Учреждение образования

«Белорусский государственный технологический университет»

**ОТЧЕТЫ**

**по дисциплине «Защита информации и надежность информационных систем»**

по лабараторным работам

Вариант 15

Выполнил:

Студент 3 курса 1 группы ФИТ

Шкабров Данила Сергеевич

Минск, 2023

**Лабораторная работа №1 ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ**

**Код шифра Виженера**

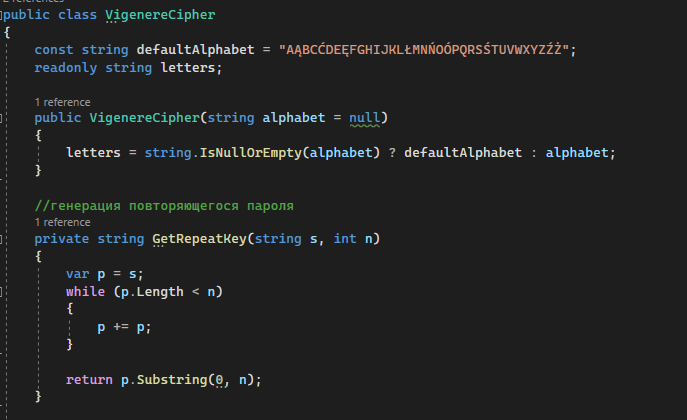


Рис. 1.1 Описание алфавита и повторения ключа

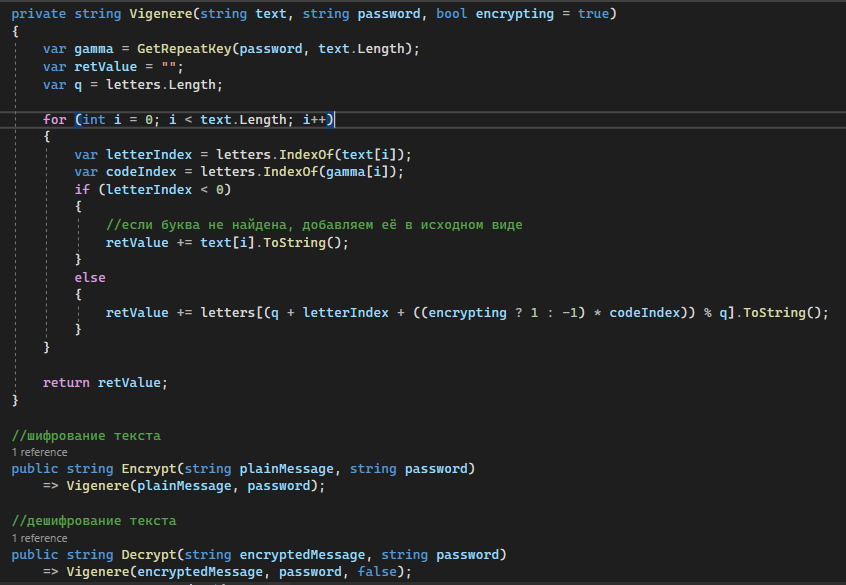


Рис. 1.2 Алгоритм шифрования Виженера

**Код шифра по соотношениям (Цезаря)**

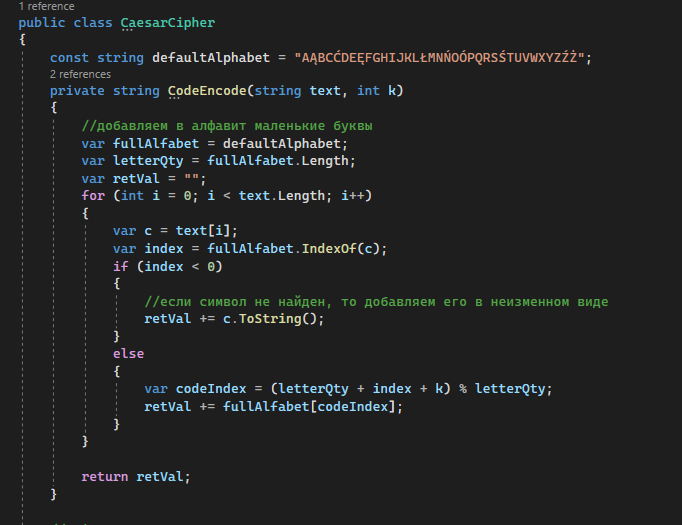


