Санкт-Петербургский политехнический университет Петра Великого
Институт Информационных технологий и управления

Программа для шифрования и подписи GPG,пакет Gpg4win

Выполнил: Сухинин А.А. гр. 53501/3 _____
Принял: Выглежанина К.Д. _____

2015 г.

1 Цель реботы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

2 Ход работы

Изучить документацию, запустить графическую оболочку Kleopatra

GPG4Win - это установочный пакет для ОС Windows (2000/XP/2003/Vista/7), содержащий набор программ и руководств для подписи и шифрования документов. Их работа основывается на алгоритмах асимметричного шифрования. Пакет содержит два руководства: один для новичков и один для продвинутых пользователей.

Версия GPG4Win 2 включает следующие программы:

1. GnuPG - программа шифрования
2. Kleopatra - графическая оболочка
3. GNU Privacy Assistant (GPA) - графическая оболочка (альтернатива)
4. GnuPG for Outlook (GpgOL) - расширение Microsoft Outlook для шифрования и подписи сообщений
5. GPG Explorer eXtension (GpgEX) - расширение Windows Explore для шифрования и подписи файлов используя контекстное меню
6. Claws Mail - полноценная программа для работы с почтой, предлагающая хорошую поддержку GnuPG

Основная идея асимметричного шифрования, в отличие от симметричного, заключается в создании пары различных ключей. Один для шифрования и один для расшифровки сообщений. Несмотря на то, что ключи связаны друг с другом, на практике оказывается невозможным нахождение одного ключа из другого.

В сочетании с хэшированием асимметричное шифрование часто используется для создания цифровой подписи. В этом случае, обычно создается и шифруется дайджест подписываемого документа, а второй ключ выкладывается в открытый доступ. При желании, любой человек может проверить, расшифровывается ли данный дайджест публичным ключом или нет. Возможность расшифровки открытым ключом подтверждает факт, что дайджест был зашифрован владельцем закрытого ключа. В тоже время, операция создания дайджеста на практике является необратимой. Это означает, что для существующего дайджеста нельзя создать новое подделанное сообщение.

Документация по GPG4Win достаточно объемная, поэтому более подробное знакомство с ней будет осуществлено по ходу выполнения работы.

Создать ключевую пару OpenPGP

Для создания ключевой пары необходимо выбрать пункт меню File - New Certificate - Create Personal OpenPGP key pair. Необходимо указать собственные данные, а также указать пароль для секретного ключа.

Экспортировать сетрификат

Для экспорта сертификата необходимо вызвать контекстное меню на сертификате и выбрать пункт Export Certificates. Данный сертификат был экспортирован в корень репозитория.

Также необходимо экспортировать секретный ключ на случай непредвиденных обстоятельств. Для этого необходимо вызвать контекстное меню на сертификате и выбрать пункт Export Secret Keys. Секретный ключ, разумеется, в репозиторий не выкладывается.

Поставить ЭЦП на файл

Поставить ЭЦП на файл можно двумя способами. Используя графическую оболочку Kleopatra это можно сделать через меню File - Sign/Encrypt Files. Далее необходимо выбрать файл и указать тип действия (шифрование, подпись, оба). Файлы lab1.tex и lab2.tex были подписаны. Их подписи расположены в том же каталоге что и сами файлы.

Существует более удобный способ подписи используя GpgEX. В проводнике достаточно в контекстном меню выбрать пункт Другие параметры GPG - Подписать. В этом случае нет необходимости выбирать действие и искать файл через диалоговое окно (да и вообще открывать графический интерфейс).

Получить чужой сертификат из репозитория

Из каталога `https://github.com/vilegzhanina/InfoSecCourse2015/tree/master/%D0%9E%D1%82%D1%87%D0%B5%D1%82%D1%8B/01_LaTeX_Git_GPG` были скачаны файлы karina.asc, myfirst.pdf, myfirst.pdf.sig.

