Лабораторная работа №13-14

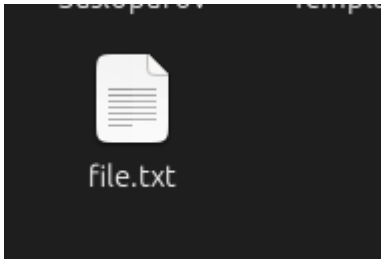
Управление файлами. Защита файлов. Шифрование.

Простейшие сценарии

1. Создать файл через терминал командой: cat > имя_файла

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cat > file.txt
```

2. Вставить текст через сочетание ctrl + shift + v В конце нажать сочетание ctrl+c для завершения работы с текстовым файлом.

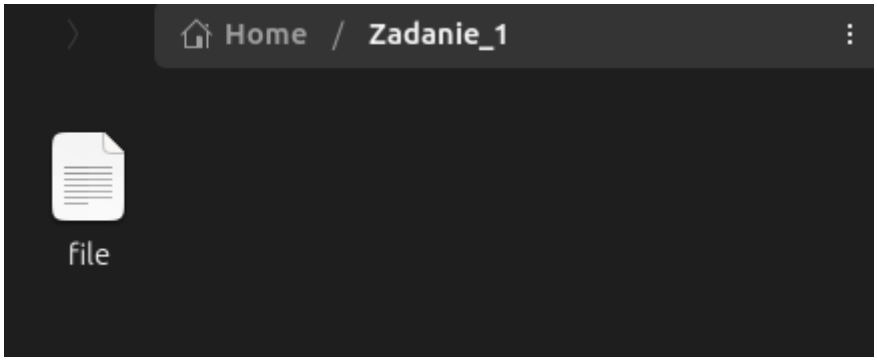


3. Создайте папку Zadanie_1 в родительской директории через команда mkdir

```
mkdir Zadanie_1
```

4. Скопируйте файл со стихом в эту директорию командой: cp имя_файла /home/имя_пользователя/Zadanie_1

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cp /home/acuioc-ubuntu/file.txt /
ubuntu/Zadanie_1
```

