

Отчет по лабораторным работам 1-3:
"L^AT_EX, Git, GPG"
по дисциплине
"Методы и средства защиты информации"

Певцов Игорь, гр.53501/3

25 мая 2015 г.

Содержание

1	Система верстки \TeX и расширения \LaTeX	3
1.1	Цель работы	3
1.2	Ход работы	3
1.2.1	Компиляция в командной строке	3
1.2.2	Оболочка \TeX works	3
1.2.3	Создание титульного листа, нескольких разделов, списка, несложной формулы	4
1.2.4	Классы документов, подключаемые пакеты	6
1.2.5	Верстка сложных формул	6
1.3	Выводы	6
2	Система контроля версий Git	7
2.1	Цель работы	7
2.2	Ход работы	7
2.2.1	Получение содержимого репозитория	7
2.2.2	Добавление новой папки и файла под контроль версий	7
2.2.3	Фиксация изменений в локальном репозитории	7
2.2.4	Просмотр различий после внесения изменений в файл	7
2.2.5	Отмена локальных изменений	7
2.2.6	Просмотр различий после внесения изменений в файл	7
2.2.7	Фиксация изменений в локальном и центральном репозиториях	8
2.2.8	Получение изменений из центрального репозитория . .	8
2.2.9	Поэкспериментировать с ветками	8
2.3	Выводы	8
3	GPG	9
3.1	Цель работы	9
3.2	Ход работы	9
3.2.1	Создание ключевой пары OpenPGP	9
3.2.2	Экспорт ключевой пары	9
3.2.3	Установка ЭЦП на файл	9
3.2.4	Получение чужого сертификата	10
3.2.5	Проверка чужой подписи импортированным сертификатом	10
3.2.6	Расшифровка стороннего файла	10
3.2.7	Работа с командной строкой	10
3.3	Выводы	11

1 Система верстки \TeX и расширения \LaTeX

1.1 Цель работы

Изучение принципов верстки \TeX , создание первого отчёта.

1.2 Ход работы

Файл `.tex` представляет из себя обычный текстовый файл содержащий макрокоманды текстовой разметки. Создать файл можно в любом текстовом редакторе, сохранив его с расширением `.tex` (Рис. 1).

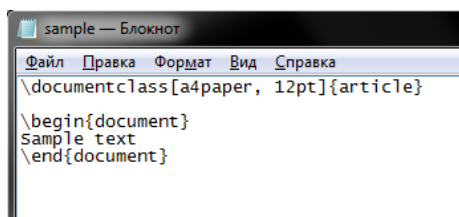


Рис. 1: Простейший \TeX документ.

1.2.1 Компиляция в командной строке

Компиляция исходного текста может производиться при помощи командной строки. После компиляции командой \LaTeX выходной файл имеет формат DVI(DeVice Independent) - аппаратно независимый формат файла, содержащий двоичные данные и не предназначенный для чтения человеком (Рис. 2).

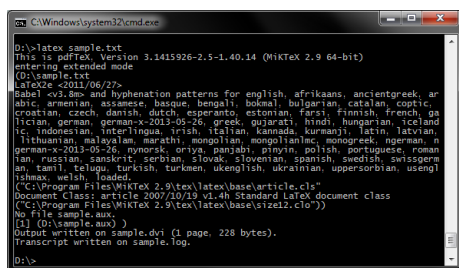


Рис. 2: Компиляция в DVI-файл.

Для перевода файла в читабельный вид(PDF-файл) необходимо выпол- нить команду \PDFLATEX (Рис. 3).

