Отчет по лабораторной работе 1: LaTeX, Git, GPG

Федор Кусов
<fdr91@mail.ru>

22 марта 2015 г.

Содержание

1 Система верстки TEX и расширения LATEX

1.1 Цель работы

Изучение принципов верстки TEX, создание первого отчета

1.2 Ход работы

1.2.1 Создание минимального файла .tex в простом текстовом редакторе – преамбула, тело документа

Документ LaTeX — это текстовый файл, содержащий специальные команды языка разметки. Документ делится на преамбулу и тело.

Преамбула содержит информацию про класс документа, использованные пакеты макросов, определения макросов, автора, дату создания документа и другую информацию. Ниже представлена простая преамбула для статьи

```
\documentclass[12pt]{article} % Класс документа article, величина шрифта 12пт.
\usepackage[russian]{babel} % Пакет поддержки русского языка
\title{Отчет по лабораторной работе 1: \Latex{} Git GPG} % Заглавие документа
\date{\today} % Дата создания
```

Тело документа содержит текст документа и команды разметки. Оно должно находиться между командами \begin{document} и \end{document}.

1.2.2 Компиляция в командной строке – latex, xdvi, pdflatex

Работа с файлами на языке latex осуществляется при помощи пакета утилит. Вот некоторые из них:

- latex – принимает файл на языке LATEX на вход, выдавая бинарный файл в формате dvi (от DeVice independent – независимый от устройства). Пример использования:

  ```
  latex report.tex
  ```

  Результатом работы команды будет файл report.dvi

- xdvi – позволяет вывести содержимое .dvi на экран

  ```
  xdvi report.dvi
  ```

  Выведет report.dvi на экран в графическом виде.

- pdflatex – преобразует .tex в формат PDF.

  ```
  pdflatex report.tex
  ```

  Преобразует report.tex в report.pdf

1.2.3 Оболочка TexMaker, Быстрый старт, Быстрая сборка

Texmaker представляет собой редактор текста и исходного кода LaTeX. TexMaker предоставляет доступ к утилитам LaTeX посредством графического интерфейса (GUI) Развитый GUI позволяет ускорить работу с документами за счет таких функций, как автодополнение, быстрое создание документов из шаблонов и т.д.

Быстрый старт (Quick Start) в TexMaker – это мастер для создания новых документов, позволяющий задать основные параметры документа, подключить нужные модули.

Быстрая сборка (Quick Build) специальная кнопка, к которой можно привязать выполнение последовательности команд для сборки и отображения документа.

1.2.4 Создание титульного листа, нескольких разделов, списка, несложной формулы

Титульный лист в LaTeX можно быстро создать командой \maketitle. В шаблон листа при этому будут подставлены такие сведения, как имя автора, учебное заведение, название работы.

Для создания раздела используется команда \section, принимающая название раздела в качестве документа. Подразделы и подподразделы создаются при помощи \subsection и \subsubsection соответственно.

Для создания списка служит пара команд \beginitemize и \enditemize. Записи в списке задаются при помощи команды \item.

LaTeX имеет средства для быстрого написания математических формул. Примеры написания простых формул:

- Индексы:

  `Верхние a^b`

  `Нижние a^b`

- Дроби:

  `a/b`

- Скобки:

  `(a) [] \{a\}`

Возможно записать и более сложные формулы. Например, следующая строка:

```
\iiint_{x^2+y^2+z^2=1} f(x,y,z) dx dy dz
```

Даст на выходе:

$$\iiint_{x^2+y^2+z^2=1} f(x,y,z)dxdydz$$

1.2.5 Понятие классов документов, подключаемых пакетов

Каждый документ в LaTeX начинается с команды `\documentclass[...]{...}`в фигурных скобках которой задаются параметры оформления стиля документа, а в квадратных — список классовых опций.

В LaTeX существует 5 основных классов документов:

- article – статья,
- report – небольшая книга, статья, разбитая на главы
- book – книга,
- proc – возможно использовать для докладов
- letter – деловое письмо.

Помимо этих основных, есть ещё множество дополнительных классов, таких как beamer.

Пакеты в позволяют расширять, если это требуется, возможности LaTeX. Для подключения пакетов используется команда `\usepackage[опции]{пакет}`.

