Лабораторная работа 1[1] : «Изучение свойств криптографических функций хеширования» [до 21 апреля]

1. О деталях реализации и средствах разработки

- OpenSSL – криптографическая библиотека с открытым исходным кодом (написана на языке C). В приложение Git входит утилита `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++ (требуется установить соответствующий плагин).

- Вызов утилиты `openssl.exe` из программы, написанной на Java:

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

- В Java определены два типа потоков ввода/ввывода – байтовый и символьный, для ввода/вывода бинарного кода и символов (в кодировке Unicode) соответственно. На самом низком уровне ввод/вывод данных является байтовым. Чтобы при чтении/записи не утратить информацию, не имеющую символьного представления, следует использовать байтовые потоки.

[1]Представление результатов: 1) выполнение работ лабораторного практикума должно сопровождаться ведением удаленного репозитория посредством системы контроля версий Git: GitHub или GitLab; 2) результаты необходимо документировать и представлять в формате PDF (лаконично, в свободной форме). *Рекомендуется* использовать систему компьютерной верстки LaTeX: TeX Live или TeX Live; 3) ссылку на репозиторий, программный код и отчет следует своевременно предоставлять преподавателю: elenakhaa@yandex.ru.

2. Постановка задачи

Напишите программу[1], генерирующую из файла `leasing.txt` эквивалентные по смыслу текстовые документы в количестве, достаточном (условно) для возникновения коллизии функции хеширования SHA-1. Типовые приемы: замена слов и словосочетаний на синонимы; исключение или включение союзов, вводных слов и эпитетов; внедрение управляющих символов. Оцените изменение объема файла после модификации.

3. Задания для подготовки к экзамену

1. xxx
2. xxx

[1]Для всех работ лабораторного практикума: непринципиально – выбор языка программирования, принципиально – использование криптографической утилиты `openssl.exe`.