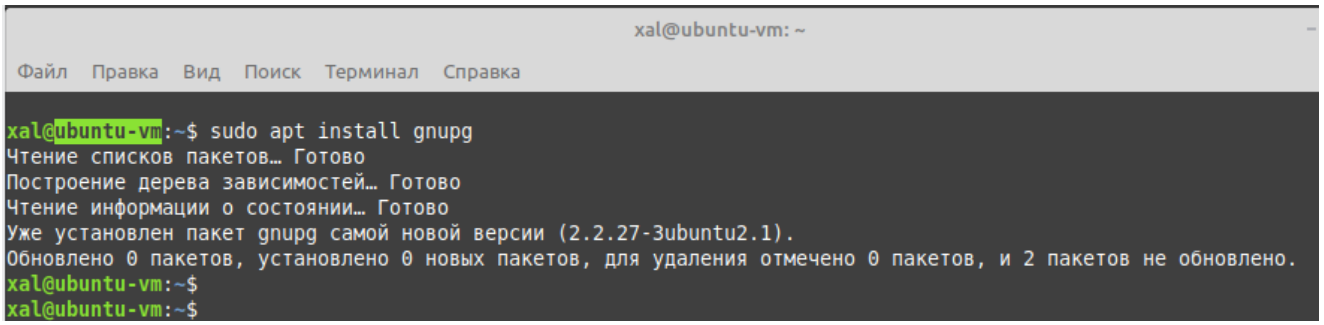
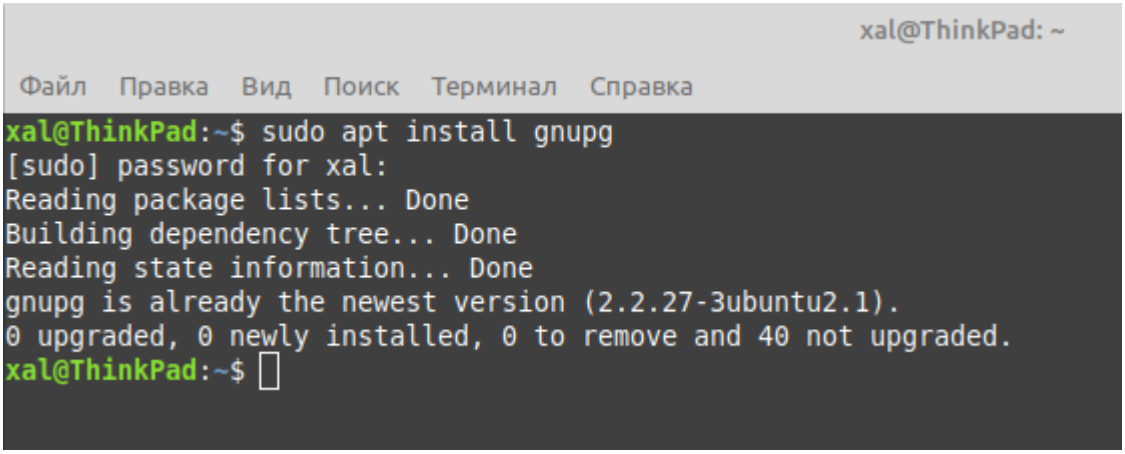
Создам, зашифрую, обменяюсь и расшифрую текстовые файлы на двух ПК (ThinkPad и ubuntu-vm).

1. Произведу установку gnupg:





У меня gnupg уже установлен «из коробки» в системах и повторной установки не требуется.

2. При попытке генерации ключа возникает проблема:

```
xal@ThinkPad:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: ThinkPad
Email address: ThinkPad@mail.ru
You selected this USER-ID:
    "ThinkPad <ThinkPad@mail.ru>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
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.
123124244142214redggf;dmenvpevepkefnpfnvpenvpenvpedmcdcdemepnvneinienvdnvxlvmcnjb nnmcvkndvd jdfnppweoweeper909u234u39
u230934093049-2394-02394-239-ri0fk3-jf-ejwf9wje9fwe-fjwe-jf-wekf=0wejfe0ighdvjdjgpofuge-ejfwjfpofjwjfew


gpg: agent_genkey failed: Timeout
Key generation failed: Timeout
```

Сперва я подумал, что нужно разогнать энтропию и принялся набирать на клавиатуре случайные символы, но оказалось, что дело в том, что ввод парольной фразы происходит при помощи скрипта **pinentry**, а по-умолчанию он пытается вывести форму на дисплей, который в переменной **$DISPLAY**, но при подключении по ssh в этой переменной пустота и процесс запроса парольной фразы прерывается по таймауту с ошибкой. Для решения проблемы необходимо генерировать ключ или находясь на самой машине, или перенастроить **pinentry**.