Рис. 1.3 Алгоритм шифрования Цезаря

**Запись сообщения для шифрования и вывод результатов**

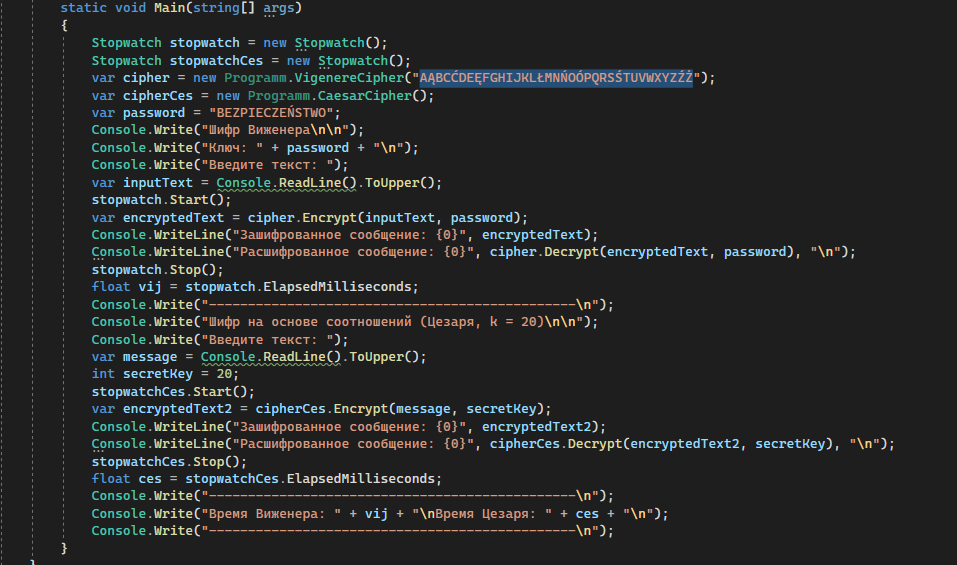


Рис. 1.4 Код вывода результатов шифрований и времени работы над ними

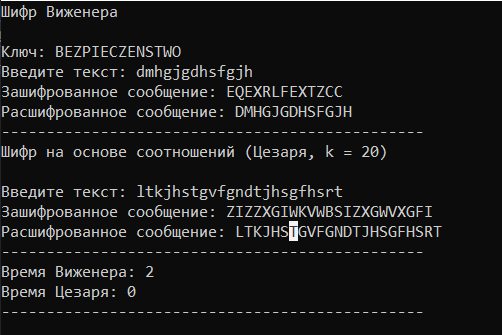


Рис. 1.5 Вывод результатов

**Гистограммы**

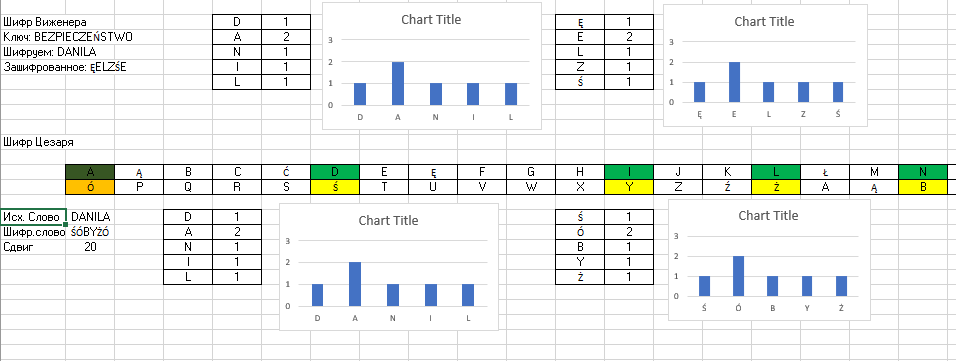


Рис. 1.6Гистограммы

**Лабораторная работа №2 ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ**

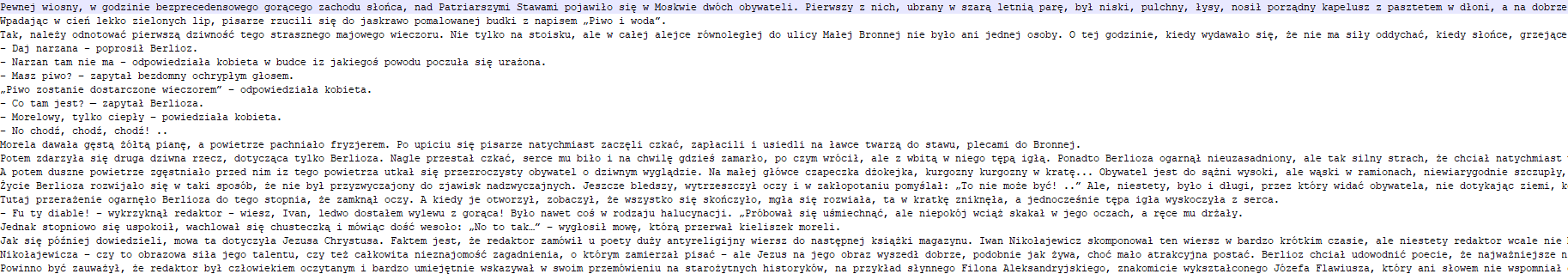
****

Рис. 2.1Файл с текстом

**Код маршрутной перестановки**

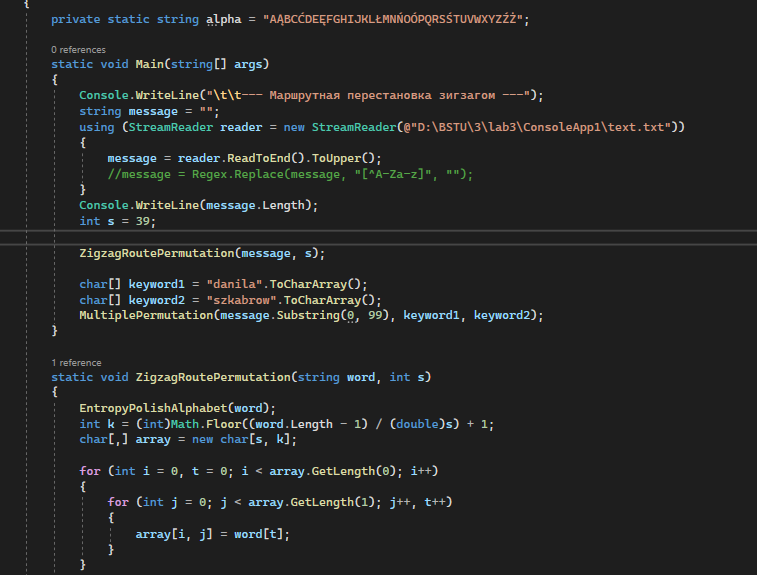
****

Рис. 2.2 Функция маршрутной перестановки

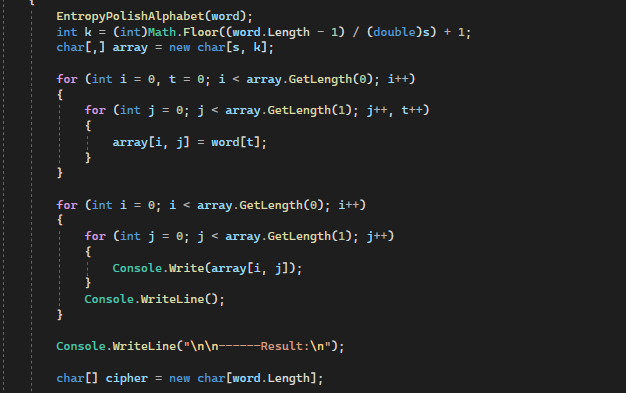
