ФЕДЕРАЛЬНОЕ АГЕНТСТВО ОБРАЗОВАНИЯ
ДИМИТРОВГРАДСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ,
УПРАВЛЕНИЯ И ДИЗАЙНА

“Шифрование и цифровая подпись”

Выполнил студент гр. ВТ-41:
Потеренко А.Г.

Димитровград 2007г.

Задание 1.1

Создадим директорию .gnupg:

```
[root@LinuxHost root]# mkdir .gnupg
```

Генерируем ключи:

```
[root@LinuxHost .gnupg]# gpg --gen-key
gpg (GnuPG) 1.2.6; Copyright (C) 2004 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: создана таблица ключей `/root/.gnupg/secring.gpg'
gpg: создана таблица ключей `/root/.gnupg/pubring.gpg'
Выберите тип ключа:
   (1) DSA и ElGamal (по умолчанию)
   (2) DSA (только для подписи)
   (4) RSA (только для подписи)
Ваш выбор (?-подробнее)? 1
Пара ключей DSA будет иметь длину 1024 бита.
Создаем новую пару ELG-E ключей.
              минимальный размер ключа   768 бит
              размер ключа по умолчанию 1024 бит
      максимально рекомендуемый размер  2048 бит
Какой размер ключа Вы выбрали? (1024)
Запрашиваемый размер ключа 1024 бит
Выберите срок действия ключа.
         0 = без ограничения срока действия
      <n>  = срок действия n дней
      <n>w = срок действия n недель
      <n>m = срок действия n месяцев
      <n>y = срок действия n лет
Ключ действителен до? (0) 0
Key не имеет ограничения срока действия
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: USER12
Email-адрес: USER12@DITUD.RU
Комментарий: user12 key
Вы выбрали следующий User ID:
    "USER12 (user12 key) <USER12@DITUD.RU>"

Сменить (N)Имя, (C)Комментарий, (E)email-адрес или (O)Принять/(Q)Выход? O

Для защиты секретного ключа необходим пароль. (qwerty)

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.
++++++++++++++++++++++++++++++++++++++++++++++++++..+++++++++++++++++++++++++++++++.+++++++++++++++++++++++++++
+.+++++++++++++++++++++++++>+++++.............>+++++.....................................d.f......d........g.
...d..f....g....d.++++g+
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.
++++++++++.+++++++++++++++.++++++++++.+++++++++++++++++++++++++++++.+++++.+++++++++++++++..++++++++++++++++r+++
++++++.e++++++++++++++++++++>+++++>+++++...g..............<+++++..........>+++++.<+++++.>.+++++.+++++^^^
gpg: /root/.gnupg/trustdb.gpg: создана таблица доверий
открытый и закрытый ключи созданы и подписаны.
ключ помечен как абсолютно доверяемый.

pub  1024D/8336DE19 2007-01-12 USER12 (user12 key) <USER12@DITUD.RU>
     Отпечаток ключа = DE93 0BED 3795 B3CB C05C  4EDE FBDA 1979 8336 DE19
sub  1024g/8AB28EBF 2007-01-12
```

В результате получим файлы в директории:

```
[root@LinuxHost .gnupg]# ls -a
.  ..  pubring.gpg  pubring.gpg~  random_seed  secring.gpg  trustdb.gpg
```

Задание 1.2

Создаем отзывающий сертификат:

```
[root@LinuxHost .gnupg]# gpg --output revoke.asc --gen-revoke USER12

sec  1024D/8336DE19 2007-01-12   USER12 (user12 key) <USER12@DITUD.RU>

Создать сертификат отзыва данного ключа? (y/n)y
Выберите причину отзыва:
  0 = Без указания причины
  1 = Ключ был скомпрометирован
  2 = Ключ заменён другим
  3 = Ключ больше не используется
  Q = Отмена
(Возможно Вы хотите выбрать здесь 1)
Ваше решение (?-подробнее)? 0
Введите необязательное пояснение; закончите пустой строкой:
>
Причина отзыва: Без указания причины
(Пояснения отсутствуют)
Все правильно? y

Необходим пароль для доступа к секретному ключу пользователя:
"USER12 (user12 key) <USER12@DITUD.RU>"
1024-бит DSA ключ, ID 8336DE19, создан 2007-01-12

Для вывода использован ASCII формат.
Сертификат отзыва создан.

Поместите его в скрытое место;  если посторонний получит доступ
к данному сертификату, он может использовать его, чтобы сделать
Ваш ключ непригодным к использованию. Можно распечатать данный
сертификат и спрятать подальше,  на случай если Ваш основной
носитель будет повреждён, но будьте осторожны: система печати
Вашей машины может сохранить данные и сделать их доступными для других!
```