Для того, чтобы парольная фраза запрашивалась в терминале необходимо:

а) Создать конфиг и прописать настройку:

```
                                                    xal@ThinkPad: ~
 Файл   Правка   Вид   Поиск   Терминал   Справка
  GNU nano 6.2                                  /home/xal/.gnupg/gpg-agent.conf
pinentry-program /usr/bin/pinentry-curses
```

б) Перезагрузить агента GPG:

```
xal@ThinkPad:~$
xal@ThinkPad:~$ gpg-connect-agent reloadagent /bye
OK
xal@ThinkPad:~$
```

3. Повторяю генерацию ключей еще раз:

```
xal@ThinkPad:~$
xal@ThinkPad:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: ThinkPad
Email address: ThinkPad@mail.ru
You selected this USER-ID:
    "ThinkPad <ThinkPad@mail.ru>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
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 perform
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: key 86438F49BB43BA99 marked as ultimately trusted
gpg: directory '/home/xal/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/xal/.gnupg/openpgp-revocs.d/4B83EB123D6771BD7353E59286438F49BB43BA99.rev'
public and secret key created and signed.

pub   rsa3072 2023-10-31 [SC] [expires: 2025-10-30]
      4B83EB123D6771BD7353E59286438F49BB43BA99
uid                      ThinkPad <ThinkPad@mail.ru>
sub   rsa3072 2023-10-31 [E] [expires: 2025-10-30]
```

```
xal@ubuntu-vm:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Замечание: "gpg --full-generate-key" вызывает полнофункциональный диалог создания ключа.

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: ubuntu
Адрес электронной почты: ubuntu@mail.ru
Вы выбрали следующий идентификатор пользователя:
    "ubuntu <ubuntu@mail.ru>"

Сменить (N)Имя, (E)Адрес; (O)Принять/(Q)Выход? O
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
gpg: ключ 9D49FBDC3A2B26B5 помечен как абсолютно доверенный
gpg: создан каталог '/home/xal/.gnupg/openpgp-revocs.d'
gpg: сертификат отзыва записан в '/home/xal/.gnupg/openpgp-revocs.d/A82345D0FC84299BA87A8EF89D49FBDC3A2B26B5.rev'.
открытый и секретный ключи созданы и подписаны.

pub   rsa3072 2023-10-31 [SC] [годен до: 2025-10-30]
      A82345D0FC84299BA87A8EF89D49FBDC3A2B26B5
uid                      ubuntu <ubuntu@mail.ru>
sub   rsa3072 2023-10-31 [E] [годен до: 2025-10-30]
```

Как видим, ключи сгенерировались успешно

Обменяюсь публичными ключами между ПК:

```
xal@ThinkPad:~$ gpg --armor --export ThinkPad
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGVA0AQBDACqaRZggJGROS0nVgJwPZyayY4EolIPzREVLD3QWzXfyP309bel
E8qmWLYTNUCJR5n1mOR+YBh2kV5wdCGNfDhu5lL8+ZNduzTaPpMoFEnomuouSZBS
euf2J3B107TdIdFPfEJPmf0luFK7d9HQsBfpixjkH5yJyGPw0XR9VBzwP517R2++
AqsxqRiq8Fn2QMnDE9KIs1cc2d/8QLsYOkYAa2/gy+gAzm8H8Wyq7t73Bsy7woY1
8DNXf4BQLWtIB9/iuo0J+EiUAqpOW1Tu4VdXSEwcsd6EVCvu9ku+xOMY2q/HklfE
```

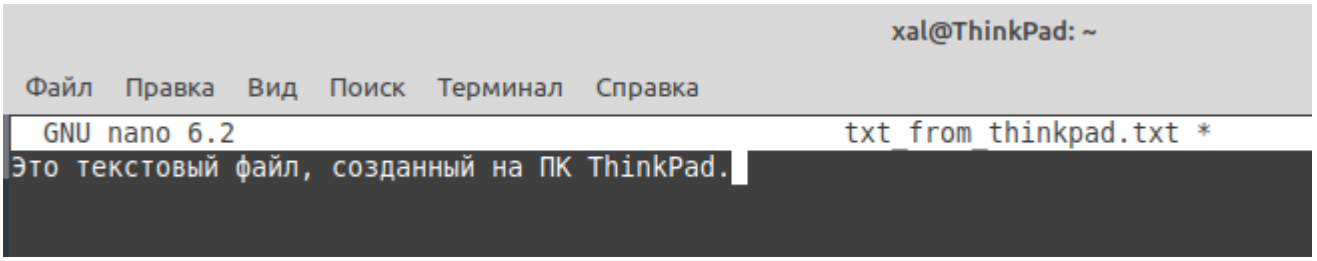
```
xal@ubuntu-vm:~$ nano public_gpg_key_from_thinkpad
xal@ubuntu-vm:~$ gpg --import public_gpg_key_from_thinkpad
gpg: ключ 86438F49BB43BA99: импортирован открытый ключ "ThinkPad <ThinkPad@mail.ru>"
gpg: Всего обработано: 1
gpg:               импортировано: 1
xal@ubuntu-vm:~$
```

