# МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

# Учреждение образования «Белорусский государственный технологический университет»

# 

# Отчёт по лабораторной работе №2

ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

Выполнил: студент 3 курса специальности ИСиТ Калоша И.В.

Проверила: Копыток Д. В.

Минск 2021

# Исследование криптографических шифров на основе подстановки (замены) символов

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

# Теоретические сведения

Сущность подстановочного шифрования состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Если исходить из того, что используемые алфавиты являются конечными множествами, то в общем случае каждой букве ax алфавита AM (ax ∈ AM) для создания сообщения Мi (Мi ∈ M) соответствует буква ay или множество букв {АхС} для создания шифртекста Сi (Сi ∈ С). Важно, чтобы во втором случае любые два множества (например, {АхС}b и {АхС}n, b ≠ n, 1 ≤ b, n, x, y ≤ N, N – мощность алфавита), используемые для замены разных букв открытого текста, не пересекались:

**{АхС}b ∩ {АхС}n = 0.**

Если в сообщении Мi содержится несколько букв ax, то каждая из них заменяется на символ ay либо на любой из символов {АхС}. За счет этого с помощью одного ключа можно сгенерировать различные Сi для одного и того же Мi. Так как множества {АхС}b и {АхС}n попарно не пересекаются, то по каждому символу Сi можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения Мi он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно. Приведенные утверждения справедливы для следующих типов подстановочных шифров:

* моноалфавитных (шифры однозначной замены или простые подстановочные);
* полиграммных;
* омофонических (однозвучные шифры или шифры многозначной замены);
* полиалфавитных.

Одним из существенных недостатков моноалфавитных шифров является их низкая криптостойкость. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста.

Данная лабораторная работа посвящена анализу одного из разделов практической криптографии. В связи с этим здесь будет уместно охарактеризовать противоположность криптографии – криптоанализ. Данный термин введен американским криптографом Уильямом Ф. Фридманом в 1920 г. Еще раз вспомним, что криптоанализ – это раздел криптологии, занимающийся методами взлома шифров или методами организации криптографических атак на шифры.

# Ход работы

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита Исследование криптографических шифров на основе подстановки (замены) символов 37 языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;

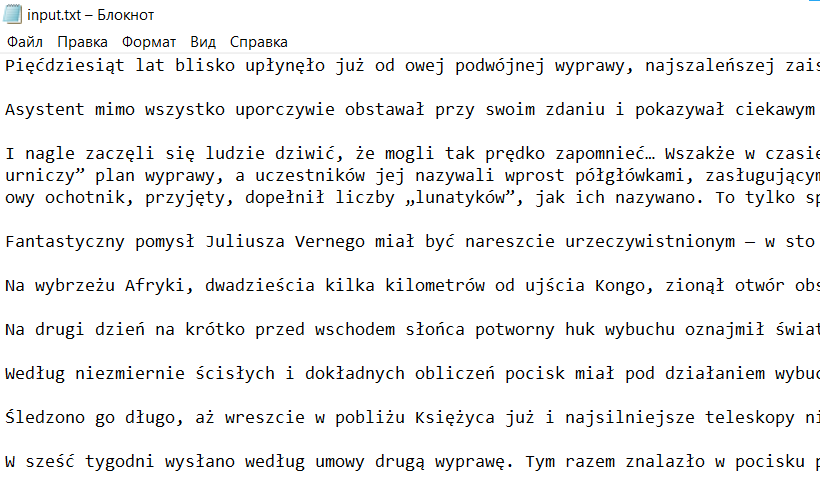


Рисунок 1 – Файл с входными данными на польском языке

Зашифруем исходные данные на основе аффинной системы подстановок Цезаря. Результат представлен на рисунке 2.



Рисунок 2 – Результат шифрования методом Аффинных подстановок Цезаря

Зашифруем исходные данные на основе шифра Порты. Результат представлен на рисунке 3.

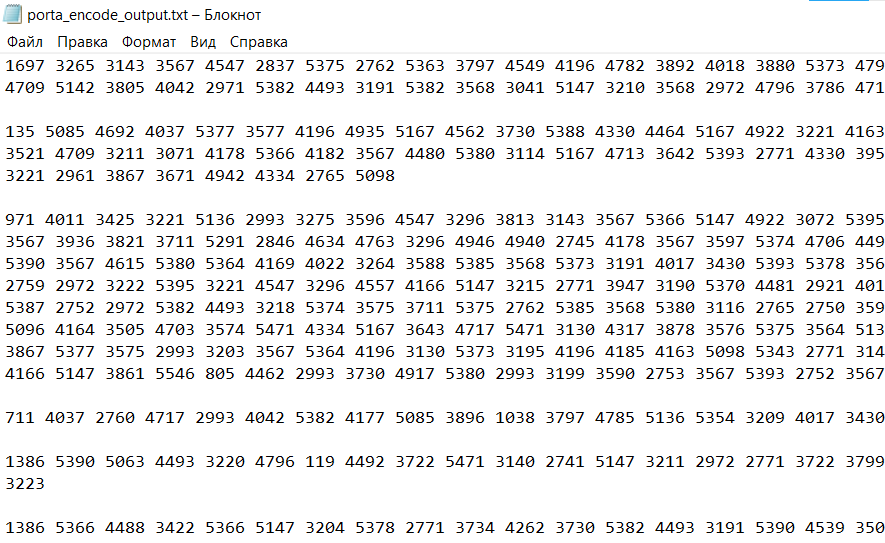
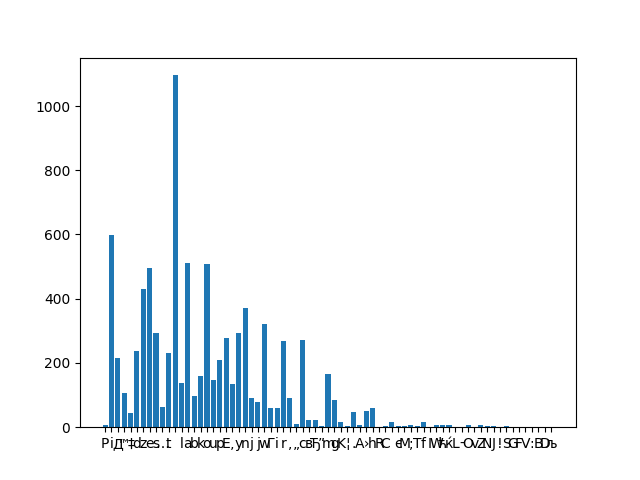


Рисунок 3 – Результат шифра Порты

• сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений;



• оценить 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)

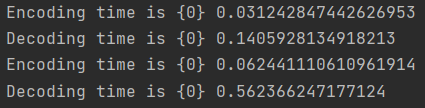


Рисунок 5 ­– Время шифровка зашифрования/расшифрования методов

Вывод. В ходе лабораторной работы были разработаны 2 метода зашифровки и расшифровки данных, основанных на подстановочных шифрах. Была протестирована возможность зашифровки и расшифровки сообщений длинной 5000 и более символов. Построен график частот появления символов, а также проанализирована скорость работы шифров. Очевидно, что шифр Порты в несколько раз медленнее, однако гораздо сложнее для взлома.