Министерство образования Нижегородской области
Государственное бюджетное образовательное учреждение
среднего профессионального образования
«Нижегородский радиотехнический колледж»

ОТЧЁТ
по лабораторной работе №1
ТЕМА «GNU PG»
Дисциплина «Технология применения программных средств защиты информационных систем»

Выполнил
студент
группы 2Ис-13-2с
Старостьянц А.М.

Проверил
преподаватель
Слугин В.Г.

г. Нижний Новгород
2015 г.

gpg -c 1.txt
gpg --decrypt-file 1.txt.gpg

Генерируем ключ:

domrachev_dmitrijj@eMac8:~$ gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2008 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.

Выберите тип ключа:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (только для подписи)
  (4) RSA (только для подписи)
Ваш выбор (?-подробнее)?
ключи RSA могут иметь длину от 1024 до 4096 бит.
Какой размер ключа Вам необходим? (2048)
Запрашиваемый размер ключа 2048 бит
Выберите срок действия ключа.
        0 = без ограничения срока действительности
     <n> = срок действительности n дней
     <n>w = срок действительности n недель
     <n>m = срок действительности n месяцев
     <n>y = срок действительности n лет
Ключ действителен до? (0)
Ключ не имеет ограничения срока действительности
Все верно? (y/N) y

Для идентификации Вашего ключа необходим User ID
Программа создаст его из Вашего имени, комментария и адреса e-mail в виде:
   "Baba Yaga (pensioner) <yaga@deepforest.ru>"

Ваше настоящее имя: Svitoslav Bzjenjovich
Email-адрес: bzjenjovich-s@kurwa.pl
Комментарий: KURWA KATYN
Вы выбрали следующий User ID:
   "Svitoslav Bzjenjovich (KURWA KATYN) <bzjenjovich-s@kurwa.pl>"

Сменить (N)Имя, (C)Комментарий, (E)email-адрес или (O)Принять/(Q)Выход? o
Для защиты секретного ключа необходим пароль.

gpg: gpg-agent недоступен в данной сессии
Необходимо сгенерировать много случайных чисел. Желательно, что бы Вы
выполняли некоторые другие действия (печать на клавиатуре, движения мыши,
обращения к дискам) в процессе генерации; это даст генератору
случайных чисел возможность получить лучшую энтропию.
.....+++++
s+df++++
sНеобходимо сгенерировать много случайных чисел. Желательно, что бы Вы
выполняли некоторые другие действия (печать на клавиатуре, движения мыши,
обращения к дискам) в процессе генерации; это даст генератору

случайных чисел возможность получить лучшую энтропию.
df.sd....s.df.s.df..+++++
....+++++
gpg: ключ D5198DC4 помечен как абсолютно доверяемый.
открытый и закрытый ключи созданы и подписаны.

gpg: проверка таблицы доверий
gpg: 3 ограниченных необходимо, 1 выполненных необходимо, PGP модель доверия
gpg: глубина: 0 корректных: 1 подписанных: 0 доверия: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/D5198DC4 2015-10-05
Отпечаток ключа = 6022 30DE E344 1B52 2BF0 4067 5FB5 5505 D519 8DC4
uid Svitoslav Bzjenjovich (KURWA KATYN) <bzjenjovich-s@kurwa.pl>
sub 2048R/B8E91807 2015-10-05

domrachev_dmitrijj@eMac8:~$ gpg --list-key
/home/domrachev_dmitrijj/.gnupg/pubring.gpg
---
pub 2048R/D5198DC4 2015-10-05
uid Svitoslav Bzjenjovich (KURWA KATYN) <bzjenjovich-s@kurwa.pl>
sub 2048R/B8E91807 2015-10-05

pub 1024R/A4040E4E 2015-10-05 [годен до: 2015-11-04]
uid Abraham Goldstein (money money money money shekil) <israel-god-killers@jesus.au>
sub 1024R/3B5596F5 2015-10-05 [годен до: 2015-11-04]

domrachev_dmitrijj@eMac8:~$ gpg --output sikret.txt --armor --export A4040E4E
domrachev_dmitrijj@eMac8:~$ cat sikret.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)