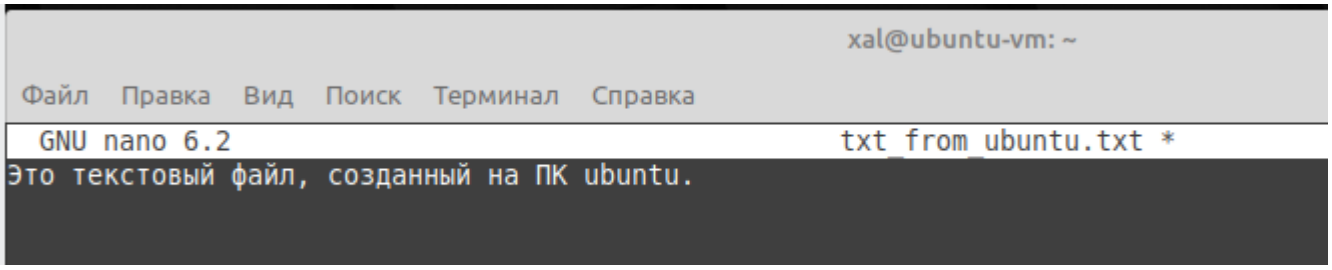
```
xal@ubuntu-vm:~$ gpg --armor --export ubuntu
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGVA1m8BDACvtv/dwO8rLSuCvPDshhLDV8uOW+zSHk5gvqx2XPLVNLreLoPh
Ew+g4ZWHI1rOBmuRnn2z4UFmPJjuTqh+zZD7rTZxDV3LZ7glTR8NZjIBopZEkrKj
of6cIS/+ry8vp3A+iS/lFjqHeSsjqJxGRcEWHNhh1E1BunTjtNpVB+3+L7XW+INz
AD82IDP57z4YRcj7bZu3jpOmgB0jGqlU4p5/dcjQj8LLiJf3JdFuM15/1PhIfK88
/icYw2lz5KeN52tE2q0SiIKPmjfBGQoIH0u3S4FNqpVlc5Lh0DDNAt6lHpvIbniC
HJF6UcSgXas65mo59EaVbj0jMB+Wc8Lip5Cy6fswyRTRQaghT/+H/38LKNfO6I29
```

```
xal@ThinkPad:~$ nano public_key_from_ubuntu
xal@ThinkPad:~$ gpg --import public_key_from_ubuntu
gpg: key 9D49FBDC3A2B26B5: public key "ubuntu <ubuntu@mail.ru>" imported
gpg: Total number processed: 1
gpg:               imported: 1
xal@ThinkPad:~$
```

4. Создаю текстовые файлы на обоих ПК:





Шифрую:

```
xal@ThinkPad:~$ gpg -e -r 'ubuntu' --output txt_from_thinkpad.txt.enc txt_from_thinkpad.txt
gpg: F21C8DD8A5160454: There is no assurance this key belongs to the named user

sub  rsa3072/F21C8DD8A5160454 2023-10-31 ubuntu <ubuntu@mail.ru>
 Primary key fingerprint: A823 45D0 FC84 299B A87A  8EF8 9D49 FBDC 3A2B 26B5
      Subkey fingerprint: CF1F B32C 1D05 12FF 4BA4  53C6 F21C 8DD8 A516 0454

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
xal@ThinkPad:~$
xal@ThinkPad:~$
xal@ThinkPad:~$
xal@ThinkPad:~$ cat txt_from_thinkpad.txt.enc
                                                
```

5. Перенесу файлы с ПК на ПК.