1.2.2 Оболочка \TeX works

Для выполнения работы был использован дистрибутив \MiKTeX 2.9 для Windows. Данный дистрибутив включает в себя редактор \TeX works (Рис. 4) с интуитивно понятным интерфейсом, а также интегрированный и от- дельный менеджеры пакетов. Редактор позволяет выбрать инструменты

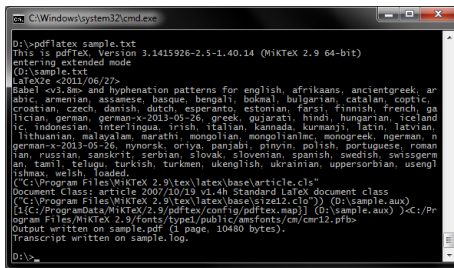


Рис. 3: Получение PDF файла.

верстки в выпадающем меню и сразу же начать верстку нажатием кнопки. Также, в редакторе сразу же доступно окно просмотра PDF-файлов (справа на Рис. 4). Редактор поддерживает добавление сценариев для расширения списка доступных функций редактора.

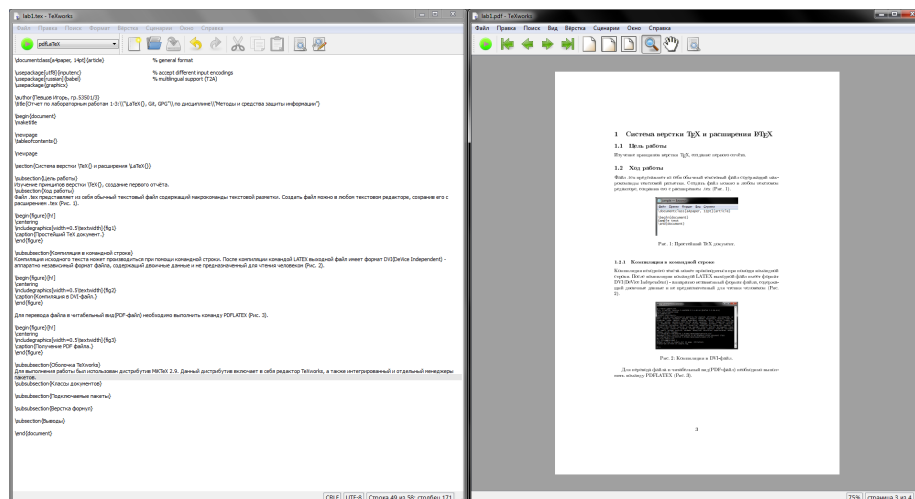


Рис. 4: Интерфейс редактора TeXworks.

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

Создание простейшего титульного листа включает в себя задаваемые в преамбуле заголовок и имя автора. Для наполнения титульного листа используются команды:

```
\author{Певцов Игорь, гр.53501/3}
\title{Отчет по лабораторным работам 1-3:\\\LaTeX\}, Git, GPG"\\
по дисциплине\\Методы и средства защиты информации"}
```

Непосредственно создание заголовка:

```
\maketitle
```

Отчет по лабораторным работам 1-3:
"L^AT_EX, Git, GPG"
по дисциплине
"Методы и средства защиты информации"
Певцов Игорь, гр.53501/3
24 мая 2015 г.

Рис. 5: Титульный лист.

Создание разделов:

```
\part[1]{Раздел 1}  
\part[2]{Раздел 2}  
\part[3]{Раздел 3}
```

Part I
1

Part II
2

Part III
3

Рис. 6: Разделы.

Создание списков (ненумерованных):

```
\begin{itemize}  
\item{one}  
\item{two}  
\item{three}  
\end{itemize}
```

Получившийся список:

- one
- two
- three

Запись формул.

$f(x,y)= 3x^3 + 15y^2 + 10$

Получившаяся формула: $f(x,y) = 3x^3 + 15y^2 + 10$

Более сложные формулы набираются с использованием

```
\begin{equation}  
formula  
\end{equation}
```

1.2.4 Классы документов, подключаемые пакеты

Каждый файл в \LaTeX начинается с команды `documentclass[...]`..., в фигурных скобках которой задаются параметры оформления стиля документа, а в квадратных — список классовых опций. Всего в \LaTeX 5 основных классов документов:

- `article` для статей
- `report` для книг и статей
- `book` для книг
- `proc` для докладов
- `letter` для оформления деловых писем .