Некоторые пакеты включены в стандартную установку LaTeX. Другие можно поставить отдельно. Информацию о существующих пакетах можно получить при помощи The LaTeX Companion.

1.3 Выводы

Рассмотрим систему LaTeX с точки зрения её достоинств и недостатков.

Недостатки:

- сложность изучения – LaTeX сложно использовать и изучать одновременно. Изучение требует сознательного обучения.
- создание новых стилей оформления – сложная задача. Как правило, обычные пользователи не в силах с ней справиться

Достоинства:

- Высокое качество результата, недоступное другим средствам полиграфической подготовки (верстки) текстов.
- Гибкость
- Простота подготовки очень сложных документов самым неискушенным пользователем.
- Большое количество макропакетов, позволяющих сделать все, что угодно.
- Низкие системные требования.

- Высокая переносимость - один и тот же результат на любой технике.
- Поддержка любых языков в рамках одного документа.
- Строгий подход к оформлению удерживает пользователя в рамках полиграфических приличий.
- Удобная работа с математическими формулами
- Пользователь должен знать всего несколько легко запоминающихся команд, которые определяют логическую структуру документа, и почти не должен знать о том, как документ форматируется.
- Сложные элементы текста, такие как сноски, библиография, оглавление, список таблиц и т.п., а также простые рисунки могут быть выполнены без особых трудностей.

Первое знакомство с LaTeX оставило приятное впечатление. Если сравнивать LaTeX с Microsoft Word, при решении таких задач, как, например, написание выпускной работы бакалавра, создается впечатление, что LaTeX позволил бы гораздо меньшими усилиями написать хорошо структурированную работу, соответствующую ГОСТам, правильно оформить рисунки, таблицы, формулы,список литературы и сноски.

2 Система контроля версий Git

2.1 Цель работы

Изучить систему контроля версий Git, освоить основные приемы работы с ней.

2.2 Ход работы

2.2.1 Изучить справку для основных команд

Справка для основных команд была изучена автором ранее при работе над студенческими проектами с использованием Github для хранения версий.

2.2.2 Получить содержимое репозитория

Для получения содержимого репозиторию используется команда clone

```
git clone https://github.com/fdr91/InfoSecCourse2015
```

2.2.3 Добавить новую папку и первый файл под контроль версий

Для этого может быть использована последовательность команд:

```
mkdir folder
git add folder
echo 1 > folder/file.txt
git add folder/file.txt
```

2.2.4 Зафиксировать изменения в локальном репозитории

```
git commit -m "Add folder/file.txt under version control"
```

2.2.5 Внести изменения в файл и просмотреть различия

```
echo 2 >> foder/file.txt
git diff folder/file.txt
```

2.2.6 Отменить локальные изменения

```
git checkout
```

2.2.7 Внести изменения в файл и просмотреть различия

```
echo 2 >> foder/file.txt
git diff folder/file.txt
```

2.2.8 Зафиксировать изменения в локальном репозитории, зафиксировать изменения в центральном репозитории

```
git commit -m "Add changes to folder/file.txt"
git push
```

2.2.9 Получить изменения из центрального репозитория

```
git commit -m "Add changes to folder/file.txt"
git pull
```

2.2.10 Поэкспериментировать с ветками

```
git checkout -b branch
echo 3 >> folder/file.txt && git add folder/file.txt
git commit -m "folder/file.txt modified. Again"
git checkout master
git merge branch
git branch -d branch
```

2.3 Выводы

Git является широкораспространенной системой контроля версий. Автору уже не раз приходилось работать с ней в рамках работы над различными студенческими проектами. Git удобен и прост в использовании. Бесплатный хостинг репозиториев GitHub делает Git доступным благодаря простоте создания собственного репозитория и наличию web-интерфейса для работы с контролем версий и багтрекинга.

