МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ»**

Студент: Бутурля Р.А.

ФИТ 3 курс 5 группа

Вариант 3

Преподаватель: Савельева М. Г.

Минск 2023

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:
   1. выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита

Для выполнения данного задания были разработаны три метода: getCipherTable(word), caesarCipher(fileName, mode), trisemusTable(fileName, mode).

Метод getCipherTable(word) формирует на основе входящего ключегого слова(параметр функции - word) строку алфавит подстановки.

|  |
| --- |
|  |

Листинг 1– метод getCipherTable(word)

Метод caesarCipher (fileName, mode) шифрует/расшифрует документы(имя документа передается параметром fileName) шифром Цезаря с ключевым словом, после чего записывает результат в выходной документ. Выполняемое действие над документом выбирается посредством передачи параметром mode(значение true – шифрование, false – расшивровка).

|  |
| --- |
|  |

Листинг 2 – метод caesarCipher (fileName, mode)

Метод trisemusTable(fileName, mode) шифрует/расшифрует документы(имя документа передается параметром fileName) таблицей Трисемуса, после чего записывает результат в выходной документ. Выполняемое действие над документом выбирается посредством передачи параметром mode(значение true – шифрование, false – расшивровка).

|  |
| --- |
|  |

Листинг 3 – метод trisemusTable (fileName, mode)

Результат работы метода getCipherTable представлены на рисунке 1 и 2.

|  |
| --- |
|  |

Рисунок 1 – Алфавит подстановки шифра Цезаря

|  |
| --- |
|  |

Рисунок 2 – Алфавит подстановки таблицы Трисемуса

* 1. оценить время выполнения операций зашифрования/расшифрования

Для оценки времени выполнения операции была разработана функция, представленая ниже.

|  |
| --- |
|  |

Листинг 4 – функция расчета затраченного времени

Результаты работы функции(2798/5411/10822 символов в сообщении):

* шифровка шифром Цезаря – 3,12 / 5,04 / 14,87 мс;
* расшифрока шифра Цезаря – 1,99 / 3,57 / 9,794 мс;
* шифровка таблицей Трисемуса – 6,84 / 15,01 / 15,784 мс;
* расшифрока таблицей Трисемуса – 4,28 / 14,98 / 10,857 мс.

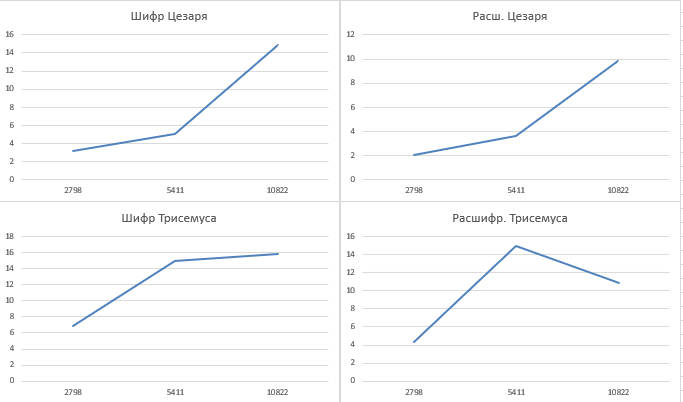


Рисунок 3 ­­­– Графики затраченного времени

1. Сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений

Для формирования гистограмм частот появления символов был разработан метод, вычисляющий эти вероятности – getCharacterFrequency(fileName). Параметр filename ­­– имя файла, в котором хранится текст для проведения расчета.

|  |
| --- |
|  |

Листинг 5 – функция расчета частот появления символов

На последующих рисунках будут указаны гистограммы частот появления символов для исходного и зашифрованного сообщений.

|  |
| --- |
|  |

Рисунок 4 – Гистограмма частот появления символов для исходного сообщения

|  |
| --- |
|  |

Рисунок 5 – Гистограмма частот появления символов для зашифрованного сообщения шифром Цезаря

|  |
| --- |
|  |

Рисунок 6 – Гистограмма частот появления символов для зашифрованного сообщения таблицей Трисемуса

**Вывод**

Изучил и приобрел практические навыки разработки и использования приложений для реализации подстановочных шифров.