Федеральное государственное бюджетное образовательное учреждение высшего образования «Петрозаводский государственный университет»

Отчёт

по лабораторной работе № 4 по курсу «Информационная безопасность и защита информации»

(Шифрование произвольного файла методом гаммирования)

Выполнил: студент 2 курса института математики и информационных технологий группы 22205 С. П. Гашков

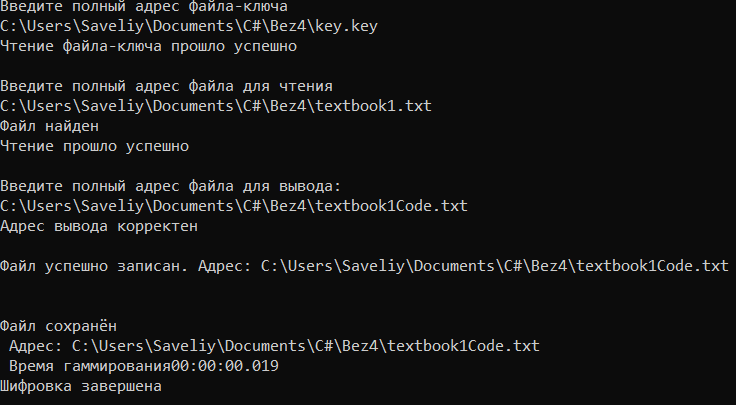
Руководитель: В. Е. Соколов

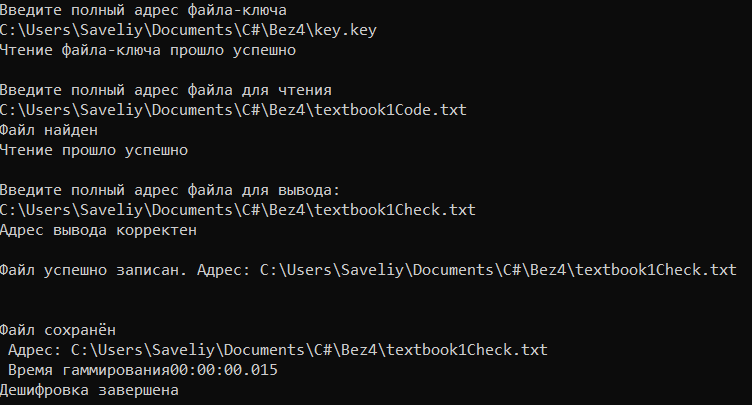
Петрозаводск

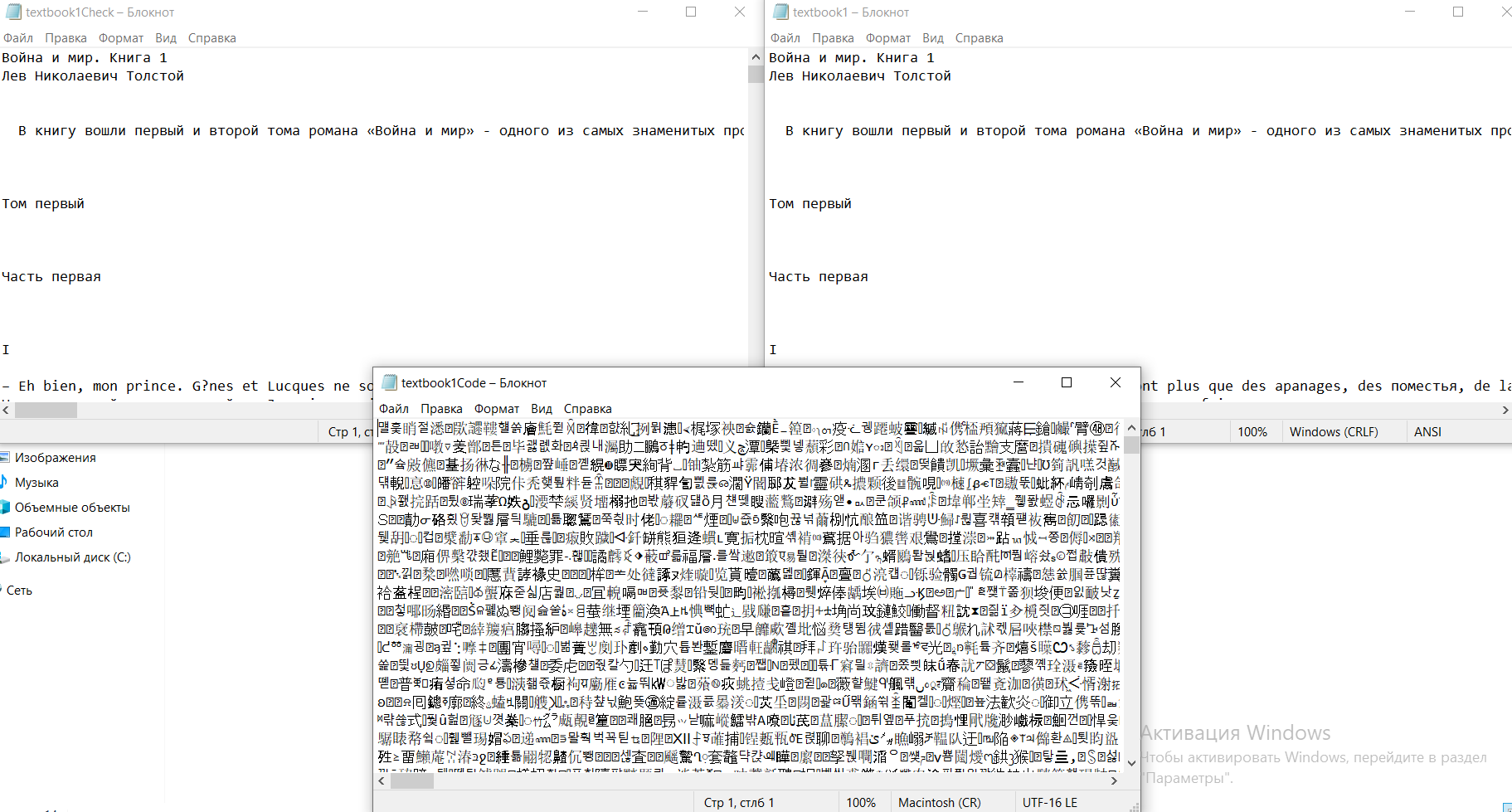
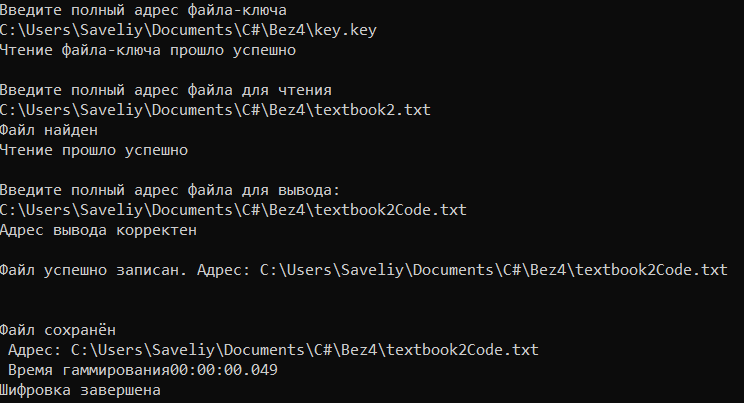
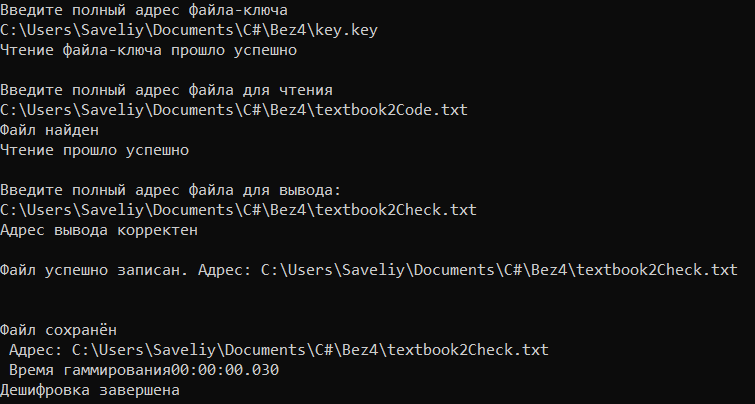
2022

