

Система PGP

Основы информационной безопасности

Мишина А. А. НПИбд-02-22

02 мая 2024

PGP (Pretty Good Privacy) - 1991 г.

- Секретность
- Установление подлинности
- Удобство



Рис. 1: Филипп Циммерман

- Наличие открытого и закрытого ключа.
- Возможность кодирования и подписи файлов.
- Сертификат ключа - идентификатор пользователя, ключ, дата создания.
- Keyring - хранилище пар ключей, сертификатов.

- GPG – GNU Privacy Guard
- Бесплатный аналог PGP

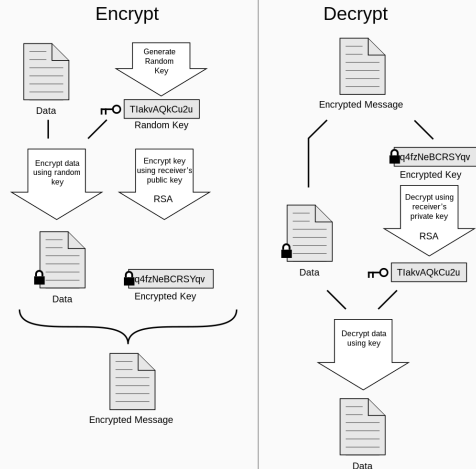


Рис. 2: Общая схема шифрования и дешифрования

```
aamishina@server:~$ sudo apt update
Сущ:1 http://ports.ubuntu.com/ubuntu-ports noble InRelease
Сущ:2 http://ports.ubuntu.com/ubuntu-ports noble-updates InRelease
Сущ:3 http://ports.ubuntu.com/ubuntu-ports noble-backports InRelease
Сущ:4 http://ports.ubuntu.com/ubuntu-ports noble-security InRelease
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
aamishina@server:~$ sudo apt install pgpgpg
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  pgpgpg
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 16,5 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 93,2 kB.
Пол:1 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 pgpgpg arm64 0.13-12 [16,5 kB]
Получено 16,5 kB за 0с (89,4 kB/s)
Выбор ранее не выбранного пакета pgpgpg.
(Чтение базы данных ... на данный момент установлено 166524 файла и каталога.)
Подготовка к распаковке ./pgpgpg_0.13-12_arm64.deb ...
Распаковывается pgpgpg (0.13-12) ...
Настраивается пакет pgpgpg (0.13-12) ...
update-alternatives: используется /usr/bin/pgpgpg для предоставления /usr/bin/pgp
р (pgp) в автоматическом режиме
Обрабатываются триггеры для man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.
```

Рис. 3: Установка GPG

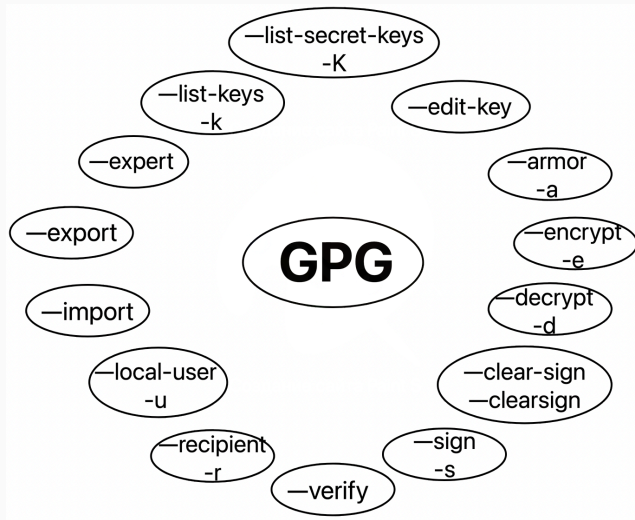


Рис. 4: Опции gpg

Генерация ключей

```
aanishina@server:~/first$ gpg --full-generate-key
gpg (GnuPG) 2.4.4; Copyright (C) 2024 g10 Code GmbH
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
  (9) ECC (sign and encrypt) *default*
  (10) ECC (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
    0 = key does not expire
    <n> = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0) 14
Key expires at Бс 12 мая 2024 19:41:47 UTC
Is this correct? (y/N) y

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

Real name: Nastya
Email address: nastya@gmail.com
Comment:
You selected this USER-ID:
    "Nastya <nastya@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
```

Рис. 5: Создание пары ключей

```
public and secret key created and signed.  
  
pub    rsa2048 2024-04-28 [SC] [expires: 2024-05-12]  
        E2E27AC8DC84DC38CA9183EC0648F9A2650556F2  
uid          Nastya <nastya@gmail.com>  
sub    rsa2048 2024-04-28 [E] [expires: 2024-05-12]  
  
aamishina@server:~/first$
```

