Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчёт**:

«Исследование криптографических шифров на основе подстановки (замены) символов»

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Чернявский А. Л.

Минск 2020

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

**Вариант 15**.

Задание: Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков) созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;

|  |  |  |
| --- | --- | --- |
| 15 | польский | 1. Виженера, ключевое слово – bezpieczeństwo  2. На основе соотношений (2.1) и (2.2); k=20 |

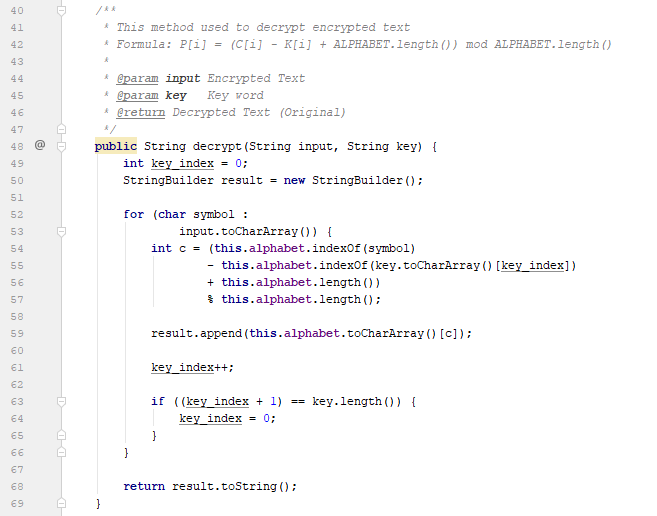
* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования).

**Листинги:**

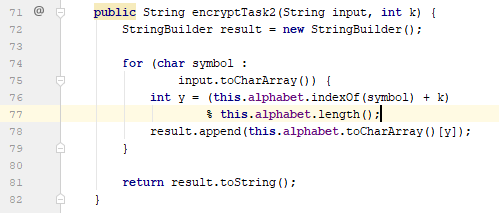
Метод для зашифрования (Виженер):



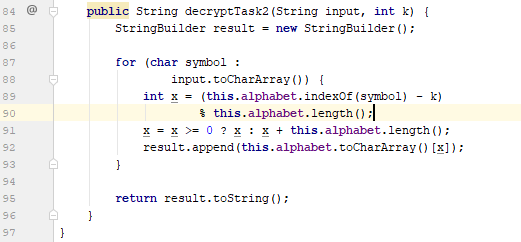
Метод для расшифрования (Виженер):



Метод для зашифрования (2 часть)

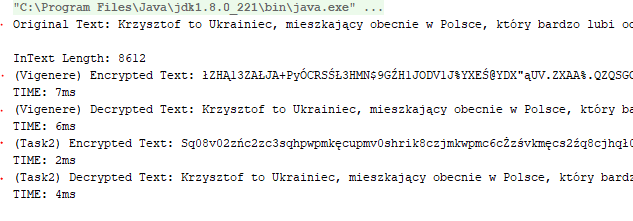


Метод для расшифрования (2 часть)



**Контрольный пример**

Результаты зашифрования и расшифрования + тайминги



Диаграммы частот (Оригинальный текст)

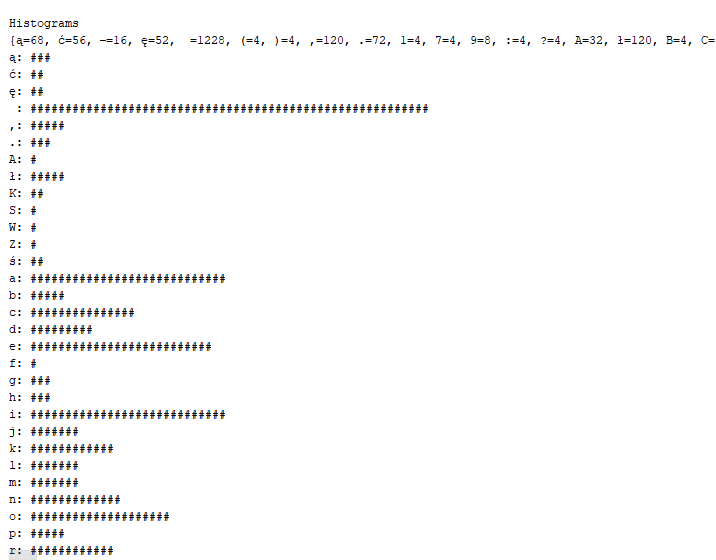


Диаграмма зашифрова­нного текста (Виженер)

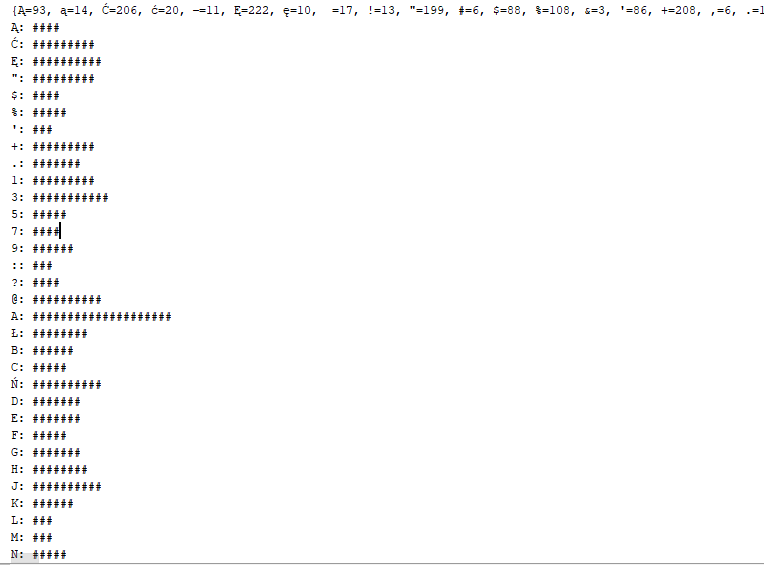


Диаграмма зашифрованного текста (2 часть)