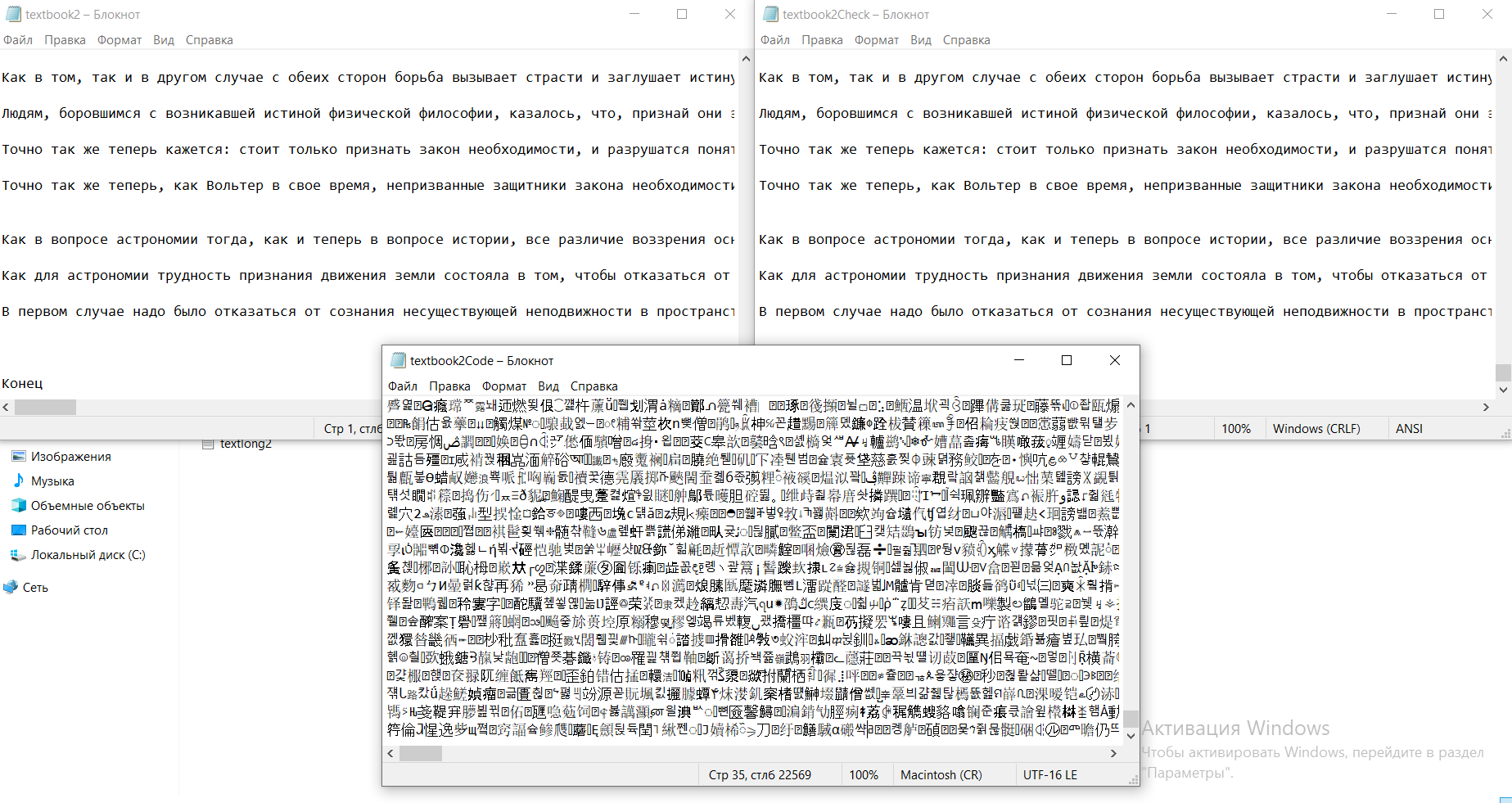
Метод гаммирования, используемый в качестве мощной одноразовой системы шифрования, заключается в наложении на биты исходного файла битов ключа посредством операции XOR (Исключающее ИЛИ). Для шифрования применяется операция XOR для битов файла и ключа. Для дешифрования используется также операция XOR для зашифрованного файла и того же ключа. Этот метод считается одним из самых криптоскойких при достаточной длине ключа.

