Раздел: Жизненный цикл ИБ
Модуль: Средства защиты информации
Выполнил: Александр Ганицев

Условия задания:

Установите GnuPG и создайте две пары ключей. Зашифруйте тестовый файл ключом из первой пары на открытом ключе второй пары, а потом расшифруйте файл.

Задание практической работы:

Установить GnuPG в разных системах.
Создать пару ключей № 1.
Создать пару ключей № 2 с указанием другой электронной почты.
Зашифровать любой файл с помощью закрытого ключа № 1 на открытом ключе № 2.
Расшифровать файл с помощью закрытого ключа № 2.

Условия реализации:

Пришлите в формате Word или PDF или в виде скриншотов содержимое терминала с командами и результатами их выполнения, которые были использованы в рамках практической работы.

Одним из вариантов решения задачи может быть установка GnuPG в двух разных системах (на двух разных виртуальных машинах) с полноценным обменом открытыми ключами и зашифрованным файлом между ними.

1. Установка/проверка наличия GnuPG в системе.

В моём случае я создаю по две пары GnuPG на двух виртуальных машинах (Ubuntu 22.10 и Ubuntu 22.04) По причине того, что я не использовал эти системы некоторое время, проверяю обновления и GnuPG:

```
skillfactory_lab@Ubuntu22:~$ sudo apt update && sudo apt install gnupg
```

Ubuntu 22.10 (на Ubuntu 22.04 последовательность шагов таже)

```
skillfactory_lab@Ubuntu22:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.10"
NAME="Ubuntu"
VERSION_ID="22.10"
VERSION="22.10 (Kinetic Kudu)"
```

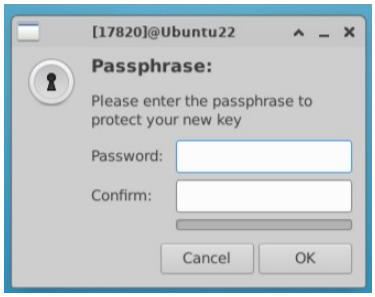
1.1 Проверяю версию gpg:

```
skillfactory_lab@Ubuntu22:~$ gpg --version
gpg (GnuPG) 2.2.35
libgcrypt 1.10.1
```

```
skillfactory_lab@Linux:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.2 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
skillfactory_lab@Linux:~$ 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/skillfactory_lab/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

1.2 Создаю пару ключей:

```
skillfactory_lab@Ubuntu22:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.35; Copyright (C) 2022 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 (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (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) 5
Key expires at Пт 07 июл 2023 19:26:04 MSK
Is this correct? (y/N) y

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

Real name: Alexandr Ganitev
Email address: alexgubuntu2210@gmail.com
Comment: AlexG_Ubuntu2210
You selected this USER-ID:
    "Alexandr Ganitev (AlexG_Ubuntu2210) <alexgubuntu2210@gmail.com>"

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 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: directory '/home/skillfactory_lab/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/skillfactory_lab/.gnupg/openpgp-revocs.d/F5E384A121CF94AC23CBC3429CD9
2E7776FACB1A.rev'
public and secret key created and signed.

pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      F5E384A121CF94AC23CBC3429CD92E7776FACB1A
uid                      Alexandr Ganitev (AlexG_Ubuntu2210) <alexgubuntu2210@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]
```



И для Ubuntu 22.04:

```
skillfactory_lab@Linux:~$ gpg --full-generate-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.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (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) 5
Key expires at Пт 07 июл 2023 19:50:16 MSK
Is this correct? (y/N) y

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

Real name: Alexandr Ganitev
Email address: alexgubuntu2204@gmail.com
Comment: AlexG_Ubuntu2204
You selected this USER-ID:
    "Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>"

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 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 1E60C438348E3134 marked as ultimately trusted
gpg: directory '/home/skillfactory_lab/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/skillfactory_lab/.gnupg/openpgp-revocs.d/364BD5D53F0BD6153D4659881E60C438348E3134.rev'
public and secret key created and signed.

pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      364BD5D53F0BD6153D4659881E60C438348E3134
uid                      Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]
```

1.3 Экспортирую публичный ключ:

```
skillfactory_lab@Ubuntu22:~$ gpg --export -a "AlexG_Ubuntu2210" > publickey_AlexG_Ubuntu2210.asc
```

```
skillfactory_lab@Ubuntu22:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  publickey_AlexG_Ubuntu2210.asc
```

```
skillfactory_lab@Linux:~$ gpg --export -a "AlexG_Ubuntu2204" > publickey_AlexG_Ubuntu2204.asc
```

```
skillfactory_lab@Linux:~$ ls
archive  Desktop  Documents  Music     Public
data     docker   Downloads  Pictures  publickey_AlexG_Ubuntu2204.asc
```

1.4 Копирую публичный ключ Ubuntu 22.10 на Ubuntu 22.04 и публичный ключ Ubuntu 22.04 на Ubuntu 22.10:

Замечание: обе VM машины работают через ssh с хостовой машины, но ssh-соединения нет между ними. На время, для копирования файлов выставил “PasswordAuthentication yes” на обоих и перегрузил ssh – sudo systemctl restart ssh.

```
skillfactory_lab@Ubuntu22:~$ scp /home/skillfactory_lab/publickey_AlexG_Ubuntu2210.asc skillfactory_lab@192.168.1.
114:/home/skillfactory_lab/
skillfactory_lab@192.168.1.114's password:
Permission denied, please try again.
skillfactory_lab@192.168.1.114's password:
publickey_AlexG_Ubuntu2210.asc                                100% 1802   805.4KB/s   00:00
```

```
skillfactory_lab@Linux:~$ ls
archive  Desktop  Documents  Music     Public                      publickey_AlexG_Ubuntu2210.asc
data     docker   Downloads  Pictures  publickey_AlexG_Ubuntu2204.asc  PycharmProjects
```

```
skillfactory_lab@Linux:~$ scp /home/skillfactory_lab/publickey_AlexG_Ubuntu2204.asc skillfactory_lab@192.168.1.127:/home/skillfactory_lab
/
publickey_AlexG_Ubuntu2204.asc                                                100% 1802   393.9KB/s   00:00
```

```
skillfactory_lab@Ubuntu22:~$ ls
Desktop    Downloads  Pictures  publickey_AlexG_Ubuntu2204.asc
Documents  Music      Public    publickey_AlexG_Ubuntu2210.asc
```

1.5. Импортирую скопированные ключи и проверяю все ключи в системе:

```
skillfactory_lab@Ubuntu22:~$ gpg --import publickey_AlexG_Ubuntu2204.asc
gpg: key 1E60C438348E3134: public key "Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
skillfactory_lab@Ubuntu22:~$ gpg --list-keys
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, 1u
gpg: next trustdb check due at 2023-07-07
/home/skillfactory_lab/.gnupg/pubring.kbx
---------------------------------------
pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      F5E384A121CF94AC23CBC3429CD92E7776FACB1A
uid           [ultimate] Alexandr Ganitev (AlexG_Ubuntu2210) <alexgubuntu2210@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]

pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      364BD5D53F0BD6153D4659881E60C438348E3134
uid           [ unknown] Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]
```

```
skillfactory_lab@Linux:~$ gpg --import publickey_AlexG_Ubuntu2210.asc
gpg: key 9CD92E7776FACB1A: public key "Alexandr Ganitev (AlexG_Ubuntu2210) <alexgubuntu2210@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
skillfactory_lab@Linux:~$ gpg --list-keys
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, 1u
gpg: next trustdb check due at 2023-07-07
/home/skillfactory_lab/.gnupg/pubring.kbx
---------------------------------------
pub   dsa1024 2010-09-20 [SC]
      C47415DFF48C09645B78609416126D3A3E5C1192
uid           [ unknown] Ubuntu Extras Archive Automatic Signing Key <ftpmaster@ubuntu.com>

pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      364BD5D53F0BD6153D4659881E60C438348E3134
uid           [ultimate] Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]