Импортировать сертификат, подписать его

Используя меню File - Import Certificates графической оболочки Kleopatra импортируем сертификат. Далее вызываем контекстное меню на сертификате и выбираем пункт Certify Cerificate. Этим действием мы подтверждаем свое доверие к источнику. В случае, если все прошло успешно, сертификат перейдет во вкладку Trusted Certificates.

Кроме того, если до этого мы экспортировали секретный ключ, мы также можем его импортировать используя File - Import Certificates. В этом случае, главное не забыть выбрать в контекстном меню Change Owner Trust и указать, что это ваш сертификат, иначе Ваша заверка не будет учтена.

Проверить подпись

Проверить подпись можно двумя способами: используя GpgEX и Kleopatra. В первом случае достаточно вызвать контекстное меню на файле в проводнике и выбрать пункт расшифровать и проверить. В случае успешной проверки будет выведено сообщение The signature is valid and the certificate's validity is fully trusted. А также показаны данные подписавшего. Для файла myfirst.pdf.sig данные выглядят следующим образом:

Signed on 2015-02-16 10:57 by k.vilegzhanina@gmail.com (Key ID: 0x391EA659).

The signature is valid and the certificate's validity is fully trusted.

Другой способ - это в графической оболочке Kleopatra выбрать пункт меню File - Decrypt/Verify File и указать файл подписи. Дальнейшие результаты и действия аналогичны.

Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой-либо текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись

Для примера был взят сертификат Баринова Д.С. и импортирован согласно предыдущим пунктам. (файл Kikersertificate.asc)

Далее был создан файл messageToBarinov.txt с текстом:

Как поживает твоя *.

Где * заменяет определенное слово. Данный текст был зашифрован для пользователей barinov и Karina Vilegzhanina <k.vilegzhanina@gmail.com>. Для этого в контекстном меню файла был выбран пункт зашифровать и подписать. Это же можно сделать при помощи меню Kleopatra.

Баринов Д.С. подтвердил получение и расшифровку сообщения и посмеялся. Также подтвердил, что документ подписан.

Предыдущий пункт наоборот

От Баринова Д.С. был получен файл messageToSuhinin.txt.gpg

Сертификат импортирован в предыдущем пункте.

Для расшифровки был в контекстном меню был выбран пункт Расшифровать и проверить. Расшифровку можно провести также и при помощи графической оболочки Kleopatra выбрав соответствующий пункт меню File.

Текст сообщения следующий: Все очень плохо(Документ подписан: Signed on 2015-05-24 22:01 by barinovdmitrii@gmail.co
(Key ID: 0x84579FB6).

Используя GNU Privacy handbook (ссылка в материалах) потренироваться в использовании gpg через интерфейс командной строки,без использования графических оболочек

1. Создание пары ключей:

   gpg –gen-key

   gpg (GnuPG) 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 keysize do you want? (2048)
Requested keysize 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: Suhinin Alexandr
Email address: suhinin.alex@gmail.com
Comment:
You selected this USER-ID:
"Suhinin Alexandr <suhinin.alex@gmail.com>"

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 52EE183C marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 2 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: depth: 1 valid: 1 signed: 0 trust: 1-, 0q, 0n, 0m, 0f, 0u
pub 2048R/52EE183C 2015-05-24
Key fingerprint = 8D1D 2045 011B 0F37 7FA4 A064 0E1E 6444 52EE
183C
uid Suhinin Alexandr <suhinin.alex@gmail.com>
sub 2048R/F6FB8620 2015-05-24

