

Отчет по лабораторной работе №1 : L^AT_EX, Git, GPG

Анастасия Тарасова

28 марта 2015 г.

1 Система верстки T_EX и расширения L^AT_EX

1.1 Цель работы

Освоить систему верстки T_EX 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 L^AT_EX является обычный текстовый файл с расширением .tex. Его можно создать в любом текстовом редакторе (блокнот, Microsoft Word, встроенный редактор Far и пр.). Он содержит текст документа вместе с командами, указывающими L^AT_EX, 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 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 Yар, распространяемой вместе с дистрибутивом MikTeX.

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

```
xdvi report1.dvi
```

Результат показан на рисунке 1.

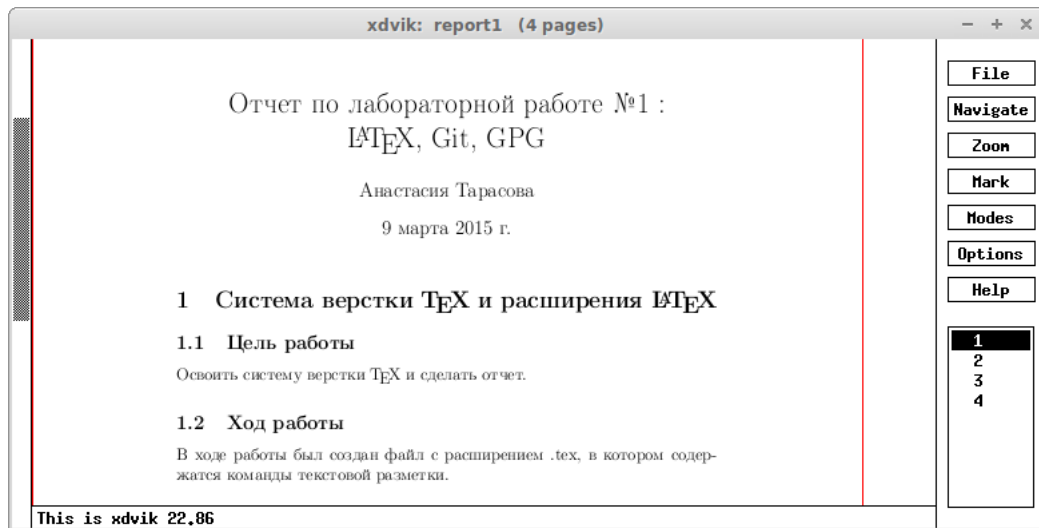


Рис. 1: Запуск xdvı

- 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 помощника "Быстрый старт"(Меню "Помошник").Этот диалог позволяет задать главные особенности Вашего документа (класс, размер бумаги, кодировку...).

1.2.3 Классы документов

В самом начале файла указывается класс документа, который задается командой

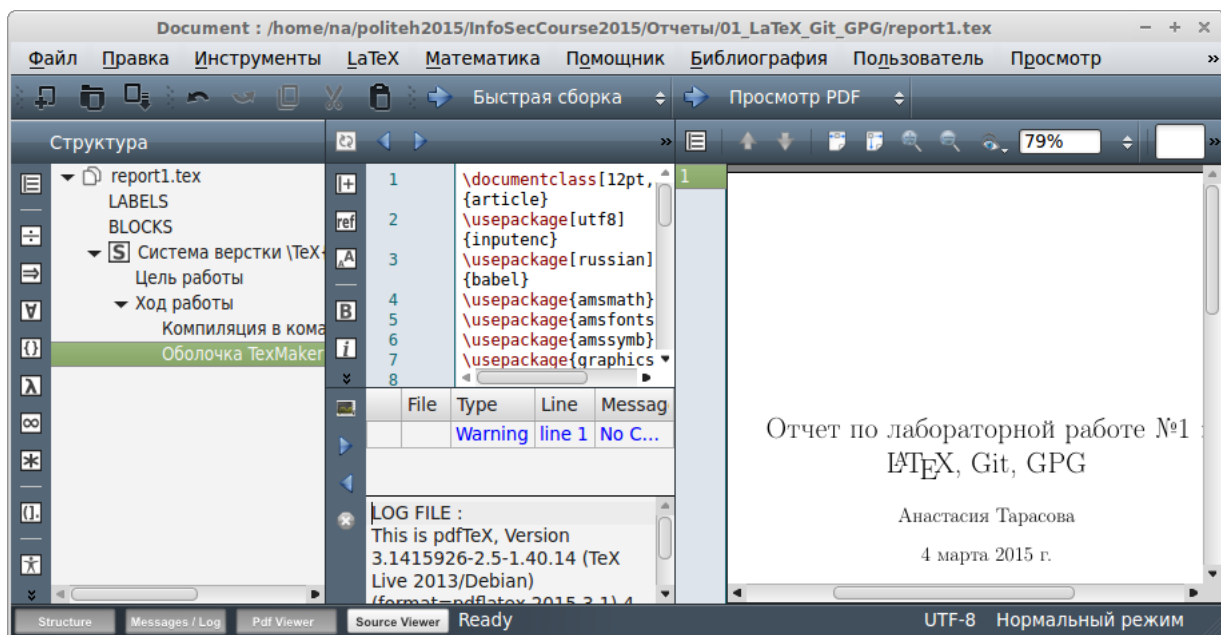


Рис. 2: Редактор TexMaker

`\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 написания 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