Основные преимущества распределённых систем — их гибкость и значительно большая (по сравнению с централизованными системами) автономия отдельного рабочего места. Каждый компьютер разработчика является, фактически, самостоятельным и полнофункциональным сервером, из таких компьютеров можно построить произвольную по структуре и уровню сложности систему, задав (как техническими, так и административными мерами) желаемый порядок синхронизации. При этом каждый разработчик может вести работу независимо, так, как ему удобно, изменяя и сохраняя промежуточные версии документов, пользуясь всеми возможностями системы (в том числе доступом к истории изменений) даже в отсутствие сетевого соединения с сервером. Связь с сервером или другими разработчиками требуется исключительно для проведения синхронизации, при этом обмен наборами изменений может осуществляться по различным схемам.

3 Программа для шифрования и подписи GPG,пакет Gpg4win

3.1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

3.2 Ход работы

3.2.1 Изучить документацию, запустить графическую оболочку Kleopatra

Kleopatra – это менеджер сертификатов, который позволяет работать с GPG. Он предоставляет графический интерфейс для работы с GPG.

3.2.2 Создать ключевую пару OpenPGP

Для создания ключевой пары используется команда File → New Certificate. Информация о созданном сертификате отображается на вкладке My Certificates.

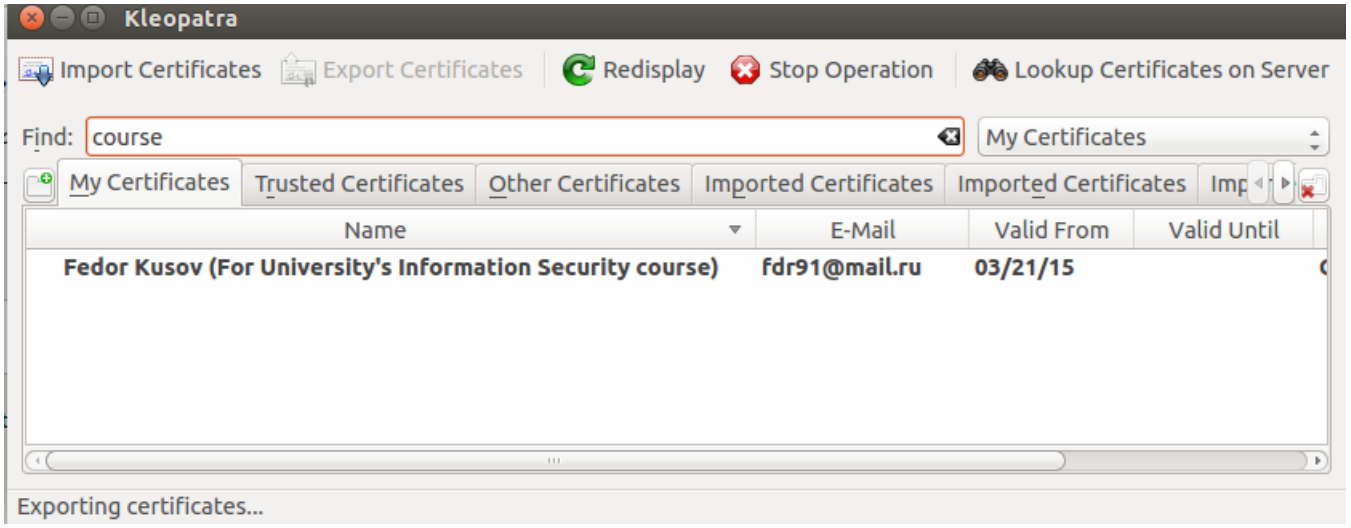

Рис. 1: Созданный сертификат

3.2.3 Экспортировать сертификат

Экспорт сертификата осуществляется командой File → Export Certificate В листинге 1. Представлено содержимое файла-сертификата.

Листинг 1: Сертификат в формате asc (ASCII Armored file)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQENBFUNa/sBCACmei2wrCQvtM9TbCooUCzMp/wcX/bn4DYtOgULyj+zFKlGRPp4
```