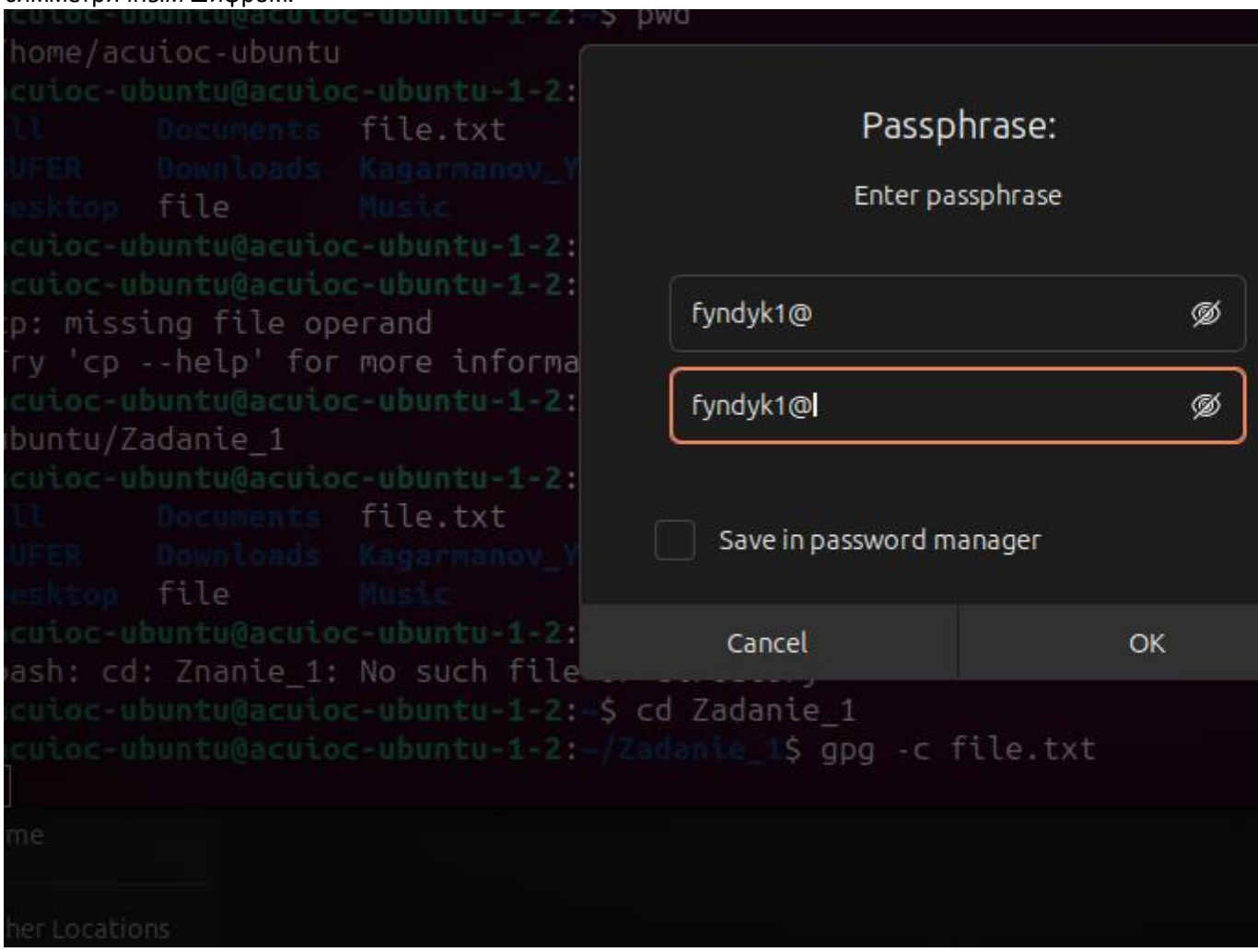


5. Перейдите в эту папку через команду cd

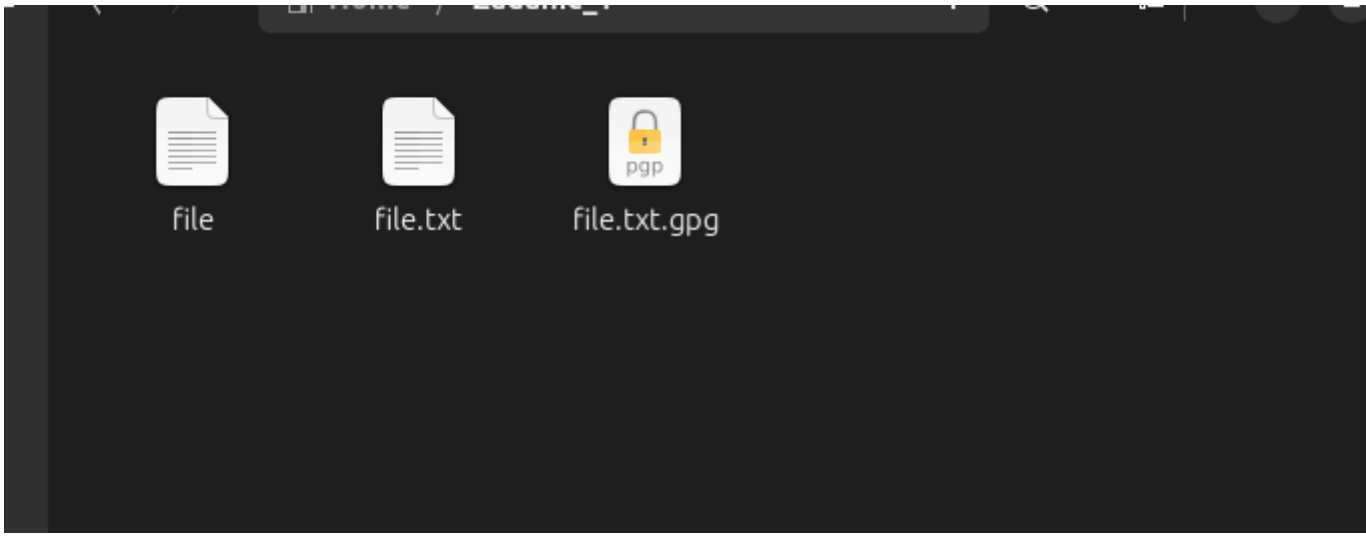
```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cd Zadanie_1
```

