

Лабораторная работа №3.
Программа для шифрования и подписи GPG,
пакет Gpg4win

Климов Сергей

21 марта 2016 г.

Оглавление

1	Цель работы	2
2	Описание работы	2
3	Ход работы	4
	3.1 Создание ключевой пары openPGP	4
	3.2 Экспорт сертификата	4
	3.3 Поставить ЭЦП на файл	4
	3.4 Работа с чужим сертификатом	7
	3.5 Использование GNU Privacy handbook	8
4	Вывод	10

1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

2 Описание работы

Цифровой сертификат – это электронный документ, который выдается и заверяется Центром Сертификации (ЦС). Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра, т.е. Центра Сертификации. Цифровой сертификат выдается физическому лицу, который является владельцем закрытого ключа электронной цифровой записи (шифрования), который соответствует открытому ключу. Цифровой сертификат содержит следующую информацию: имя и идентификатор владельца сертификата, открытый ключ подписи, имя, идентификатор и цифровую подпись Центра Сертификации, серийный номер, версию и срок действия сертификата. Владелец сертификата может быть уверен, что информация, которая передается им электронным способом, не будет прочитана, похищена или подменена во время ее передачи через интернет. securitylab.ru

Шифрование – метод, используемый для преобразования данных в шифрованный текст для того, чтобы они были прочитаны только пользователем, обладающим соответствующим ключом шифрования для расшифровки содержимого. Шифрование используется тогда, когда требуется повышенный уровень защиты данных - при хранении данных в ненадежных источниках или передачи данных по незащищенным каналам связи. В зависимости от структуры используемых ключей, среди методов шифрования выделяют симметричное шифрование и асимметричное шифрование. Симметричное шифрование предусматривает доступность алгоритма шифрования посторонним лицам, однако ключ (одинаковый для отправителя и получателя) остается неизвестным. При асимметричном шифровании посторонним лицам известен алгоритм шифрования и открытый ключ, однако закрытый ключ известен только получателю. securitylab.ru

Электронная цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося. russika.ru

При выполнении лабораторной работы для создания сертификатов, шифрования и создания ЭЦП используется пакет Gpg4win. Он включает в себя:

- версию GnuPG — свободная программа для шифрования информации и создания электронных цифровых подписей;
- Kleopatra (менеджер сертификатов для OpenPGP и X.509);
- GPA (альтернативный менеджер сертификатов (GNU) для OpenPGP и X.509);

- другие компоненты.

3 Ход работы

Для работы будем использовать графическую оболочку "**Клеопатра**".

3.1 Создание ключевой пары openPGP

Для создания новой ключевой пары OpenPGP была выполнена команда "*File -> New Certificate*". После чего была введена персональная информация: имя сертификата, адрес электронной почты пользователя.

После этого созданный сертификат был импортирован в графическую оболочку "**Клеопатра**" (рисунок 1).

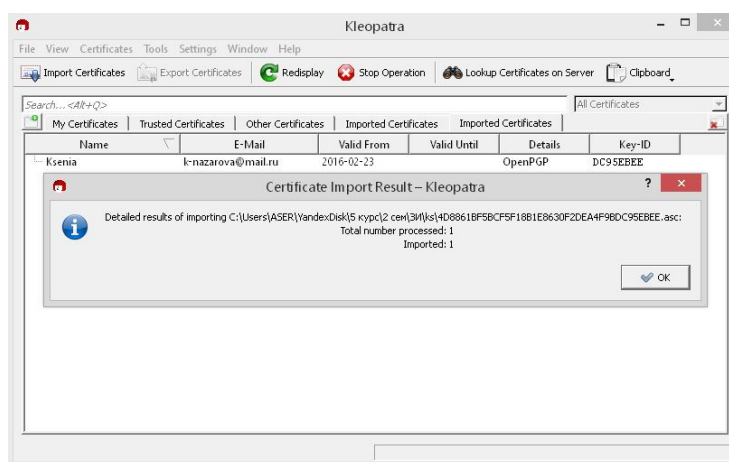


Рис. 1: Окно для ввода персональных данных.

3.2 Экспорт сертификата

Для экспорта сертификата выполним команду "*File -> Export Certificate*".