Задание 1.3

Список открытых ключей на локальном компьютере:

```
[root@LinuxHost ~]# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub  1024D/8336DE19 2007-01-12 USER12 (user12 key) <USER12@DITUD.RU>
sub  1024g/8AB28EBF 2007-01-12
```

Экспорт открытого ключа:

```
[root@LinuxHost .gnupg]# gpg --armor --output DBA.gpg --export USER12
[root@LinuxHost .gnupg]# more DBA.gpg
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.6 (GNU/Linux)

mQGiBEWn2m0RBAD9h48itGIuUjSZhi/6Pw5mKspobJ6nmcP/OMefHgeYOstRNZ78
Vnh8B3XTEFKSNQdWYsqhLx4KmIzZwVgPHHKTA2NpdkuYJ3EvM1CI3fsCqlw62pXY
g9lAjTT7RPzxB/GvkAtjPP9PDYRKFJq8EFq9JD3Ryn4EjpSWRC0U6tzUBwCgo3MP
XenKSf+QJugttMQ6iEL4s3sEALOhVibYQ9ugioJvOpzHmiK/NWHwtdRq2j9pA3/B
Mzf8ObANeQCkNsYIgzuq2Vi7gRw2xNRzmHWX849IKvNfCl7Z6IV0JgCSzbYnjoNN
a2hl31liKB6EZFTpwztwZnqkKwlmsJifrSgoDkz4Fxe8wUP2by2+xXPbQOwwr5e3
dZokA/0aqv7IfmLiIYJjXtsXgkZwdYRrWgfIzxJ/MDdF9C7no/r/L5m08YtNs0w/
USNzxEQbwLMBOLTQvGmC+HC1mBh9aWhboo1LzuCJU0BtqJwcN4ufKw6Wzo+fVooo
grY+1ze4yINBRuis5WlPwwYxjEG2dw2PaTf7rz9aEbEPBE7+2LQlVVNFUjEyICh1
c2VyMTIga2V5KSA8VVNFUjEyQERJVFVELlJVPoheBBMRAgAeBQJFp9ptAhsDBgsJ
CAcDAgMVAgMDFgIBAh4BAheAAAoJEPvaGXmDNt4ZHmoAnj0aLpfFoB9+d2lLMn22
9tV3dUUIAJwIvDvL8tkYrUy1iRf5NV6ivxmkCrkBDQRFp9pvEAQAnZU72vXs+Ioy
n5A23UaBDAFiwQQHPMZ8SWOkN1tsfiki0AK9sDFnAcbeWOFPcnUphLKuul7rxJfU
du7xIJd539RAmQF2EkbcnKOmg8+msb/RUYYLOatIPeXwT7k/6gjk1Vu3I6dJleSt
MmbqEhLb33neb6cU3CPwOAgAi6EPmicAAwUD/Ri4X382wY3dxJewBf7tVTyTvVMm
TgLz0l4qVWYWJJR+jpqfaTz928muko632pAlEd0qMr5OBgB9183mJD8WHEYaqCxk
+S0jMLenDajQM9t3kLD6utusSIeBpWPQBVLQgRQYj6UwhhTfvsQIoX6vk/YSouhJ
nRHF5D3qO3OPPaKRiEkEGBECAAkFAkWn2m8CGwwACgkQ+9oZeYM23hlRnwCghdaG
FYUsovrHDPFl2juqz59rWaAAoIjMBB5TYdrFckm4XPR/jkcU9iyc
=lBH0
-----END PGP PUBLIC KEY BLOCK-----
```

Просмотр отпечатка ключа USER12:

```
[root@LinuxHost .gnupg]# gpg --fingerprint USER12
pub  1024D/8336DE19 2007-01-12 USER12 (user12 key) <USER12@DITUD.RU>
     Отпечаток ключа = DE93 0BED 3795 B3CB C05C  4EDE FBDA 1979 8336 DE19
sub  1024g/8AB28EBF 2007-01-12
```