6. Зашифруйте файл командой: gpg –c имя_файла.txt . Система попросит задать фразу-пароль где gpg – программа для шифрования (GnuPG – GNU Privacy Guard) -c – флаг шифрования

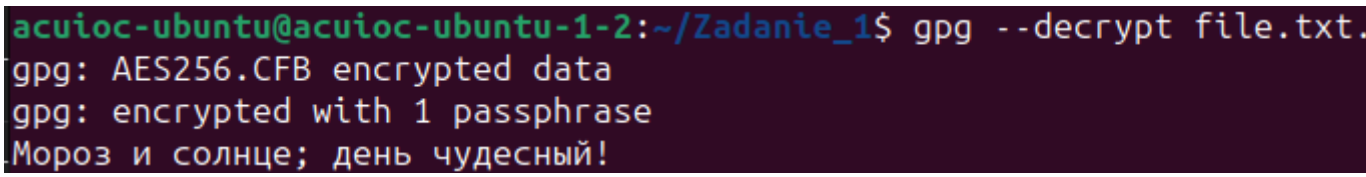
симметричным шифром.



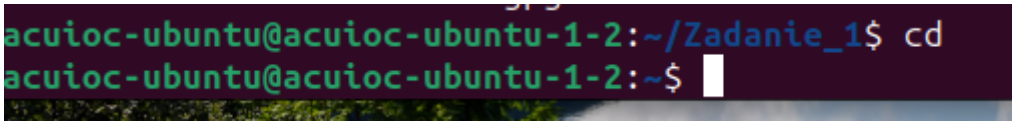
7. Проверьте созданный файл с расширение .gpg



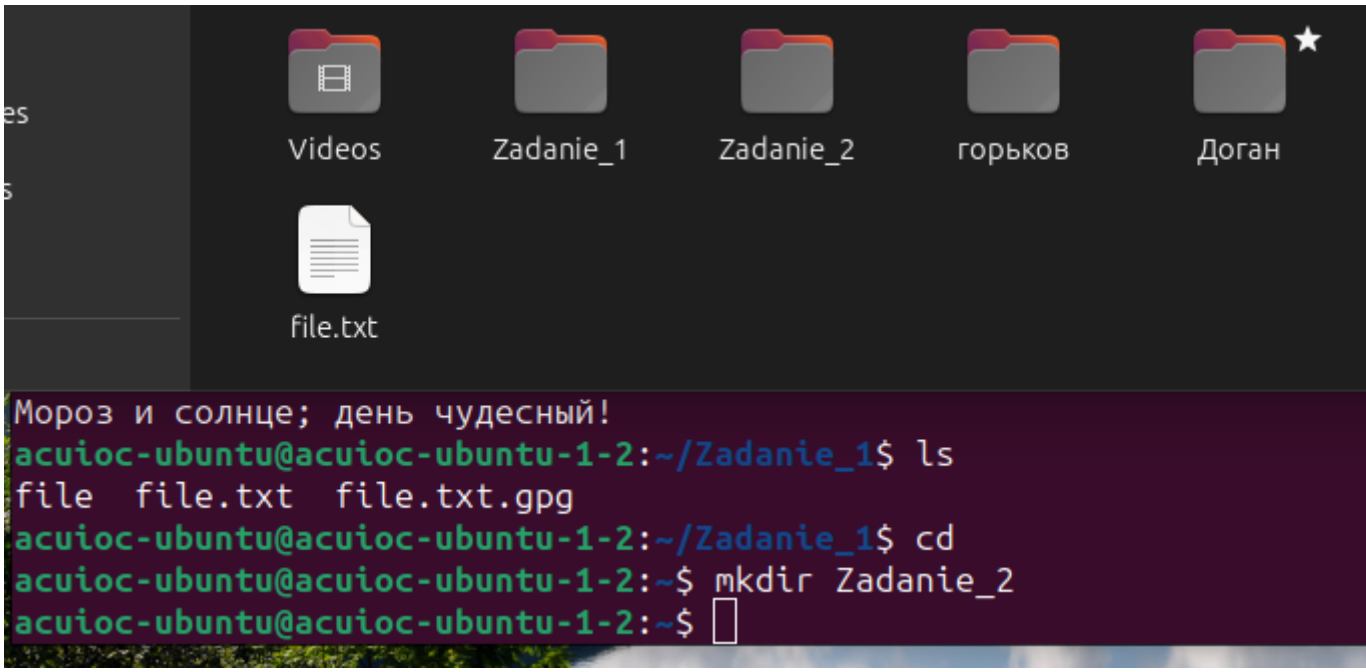
8. Теперь расшифруем файл командой gpg --decrypt имя_файла.txt.gpg. Вводим указанную фразу-пароль Шифрование файла с помощью ключей