****

Рис. 2.3 Шифровка

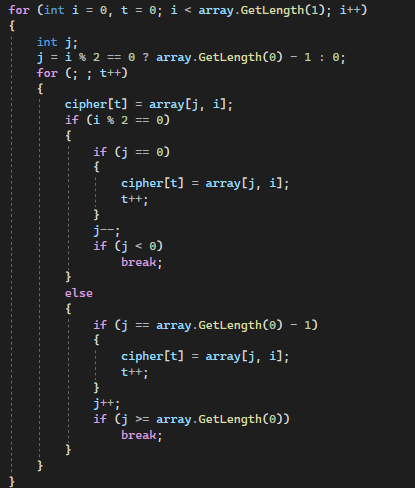
****

Рис. 2.4 Расшифровка

**Код множественной перестановки**

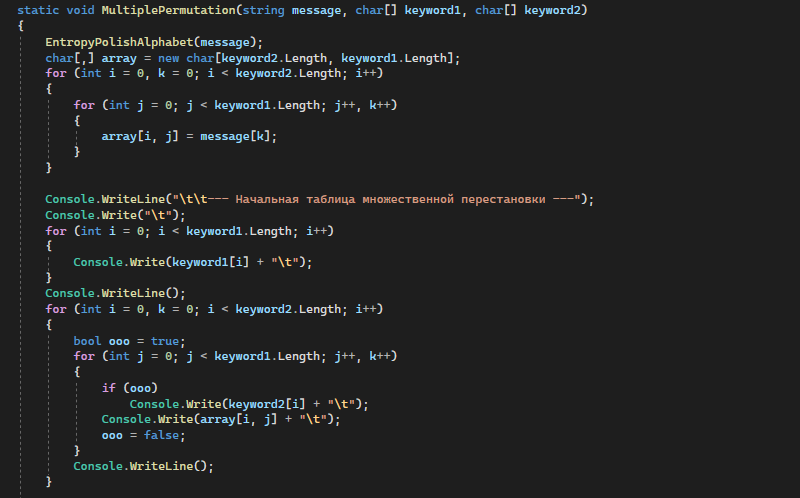


Рис. 2.5 Функция для множественной перестановки и формирование таблицы

****

Рис. 2.6 Сверение длин

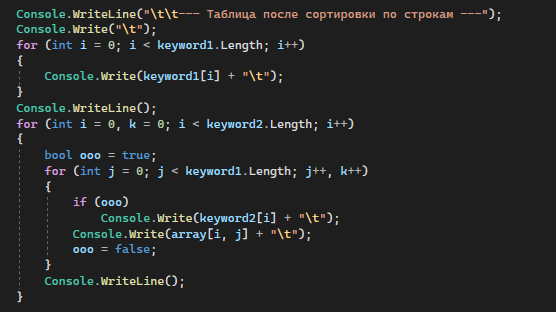
****

Рис. 2.7 Таблица после сортировки

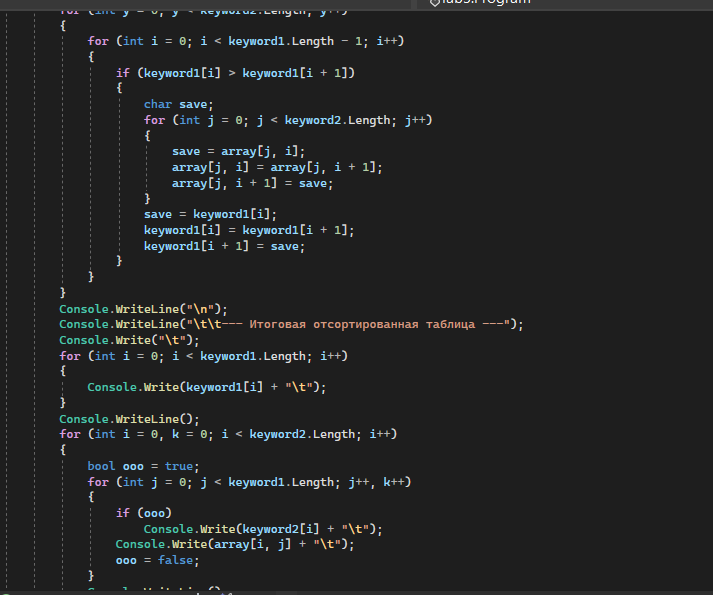
****

Рис. 2.8 Итоговая таблица

**Код Энтропии**

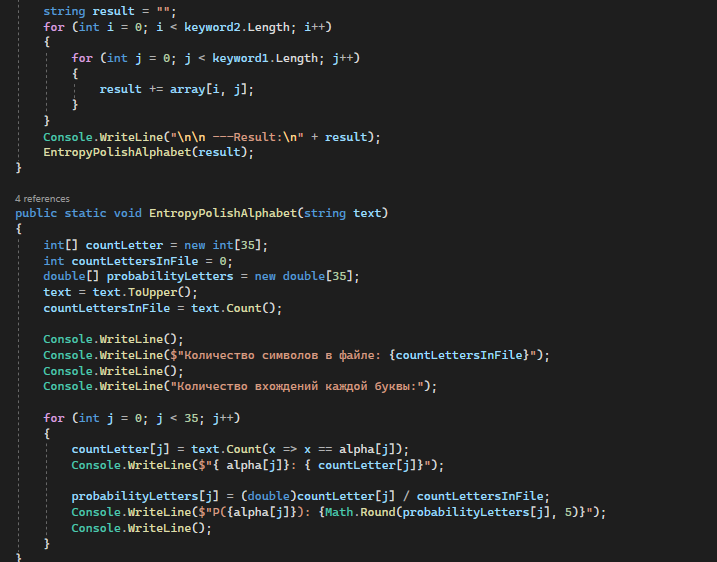
****

Рис. 2.9 Функция для определения энтропии

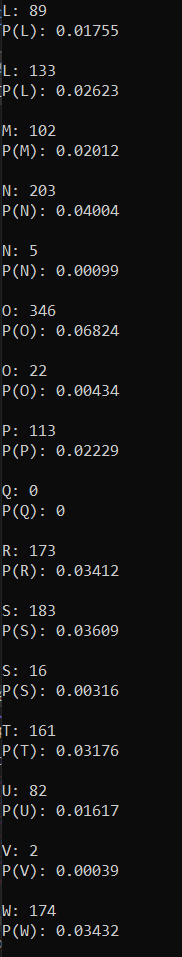
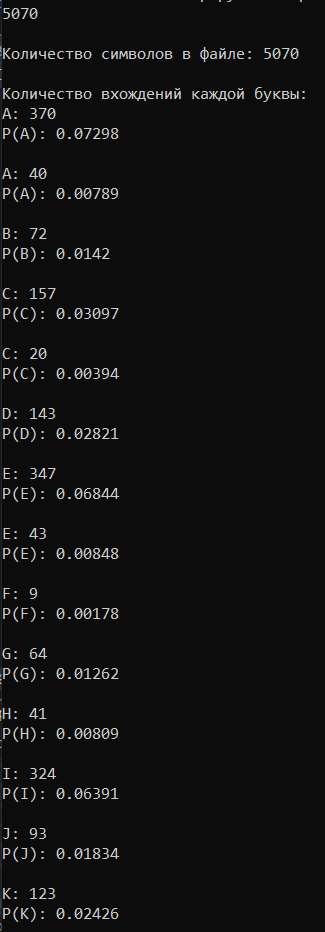
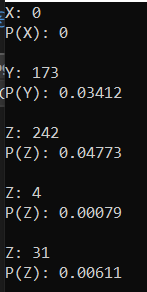
****