Редактирование и просмотр свойств ключа USER12:

```
[root@LinuxHost .gnupg]# gpg --edit-key USER12
gpg (GnuPG) 1.2.6; Copyright (C) 2004 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Секретный ключ доступен.

pub  1024D/8336DE19  создан: 2007-01-12 истекает: никогда    доверие: u/u
sub  1024g/8AB28EBF  создан: 2007-01-12 истекает: никогда
(1). USER12 (user12 key) <USER12@DITUD.RU>

Команда> help
quit       выйти из этого меню
save       сохранить и выйти
help       показать эту справку
fpr        показать отпечаток
list       вывести список ключей и User ID
uid        выбрать User ID N
key        выбрать вторичный ключ N
check      вывести список подписей
sign       подписать ключ
lsign      локально подписать ключ
nrsign     подписать ключ без возможности отзыва
nrlsign    подписать ключ локально и без возможности отзыва
adduid     добавить User ID
addphoto   добавить фото ID
deluid     удалить User ID
addkey     добавить вторичный ключ
delkey     удалить вторичный ключ
addrevoker добавить ключ отзыва
delsig     удалить подпись
expire     сменить срок действия
primary    пометить User ID как главный
toggle     переключение между открытым и закрытым ключами
pref       список предпочтений (экспертам)
showpref   список предпочтений (подробный)
setpref    установить предпочтения
updpref    обновить предпочтения
passwd     сменить пароль
trust      изменить уровень доверия владельцу
revsig     отзыв подписей
revuid     отзыв User ID
revkey     отзыв подключей
disable    отключить ключ
enable     включить ключ
showphoto  показать фото ID

Команда> check
uid  USER12 (user12 key) <USER12@DITUD.RU>
sig!3       8336DE19 2007-01-12   [самоподпись]
```

Импортирование открытого ключа DBA.gpg на хост LinuxDBA:

На хосте LinuxDBA создаем новую таблицу открытых ключей и копируем файл DBA.gpg в папку /root/.gnupg, затем импортируем открытый ключ DBA.gpg хоста LinuxHost:

```
[root@LinuxDBA ~]# gpg --list-keys
gpg: создана таблица ключей `/root/.gnupg/pubring.gpg'
```

Создаем пару ключей на хосте LinuxDBA также как на хосте LinuxHost:

```
pub  1024D/16A32630 2007-01-12 USER11 (user11 key) <USER11@DITUD.RU>
     Отпечаток ключа = 8CE7 02AC 864F F232 FAFD  31ED CA1E 2185 16A3 2630
sub  1024g/26DC2141 2007-01-12

[root@LinuxDBA .gnupg]# gpg --import DBA.gpg
gpg: /root/.gnupg/trustdb.gpg: создана таблица доверий
gpg: ключ 8336DE19: открытый ключ "USER12 (user12 key) <USER12@DITUD.RU>" импортирован
gpg: Всего обработано: 1
gpg:                импортировано: 1
```

Достоверность импортированного ключа должна быть подтверждена. Проверяем отпечаток ключа DBA.gpg, полученного с хоста LinuxHost и сверяем с тем, что нам скажет человек из бригады LinuxHost. Он ответил нам, что его ключ имеет такой отпечаток:
DE93 0BED 3795 B3CB C05C 4EDE FBDA 1979 8336 DE19 **(1)**

Теперь проверяем отпечаток импортируемого ключа с отпечатком ключа выше:

```
[root@LinuxDBA .gnupg]# gpg --fingerprint
/root/.gnupg/pubring.gpg
------------------------
pub  1024D/8336DE19 2007-01-12 USER12 (user12 key) <USER12@DITUD.RU>
     Отпечаток ключа = DE93 0BED 3795 B3CB C05C  4EDE FBDA 1979 8336 DE19          (2)
sub  1024g/8AB28EBF 2007-01-12

pub  1024D/16A32630 2007-01-12 USER11 (user11 key) <USER11@DITUD.RU>
     Отпечаток ключа = 8CE7 02AC 864F F232 FAFD  31ED CA1E 2185 16A3 2630
sub  1024g/26DC2141 2007-01-12
```