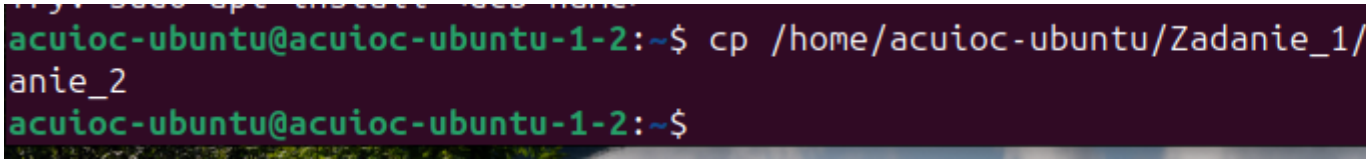
1. Вернитесь в родительскую директорию



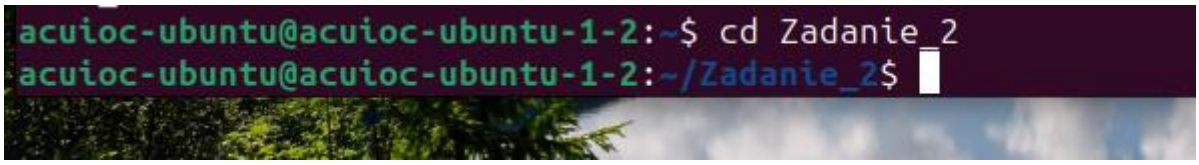
2. Создайте папку Zadanie_2 в родительской директории



3. Скопируйте файл со стихом в эту папку



4. Перейдите в эту папку



5. Создать ключи: gpg --full-generate-key Выберите: • тип ключа • размер (3072 бит) • срок действия • идентификатор пользователя = идентификатор ключа (не менее 5 символов) • комментарий После задания параметров для ключа подтвердите корректность информации и придумайте фразу-пароль. В итоге будут созданы ключи шифрования, на скриншоте RSA, 3072 бита, без срока использования. Можете проверить, что в скрытой директории ~./gnupg появились файлы с ключами. В файле pubring.gpg публичный ключ, а в secring.gpg - приватный.

```
Email address: rusik@yandex.ru
Comment: jj
You selected this USER-ID:
    "Ruslan (jj) <rusik@yandex.ru>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perf
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perf
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: directory '/home/acuioc-ubuntu/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/acuioc-ubuntu/.gnupg/op
.d/B2252BBBF94D2B22A772C3C827C5945F886751D4.rev'
public and secret key created and signed.

pub   rsa3072 2025-03-27 [SC]
      B2252BBBF94D2B22A772C3C827C5945F886751D4
uid                      Ruslan (jj) <rusik@yandex.ru>
sub   rsa3072 2025-03-27 [E]
```

6. Проверьте какие ключи у вас доступны командой: gpg -- list-key

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadanie_2$ gpg --list-key
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1
/home/acuioc-ubuntu/.gnupg/pubring.kbx
------------------------------------
pub   rsa3072 2025-03-27 [SC]
      B2252BBBF94D2B22A772C3C827C5945F886751D4
uid           [ultimate] Ruslan (jj) <rusik@yandex.ru>
sub   rsa3072 2025-03-27 [E]
```

7. Чтобы зашифровать файл с помощью ключа необходимо включить программу шифрования, атрибуты –e и –r идентификатор пользователя и имя файла.

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadanie_2$ gpg -e -r Ruslan file.
```

8. Дешифруйте файл, используя атрибут –d Использование цифровой подписи для файла Цифровая подпись — это электронная зашифрованная печать, удостоверяющая подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы.

