Отчет лабораторной работы №2

По дисциплине “Криптография”

Выполнил Кондратьев Егор М8О-306Б-19

Сначало мною был сгенерирован ключ.

**gpg --full-gen-key** # создание ключа

**gpg -a -o dukend.asc --export A32CB4789DCF616315D6DD9B5EC776B79907F6A0** # создание сертификата открытого ключа

**gpg --list-sigs** # просмотр подписей

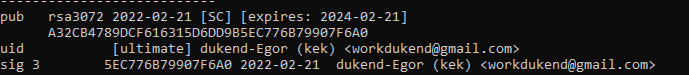
Я решил не мелочиться и сделал его до 2024 года, хотя вряд ли мне это в скором времени понадобиться, но будем надеяться мне задание понравилось.

*pub rsa3072 2022-02-21 [SC] [expires: 2024-02-21]*

*A32CB4789DCF616315D6DD9B5EC776B79907F6A0*

*uid [ultimate] dukend-Egor (kek) <workdukend@gmail.com>*

*sig 3 5EC776B79907F6A0 2022-02-21 dukend-Egor (kek) <workdukend@gmail.com>*



Далее по заданию требовалось обменяться с десятью сокурсниками подписями под сертификатами.

Тут началось веселое повторение одного и того же действия. Я решил дабы ускорить процесс просто всем(**Человек 50**) разослать пасту по типу:

привет, надеюсь ты уже начал заниматься криптой

вот мой сертификат.

gpg --import dukend.asc

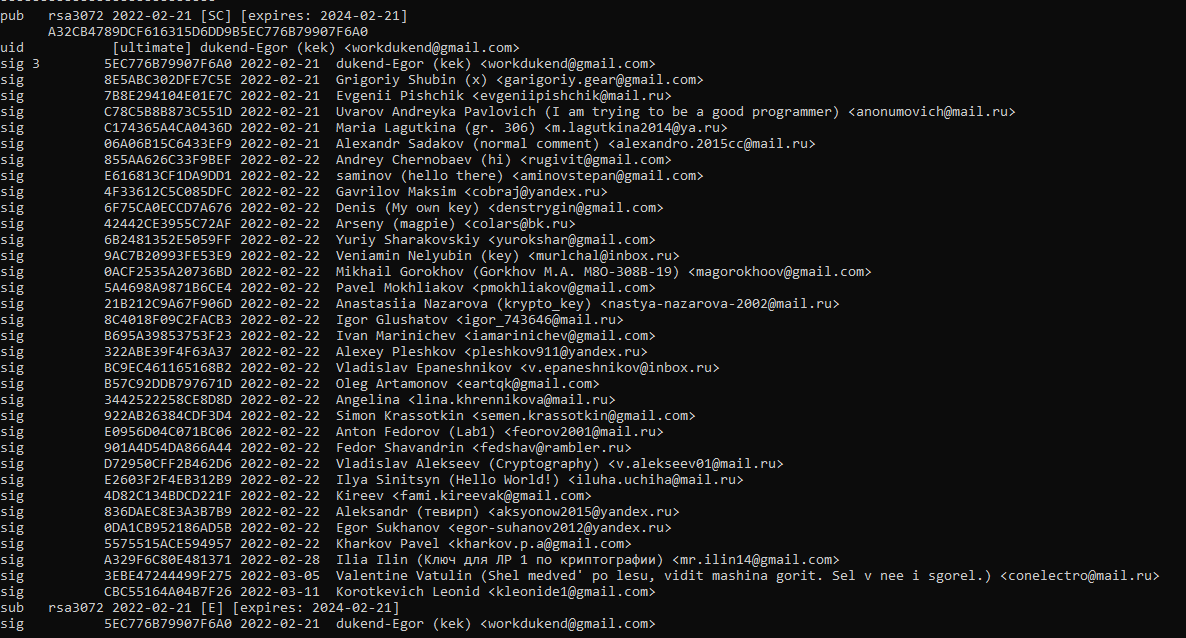
gpg --sign-key 5EC776B79907F6A0

gpg -a -o dukend\_kek.asc --export 5EC776B79907F6A0

И даже инструкцию им выслал.

Собрал я все довольно быстро, но все хотят, чтобы им все объяснили, и на десятый мб пятнадцатый раз откровенно стало подбешивать.

В итоге 35 подписей, не считая тех, кто кидал позже, я забил



Далее требовалось обменяться ключами с преподавателем. А после зашифровать и расшифровать сообщения.

**gpg --recipient awh --encrypt 1.txt**

**gpg --decrypt 2.txt.gpg**

Ну собственно конец

По поводу вывода

Я научился пользоваться шифрованием и подписью на примере pgp.

Механизм работы pgp показался мне интересным. Под капотом много классных алгоритмов шифрования, сжатия, хеширования. Наверно, интересно было бы написать прототип такой системы.

**З,Ы,** Команда **gpg --list-sigs** мне не понравилась, ведь при большом количестве сертификатов эта частая всплывающая информация начинает сводить с ума, но замены я не нашел.

Тадам!

