Отчет по лабораторной работе №1 : LaTeX, Git, GPG

Анастасия Тарасова

18 мая 2015 г.

1 Система верстки TeX и расширения LaTeX

1.1 Цель работы

Освоить систему верстки TeX и сделать отчет.

1.2 Ход работы

В ходе работы был создан файл с расширением .tex, в котором содержатся команды текстовой разметки.

1.2.1 Компиляция в командной строке

Исходными данными для LaTeX является обычный текстовый файл с расширением .tex. Его можно создать в текстовом редакторе. Существуют текстовые редакторы общего назначения с поддержкой LaTeX (Emacs, vim, geany, Eclipse, Notepad++, TextMate, Sublime Text и т.д.), специализированные текстовые LaTeX-редакторы (TeXstudio, Texmaker, gummi, Kile, TexShop, TeXnicCenter, WinEdt и т.д.), визуальные редакторы (LyX, TeXmacs и BaKoMa TeX Word). Tex-файл содержит текст документа вместе с командами, указывающими LaTeX, каким образом верстать текст. Создание pdf-документа по входному файлу выполняется следующим образом:

- В командной строке необходимо выполнить команду

  `latex <имя входного файла без расширения>`

  Команда преобразует входной файл в в файл формата dvi (Device Independent), пригодный к распечатке. В настоящее время файлы

формата dvi используются для предпросмотра итогового документа. Файл dvi можно просмотреть при помощи утилиты Yap, распространяемой вместе с дистрибутивом MikTeX.

- xdvi одна из программ DVI-драйверов, позволяющих отображать данные в формате DVI в X Window системах

  `xdvi report1.dvi`

  Результат показан на рисунке 1.

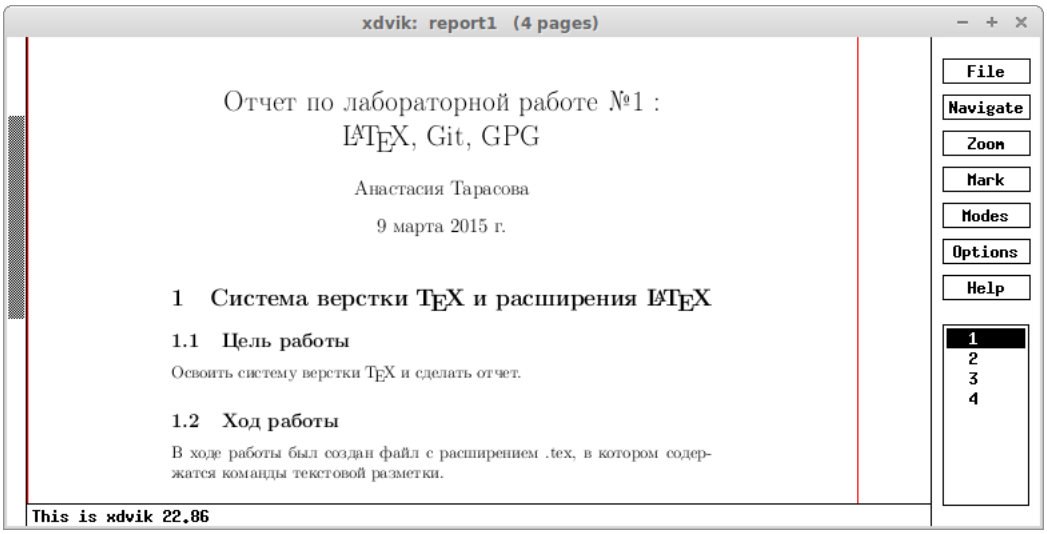

Рис. 1: Заппуск xdvi

- `pdflatex report1.tex`

  Команда создает итоговый pdf-документ.

1.2.2 Оболочка TexMaker

TexMaker - текстовый редактор, работающий с языком разметки LaTeX. TexMaker позволяет работать с фишками профессионального оформления. Внешний вид редактора представлен на рисунке 1. В редакторе TexMaker имеется возможность быстрой сборки и быстрого старта. Чтобы задать преамбулу документа, можно использовать помошника "Быстрый старт"(Меню "Помошник").Этот диалог позволяет задать главные особенности Вашего документа (класс, размер бумаги, кодировку...).