Рис. 2.10-12 Энтропия до маршрутной перестановки

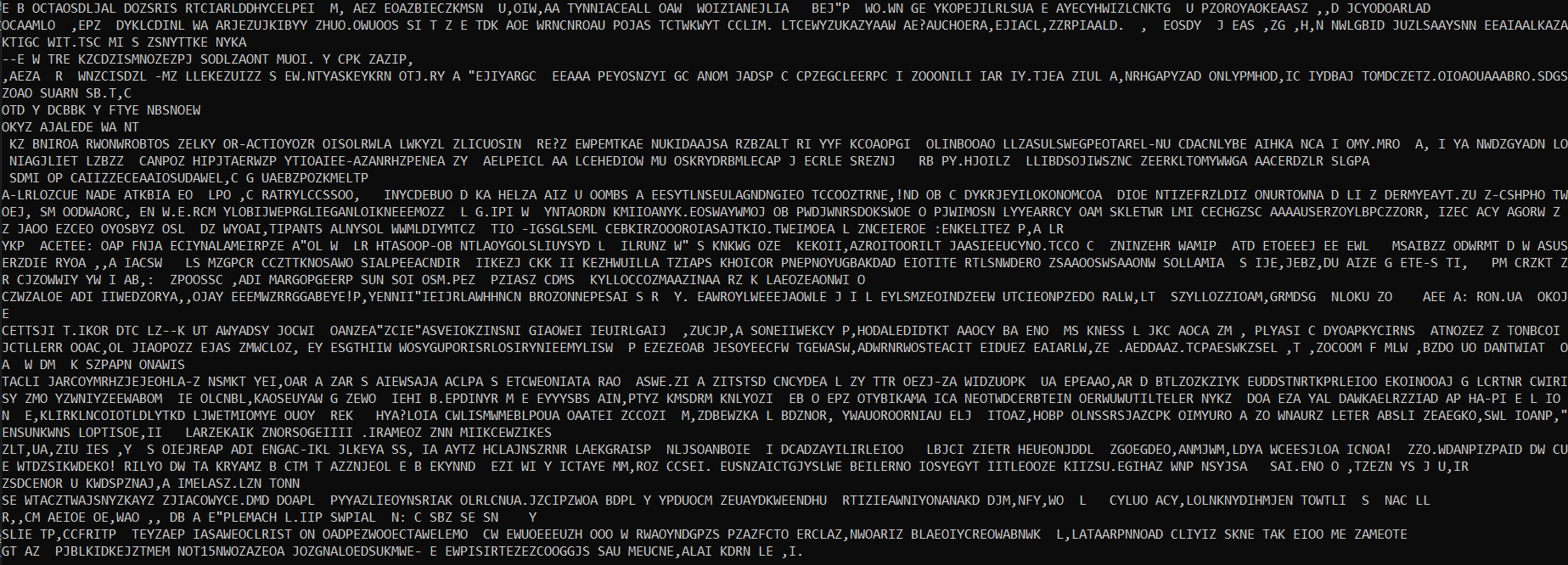


Рис. 2.13 Зашифрованный текст

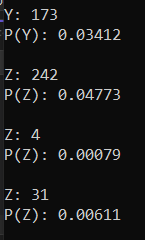
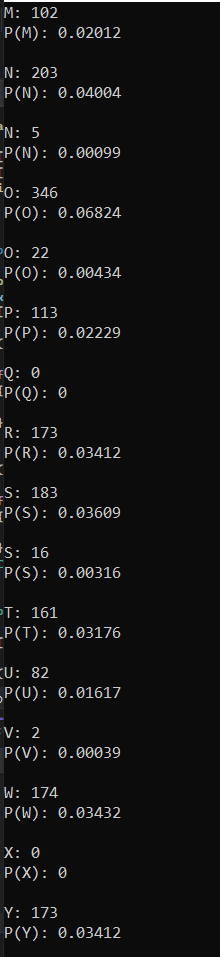
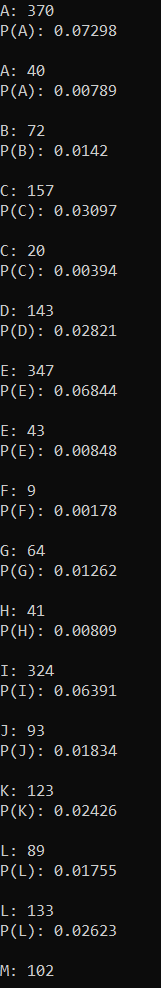


Рис. 2.14-16 Энтропия после маршрутной перестановки

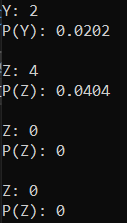
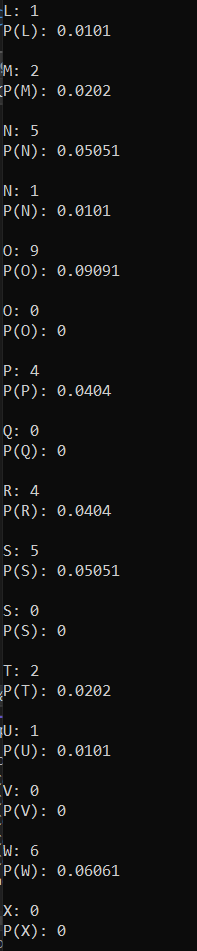
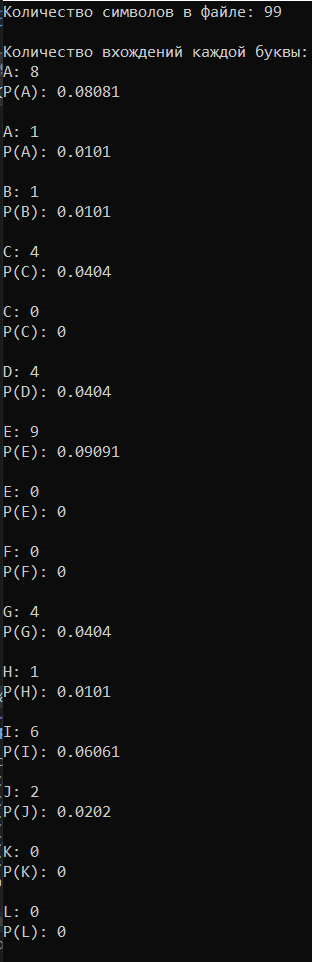