pub   rsa2048 2023-07-02 [SC] [expires: 2023-07-07]
      F5E384A121CF94AC23CBC3429CD92E7776FACB1A
uid           [ unknown] Alexandr Ganitev (AlexG_Ubuntu2210) <alexgubuntu2210@gmail.com>
sub   rsa2048 2023-07-02 [E] [expires: 2023-07-07]
```

Процесс шифрования и дешифрования

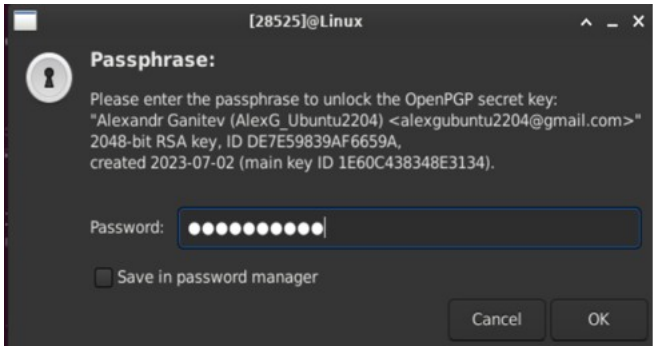
1. Создаю файл для последущей зашифровки:

```
skillfactory_lab@Ubuntu22:~$ vim encrypted_msg_on_U2210.txt
skillfactory_lab@Ubuntu22:~$ cat encrypted_msg_on_U2210.txt
This message has been created to be encrypted on Ubuntu 22.10 and it's destined for Ubuntu 22.04.
Creator Alex Ganitev
```

2. Зашифровываю и копирую на Ubuntu 22.04:

```
skillfactory_lab@Ubuntu22:~$ gpg --encrypt --recipient "AlexG_Ubuntu2204" --output encrypted_msg_on_U2210.txt.enc
encrypted_msg_on_U2210.txt
gpg: DE7E59839AF6659A: There is no assurance this key belongs to the named user

sub  rsa2048/DE7E59839AF6659A 2023-07-02 Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>
 Primary key fingerprint: 364B D5D5 3F0B D615 3D46  5988 1E60 C438 348E 3134
      Subkey fingerprint: A7AE F9F0 039A 869C B1C6  A857 DE7E 5983 9AF6 659A

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
skillfactory_lab@Ubuntu22:~$ ls
Desktop    encrypted_msg_on_U2210.txt      Pictures                      publickey_AlexG_Ubuntu2210.asc  Videos
Documents  encrypted_msg_on_U2210.txt.enc  Public                        snap
Downloads  Music                           publickey_AlexG_Ubuntu2204.asc  Templates
skillfactory_lab@Ubuntu22:~$ scp /home/skillfactory_lab/encrypted_msg_on_U2210.txt.enc skillfactory_lab@192.168.1.
114:/home/skillfactory_lab
skillfactory_lab@192.168.1.114's password:
encrypted_msg_on_U2210.txt.enc                                  100%  454   201.6KB/s   00:00
```

3. Расшифровываем файл на Ubuntu 22.04:




```
skillfactory_lab@Linux:~$ ls
archive  docker     encrypted_msg_on_U2210.txt.enc  Public                        PycharmProjects
data     Documents  Music                           publickey_AlexG_Ubuntu2204.asc  snap
Desktop  Downloads  Pictures                        publickey_AlexG_Ubuntu2210.asc  Templates
skillfactory_lab@Linux:~$ gpg --decrypt encrypted_msg_on_U2210.txt.enc
gpg: encrypted with 2048-bit RSA key, ID DE7E59839AF6659A, created 2023-07-02
      "Alexandr Ganitev (AlexG_Ubuntu2204) <alexgubuntu2204@gmail.com>"
This message has been created to be encrypted on Ubuntu 22.10 and it's destined for Ubuntu 22.04.
Creator Alex Ganitev
```

4. Восстанавливаю доступ по ssh, перегружаю ssh сервер на обоих виртуальных машинах:

```
skillfactory_lab@Ubuntu22:~$ scp /home/skillfactory_lab/encrypted_msg_on_U2210.txt.enc skillfactory_lab@192.168.1.
114:/home/skillfactory_lab
skillfactory_lab@192.168.1.114: Permission denied (publickey).
scp: Connection closed
```