$$a^2 + b^2 = c^2;$$

$$a_2 - b_2 = c_2;$$

$$a_3^2 + b_3^2 = c_3^2;$$

- Дробь

$$\frac{a_3^2 + b_3^2}{c_3^2};$$

- Скобки

$$f\{x, y\} = (x^2 + y^2)^2;$$

$$[X], [Y], \langle Z \rangle;$$

- Корни, интегралы и дифференциалы

$$\sqrt[3]{x + y};$$

$$\int_0^3 f(x) dx;$$

$$\iint_{x^2 + y^2 = 1} f(x, y) dx dy;$$

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

$$dz = \frac{\partial z}{\partial x} dx + \frac{\partial z}{\partial y} dy;$$

1.3 Выводы

L^AT_EX – это система набора текста, основанная на специальном скриптовом языке программирования. L^AT_EX уже давно является стандартом де-факто при наборе научных статей, курсовых и дипломных работ, технических спецификаций, учебников и т. д. Главным преимуществом L^AT_EX 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

Клеопатра 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 тексто- вый 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 mQENBFT+
   EDIBCADJUikrI3ECcoEWasgu1frvGSvbSN1nqFRNK2aEAR6qu7dAh5Mc
5 usCPEP2k9+qHZ1/Gh6/1
   kmwcuYk7nQ8wMqRRvTPki9qs0aAz4Ies7yM6BAqErZ7a
6 Me0NtdDAeiJ5mGsTjMa73p135tKIsQ0t7TsWM0vaoC1fg89BiuEF9KqLLTo+y
   +9p
7 ikuaK41mCiKVTM5kN1LBwq6IFZb9iLGrzqrgIgZg5HFeETVdlJEoX66+
   CRpG1YJG
8 OjXDuzdmTecAZZbtBhDK1TJdX+9
   LUbiJYA063K1XrFreyZhWGPT9x008T1Tsu0uN
9 YHnqRcDYyn3e/iNT8b00SABXTr9KBvS+
   rCyNABEBAAGOLEFuYXNOYXNpeWEgVGFy
10 YXNvdmEgPHRhbmfzdgGFzaWlhYUBnbWFpbC5jb20+iQE5BBMBAgAjBQJU/
   hAyAhsP
11 BwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AACgkQ20BZKkYt+cBlkwf+
   IPjXbe2Q
12 apI7DfSw/yb8v/KaDN2k69JvxwXCDGF0yl9qr6eZvH1w00JjXQnyn+bDJ+
   DT4uNe
13 fPCY0EpXZA0Hotvu8ackLtNgiU8SCjVWQeZi44U0Y942uI9z8FhDEgUISffK3ZCx
14 0I7ZJuZm8yIYhYxRDwn5XHH19zfjqBpFx8vKj0XhK7NRpjd330b5pqKZ/8
   zcjZpg
15 fIdDjHwVga0pgn7gIe66f06ndazrL509vU8+
   RlwE6Y0aTlBDZ5bvghaNdA3TosXu
```

```

16 QJPeWZjsw+89eTh02656qwQhWe12BkNpShtpezCh7UjeDB/5
    TxGsSW2c7DL0zXnu
17 xH096/KySDPhIA==
18 =Vacq
19 -----END PGP PUBLIC KEY BLOCK-----

```

Имея свой сертификат, можно подписать любой имеющийся документ. 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.

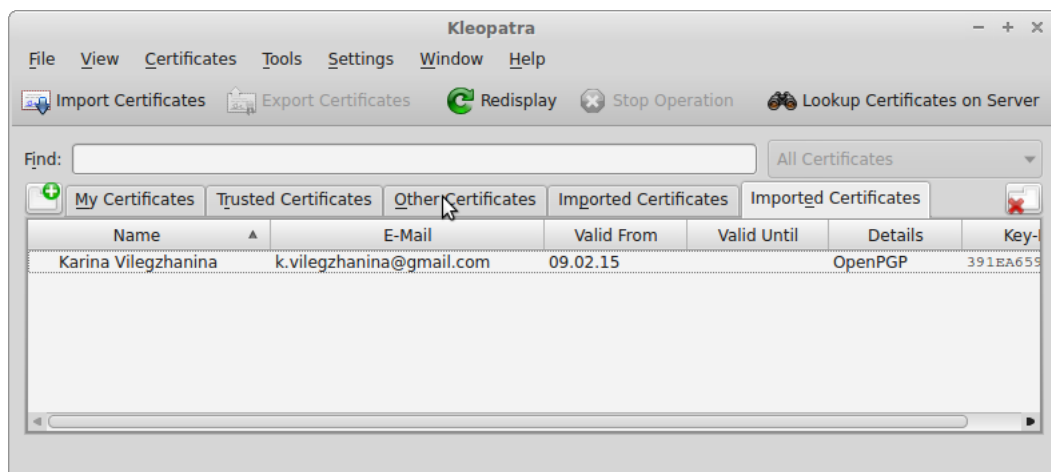


Рис. 3: Импорт чужого ключа в Kleopatra

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