Рис. 2.17-19 Энтропия до множественной перестановки

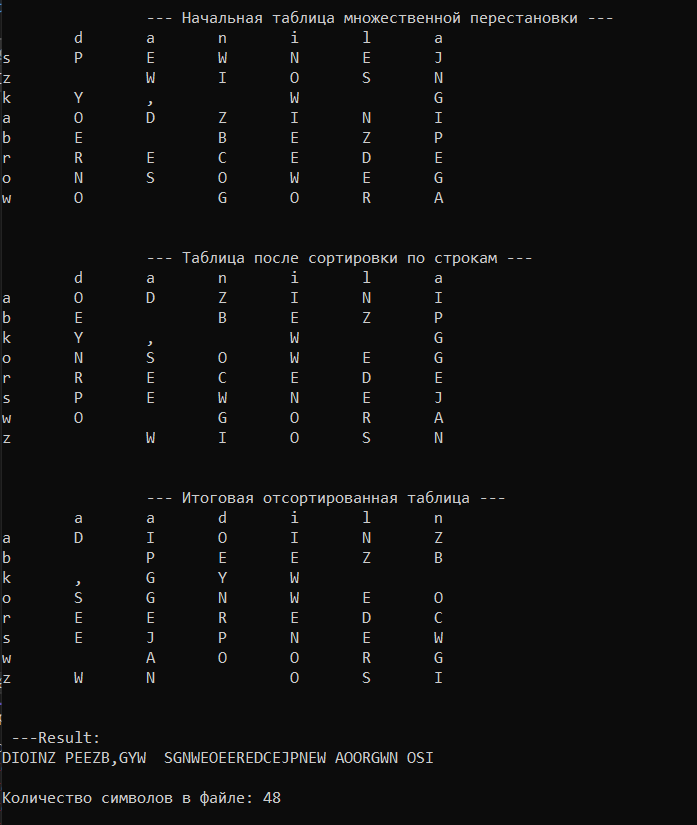


Рис. 2.20 Результат множественной перестановки

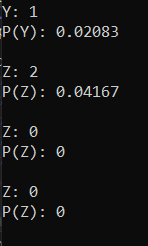
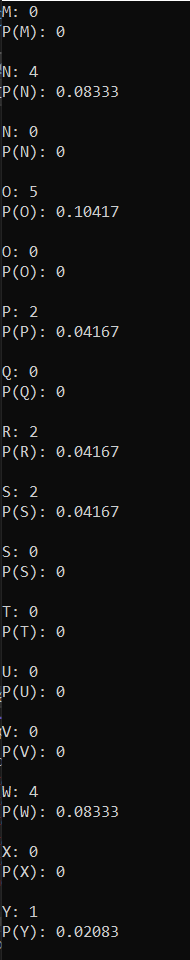
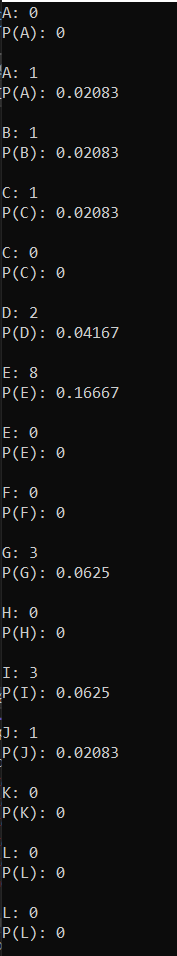