3.3 Поставить ЭЦП на файл

Для того, что бы поставить ЭЦП на файл была выполнена команда "*File -> Sign/Encrypt Files*", затем был выбран файл, на который необходимо поставить ЭЦП.

После выберем одно из трех предложенных действий.

- Sign and Encrypt
- Encrypt
- Sign

Был выбран пункт *Sign and Encrypt* - создание цифровой подписи и шифрование файла (рисунок 2).

Был выбран открытый ключ получателя (рисунок 3).

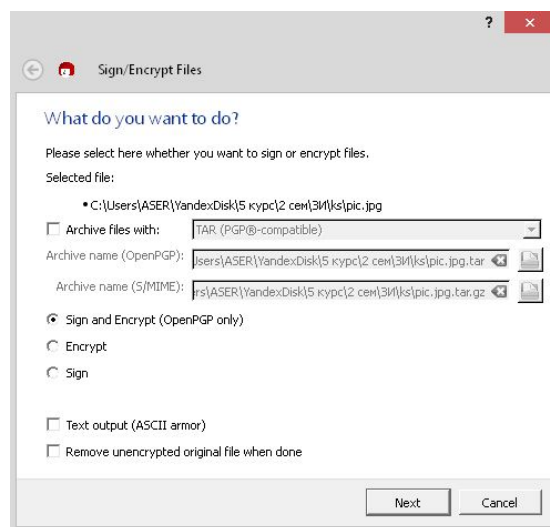


Рис. 2: Поставить ЭЦП на файл и зашфровать

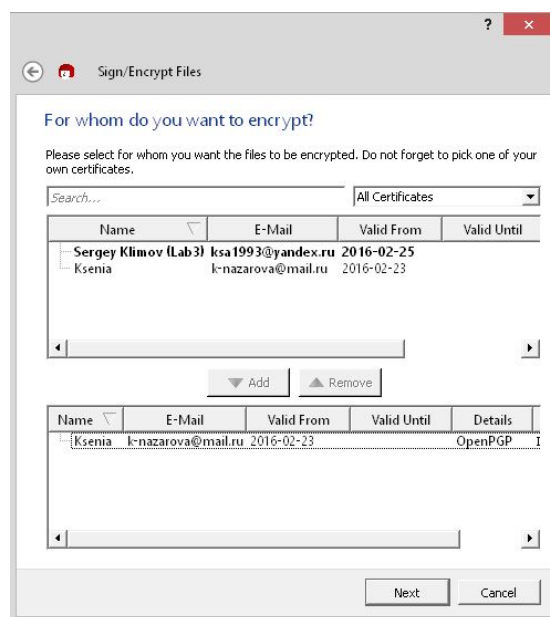


Рис. 3: Выбор открытого ключа получателя

Был выбран стандарт OpenPGP для подписи и сертификат, созданный ранее (рисунок 4).