Помимо основных, есть ещё множество дополнительных.

В \LaTeX помимо стандартных настроек существует возможность подключения сторонних пакетов со специфическими настройками. Такие пакеты расширений подключаются в шапке документа.

`usepackage{listings}` % предоставляет возможности цитирования кода в тексте с сохранением исходного форматирования.

1.2.5 Верстка сложных формул

Сложные формулы, на которые надо будет ставить ссылки в тексте, можно набирать, используя класс `equation`. Все ссылки подсчитываются автоматически, надо лишь сослаться на какую-либо ссылку при помощи команды `ref`.

$$L' = L\sqrt{1 - \frac{v^2}{c^2}} \quad (1)$$

1.3 Выводы

\LaTeX очень удобен при наборе сложных документов, имеющих множество формул, разделов и пр. \LaTeX позволяет сконцентрироваться на изменении содержания документа и переложить все форматирование на систему верстки. Пакет позволяет автоматизировать многие задачи набора текста и подготовки статей, включая набор текста на нескольких языках, нумерацию разделов и формул, перекрёстные ссылки, размещение иллюстраций и таблиц на странице, ведение библиографии и др. Кроме базового набора существует множество пакетов расширения \LaTeX . Готовя свой документ, автор указывает логическую структуру текста (разбивая его на главы, разделы, таблицы, изображения), а \LaTeX решает вопросы его отображения. Так содержание отделяется от оформления. Оформление при этом или определяется заранее (стандартное), или разрабатывается для конкретного документа.

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 Получение содержимого репозитория

Содержимое репозитория получается простой консольной командой

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

2.2.2 Добавление новой папки и файла под контроль версий

Добавление папок и файлов производится командой add с различными вариациями аргументов. Аргумент `-all` указывает на то, что Git должен добавить всю текущую директорию под контроль версий

```
mkdir testdir
cd testdir
echo abcd >> tmp
git add --all
```

2.2.3 Фиксация изменений в локальном репозитории

Изменения в локальном репозитории фиксируются командой commit

```
git commit -a -m "pew"
```

2.2.4 Просмотр различий после внесения изменений в файл

Просмотр различий выполняется командой diff

```
echo 123 >> tmp
git diff master:./tmp ./tmp
```

2.2.5 Отмена локальных изменений

Сброс выполняется командой reset. Команда checkout возвращает репозиторий к указанному состоянию.

```
git reset HEAD ./tmp
git checkout ./tmp
```

2.2.6 Просмотр различий после внесения изменений в файл

```
echo qwerty >> tmp
git diff master:./tmp ./tmp
```

2.2.7 Фиксация изменений в локальном и центральном репозиториях

```
git commit -a -m "pew2"  
git push
```

2.2.8 Получение изменений из центрального репозитория

```
git pull
```

2.2.9 Поэкспериментировать с ветками

```
git checkout -b tmpbranch  
git commit -a -m "pew3"  
git push  
git checkout master  
git merge tmpbranch  
git branch -D tmpbranch
```

2.3 Выводы

Система контроля версий Git ориентирована на работу с изменениями, а не с файлами. Преимуществами системы перед другими распределенными системами контроля версий является высокая производительность, развитые средства интеграции с другими VCS и продуманная система команд. Из недостатков можно отметить отсутствие сквозной нумерации коммитов, привязанность к ANSI-символам и применение хэшей SHA1 для идентификации ревизий.