Рис. 2.21-23 Энтропия после множественной перестановки

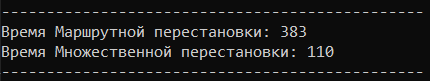


Рис. 2.24 Время выполнения перестановок

**Лабораторная работа №3 ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**

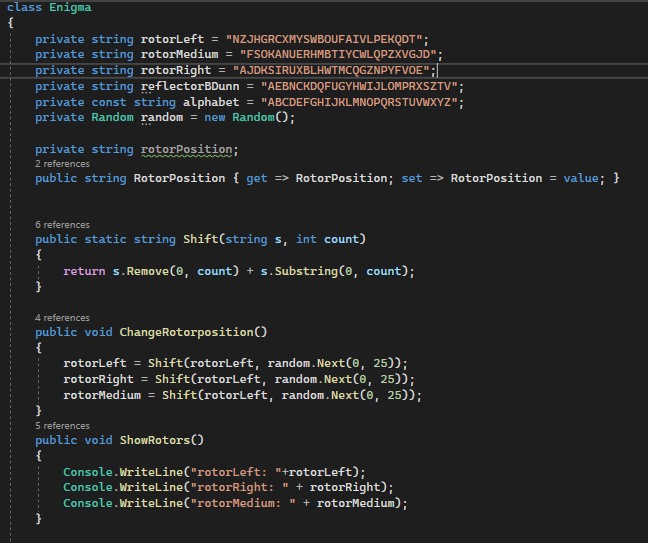


Рис.3.1 Задание роторов, функции перемещения, изменения и вывода роторов

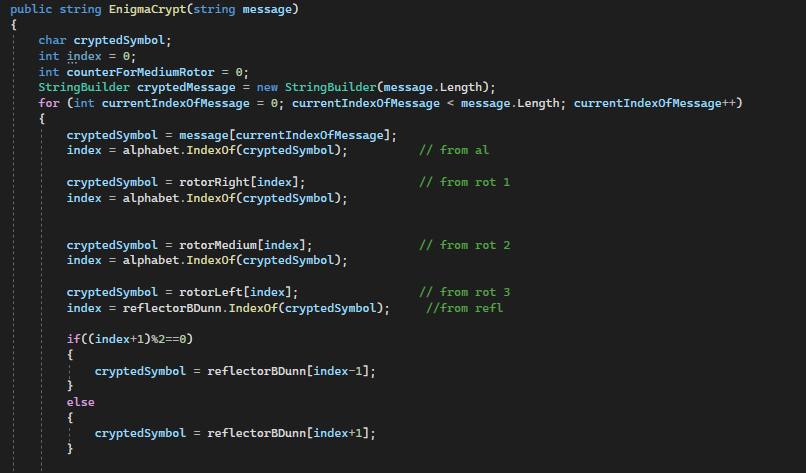


Рис. 3.2 Функция Энигмы

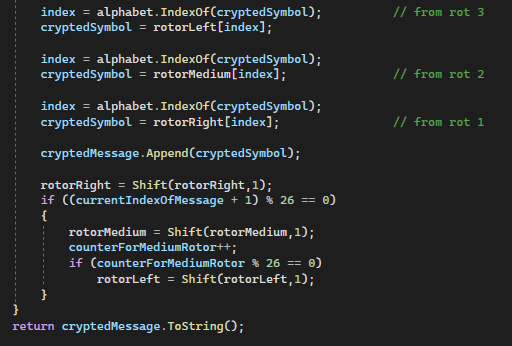


Рис. 3.3 Продолжение функции Энигмы



Рис. 3.4 Код вывода результатов

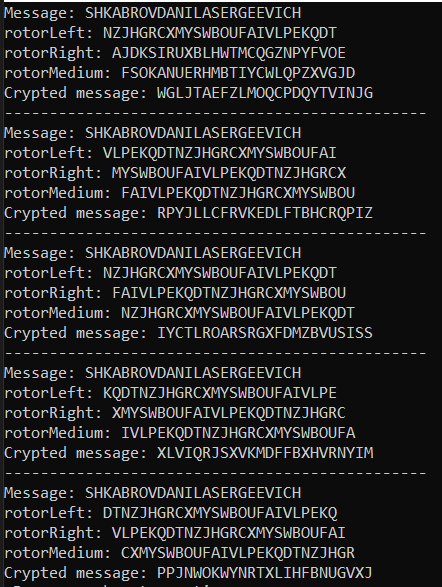


Рис. 3.5 Результат

**Лабораторная работа №4 ИССЛЕДОВАНИЕ БЛОЧНЫХ ШИФРОВ**

***КОД DES EDE-2***

Рис. 4.1 Код DES EDE-2 используя библиотеку pyDES

**Ключ слабый, текст маленький**

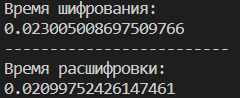


Рис. 4.2 Время на шифровку и расшифровку

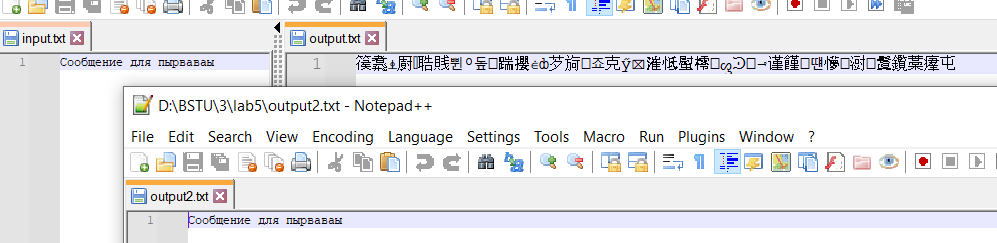


Рис. 4.3 Результат

**Ключ полуслабый, текст маленький**

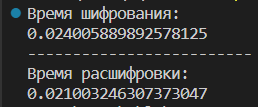


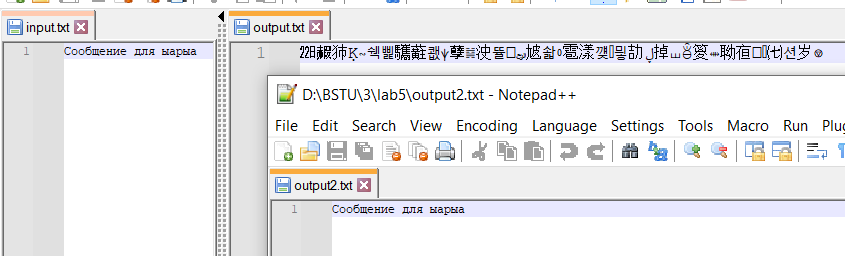
Рис. 4.4 Время на шифровку и расшифровку 