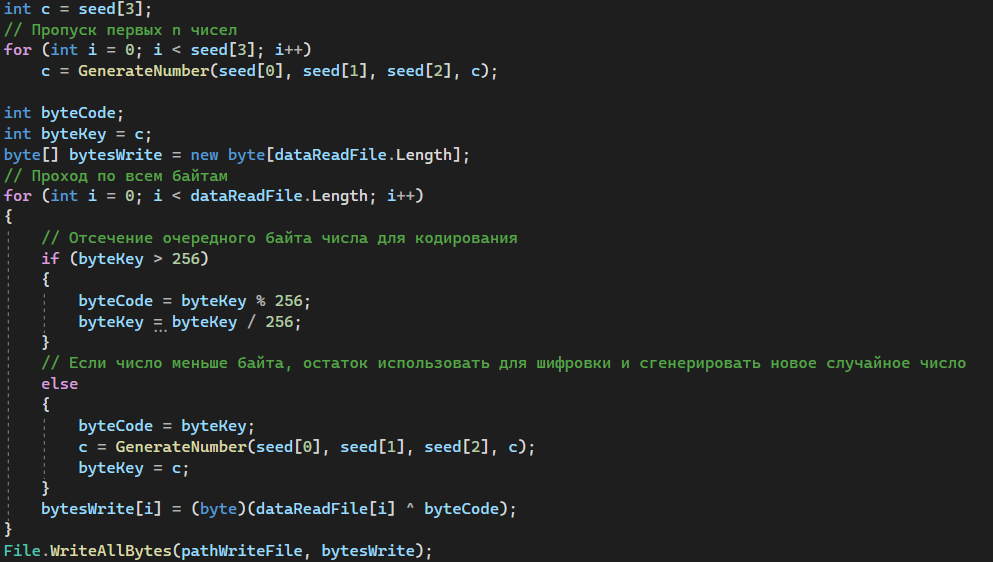
В данной реализации в качестве ключа используется зерно (сид) к ГСПЧ, записанное в формате строки, в которой каждое из 4 целых значений отделяется друг от друга пробелом.

В качестве мерки для статистики скорости шифрования используются роман «Война и мир» Л. Толстого (textbook1.txt – 1 и 2 том, textbook2.txt – весь роман)





Исходя из результатов измерений, можно заключить, что алгоритм обладает линейной сложностью (т.е. при увеличении входа в 2 раза, время работы увеличивается в 2 раза), что соответствует логике работы метода (проход по всем битам 1 раз).

Основная функция шифрования:

Функция принимает:

1. seed[] – массив из 4 чисел, составляющих зерно генерации:

seed[0] = a

seed[1] = b

seed[2] = c0

seed[3] = m

1. dataReadFile – массив значений байтов, которые в совокупности составляют переданный для шифрования файл
2. pathWriteFile – строка, являющаяся адресом выходного файла
3. GenerateNumber – функция линейного конгруэнтного ГСПЧ, где:

seed[0] = a

seed[1] = b

seed[2] = предыдущий сгенерированный элемент

seed[3] = m