/home/l4zzur/password.txt
ecryptfs_sid=0a18885753008ddb
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Добавляем строку в fstab

```
  GNU nano 4.8                          /etc/fstab                          Modified
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda5 during installation
UUID=913592fa-cbf0-49c8-bb14-3285dd3af600 /               ext4    errors=remou>
# /boot/efi was on /dev/sda1 during installation
UUID=1992-85BF  /boot/efi       vfat    umask=0077      0       1
/swapfile                                 none            swap    sw            >
/mnt/ecryptfs-demo /mnt/ecryptfs-demo ecryptfs defaults 0 0
```

Перезагружаем для применения

```
/mnt/ecryptfs-demo  9,3G  7,0G  1,9G  79% /mnt/ecryptfs-demo
/dev/sda1           511M  4,0K  511M   1% /boot/efi
tmpfs                98M   20K   98M   1% /run/user/1000
root@l4zzur-VirtualBox:/home/l4zzur# cat /mnt/ecryptfs-demo/file1.txt > file
root@l4zzur-VirtualBox:/home/l4zzur# cat file
Sample Text
root@l4zzur-VirtualBox:/home/l4zzur#
```