После ввода пароля выводится сообщение об успешном создании подписи

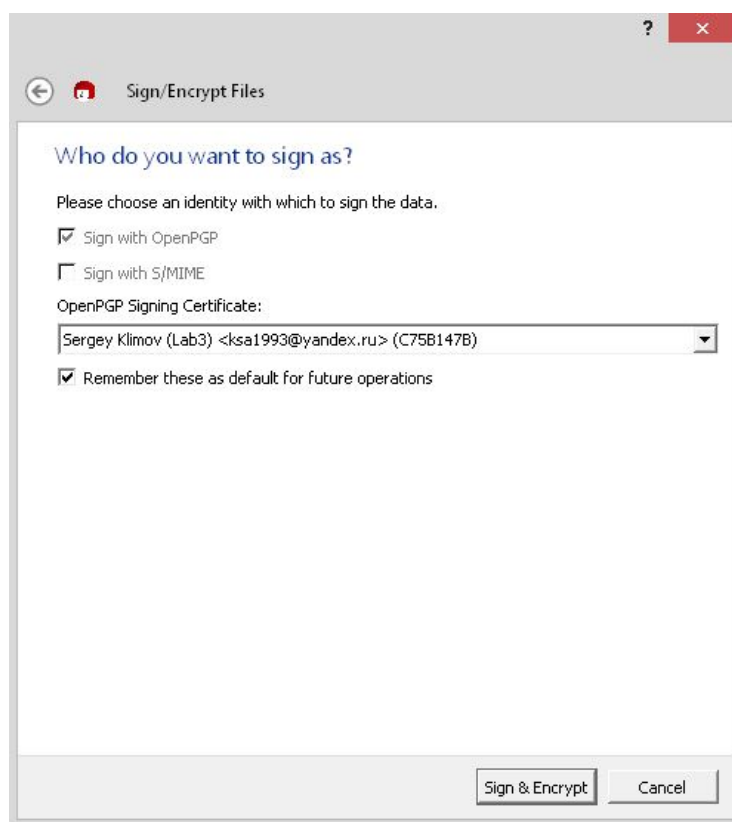


Рис. 4: Выбор стандарта OpenPGP и сертификата для ЭЦП на файл (рисунок 5).

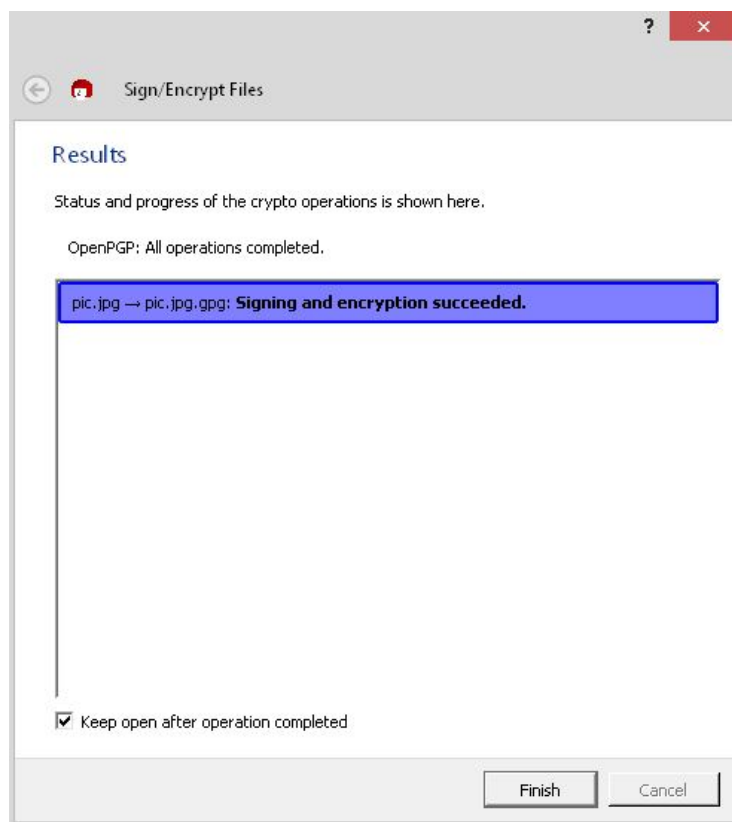


Рис. 5: Успешная подпись файла

3.4 Работа с чужим сертификатом

Был импортирован сторонний сертификат, после этого с его помощью был зашифрован и подписан документ *pic.jpg*. Далее зашифрованный файл *pic.jpg.gpg* был отправлен коллеге для расшифровки.

Далее от коллеги был получен файл *hello.txt.gpg*, который был подписан при помощи моего открытого ключа. Затем командой *File -> Decrypt/Verify Files* расшифруем документ (рисунок 6).

После ввода пароля видим окно с сообщением об удачном расшифровании файла (рисунок 7), также появился файл *hello.txt*, который можно прочитать.