3 GPG

3.1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

3.2 Ход работы

3.2.1 Создание ключевой пары OpenPGP

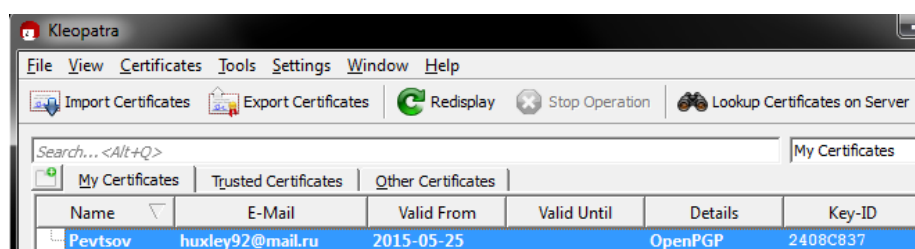


Рис. 7: Ключи созданы.

3.2.2 Экспорт ключевой пары

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFViaaUBCACrPIqaN0N0kTWoEWE8XXF5XrmdGj9P1EhGUKavI/+100gdesFQ
LFz5xKvMeBP5PcSyygJBojZ6W6ft8nNL8XI8Iv4PdUKyxuP8qio3q574eKMPSdiiQ
AbGb/FCjZa5Enz0Fz30f3h974pgAy4q1lkrB7wm9Iuyx5RDFHkNLS0TH1D/fDyG
ng6MSfdWKhrtZt0pHriEF0F5gw18tP2Eoz52M16Ax7aoBxJivqL2npCGWNB9ary3
tzKnWSskh55HbwMJPujgTcPYbFIF5u+1t0xxM1aSSq+RbKp8ntL/0UAD8+qSuc3p
ZwxcaG/3F/32TsUxtsTqI93X8bsejxBkQwD/ABEBAAQ0G1B1dnRzb3YgPGh1eGx1
eTkyQG61haWwucnU+iQE5BBMBCAAjBQJUYmm1AhsPBwsJCACDAgEGFQgCCQoLBBYC
AwECHgECF4AACGkQ+scn7CQIyDeS6Af/R/y354QX0hBhyeEXoLpUxPoJX5NVfi9r
PTrgt6LQ5a0bmbLDBPttnhmRUv6vEC6eL6iVEEAfKI1TNT3jML0yjrIP0xqc1BueT
Faio4cBM1d0EnkH4+F0UcbyGua3bEdGhuYr9Z72jggM2RaBbr20pWumo70LqdYsH
LyM1pt31UW4H70T/djgy1rRL1Jy2CFvHjeCrSVjB3PiUdYmq/Z8awsr3RZf+EmPL
UFmv7KjDbhmj5U11b4RbvQQ1ix23dE8B0LgfkUutdHP5B+zjN/yquWrsGnMZEUY