Рис 4.5 Результат

**Ключ слабый, текст побольше**

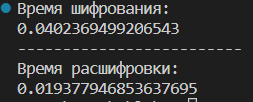
****

Рис. 4.6 Время на шифровку и расшифровку

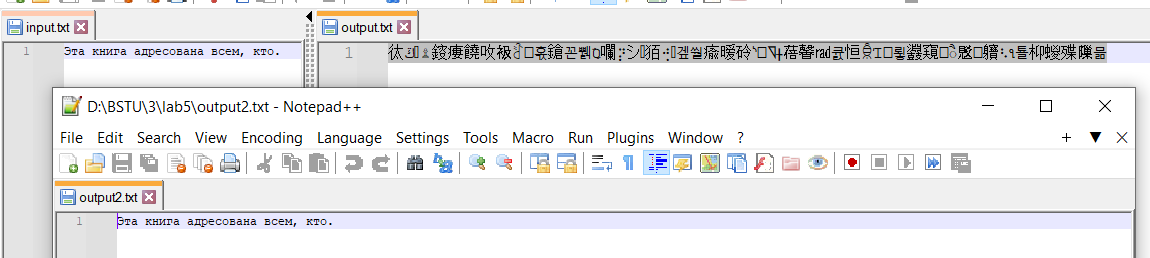


Рис. 4.7 Результат

**Ключ полуслабый, текст побольше**

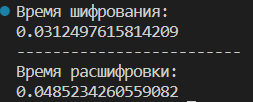


Рис. 4.8 Время на шифровку и расшифровку

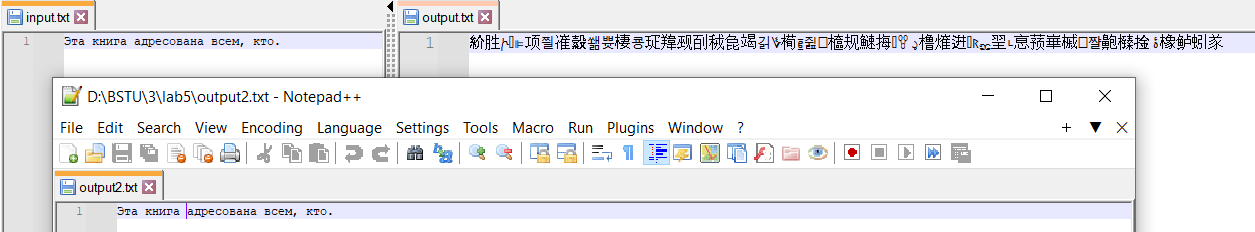
****

Рис. 4.9 Результат

**Лабораторная работа № 5 ИССЛЕДОВАНИЕ ПОТОКОВЫХ ШИФРОВ**

**Код BBS**

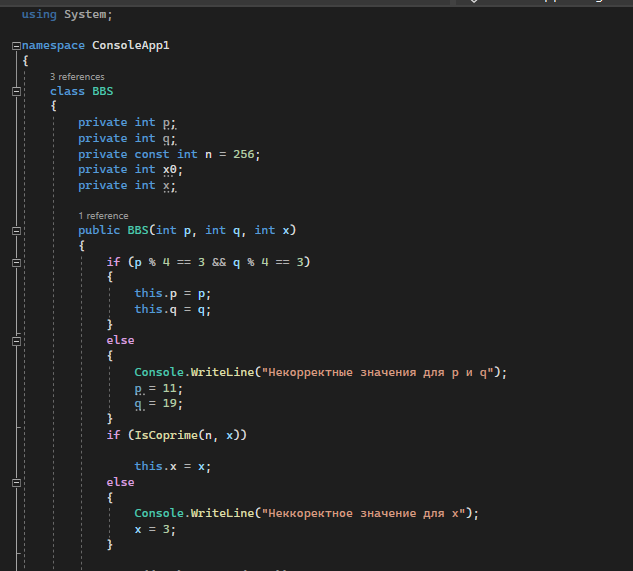


Рис. 5.1 Код класса BBS

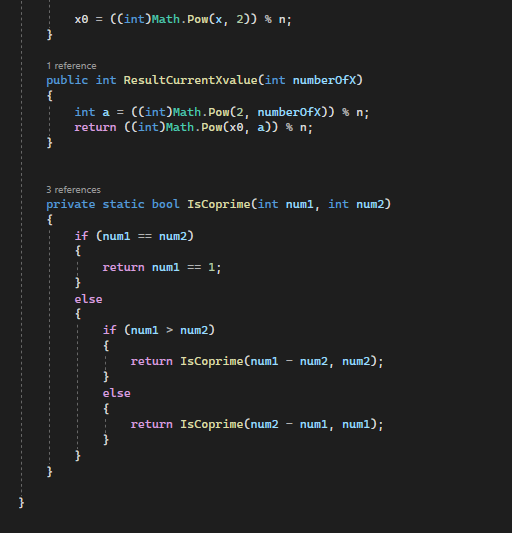


Рис. 5.2 Код класса BBS

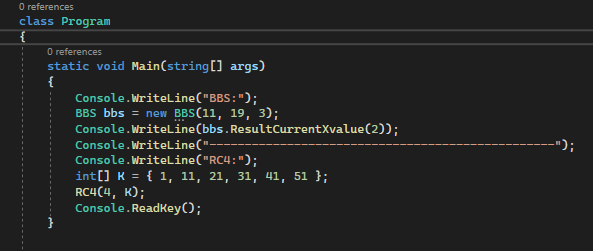


Рис. 5.3 Ввод данных для вывода результатов кода

**Код RC4**

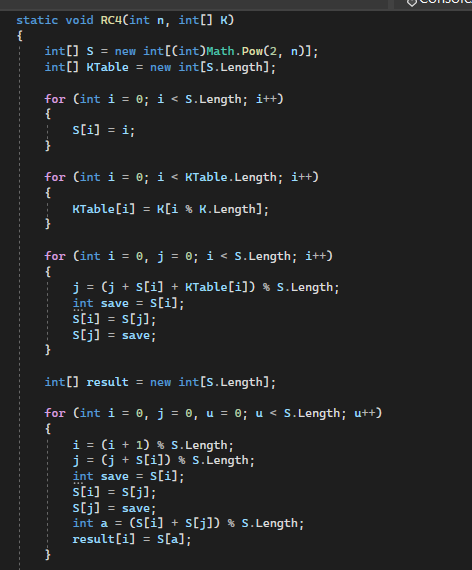


Рис. 5.4 Koд метода RC4

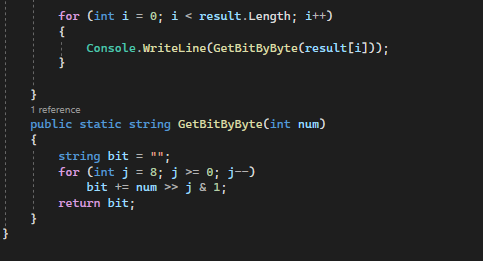


Рис. 5.5 Koд метода RC4 и сдвига

**Результат**

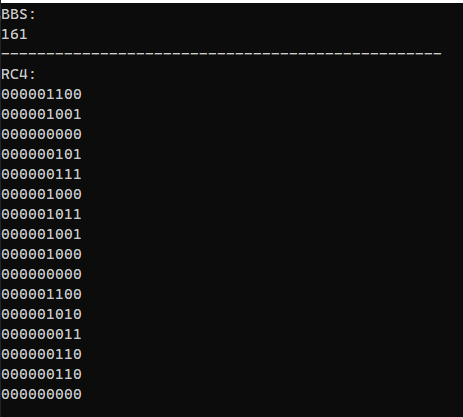
****

Рис. 5.6 Результат

