Лабораторная работа 1[1](#_bookmark0) : <Изучение свойств криптографических функций хеширования> [до 21 апреля]

# О средствах разработки

* + [OpenSSL](https://www.openssl.org/) – криптографическая библиотека с открытым исходным кодом (написана на языке C). В приложение [Git](https://git-scm.com/) входит утили- та openssl.exe: "C:\Program Files\Git\usr\bin\openssl.exe"(удобно вызывать в консоли через предварительно созданную переменную среды openssl).
  + Вычисление хешкода файла:

openssl dgst -sha1 filename.in

openssl dgst -sha1 filename.in > filename.out

* + В качестве HEX-редактора удобно использовать [Notepad++](https://notepad-plus-plus.org/) (тре- буется установить соответствующий плагин).
  + Вызов утилиты openssl.exe из программы, написанной на Java:

Process process = new ProcessBuilder(); process.command(*" C: \\ ... \\ openssl.exe "* ,*" arg1 "* ,*" arg2 "* , ...); process.start();

# Постановка задачи

Напишите программу, генерирующую из файла leasing.txt эквивалент- ные по смыслу текстовые документы в количестве, достаточном для воз- никновения коллизии функции хеширования SHA-1. Типовые приемы:

1Представление результатов: 1) выполнение работ лабораторного практикума должно сопровождаться ведением удаленного репозитория посредством системы кон- троля версий Git: [GitHub](https://github.com/) или [GitLab](https://about.gitlab.com/); 2) результаты необходимо документировать и представлять в формате PDF (лаконично, в свободной форме). *Рекомендуется* ис- пользовать систему компьютерной верстки LATEX: [TeX Live](http://www.tug.org/texlive) или [TeX Live;](http://www.tug.org/texlive) 3) ссылку на репозиторий, программный код и отчет следует своевременно предоставлять пре- подавателю: [elenakhaa@yandex.ru.](mailto:elenakhaa@yandex.ru)

замена слов и словосочетаний на синонимы; исключение или включение союзов, вводных слов и эпитетов; внедрение управляющих символов.

# Задания для подготовки к экзамену

1. xxx
2. xxx