z32zXF/0UCi5Tq2YDGuT6F80705MsYuGzeGvEHLXVZHiKwjggsPjXg==
=BwpT
-----END PGP PUBLIC KEY BLOCK-----
```

Рис. 8: Ключи экспортированы.

3.2.3 Установка ЭЦП на файл

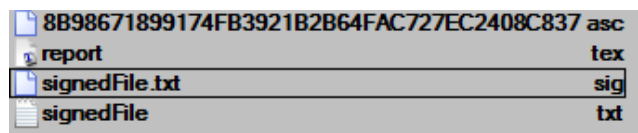


Рис. 9: Файл подписан ЭЦП.

3.2.4 Получение чужого сертификата

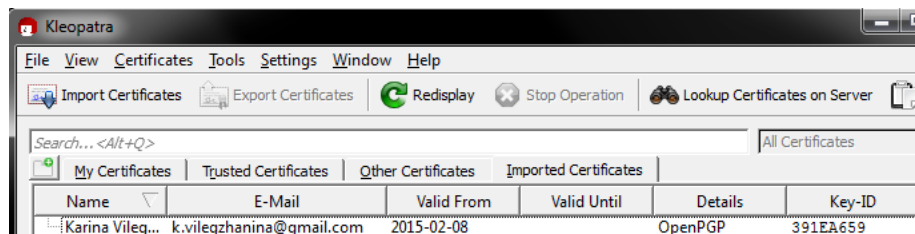


Рис. 10: Чужой сертификат (karina.asc) подписан.

3.2.5 Проверка чужой подписи импортированным сертификатом

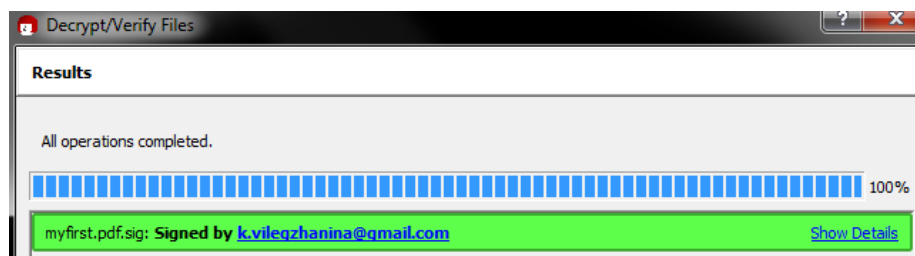


Рис. 11: Подлинность файла myfirst.pdf.sig подтверждена.

3.2.6 Расшифровка стороннего файла

Файл с исходным текстом и зашифрованный файл доступны по адресу:

https://vk.com/away.php?to=https%3A%2F%2Fgithub.com%2FluaraAmsterdam%2FInfoSecCourse2015%2Ftree%2Fmaster%2F%25D0%259E%25D1%2582%25D1%2587%25D0%25B5%25D1%2582%25D1%258B%2F01_LaTeX_Git_GPG%2FForIgor

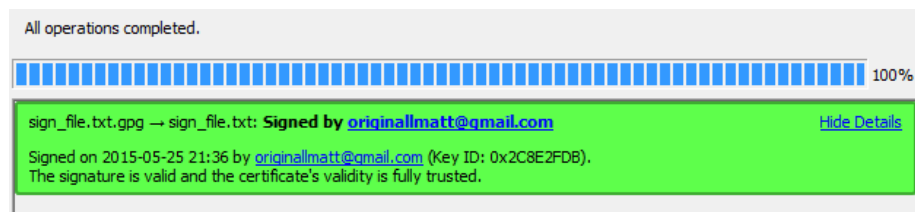
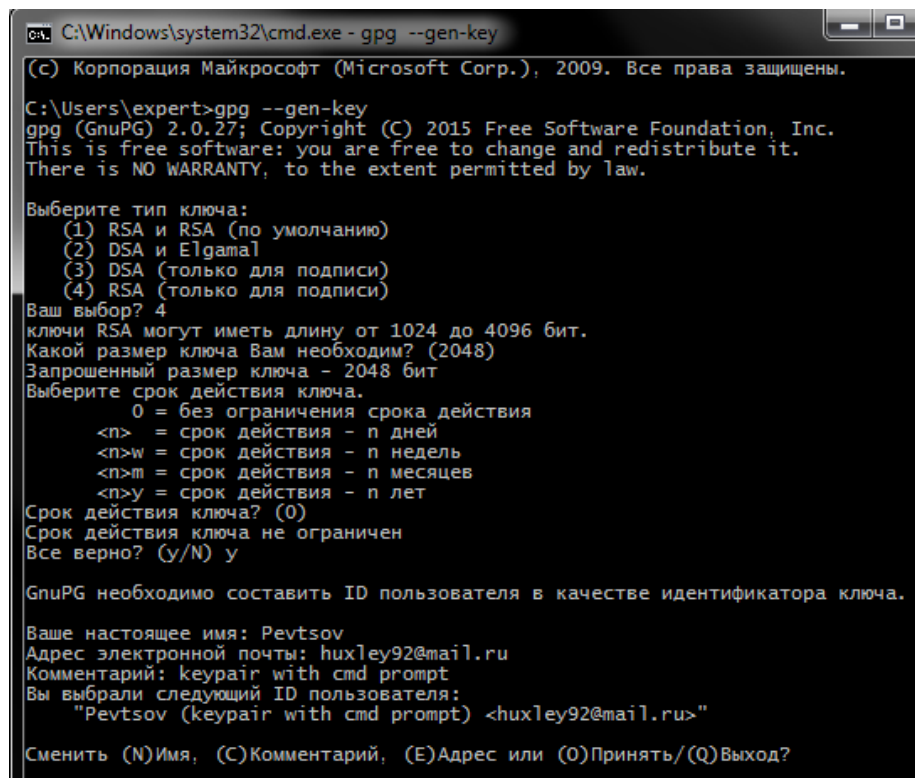


Рис. 12: Файл успешно расшифрован.

3.2.7 Работа с командной строкой

Создание ключа осуществляется командой:

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