Как видно (1) и (2) отпечатки совпадают, поэтому можно спокойно подписывать полученный ключ:

```
[root@LinuxDBA ~]# gpg --edit-key USER12
gpg (GnuPG) 1.2.6; Copyright (C) 2004 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


pub  1024D/8336DE19  создан: 2007-01-12 истекает: никогда    доверие: -/-
sub  1024g/8AB28EBF  создан: 2007-01-12 истекает: никогда
(1). USER12 (user12 key) <USER12@DITUD.RU>

Команда> sign

pub  1024D/8336DE19  создан: 2007-01-12 истекает: никогда    доверие: -/-
 Отпечаток главного ключа: DE93 0BED 3795 B3CB C05C  4EDE FBDA 1979 8336 DE19

     USER12 (user12 key) <USER12@DITUD.RU>

Как хорошо Вы проверили то, что ключ действительно принадлежит человеку,
чье имя указано в User ID ключа?
  Если Вы не знаете что ответить, введите "0".

   (0) Не буду отвечать. (по умолчанию)
   (1) Я не проверял совсем.
   (2) Я проверил частично.
   (3) Я проверил очень тщательно.

Ваш выбор? (введите '?' для большей информации): 3
Вы уверены, что хотите подписать этот ключ
своим ключом: "USER11 (user11 key) <USER11@DITUD.RU>" (16A32630)

Я очень тщательно проверил этот ключ.

Действительно подписать? y

Необходим пароль для доступа к секретному ключу пользователя:
"USER11 (user11 key) <USER11@DITUD.RU>"
1024-бит DSA ключ, ID 16A32630, создан 2007-01-12

Команда> quit
Сохранить изменения? y
[root@LinuxDBA ~]#
```

Просматриваем список подписей на ключе DBA.gpg и видим свою только что добавленную:

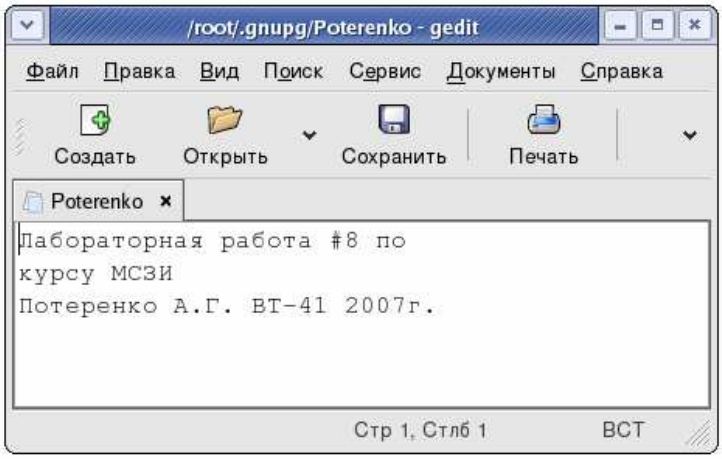
```
[root@LinuxDBA ~]# gpg --edit-key USER12
gpg (GnuPG) 1.2.6; Copyright (C) 2004 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


gpg: проверка таблицы доверий
gpg: проверка на глубину 0 подписаны=1 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: проверка на глубину 1 подписаны=0 ot(-/q/n/m/f/u)=1/0/0/0/0/0
pub  1024D/8336DE19  создан: 2007-01-12 истекает: никогда    доверие: -/f
sub  1024g/8AB28EBF  создан: 2007-01-12 истекает: никогда
(1). USER12 (user12 key) <USER12@DITUD.RU>
```

```
Команда> check
uid  USER12 (user12 key) <USER12@DITUD.RU>
sig!3       8336DE19 2007-01-12   [самоподпись]
sig!3       16A32630 2007-01-12   USER11 (user11 key) <USER11@DITUD.RU>
```

Задание 1.4

Ассиметричный ключ

Зашифруем файл /root/.gnupg/Poterenko с помощью открытого ключа на хосте LinuxDBA и отошлем файл на хост LinuxHost. Т.к. на хосте LinuxDBA уже имеется открытый ключ DBA.gpg, то с его помощью зашифруем сообщение в файле Poterenko.




```
[root@LinuxDBA .gnupg]# gpg --output messagePoterenko.gpg --encrypt --recipient USER12 Poterenko
[root@LinuxDBA .gnupg]# ls
DBA.gpg  messagePoterenko.gpg  Poterenko  pubring.gpg  pubring.gpg~  random_seed  secring.gpg  trustdb.gpg
```

Перемещаем файл messagePoterenko.gpg на хост LinuxHost для расшифровки:

```
[root@LinuxHost .gnupg]# gpg --output messageDecryptPoterenko --decrypt messagePoterenko.gpg

Необходим пароль для доступа к секретному ключу пользователя:
"USER12 (user12 key) <USER12@DITUD.RU>"
1024-бит ELG-E ключ, ID 8AB28EBF, создан 2007-01-12 (главный идентификатор ключа 8336DE19)

gpg: зашифровано 1024-битным ключом ELG-E, ID 8AB28EBF, созданным 2007-01-12
      "USER12 (user12 key) <USER12@DITUD.RU>"

[root@LinuxHost .gnupg]# more messageDecryptPoterenko
Лабораторная работа #8 по
курсу МСЗИ
Потеренко А.Г. ВТ-41 2007г.
```