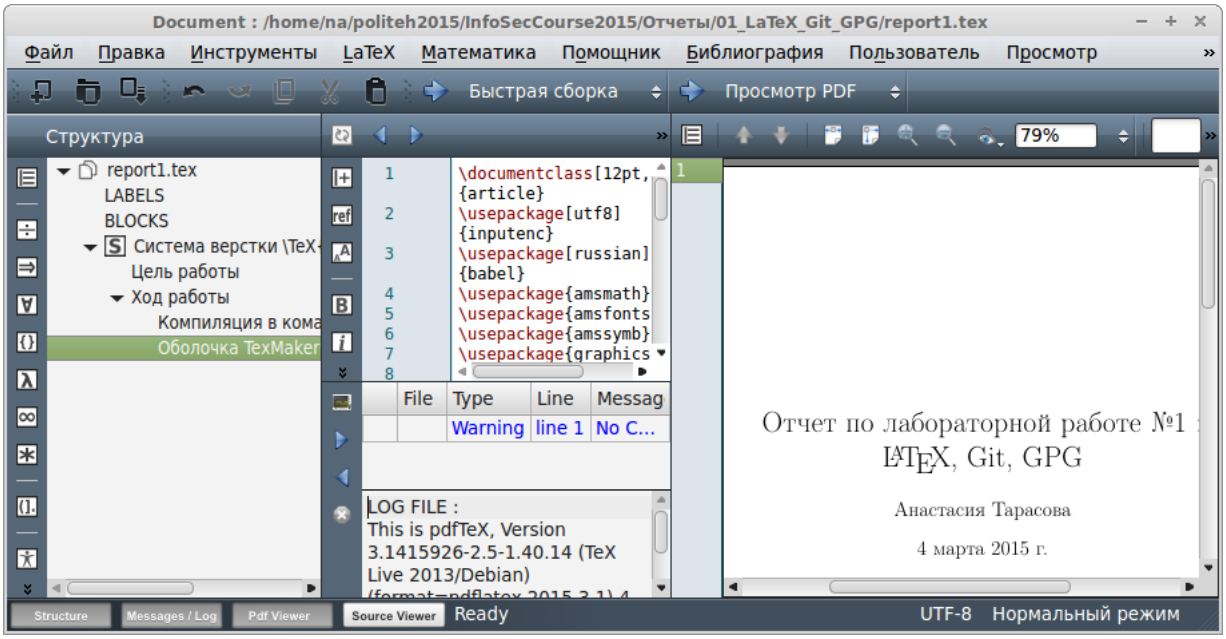

Рис. 2: Редактор TexMaker

1.2.3 Классы документов

В самом начале файла указывается класс документа, который задается командой

`\documentclass[опции]{класс}`

Здесь класс определяет тип создаваемого документа. Опции изменяют поведение класса.

`\documentclass[12pt,a4paper]{article}`

Эта строчка заставляет LaTeX применить следующие правила для документа:

Набирать документ как статью

Базовый размер шрифта - 12

Форматирование для печати на бумаге формата A4

1.2.4 Подключаемые пакеты

В процессе написание документа в некоторых областях базовый LaTeX не сможет решить некоторые проблемы. В подключаемых пакетах можно указать особые настройки.

```
\usepackage{lscape}
```

Данный пакет меняет положение страницы на ландшафтное

1.2.5 Верстка формул

- Степени и индексы
  $a^2 + b^2 = c^2$;
  $a_2 - b_2 = c_2$;
  $a_3^2 + b_3^2 = c_3^2$;
- Дроби
  $\frac{a_3^2+b_3^2}{c_3^2}$;
- Скобки
  $f\{x, y\} = (x^2 + y^2)^2$;
  $\lceil X \rceil, \lfloor Y \rfloor, \langle Z \rangle$;
- Корни, интегралы и дифференциалы
  $\sqrt[3]{x + y}$;
  $\int_0^3 f(x)dx$;
  $\iint_{x^2+y^2=1} f(x, y)dxdy$;
  $\iiint_{x^2+y^2+z^2=1} f(x, y, z)dxdydz$;
  $dz = \frac{\partial z}{\partial x}dx + \frac{\partial z}{\partial y}dy$;

1.3 Выводы

LaTeX – это система набора текста, основанная на специальном скриптовом языке программирования. LaTeX уже давно является стандартом дефакто при наборе научных статей, курсовых и дипломных работ, технических спецификаций, учебников и т. д. Главным преимуществом LaTeX является абсолютно одинаковый внешний вид готовых страниц во всех

операционных системах и непревзойденное до сих пор качество полиграфических текстов и математических формул. Кроме этого, скриптовый язык латеха – это универсальный язык для обмена формулами.

