Создание ключа
ТЫ создаешь ключ (ОДИН РАЗ): **gpg --full-gen-key**
>1
> любой размер от 1024 до 4096 (я брал 2048)
> 4m (это живучесть ключа можно указать в днях, неделях месяцах и годах. Я выбрал до конца семестра)
> y
> вводишь имя, желательно Имя Фамилия (чтоб в сертефикате других людей это отображалось)
> .....
> .....
> .....
теперь у тебя есть сертификат открытого ключа, например vasya.asc

gpg -a -o vasya.asc --export ключ_свой

(пример: DF2533E58ECDA27B7DA1833F9FE64CEE5AE4BAF0)

Как его найти?
> **gpg --list-sigs** - во второй строке будет в разделе pub будет твой ключ.

Подписываем сертификаты:
2 варианта развития дел:

1)
Тебе прислали сертификат открытого ключа name.asc (вообще любое имя, обычно это имя.asc или фамилия.asc, но не принципиально)

gpg --import name.asc
gpg --sign-key ключ собеседника
gpg -a -o name_signed.asc --export ключ собеседника
gpg -a -o vasya.asc --export [ключ свой]

затем ты собеседнику отсылаешь 2 файла vasya.asc и name_signed.asc (можно через почту, можно через тг, да хоть в конверте на флэшке)

собеседник после махинаций(*) пришлет тебе файл vasya_signed.asc

ты сделаешь:
gpg --import vasya_signed.asc

ПРОВЕРЬ **gpg --list-sigs**

там будут указаны твои подписки и подписи.

2) (*)

gpg -a -o vasya.asc --export [ключ свой]
Ты отправлешь челику(собеседнику) свой файл vasya.asc

после махинаций и танцами с бубном у терминала (см. п. 1)

тебе прилетают 2 файла
name.asc и vasya_signed.asc

gpg --import name.asc
gpg --import vasya_signed.asc
gpg --sign-key ключ_того_челика
gpg -a -o name_signed.asc --export ключ_того_челика

Присылаешь name_signed.asc собеседнику

ПРОВЕРЬ **gpg --list-sigs**

Все теперь чтобы выжить соберите 10 подписей.
Да начнутся голодные игры!

Благодаря тому, что мы добавили их и сертифицировали, мы можем общаться друг с другом в зашифрованными сообщениями. Мы можем их прочитать, а другие - нет.

Благодарности:

Спасибо Ивану Мариничеву, Игорю Королеву за лучшее объяснение этого материала!