```
C:\Windows\system32\cmd.exe - gpg --gen-key
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\expert>gpg --gen-key
gpg (GnuPG) 2.0.27; Copyright (C) 2015 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.

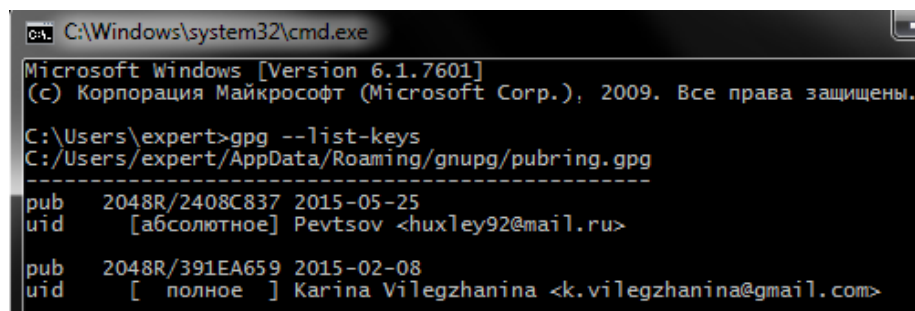
Выберите тип ключа:
  (1) RSA и RSA (по умолчанию)
  (2) DSA и ElGamal
  (3) DSA (только для подписи)
  (4) RSA (только для подписи)
Ваш выбор? 4
ключи RSA могут иметь длину от 1024 до 4096 бит.
Какой размер ключа Вам необходим? (2048)
Запрошенный размер ключа - 2048 бит
Выберите срок действия ключа.
  0 = без ограничения срока действия
  <n> = срок действия - n дней
  <n>w = срок действия - n недель
  <n>m = срок действия - n месяцев
  <n>y = срок действия - n лет
Срок действия ключа? (0)
Срок действия ключа не ограничен
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора ключа.
Ваше настоящее имя: Pevtsov
Адрес электронной почты: huxley92@mail.ru
Комментарий: keypair with cmd prompt
Вы выбрали следующий ID пользователя:
  "Pevtsov (keypair with cmd prompt) <huxley92@mail.ru>"
Сменить (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход?
```

Рис. 13: Создание ключа через консоль.

Просмотреть список ключей можно используя команду list

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



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\expert>gpg --list-keys
C:/Users/expert/AppData/Roaming/gnupg/pubring.gpg
-----
pub 2048R/2408C837 2015-05-25
uid [абсолютное] Pevtsov <huxley92@mail.ru>
-----
pub 2048R/391EA659 2015-02-08
uid [ полное ] Karina Vilegzhanina <k.vilegzhanina@gmail.com>
```

Рис. 14: Просмотр списка ключей.

Для импорта ключей используется команда

```
gpg --import importable.asc
```

Для экспорта применяется команда

```
gpg --armor --output exportable.asc --export exporter@mail.ru
```

3.3 Выводы

GPG позволяет выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске. GPG включает в себя внутреннюю схему проверки сертификатов, названную web of trust. GPG поддерживает аутентификацию и проверку целостности посредством цифровой подписи. По умолчанию она используется совместно с шифрованием, но также может быть применена и к открытому тексту. Отправитель использует GPG для создания подписи алгоритмом RSA или DSA.