2. Экспорт сертификата:

   gpg –armor –export suhininalex@gmail.com
   —BEGIN PGP PUBLIC KEY BLOCK—
   Version: GnuPG v1.4.13 (MingW32)

   mQENBFVhpmMBCADoxGYGXVqwuf/X48f5bV91ds5susOX2mR77GmdBsidrF8ECwQq
   aLAEEtHJqvvrBzNrD0++o+kgmb9IZZ5NGY67cR2fkgAxBOnm2ukgzho9iJJipd5W
   0KSrsfx/6gLiopHBUNDjAOZRnzXT3AQ2zjMgFYjAEw/iexuMa5qqefaGFkUKWD2T
   dGKQ8/C2zeUhFpUt1bk/0W1ISFSIEac2OCYI6E2eNu0k3jgF0DfCPPc3t7JpDgpu
   XvRFv/GPY/S8eEJRRi8LcR9bXM3c9m0zI0JB7oRvpkmgBPjFmGo8Xehy7Qq051Mr
   4yZkfiQiAGCRR2gGSIXsrPPJdDWmVKmQFqBZABEBAAG0JFN1aGluaW4gQWxleCA8
   c3VoaW5pbmFsZXhAZ21haWwuY29tPokBOQQTAQgAIwUCVWGmYwIbDwcLCQgHAwIB
   BhUIAgkKCwQWAgMBAh4BAheAAAoJENcnscQquDRqbGcH/0hRNiVcLlnqFBITvQnS
   /pfG198Z4cPYneaacHUtNDX9ywYgTmjfDN9D93uzoWsOg32fTM0A5ZBhgLokUhvz
   ZfVhePAez0ffK9Z9URb2PRe+HaCIzYXBmjfXMYT/7gsUSppQh66B6Rs3KdJc9dP3
   9vw3ZiHjJaC5nqIIHJYOQkYVviuuVDsrZVN8WHbuS5+Nj5ea526dRS+plGr14McA
   TN2IrvUQp0w2VCXkagWXwYye4qnpuuXITjXPUgGbSaSTz8JuPo436a4RVoGAFT02
   4QqAKb9WEQMrNYujU9PE++VHMH3UIfXcJwAJ4h1Ri5cX8oWEkT/pMVP6RiSCciUf
   j8w=
   =7xTM
   —END PGP PUBLIC KEY BLOCK—

3. Подпись:

   gpg –detach-sign lab3.tex

   You need a passphrase to unlock the secret key for
   user: "Suhinin Alex <suhininalex@gmail.com>"
   2048-bit RSA key, ID 2AB8346A, created 2015-05-24

4. Проверка подписи:

   gpg –verify lab2.tex.sig

   gpg: Signature made 05/24/15 13:25:27 using RSA key ID 2AB8346A
   gpg: Good signature from "Suhinin Alex <suhininalex@gmail.com>"

5. Другие команды:

   gpg –encrypt –recipient blake@cyb.org doc

   gpg –decrypt doc.gpg

   gpg –import blake.gpg

3 Выводы

В ходе работы были опробованы основные возможности GPG4win. Создание пары ключей, сохранение и экспорт сертификата, импорт сертификатов и их проверка, подпись и проверка подписи файлов, шифрование и расшифровка файлов. В ходе работы был опробован графический интерфейс Kleopatra и расширение GpgEX. Некоторые основные команды были также опробованы в консоли.

Личные впечатления от работы с GPG4win остались положительные. Большинство интерфейсов понятны и просты в использовании. Особенно понравилось расширение GpgEX позволяющее подписывать, проверять, шифровать и расшифровывать файлы в несколько кликов. Графический интерфейс Kleopatra также удобен, но требует излишних действий (особенно надоедает постоянный поиск файлов в диалоговом окне). Таким

образом, в будущем, я буду использовать Kleopatra для управления сертификатами, а GpgEX для работы с файлами.

Некоторые основные команды были опробованы также через консоль. Обычно я избегаю использования консоли без необходимости. Консольные команды обычно громоздки и сложны для запоминания,однако в этом случае они просты и интуитивно понятны. И, хотя, при наличии графической оболочки я бы все-равно отдал предпочтение GpgEX, тем не менее использование консоли также является удобным.

В качестве заключения следует еще раз отметить удобство и простоту GPG4win. С уверенностью можно сказать что данный пакет приложений полностью оправдывает свой девиз. Gpg4win - Cryptography for Everyone.