mI0EVhJaEAEEAOP0dt72+UP65C0SYQ0UMtml9q8ycUXxyX0lGa4T+UPfZwC/T6F0
dS34tNUg3kPnsrci0ixLg5UWdCpQYah+f7lf57Msu03sc2Y37ElD/MHTexo9FOPF
cpvHA1FXHrU7wF8vKN9ql3aB3BLe9ogiOvqDWMsbld7VdNc6shV2GZLnABEBAAG0
UEFicmFoYW0gR29sZHN0ZWluIChtb25leSBtb25leSBtb25leSBtb25leSBzaGVr
aWwpIDxpc3JhZWwtZ29kLWtpbGxlcnNAamVzdXMuYXU+iL4EEwECACgFAlYSWhAC
GwMFCQAnjQAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEJD1+mGkBA5ODMc
E
AIDWkKETlIFZ+cAiyFYW2BCcreS2OD/6ufQHgwmGR3C8DqcQrawRCdd4IHxG2frC
8NSucXm2TORyM46h9lh1WI2nFvyl0xrCyP5272aTSGiDcbtwRIfGncXZRdDYD6Rh
kx0CLWprw601lM8KGCWdyDUnkDwEhWH8Xru4PgLqyxC9uI0EVhJaEAEEALfaXvJk
DrQMJdJr0KmcktGtUdzWXK5Z6c+lUAQW0hjt3O09fSUieHxja6ie6VB1AdqUlR2m
gUhI0dEndPOh5f/baJ655xo/KcE+dxEzYrP/bdm7DyxY1d+0jSe0Ym7z5PThLVSp
GO2KTmUI/gDKD8bloJs+NQAWBFgd9+Wb5DnnABEBAAGIpQQYAQIADwUCVhJaEAIb
DAUJACeNAAAKCRCQ9fphpAQOTm2BA/4g904mNOUlLGbUN8N2E+N2a4Gbcc8boUkN
BGLmHG+wRo6twuVQ6mLlWzNFLhba4/Y5tTSDCQc2tJtNa3g0/ZOZZHn8GbQ+QviQ
iUi5lnM9bwb2AtF1etMEvipx3aYMvtKPaSCetYXEshBOgUm+EwHNnrEUpsOBjFaV
O45U8buC0g==
=LLvV

-----END PGP PUBLIC KEY BLOCK-----

domrachev_dmitrijj@eMac8:~$ gpg --import sikret_big.bin
gpg: создан каталог `/home/domrachev_dmitrijj/.gnupg'
gpg: создан новый файл настроек `/home/domrachev_dmitrijj/.gnupg/gpg.conf'
gpg: ВНИМАНИЕ: параметры в `/home/domrachev_dmitrijj/.gnupg/gpg.conf' еще не активны при этом запуске
gpg: создана таблица ключей `/home/domrachev_dmitrijj/.gnupg/secring.gpg'
gpg: создана таблица ключей `/home/domrachev_dmitrijj/.gnupg/pubring.gpg'
gpg: ключ D5198DC4: секретный ключ импортирован
gpg: /home/domrachev_dmitrijj/.gnupg/trustdb.gpg: создана таблица доверий
gpg: ключ D5198DC4: открытый ключ "Svitoslav Bzjenjovich (KURWA KATYN) <bzjenjovich-s@kurwa.pl>" импортирован
gpg: Всего обработано: 1
gpg: импортировано: 1 (RSA: 1)
gpg: прочитано секретных ключей: 1
gpg: импортировано секретных ключей: 1
domrachev_dmitrijj@eMac8:~$ gpg --list-key
/home/domrachev_dmitrijj/.gnupg/pubring.gpg
---
pub   2048R/D5198DC4 2015-10-05
uid   Svitoslav Bzjenjovich (KURWA KATYN) <bzjenjovich-s@kurwa.pl>
sub   2048R/B8E91807 2015-10-05

gpg --recipient D5198DC4 --encrypt lax_big.txt
gpg --recipient D5198DC4 --decrypt-files lax_big.txt.gpg

gpg --sign lax_big.txt
gpg --decrypt-file lax_big.txt