Лабораторная работа № 2 по курсу: криптография

Выполнил студент группы М8О-308Б-17 МАИ *Милько Павел.*

Часть 1

Создать пару OpenPGP-ключей, указав в сертификате свою почту.

```
gpg --generate-key
```

```
gpg (GnuPG) 2.2.19; Copyright (C) 2019 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: Милько Павел Алексеевич
Email address: p.milko1999@yandex.ru
You are using the 'iso-8859-1' character set.
You selected this USER-ID:
    "Милько Павел Алексеевич <p.milko1999@yandex.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 4DF7496E16FD3CBC marked as ultimately trusted
gpg: revocation certificate stored as '/home/lol/.gnupg/openpgp-revocs.d/703
    FD5D038947C5B57CCE5A64DF7496E16FD3CBC.rev'
public and secret key created and signed.

pub   rsa2048 2020-03-10 [SC] [expires: 2022-03-10]
      703FD5D038947C5B57CCE5A64DF7496E16FD3CBC
uid                      Милько Павел Алексеевич <p.milko1999@yandex.ru>
sub   rsa2048 2020-03-10 [E] [expires: 2022-03-10]
```