Рис. 6: Состав ключа


```
aamishina@server:~/first$ gpg --export --armor Nastya > public.key
aamishina@server:~/first$ cat public.key
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBGYupokBCADj0jifPsXGzwQCw+YUDjL0dvrD8MSXe0jj0rc/hlWXZJPsfgo
DCozsUBS3wY+xgn/xhYBsHr1eZD0ehG19zAke4vPUi4vT2EGhhe4piHe/GHA7+Y
xNLw09uKb0LxYAiZzUmgSgF6eKSIQIasltf2sF0bNQYx3sm/V695QxHsm0bVS
STkVctblR6PvOdQex/iwTLQUjyLnXjq2Xdwb9FNqU+1raGuPOB63BEDkuyjQPhrX
5yPC+Im2MDEc/urb3k+sXZ8eu6S9ki4zvHJkGenowDJNHiP1Gnc3Qp7urKQ0/Sw6
OsW0uB+uoB9qgEM0DE2MAwIofv2L9FcoRNmHABEBAAG0GUShc3R5SVA8bmFzdHlh
QGdtYWlsLmNvbT6JAVcEEwEKAEEWIQTi4nrI3ITcOMqRg+wGSPmiZQVW8gUCZi6m
iQIBAwUJABJ1AAULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRAGSPmiZQVW
8h2SB/40Ixp9SdNgk9Ut9zRefkePxZgZ9rc1FRsuitz10smbvd01gsnTnoFM3amG
EmhmeTOASRFz3zgzR8HCpfRzm6VKsxi+48PzW/snhCJXzkgNJd9T3kyTL5IGfnKF
j6JuTpLusS34rQak7n0V+d8/rQMqD8J9MNTqo7x0T7SevZhdgNv8LniPoxpryHlA
05hNVC/EndXEkcucqTcWfU+zIe9zFDXCMFgmI49gDaELJAJXV/Zhju0tYBdi5tKWj
VEF24ocBtGAt8uXD5vuqylQQDPMm2Fla0mdPXlHRLG2yvDKTxgcbqGMftFnEsWhv
tM/RcJvCoC8Y3vdEMRGBWSFCpIwkuQENBGYupokBCACy8faezTEjRzYOLm0JBCEu
0IUIZ22vfPDy4v5VuYL4TdYLWPTXvjHzLnd09I848GWgzAjJmNEZe+KyrXVjuS40
ufNxnNZHu0XEkaW8KwXYXCA1l2pwHgu9eZL9f5wF00VC5Q4LAQVkhRbD4pRDptTj
UxOF2Vkr5ZlPKPtBDvZiZoiWehrL8RaQahuzEMKMcr3j2p6PtWBL/BbKC/HPaBJ
/ahX/Bgl2/nVgubFvS3C2d2kx3RBMBDQLX5KM2GSW+UTTYP/koGxdYzVN0PyW0x
hk957/j1Z1LwXKxRWc0lypmPZkF0f9ELL4ru0u1LAz7XhpSdBg1nr2rWKSALwT
ABEBAAGJATWEGAECACYWIQTi4nrI3ITcOMqRg+wGSPmiZQVW8gUCZi6miQIBDAUJ
ABJ1AAKCRAGSPmiZQVW8oAwCADjXwix7UrbKpHRdWVEk3oDTjLQ+Tu20XXJbqlw
yBDUZtQ/bnZ9bX05pihWmngdg3LeNDzSQ9v7QUpSb2xspgzBV/TYXqvD52CIgpTu
+Whua6+B9K9XSgMg0LH7Snl7eBbKE7aTVrT+xhkIMIS5INZr2BN503y0F0YQwQ5
gxQKZREjQ5CILFAi0un6FtIMfQZGssYdNHSw5V9rTvfiHqhP3qUK6Z0QGoG0pVPp
a3LIBitV9+CrNnbic2AS2MicwqAtHYPMg0M7r6cNTStn04QQ1/R9gY9o0V65dqh
jGY+nNsNaQyOnExo8azXSxYKqWvCzoieyDJNMiMzNGRqdHu
=5Lzw
-----END PGP PUBLIC KEY BLOCK-----
aamishina@server:~/first$
```

Рис. 7: Экспорт ключа

```
aamishina@server:~/first$ scp ~/first/public.key ~/second/  
aamishina@server:~/first$
```

Рис. 8: Передача ключа

```
aamishina@server:~/second$ gpg --import public.key  
gpg: key 0648F9A2650556F2: "Nastya <nastya@gmail.com>" not changed  
gpg: Total number processed: 1  
gpg: unchanged: 1
```

Рис. 9: Импорт ключа

```
aamishina@server:~/first$ touch secret_file.txt  
aamishina@server:~/first$ vi secret_file.txt  
aamishina@server:~/first$
```