```
4mRU42UDsVaspRSdV1VRLNn5+SHOaPoKfdjW1IM1dvOOurPrzPSwqEUv2dI8Or2J
Qe6EESMpfAJgK5wdmMLl7X4vJIcVMOlJbXuKg4yMiFTGIRrBnoysB19BC2UTFhWD
z6ZkVe4Nh+dwF1vAJhi8chxyFPwOY6itciLftZgLgwwaTQvPjXW7uDZF8kyuxe3x
gzf/+dNS/t1br14DplWgu2u9nC5DHe3OQcCBWRYh2SakUkmZs/jeV+sWuwqJksvn
QQsR/NZjBy9Ibv8+v2czioetBCjCrPL4ew59ABEBAAG0SkZlZG9yIEt1c292ICHG
b3IgVW5pdmVyc2l0eSdzIEluZm9ybWF0aW9uIFNlY3VyaXR5IGNvdXJzZSkgPGZk
cjkxQG1haWwucnU+iQE5BBMBAgAjBQJVDWv7AhsPBwsJCAcDAgEGFQgCCQoLBBYC
AwECHgECF4AACgkQlhmhS7ALJDyTZggAjjCvkkSKVHMlA1hUP8V07bOl1RkArlok
GzotjMXl6eyzEp7J4OKVT0hS1j1QGranjIMHNGBaz1ERs2PnmoXl4rflbBGeIAU3
+/rIIjckyXVPZG+PSY8EBqVYKgzTYsz25U9jv4R+GSJfOEKAinmFLzhALF85HYbd
UbLT8xA1UmxhxAdVIg4AI1F9G4S0yDCRleUot9L/D0osPvhUw1wVIqeQ4A6hQ1U0
IZjC7P37k496k8ozrXrt2RDEAK74knq3P1CJg/+yNot8CesVluvh/yrPTtR2Puxb
zdJiFvFewS/zK2ozRm64p1QfvlEMtJNtQhi2VAALPvTDlKg+J2gSng==
=maKR
-----END PGP PUBLIC KEY BLOCK-----
```

3.2.4 Поставить ЭЦП на файл

Для того, чтобы поставить ЭЦП на файл, используется команда File → Sign/Encrypt Files. Результатом выполнения станет появление файла с расширением .sig.

3.2.5 Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой (подписью)

В качестве чужого сертификата был использован сертификат Семена Мартынова из репозитория https://github.com/SemenMartynov/InfoSecCourse2015

3.2.6 Импортировать сертификат, подписать его

Импортирование осуществляется командой File → Import Certificates. Импортированый сертификат отображается во вкладке Imported Certificates Импортированный сертификат