```

Terminal - xu-adm@xu-dev: ~
File Edit View Terminal Tabs Help
xu-adm@xu-dev:~$ gpg --list-keys
/home/xu-adm/.gnupg/pubring.gpg
-----
pub   2048R/CC6F819A 2015-03-09
uid           Anastasiya Tarasova <tanastasiiaa@gmail.com>

pub   2048R/391EA659 2015-02-08
uid           Karina Vilegzhanina <k.vilegzhanina@gmail.com>

xu-adm@xu-dev:~$

```

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

Пакет Kleopatra имеет большое количество зависимостей, среди которых akonadi-backend-mysql, akonadi-server, dirmngr, docbook-xml, docbook-xsl, gnupg-agent, gnupg2, gpgsm, icoutils, kate-data, katepart, kde-runtime, kde-runtime-data, kdelibs-bin, kdelibs5-data, kdelibs5-plugins, kdepim-runtime,

kdepimlibs-kio-plugins, kdoctools, kleopatra, kubuntu-debug-installer, libaccounts-qt1, libakonadi-calendar4, libakonadi-contact4, libakonadi-kabc4, libakonadi-kcal4, libakonadi-kde4, libakonadi-kmime4, libakonadi-notes4, libakonadi-socialutils4, libakonadi-protocolinternals1, libattica0.4, libbaloo-core4, libbaloo-files4, libbaloo-pim4, libbaloo-xapian4, libboost-program-options1.54.0, libcalendarsupport4, libdlrestrictions1, libdmtx0a, libepub0, libgpgme++2, libgrantlee-core0, libgrantlee-gui0, libincidenceeditorsng4, libkabc4, libkactivities-bin, libkactivities-models1, libkactivities6, libkalarmcal2, libkatepartinterfaces4, libkcal4, libkcal-core4, libkcalutils4, libkcmutils4, libkde3support4, libkdeclarative5, libkdecore5, libkdepim4, libkdepimdbusinterfaces4, libkdesu5, libkdeui5, libkdeWebKit5, libkdgantt2-0, libkdnssd4, libkemoticons4, libkfbapi1, libkfile4, libkgapi2-2, libkholibday4, libkhtml5, libkidletime4, libkimap4, libkio5, libkjsapi4, libkjsembed4, libkldap4, libkleo4, libkmailbox4, libkmediaplayer4, libkmime4, libknewstuff3-4, libknotifyconfig4, libkntlm4, libkolab0, libkolabxml1, libkparts4, libkpgp4, libkpimidentities4, libkpimtextedit4, libkpimutils4, libkprintutils4, libkpty4, libkresources4, libkrosscore4, libksba8, libktexteditor4, libktnef4, libkubuntu0, libxmlrpcclient4, libmailcommon4, libmailimporter4, libmailtransport4, libmessagecomposer4, libmessagecore4, libmessageviewer4, libmicroblog4, libmysqlclient18, libnepomuk4, libnepomukcleaner4, libnepomukcore4abi1, libnepomukquery4a, libnepomukutils4, libntrack-qt4-1, libntrack0, libphonon4, libpimcommon4, libplasma3, libpolkit-qt-1-1, libprison0, libpth20, libqapt2, libqapt2-runtime, libqca2, libqgpgme1, libqjson0, libqmobipocket1, libqrencode3, libqt4-qt3support, libqt4-sql-mysql, libsendlater4, libsignon-qt1, libsolid4, lib soprano4, libstreamanalyzer0, libstreams0, libtemplateparser4, libthreadweaver4, libvirtodbc0, libxerces-c3.1, libxml2-utils, libzip2, mysql-client-core-5.5, mysql-server-core-5.5, nepomuk-core-data, nepomuk-core-runtime, ntrack-module-libnl-0, odbinst, odbinst1debian2, oxygen-icon-theme, phonon, phonon-backend-gstreamer, phonon-backend-gstreamer-common, phonon-backend-gstreamer1.0, pinentry-gtk2, pinentry-qt4, plasma-scriptengine-javascript, qapt-batch, sdaemon, sgml-data, shared-desktop-ontologies, soprano-daemon, ttf-dejavu-core, virtuoso-minimal, virtuoso-opensource-6.1-bin, virtuoso-opensource-6.1-common. В общей сложности, эти пакеты требуют порядка 300 мегабайт, что делает использование интерфейса командной строки более предпочтительным вариантом.