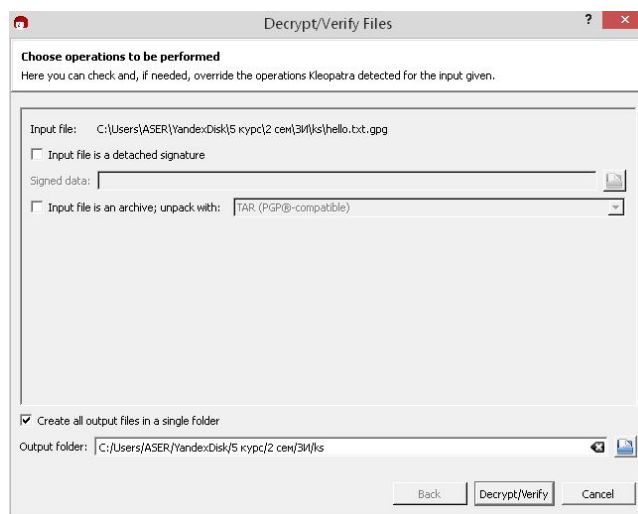


Рис. 6: Расшифровка файла

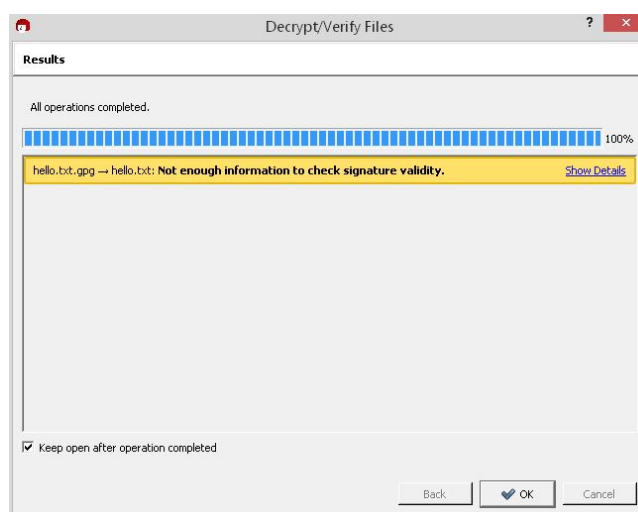


Рис. 7: Успешное расшифрование файла

3.5 Использование GNU Privacy handbook

С помощью GNU Privacy handbook проделаем некоторые действия по использованию gpg через командную строку.

Для создания ключевой пары введем в консоле команду *gpg --gen-key*. Далее выберем тип ключа, его размер, срок действия, укажем ID пользователя, электронную почту, введем пароль, после чего создастся ключевая пара. Был создан ключ типа RSA, размером 2048, с неограниченным сроком действия (рисунок 8).

```
C:\Windows\system32\cmd.exe

D:\Serg_workspace\InfoSecCourse\InfoSecCourse\gpg\cmd>gpg --gen-key
gpg (GNU GPG) 1.4.13; Copyright (C) 2012 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.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysizes do you want? (2048) 2048
Requested keysizes is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Sergey Klimov
Email address: ksa1993@yandex.ru
Comment: Lab1
You selected this USER-ID:
"Sergey Klimov (Lab1) <ksa1993@yandex.ru>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

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 C9B5B6F2 marked as ultimately trusted
public and secret key created and signed.
```

Рис. 8: Создание сертификата

Выведем список всех ключей командой `gpg --list-keys` (рисунок 9).
Подпишем файл `pic.jpg` (рисунок 10).

```
C:\Windows\system32\cmd.exe

D:\Serg_workspace\InfoSecCourse\InfoSecCourse\gpg\cmd>gpg --list-keys
C:/Users/ASER/AppData/Roaming/gnupg/pubring.gpg
-----
pub   2048R/C75B147B 2016-02-25
uid   Sergey Klimov (Lab3) <ksa1993@yandex.ru>
sub   2048R/409CA923 2016-02-25

pub   2048R/DC95EBEE 2016-02-23
uid   Ksenia <k-nazarova@mail.ru>
sub   2048R/AD121C7E 2016-02-23

pub   2048R/1A835486 2016-02-28
uid   Name Test (test certificate) <test@example.com>
sub   2048R/7E07D464 2016-02-28

pub   2048R/C9B5B6F2 2016-03-20
uid   Sergey Klimov (Lab1) <ksa1993@yandex.ru>
sub   2048R/5CABD3CA 2016-03-20
```

Рис. 9: Список сертификатов

```

D:\Serg_workspace\InfoSecCourse\InfoSecCourse\gpg\cmd>gpg --output pic.jpg.gpg -
-sign pic.jpg

You need a passphrase to unlock the secret key for
user: "Sergey Klimov (Lab1) <ksa1993@yandex.ru>"
2048-bit RSA key, ID C9B5B6F2, created 2016-03-20

File 'pic.jpg.gpg' exists. Overwrite? (y/N) y