Симметричный ключ

Проделываем те же самые действия, но с использованием симметричного ключа:

```
[root@LinuxDBA .gnupg]# gpg --output messagePoterenko.gpg --symmetric Poterenko
Введите пароль:
[root@LinuxDBA .gnupg]# ls
DBA.gpg  messagePoterenko.gpg  Poterenko  pubring.gpg  pubring.gpg~  random_seed  secring.gpg  trustdb.gpg
```

А теперь расшифровываем на хосте LinuxHost:

```
[root@LinuxHost .gnupg]# gpg --output messageDecryptPoterenko --decrypt messagePoterenko.gpg
gpg: Данные зашифрованы алгоритмом CAST5
gpg: зашифровано 1 паролем
gpg: ВНИМАНИЕ: целостность сообщения не защищена
[root@LinuxHost .gnupg]# more messageDecryptPoterenko
Лабораторная работа #8 по
курсу МСЗИ
Потеренко А.Г. ВТ-41 2007г.
```

Задание 2.1

На хосте LinuxHost подпишем прозрачной цифровой подписью файл Poterenko.

```
[root@LinuxHost .gnupg]# gpg --output docPoterenko.asc --clearsign Poterenko

Необходим пароль для доступа к секретному ключу пользователя:
"USER12 (user12 key) <USER12@DITUD.RU>"
1024-бит DSA ключ, ID 8336DE19, создан 2007-01-12

[root@LinuxHost .gnupg]# ls
DBA.gpg           Poterenko    pubring.gpg~  revoke.asc   trustdb.gpg
docPoterenko.asc  pubring.gpg  random_seed   secring.gpg

[root@LinuxHost .gnupg]# more docPoterenko.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Лабораторная работа #8 по
курсу МСЗИ
Потеренко А.Г. ВТ-41 2007г.
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.6 (GNU/Linux)

iD8DBQFFqAKu+9oZeYM23hkRAtgSAJwOQDb32An5VZIqpRGKDLSuP0ZF4gCfXRNr
KzkuxPxitYNNTJpU2OHsUhU=
=oOZ+
-----END PGP SIGNATURE-----
```

Теперь на хосте LinuxDBA с помощью открытого ключа проверим цифровую подпись с **неискаженным документом** docPoterenko.asc:

```
[root@LinuxDBA .gnupg]# gpg --verify docPoterenko.asc
gpg: Подпись создана Сбт 13 Янв 2007 00:50:38 MSK ключом DSA с ID 8336DE19
gpg: Действительная подпись от "USER12 (user12 key) <USER12@DITUD.RU>"
```

с **искаженным документом** docPoterenko.asc:

```
[root@LinuxDBA .gnupg]# gpg --verify docPoterenko.asc
gpg: Подпись создана Сбт 13 Янв 2007 00:50:38 MSK ключом DSA с ID 8336DE19
gpg: ПЛОХАЯ подпись от "USER12 (user12 key) <USER12@DITUD.RU>"
```

Задание 2.2

На хосте LinuxHost подпишем отделенной цифровой подписью файл Poterenko.

```
[root@LinuxHost .gnupg]# gpg --output Poterenko.sig --detach-sign Poterenko

Необходим пароль для доступа к секретному ключу пользователя:
"USER12 (user12 key) <USER12@DITUD.RU>"
1024-бит DSA ключ, ID 8336DE19, создан 2007-01-12

[root@LinuxHost .gnupg]# ls
DBA.gpg           Poterenko      pubring.gpg   random_seed  secring.gpg
docPoterenko.asc~ Poterenko.sig  pubring.gpg~  revoke.asc   trustdb.gpg

[root@LinuxHost .gnupg]# more Poterenko.sig
?
```

Теперь на хосте LinuxDBA с помощью открытого ключа проверим цифровую подпись с **неискаженным документом** Poterenko:

```
[root@LinuxDBA .gnupg]# gpg --verify Poterenko.sig Poterenko
gpg: Подпись создана Сбт 13 Янв 2007 01:04:28 MSK ключом DSA с ID 8336DE19
gpg: Действительная подпись от "USER12 (user12 key) <USER12@DITUD.RU>"
```

с **искаженным документом** Poterenko:

```
[root@LinuxDBA .gnupg]# gpg --verify Poterenko.sig Poterenko
gpg: Подпись создана Сбт 13 Янв 2007 01:04:28 MSK ключом DSA с ID 8336DE19
gpg: ПЛОХАЯ подпись от "USER12 (user12 key) <USER12@DITUD.RU>"
```