**Лабораторная работа № 6 ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ**

**Код**

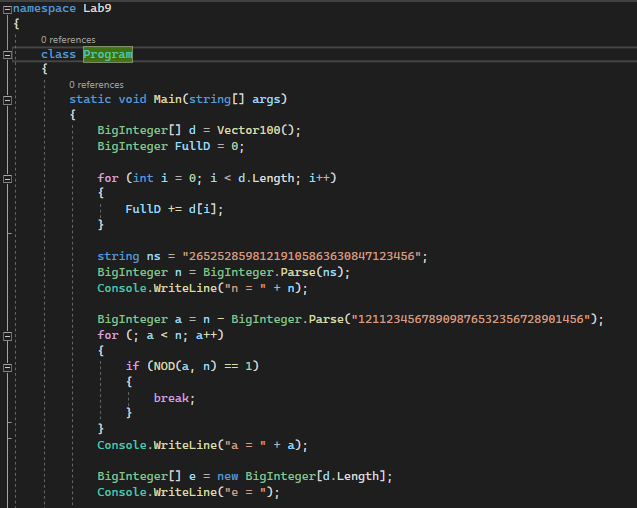
****

Рис. 6.1 Объявление переменных

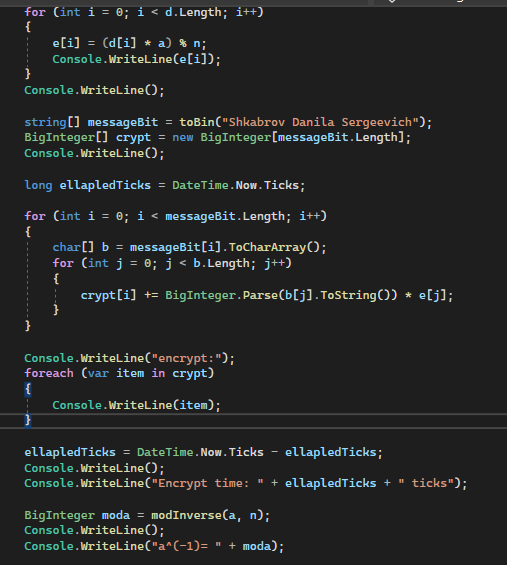


Рис. 6.2 Текст для зашифровки и расшифровки

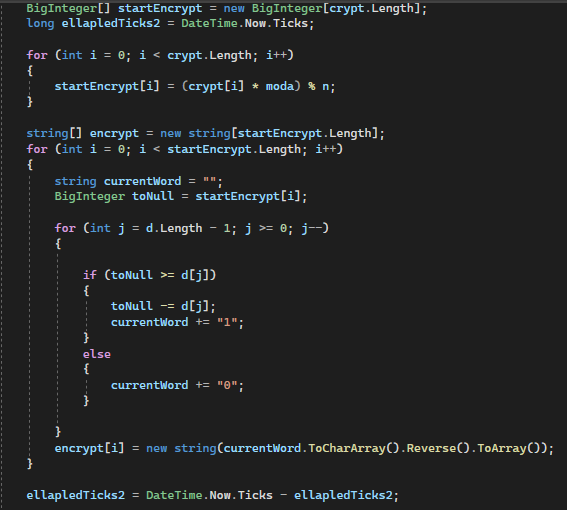


Рис. 6.3 Шифровка



Рис. 6.4 Расшифровка

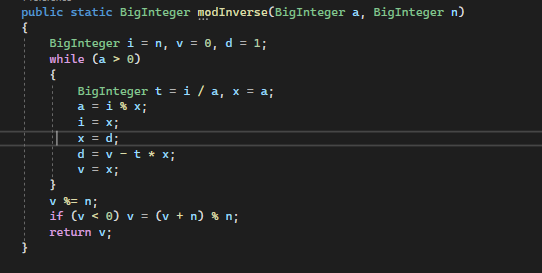


Рис. 6.5 Модуль для расшифровки

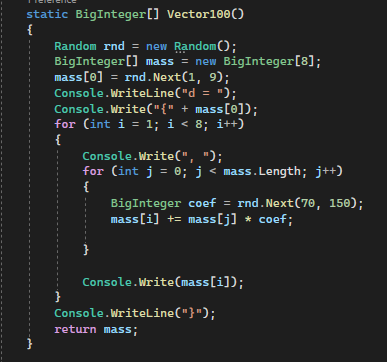


Рис. 6.6 Генерация чисел для d (чтобы она была сверпоследовательностью)

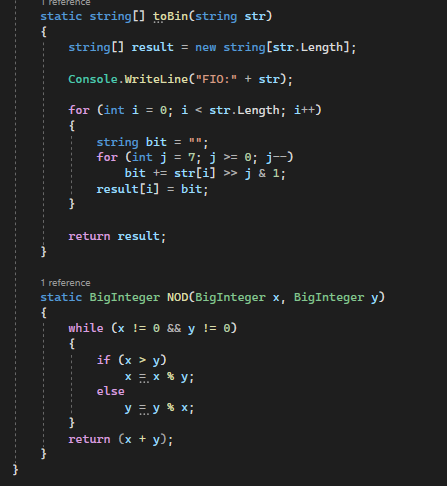


Рис. 6.7 Методы для перевода в бинарный вид и НОД

**Результат**

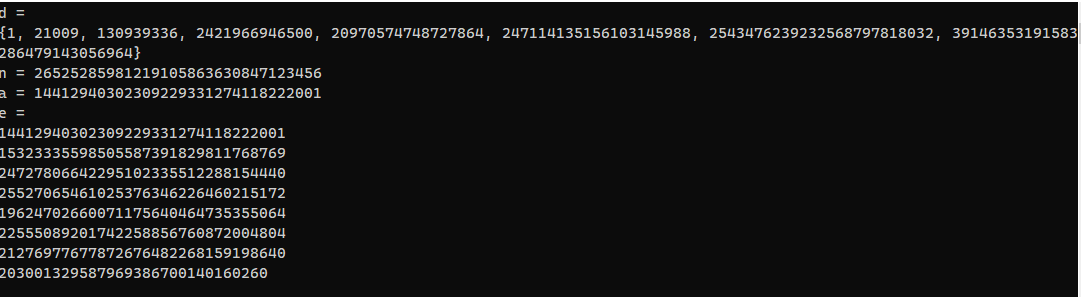


Рис. 6.8 Вывод чисел

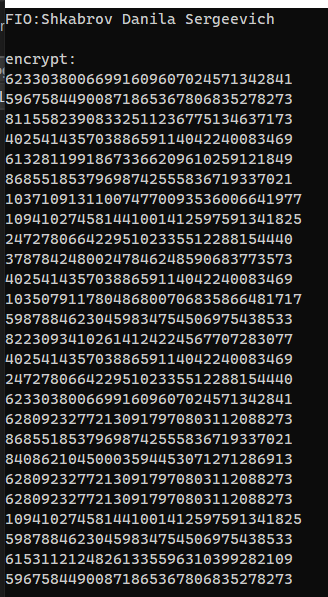


Рис. 6.9 Результат шифрования

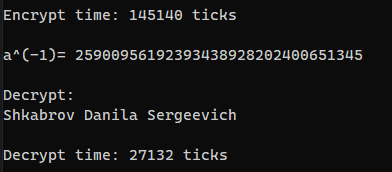


Рис. 6.10 Результат расшифровки и время

**Лабораторная работа № 7 ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ RSA И ЭЛЬ-ГАМАЛЯ**