```

Рис. 10: Создание сертификата

Выведем на консоль содержимое файла сертификата (рисунок 11).

```

D:\Serg_workspace\InfoSecCourse\InfoSecCourse\gpg\cmd>gpg --armor --export ksa19
93@yandex.ru
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.13 (Mingw32)

mQENBFbYCTUBCAP3qAXHgt3NUSFXDX28j8I6h4yUyc0CwaA/Ku19Vdd2GzeqkI8
cS/s/c+hIeKSLNUGT7MH8DmbbX0D7Qvxyo/MpuY5jz01xfIN6esj3xiScub9KtZ
Ik+YbE965GP6PDgu53YDEN9b6v3ksa6p6QHnq4XTeda9V7mXqe8DpLV1Y1zHXG1
Qaver3SMcC5gZKRqkjaAT65Y8hSe6ro/o/Qko2/jpJHysLdISQKgz63oImJ/T2w
ZZvhluxrrant/MtCV4LdADA173w7SUKWGD0MIXCsjcNAKXPVOSLR8s0AgxZXloqn
xFeZw8tAqBa8j8Kn18xv8GYSPd9EIHfFHBv3ABEBAAG0KFN1cmdleSBLbGltb3Yg
KEXhYjEpIDxrc2ExOTkzQH1hbMR1ec5ydt6JATgEewECACIFAlbYCTUCGwMGcwKI
BwMCBhUIAgKCKCwQWAgMBAh4BAheAAAOjEkoQHkFJtbby4G8IAPGxQx1Aw1FKKApe
hZqaCipYtXIuZ4t9D2N2ygd7pYfVfudMnnJEPcSqVXvwj28XSAETggDhoGn96e2T
1srXRQ19TjefIJfVioPqu5gw4C90fdyBUmKUKK14jLmmNsRMCWFZi2wwwr1o7C9
CRW2PTS/Rx/JVFGDMYeyb0cT287uzrS/w8DmRfcanez17Yid9v6FIUuEt01aBH7y
WITWpn48PocxVT1qcb8gQxaYwPQWZw1jQfE+bwAi+fYwkFB1xVp3ofrww42Xea+Qe
5VB5nYZKE4khp/8S14pE04EuXMMbncIn62XGd5zrAFwD4k9YXbIGd1UarkTJpER
kzxx1t65AQ0EVu8IhQEIAN0RVIRZPhtFL4pPQMj/12Zy20Xgu6A9RqDJpKRC3zt5
PffVfaeExKbuZc1bV95vQ5j1R5SLmb94nj11E9tbX8fD0j9Ib/nTRvpt8Dau/8Bw
bc6n/VScE4oYcnuDxwIN/z5Hg1ltGiutQPrLOPVt3TTbmc1TVeL3oULR2h80EAYv
ax4zt5Q+xxw+leuIj0TV12rJN2QIwOVVsTw9w1n8H9s0as24Vv73ED824wPiygvZ
OgoQIAyda8XrzgZyT+gxZ/ykVgv/t/PbfwOXGpcmlb631CyoqpugnSQdiga1fAAS
2pPM7sUdxY8aesmN5/rjxOPJlFKhoQ54Hxxp+N1ZTw0AEQEAAYk8hwQYAQIAACOU
Vu8IhQIbDAACRCRCqEISqybW28gi5B/4/Y7Cra9/xmTtFbFgbcNQuQCieptd70k/I
KX/73TtjSiz/qGBecjFwISEEa/t21fZ1vB1gf08Yde5qajsQofov06y6g0QzXm7c
uLp6vuz/j8c8dGVCyhIb/Lru/Ja5ZJbvM6Ccx81k5xFz50UVKC4D8m1N1HF1ie75
FWVTqfS0mc3YM6s5ioYqWL27KFGnnshko6Pee6Q4C33d7RV1tue8CG9XAuo1ZCJ
0Ty1GUFnzsgFEmCNGUAWEG017PCvjkaCvZjBkoof8dc/3jta51hf
=k+MF
-----END PGP PUBLIC KEY BLOCK-----

```

Рис. 11: Содержимое файла сертификата

4 Вывод

В результате выполнения лабораторной работы был изучен пакет Gpg4win. Были получены практические навыки создания ключевых пар, подписи, шифрования и дешифрования файлов при помощи графической оболочки **Kleopatra**, а также при помощи консольной утилиты **gpg**.