Т.к. у ПК ThinkPad и ПК ubuntu-vm нет связи по ssh, то воспользуюсь своим основным компьютером, у которого есть все доступы:

```
xal@xal-Swift-SF314-43: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
xal@xal-Swift-SF314-43:~$ scp xal@192.168.88.113:/home/xal/txt_from_thinkpad.txt.enc ~
scp xal@192.168.88.21:/home/xal/txt_from_ubuntu.txt.enc  ~

scp txt_from_thinkpad.txt.enc xal@192.168.88.21:/home/xal/
scp txt_from_ubuntu.txt.enc xal@192.168.88.113:/home/xal/
txt_from_thinkpad.txt.enc                                     100%  546    14.8KB/s   00:00
txt_from_ubuntu.txt.enc                                       100%  540   832.1KB/s   00:00
txt_from_thinkpad.txt.enc                                     100%  546   817.4KB/s   00:00
txt_from_ubuntu.txt.enc                                       100%  540   741.6KB/s   00:00
xal@xal-Swift-SF314-43:~$
```

Файлы на месте:

```
xal@ThinkPad:~$ ls
11.png   Documents  hw_k8s    Music     Public  Templates             txt_from_thinkpad.txt.enc  uurrll
Desktop  Downloads  minikube  Pictures  snap    txt_from_thinkpad.txt  txt_from_ubuntu.txt.enc   Videos
xal@ThinkPad:~$
```

```
xal@ubuntu-vm:~$ ls
 archive          docker_test   id_rsa.pub  'Postman Agent'       Templates                txt_from_ubuntu.txt.enc
 bash-script.sh   Documents     mbox         Public                tmp                      Videos
 dead.letter      Downloads     Music       'Skvoznaya zadacha'    txt_from_thinkpad.txt.enc
 Desktop          id_rsa        Pictures     snap                  txt_from_ubuntu.txt
xal@ubuntu-vm:~$
```

6. Теперь, когда публичные ключи есть на обоих ПК:

```
xal@ThinkPad:~$ gpg --list-keys
/home/xal/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-10-31 [SC] [expires: 2025-10-30]
      4B83EB123D6771BD7353E59286438F49BB43BA99
uid           [ultimate] ThinkPad <ThinkPad@mail.ru>
sub   rsa3072 2023-10-31 [E] [expires: 2025-10-30]

pub   rsa3072 2023-10-31 [SC] [expires: 2025-10-30]
      A82345D0FC84299BA87A8EF89D49FBDC3A2B26B5
uid           [ unknown] ubuntu <ubuntu@mail.ru>
sub   rsa3072 2023-10-31 [E] [expires: 2025-10-30]
```

```
xal@ubuntu-vm:~$ gpg --list-keys
/home/xal/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-10-31 [SC] [годен до: 2025-10-30]
      A82345D0FC84299BA87A8EF89D49FBDC3A2B26B5
uid           [  абсолютно ] ubuntu <ubuntu@mail.ru>
sub   rsa3072 2023-10-31 [E] [годен до: 2025-10-30]

pub   rsa3072 2023-10-31 [SC] [годен до: 2025-10-30]
      4B83EB123D6771BD7353E59286438F49BB43BA99
uid           [ неизвестно ] ThinkPad <ThinkPad@mail.ru>
sub   rsa3072 2023-10-31 [E] [годен до: 2025-10-30]
```

Попробую расшифровать файлы:

```
xal@ThinkPad:~$ gpg -d -o txt_from_ubuntu.txt txt_from_ubuntu.txt.enc
```

```
Please enter the passphrase to unlock the OpenPGP secret key:
"ThinkPad <ThinkPad@mail.ru>"
3072-bit RSA key, ID 90137C5E3E4C9EC8,
created 2023-10-31 (main key ID 86438F49BB43BA99).


Passphrase: *******

        <OK>                                    <Cancel>
```

```
gpg: encrypted with 3072-bit RSA key, ID 90137C5E3E4C9EC8, created 2023-10-31
      "ThinkPad <ThinkPad@mail.ru>"
xal@ThinkPad:~$ cat txt_from_ubuntu.txt
Это текстовый файл, созданный на ПК ubuntu.
xal@ThinkPad:~$
```

Та же история и на втором ПК:

```
xal@ubuntu-vm:~$ gpg -d -o txt_from_thinkpad.txt txt_from_thinkpad.txt.enc
gpg: зашифровано 3072-битным ключом RSA с идентификатором F21C8DD8A5160454, созданным 2023-10-31
      "ubuntu <ubuntu@mail.ru>"
xal@ubuntu-vm:~$ cat txt_from_thinkpad.txt
Это текстовый файл, созданный на ПК ThinkPad.
xal@ubuntu-vm:~$
```