

Шифрование и расшифрование файлов

1. Установка GnuPG в разных системах.

```
user@user-Lenovo: ~  
user@user-Lenovo:~$ gpg --version  
gpg (GnuPG) 2.2.27  
libgcrypt 1.9.4  
Copyright (C) 2021 Free Software Foundation, Inc.  
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/user/.gnupg  
Поддерживаются следующие алгоритмы:  
С открытым ключом: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Симметричные шифры: IDEA, 3DES, CAST5, BLOWFISH,  
AES, AES192, AES256, TWOFISH, CAMELLIA128,  
CAMELLIA192, CAMELLIA256  
Хеш-функции: SHA1, RIPEMD160, SHA256, SHA384, SHA512,  
SHA224  
Алгоритмы сжатия: Без сжатия, ZIP, ZLIB,  
BZIP2  
user@user-Lenovo:~$
```

```
ubuntu@ubuntu-VirtualBox: ~  
ubuntu@ubuntu-VirtualBox:~$ gpg --version  
gpg (GnuPG) 2.2.27  
libgcrypt 1.9.4  
Copyright (C) 2021 Free Software Foundation, Inc.  
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/ubuntu/.gnupg  
Поддерживаются следующие алгоритмы:  
С открытым ключом: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Симметричные шифры: IDEA, 3DES, CAST5, BLOWFISH,  
AES, AES192, AES256, TWOFISH, CAMELLIA128,  
CAMELLIA192, CAMELLIA256  
Хеш-функции: SHA1, RIPEMD160, SHA256, SHA384, SHA512,  
SHA224  
Алгоритмы сжатия: Без сжатия, ZIP, ZLIB,  
BZIP2  
ubuntu@ubuntu-VirtualBox:~$
```

2. Создание пары ключей №1.

```
user@user-Lenovo: ~  
user@user-Lenovo:~$ 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: Ignat Ilyukhin  
Адрес электронной почты: ignatilyukhin@gmail.com  
Вы выбрали следующий идентификатор пользователя:  
"Ignat Ilyukhin <ignatilyukhin@gmail.com>"  
  
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 C5D2616AF34CD570 помечен как абсолютно доверенный  
gpg: создан каталог '/home/user/.gnupg/openpgp-revocs.d'  
gpg: сертификат отзыва записан в '/home/user/.gnupg/openpgp-revocs.d/5450E080E2AEF186244281FBC5D2616AF34CD570.rev'.  
открытый и секретный ключи созданы и подписаны.  
  
pub   rsa3072 2023-11-04 [SC] [годен до: 2025-11-03]  
      5450E080E2AEF186244281FBC5D2616AF34CD570  
uid           Ignat Ilyukhin <ignatilyukhin@gmail.com>  
sub   rsa3072 2023-11-04 [E] [годен до: 2025-11-03]  
  
user@user-Lenovo:~$
```

3. Создание пары ключей №2 с другой почтой.

```
ubuntu@ubuntu-VirtualBox: ~  
ubuntu@ubuntu-VirtualBox:~$ 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.  
  
gpg: создан каталог '/home/ubuntu/.gnupg'  
gpg: создан чит с ключами '/home/ubuntu/.gnupg/pubring.kbx'  
Замечание: "gpg --full-generate-key" вызывает полнофункциональный диалог создания ключа.  
  
GnuPG должен составить идентификатор пользователя для идентификации ключа.  
  
Ваше полное имя: Ignat Ilyukhin  
Адрес электронной почты: ignat-ilyukhin@yandex.ru  
Вы выбрали следующий идентификатор пользователя:  
"Ignat Ilyukhin <ignat-ilyukhin@yandex.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: /home/ubuntu/.gnupg/trustdb.gpg: создана таблица доверия  
gpg: ключ 4FC48B5E3240B271 помечен как абсолютно доверенный  
gpg: создан каталог '/home/ubuntu/.gnupg/openpgp-revocs.d'  
gpg: сертификат отзыва записан в '/home/ubuntu/.gnupg/openpgp-revocs.d/DDCCF7BA9DB1F1D214E691BD4FC48B5E3240B271.rev'.  
открытый и секретный ключи созданы и подписаны.  
  
pub   rsa3072 2023-11-04 [SC] [годен до: 2025-11-03]  
      DDCCF7BA9DB1F1D214E691BD4FC48B5E3240B271  
uid           Ignat Ilyukhin <ignat-ilyukhin@yandex.ru>  
sub   rsa3072 2023-11-04 [E] [годен до: 2025-11-03]  
  
ubuntu@ubuntu-VirtualBox:~$
```

```
user@user-Lenovo: ~/Документы
user@user-Lenovo:~/Документы$ gpg -d -o original_msg_Ubuntu.txt encrypted_msg_UbuntuVB.txt.enc
gpg: зашифровано 3072-битным ключом RSA с идентификатором 05F38AAEF6F97ADE, созданным 2023-11-04
"Ignat Ilyukhin <ignatilyukhin@gmail.com>"
user@user-Lenovo:~/Документы$ ll
итого 20
drwxr-xr-x  2 user user 4096 ноя  4 21:49 ./
drwxr-xr-x 20 user user 4096 ноя  4 21:24 ../
-rw-rw-r--  1 user user 546 ноя  4 21:46 encrypted_msg_UbuntuVB.txt.enc
-rw-r--r--  1 root root  41 окт 19 20:46 Git token.txt
-rw-rw-r--  1 user user  67 ноя  4 21:49 original_msg_Ubuntu.txt
user@user-Lenovo:~/Документы$ cat original_msg_Ubuntu.txt
This message was created for encryption on the Ubuntu_VB machine.
```