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadanie_2$ gpg -d --decrypt file.
gpg: encrypted with 3072-bit RSA key, ID ECCCFB6C02F7C038, created
      "Ruslan (jj) <rusik@yandex.ru>"
Мороз и солнце день чудесный!
Еще ты дремлешь друг прелестный -
Пора красавица проснись:
Открой сомкнуты негой взоры
Навстречу северной Авроры
Звездою севера явись!

Вечор ты помнишь вьюга злилась
На мутном неме мгла носилась
Луна как бледное пятно
Сквозь тучи мрачные желтела
И ты печальная сидела -
А нынче... погляди в окно:

Над голубыми небесами
```

1. Вернитесь в родительскую директорию

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadanie_2$ cd
acuioc-ubuntu@acuioc-ubuntu-1-2:~$
```

2. Создайте папку Zadanie_3 в родительской директории

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ mkdir Zadamie_3
acuioc-ubuntu@acuioc-ubuntu-1-2:~$
```

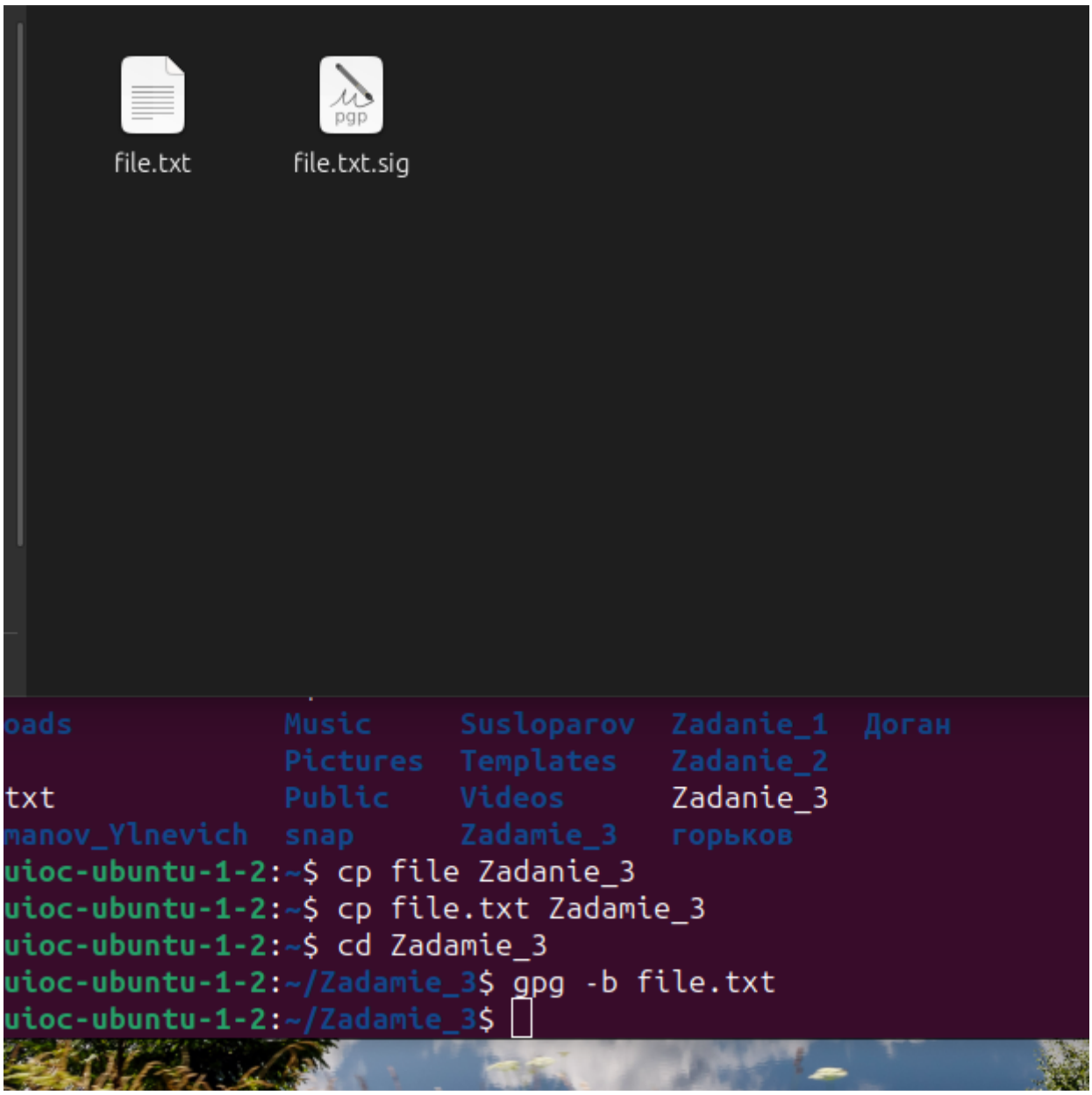
3. Скопируйте файл со стихом в эту папку

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cp file.txt Zadamie_3
```