Рис. 10: Создание секретного файла

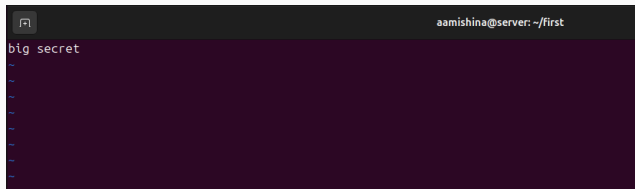
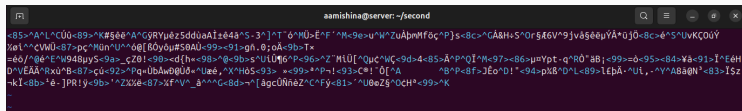


Рис. 11: Файл secret_file.txt



```
aamishina@server: ~/first
$ cat file
89>^AE^D^@^A
^@/^V!^D4&zEÜ<84>Ü8E<91><83>^FHÜce^EV0^E^Bf.^tg^Q\^nastya@gmail.com^@
^P^FHÜce^EV0C^C^pX%`d^P<95>AX^N^BýXNÄ~s:{±<88>^H^KEE^]<99>4m<9c>Ü0^DKDl~<95>e+0^Zq C^h<84><9c>k ^@/<8f>â%Êh3ZeL^G
_baÊH^@I^H<88>06Z<93>(^_gg^S^@`<81>e0^Ü^<93>e,<89>b0P<90>0<82>^Rç<8f><82>AD<91>áf<8d>^Ne<97>^?DZ0^M7w^Slc)ÖbmÄ<93>80<9e>l^Ie^RRI:~<8b>
^Z~<^E0$~.Ä^HÜ^?o^<90>V>vUKs\FY%<89>úâÊDoH^FBEG^DU^C^+0Lz^M1_Ä^V~±<99>Y0,{.#}e^MD^K,Ç^C<88>0%7â*l0ú^RÖz^M^P<87>l<99>t^M>ZjyÜ0py;F^@e<9d
>^xzx^DE^4
```

Рис. 13: Файл цифровой подписи



```
aamishina@server: ~/second
$ cat file
<85>^A^L^CÜ0<89>^K$ëe^A^GgRYpéz5ddüaAÍ±ë48^S-3^] ^T^6^HÜ>Ê^F^M<9e>u^M^ZuÄbmFöç^P}s<8c>^GÄH+S^Or$Æ6V^9jvâ$ëëµYÄ^üj0<8c>ê^S^UvKÇ0ÜY
%0!^C^VWÜ<87>pç^Mün^U^^0@[BÖy0µ#S0AÜ<99><91>gñ.0;oÄ<9b>Tx
=é0/^0é^E^W948uyS<9a>_çZ0!<90><d{h<98>^0<9b>s^U!Ü^6^P<96>^Z^M!Ü[^Qµç^Wç<9d>4<85>Ä^P^QI^M<97><86>µµYpt.q^R0^aB;<99>=0<95><84>Yâ<91>I^EéH
D^VEÄÄ^R^xü^B<87>çü<92>^Pq=ÜbAw00ü0^Uzê,^X^H0$<93> *<99>^P~l<93>C^!^0[ ^A ^B^P<8f>JÊo^D!^<94>pXB^D^L<89>lEbÄ.^Ui,-^Y^A8a0N^<83>I$z
~kY<8b>ë-]PR!y<9b>^AZ%e<87>%f^V^_ä^C<8d>~^[ägçÜñëZ^C^Fy<81>^U0eZ$0çH^<99>^K
```

Рис. 14: Зашифрованный файл с текстом

```
aamishina@server:~/first$ scp secret_file.txt.sig /home/aamishina/second/
aamishina@server:~/first$ scp secret_file.txt.gpg /home/aamishina/second/
aamishina@server:~/first$ cd ~/second
aamishina@server:~/second$ ls
public2.key public.key secret_file.txt.gpg secret_file.txt.sig
aamishina@server:~/second$ gpg -d -o decrypted.txt secret_file.txt.gpg
gpg: encrypted with rsa2048 key, ID DAFB890B23A7EAEB, created 2024-04-28
      "Ira <ira@gmail.com>"
aamishina@server:~/second$ gpg --verify secret_file.txt.sig decrypted.txt
gpg: [don't know]: invalid packet (ctb=0a)
gpg: Signature made Bc 28 anp 2024 20:28:23 UTC
gpg:          using RSA key E2E27AC8DC84DC38CA9183EC0648F9A2650556F2
gpg:          issuer "nastya@gmail.com"
gpg: Good signature from "Nastya <nastya@gmail.com>" [ultimate]
```

Рис. 15: Дешифровка и проверка подписи

```
aamishina@server:~/second$ cat decrypted.txt
big secret
aamishina@server:~/second$ █
```

Рис. 16: Просмотр дешифрованного файла

- PGP эффективен.
- Применение: защита личной переписки, шифрование дисков, безопасность бизнеса, обмен файлами, работа с github.
- Свободный доступ системы PGP.