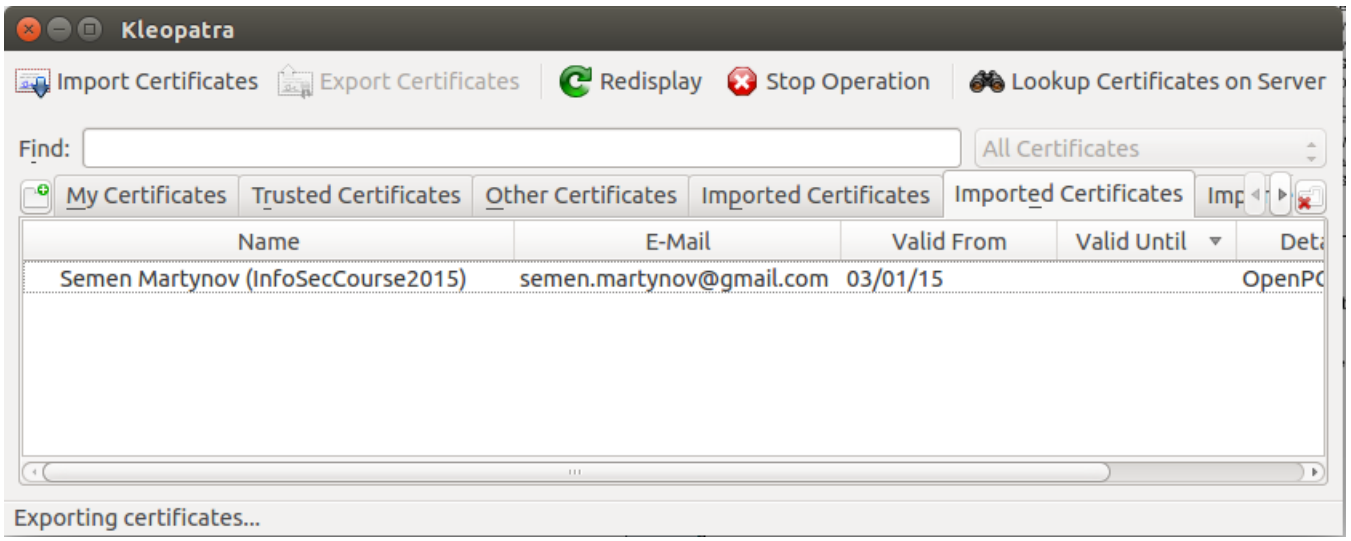

Рис. 2: Импортированный сертификат

нужно подписать. Для этого нужно: Щелкнуть правой кнопкой мышью на сертификате

→ Certify Certificate В открывшемся окне нужно поставить флажок "I have verified the fingerprint".

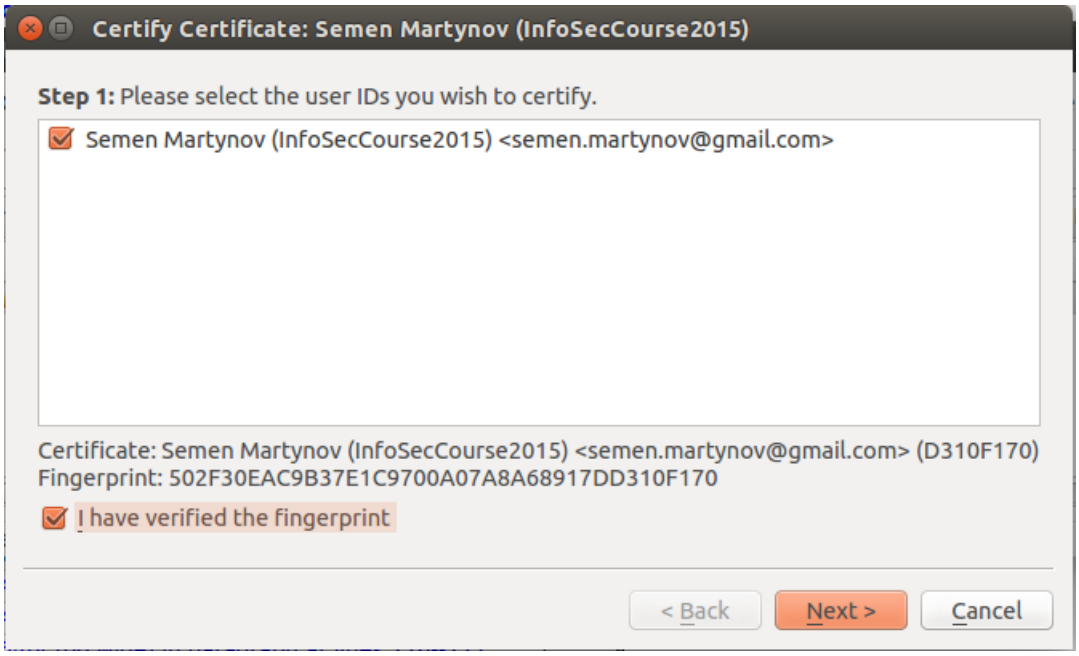

Рис. 3: Импортированный сертификат

3.2.7 Проверить подпись

Для проверки сертификата используется команда File → Verify Certificate.

3.2.8 Используя GNU Privacy handbook потренироваться в использовании gpg через интерфейс командной строки, без использования графических оболочек

Результат, полученный при помощи Kleopatra легко повторить используя терминал. Генерация ключа происходит в диалоговом режиме после ввода команды

```
gpg --gen-key
```

В процессе работы, мастер создания ключа запросит следующую информацию:

- Тип ключа (по умолчанию это DSA и ElGamal).
- Размер ключа (с DSA/ElGamal ключами не использую длину больше чем 2048).
- "срок годности"ключа.
- Информацию о пользователе (имя, электронный адрес).
- Пароль для ключа (если нужен).

В процессе генерации ключа, GnuPG использует энтропию. Для способствования её сбору рекомендуется активно двигать мышкой или запустить mp3 в фоновом режиме.

Просмотреть доступные в системе ключи позволяет команда

```
gpg --list-keys
```

Её вывод показан на рисунке 7.

Для экспорта можно использовать команду

```
gpg --armor --output john.asc --export john@mail.ru
```

Для импорта используется

```
gpg --import tomas.asc
```