4. Перейдите в эту папку

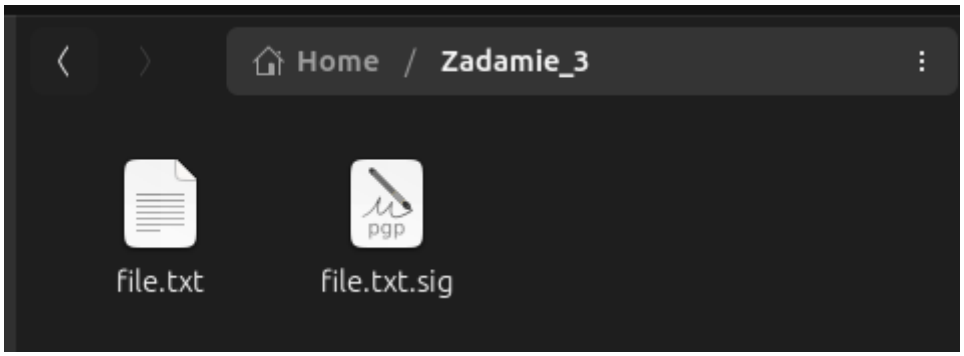
```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cd Zadamie_3
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$
```

5. Создайте цифровую подпись, по аналогии с предыдущими заданиями командой: gpg -b имя_файла



6. Придумайте фразу-пароль

7. Проверьте появился ли файл с расширением sig в папке Zadanie_3



8. Проверьте подлинность файла командой: gpg --verify имя_файла.sig имя_файла

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~$ cd Zadamie_3
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$ gpg -b file.txt
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$ gpg --vetify file.txt.s
invalid option "--vetify"
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$ gpg --verify file.txt.s
gpg: Signature made Thu 27 Mar 2025 06:02:57 AM GMT
gpg:                using RSA key B2252BBBF94D2B22A772C3C827C5945F88
gpg: Good signature from "Ruslan (jj) <rusik@yandex.ru>" [ultimate]
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$
```

В этом случае система говорит нам о том, что файл не был изменен.

9. Внесите изменения в текстовый файл, добавьте или удалите любое слово/строку/символ.

Добавлен « ». в file.txt

10. Проверьте подлинность файла еще раз

```
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$ gpg --verify file.txt
gpg: Signature made Thu 27 Mar 2025 06:02:57 AM GMT
gpg:                using RSA key B2252BBBF94D2B22A772C3C827C5945F
gpg: BAD signature from "Ruslan (jj) <rusik@yandex.ru>" [ultimate]
acuioc-ubuntu@acuioc-ubuntu-1-2:~/Zadamie_3$
```

11. Что указывает на то, что файл был изменен?

Программа выдала BAD signature

Файл был изменен