2 Система контроля версий Git

2.1 Цель работы

Научиться работать с системой Git.

2.2 Ход работы

- Получить содержимое репозитория

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

- Работа с ветками

  `git checkout -b laba1` -создвем ветку

  `git push origin laba1` - публикуем ее

  `git branch` - смотрим список веток

  `git checkout master` - переключаемся на ветку master

- Зафиксировать изменения в локальном и центральном репозитории

  `git commit -a -m "file changed"`

  `git push`

- Вытянуть изменения

  `git pull`

2.3 Выводы

GitHub это социальный репозиторий для проектов с открытым исходным кодом, использующих Git для контроля версий исходного кода. Главная задача GitHub - сделать процесс разработки простым и увлекательным, в особенности когда над проектом одновременно работает несколько человек. Использование GitHub также позволяет научиться многим вещам. Базовым кирпичиком git репозитория является коммит (commit). Код со временем меняется, но если вы делаете коммиты, то к любому из них можно вернуться, отмотав время назад с помощью git.

3 Создание электронных цифровых подписей с PGP

3.1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

3.2 Ход работы

3.2.1 Знакомство с пакетом Kleopatra

Kleopatra это графический интерфейс к GnuPG и предназначенных для работы под окружением KDE и портированный на MS Windows (доступные в составе пакета Gpg4win).

При помощи мастера, графический интерфейс позволяет создать сертификат. Его текстовый вид представлен в листинге 1.

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

```
1  -----BEGIN PGP PUBLIC KEY BLOCK-----
2  Version: GnuPG v2
3
4  mQENBFVZFKUBCADK909sWG0ZHkoiObZa+EfLdM+
       SvevHh1qMfa86xtANuobQ2ezC
5  u5bGDL1HA+xg5cJSypk0W3twZ1OcEQGSb529sc/8
       G2aTqx7VW3HYl2t8W9TS8OdG
6  DfcYkNTumr9ymtf2Kl7WbFQ8Zy7z00RM2oIKpfKqLaafbs3FpwMe/
       RdRWZ1kzU/3
7  /fj+
       CQw2tZtNywL1N2VlVj0AdyDf0MYZh0dxotfIfYugCoF7n2sTjB3EjkN9U1fv

8  r8cDUQxh5kEBAuAenAbEbk0AC0ZeWIsw02sDzXIyD1XCAzeWCUmgPbqAH8eD3Pvl

9  1LluXVsXu/EqCK/+rs/
       mke0z2VSkOz4lGXV7ABEBAAG0K0FuYXN0YXNpeWFUYXJh
10 c292YSA8dGFuYXN0YXNpaWFhQGdtYWlsLmNvbT6JATkEEwEIACMFAlVZFKUCGw8H

11 CwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCg8wqfwCAo/BUtB/42
       qnHxiYTp
12 krCyoLGwnL/4OwZBiX6Vw3G1XzuiBjjb/
       eMlDFySuMqV6WHEHDkIOcnl6MRZTMMO
13 8pKzjYQftSKSU79+
       L6nAJaTqHx3MOhQO5wgei8mtRK7Kkp7VQN3eO4pTiSai4ic2
14 FB2y8OZ3+uGwlNcVny3wFrRnXLJGgDV0NWSD7rQAxM3j1tzkspK/Nj+0
       dklOc17k
15 LiIEQqxg1aDLJdUHJ/Or5VMOvVaK1SlcA8B6DOJpepblLGurP5+
       ua0EPFmreiYeD
```

```
16 yY/At4QS5uE/N2w5FAhAWds8f1HFaUUGNqYy+
     klkidVvrHV9NrZaRbJU8IyL0AJy
17 3s60L7E5/T0J
18 =+LxZ
19 -----END PGP PUBLIC KEY BLOCK-----
```

Подпись документа можно сделать используя закрытый ключ. Цифровая подпись сохраняется в отдельный файл с расширением sig. Если зашифровать файл *report1.pdf*, то подпись будет сохранена в файле *report1.pdf.sig* (см. рис. 5).

Программа позволяет импортировать чужие сертификаты, и проверять подписи. На рисунке 6 показан итог импорта чужого файла.

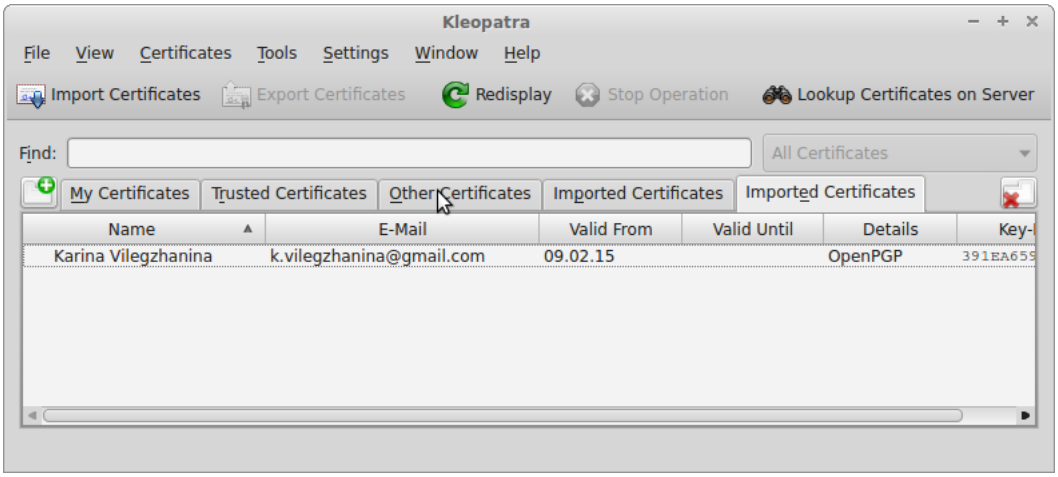

Рис. 3: Импорт чужого ключа в Kleopatra

3.2.2 Использование gpg через интерфейс командной строки

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 ниже. Для экспорта можно использовать команду

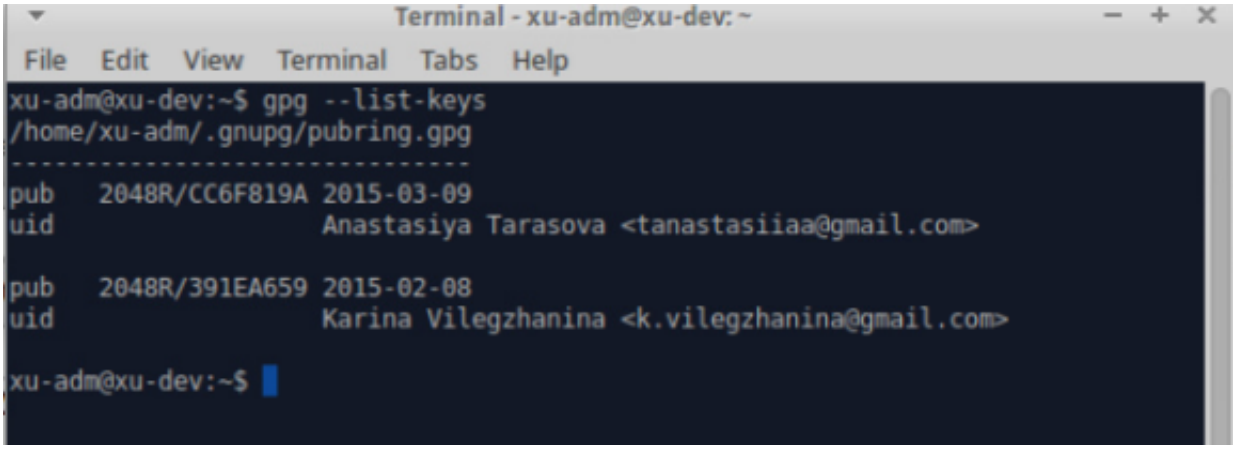

Рис. 4: Список ключей в системе.

(ключ определяется по электронному адресу)

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

Для импорта используется

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

3.3 Выводы

GnuPG шифрует сообщения, используя асимметричные пары ключей, генерируемые пользователями GnuPG. Открытыми ключами можно обмениваться с другими пользователями различными путями, в том числе и через интернет с помощью серверов ключей. Также GnuPG позволяет добавлять криптографическую цифровую подпись к сообщению, при этом целостность и отправитель сообщения могут быть проверены.