МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное бюджетное образовательное учреждение высшего образования

**«Вологодский государственный университет»**

**Институт математики, естественных и компьютерных наук**

**Информатика и вычислительная техника**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7**

Изучение симметричного блочного алгоритма шифрования IDEA.

Дисциплина: «Защита информации»

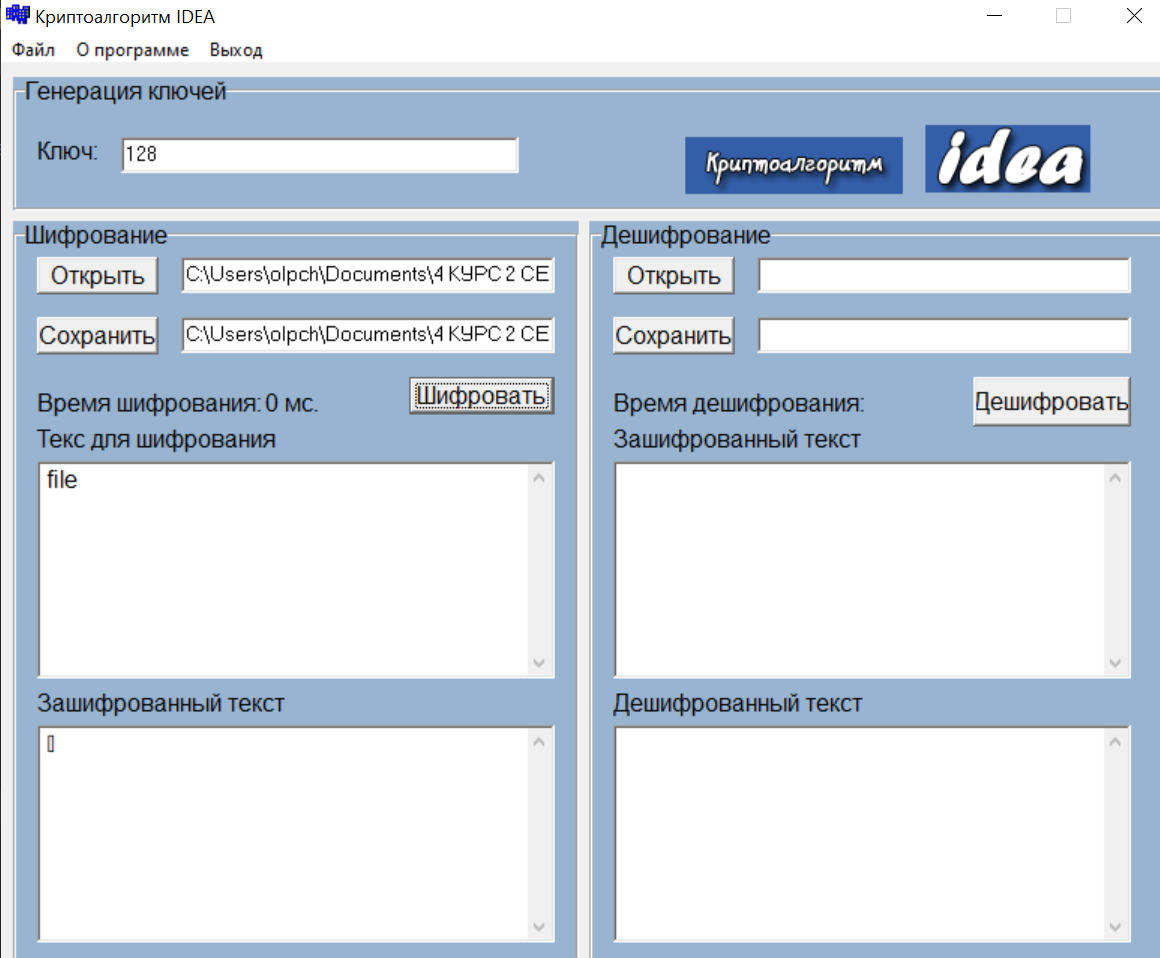
Направление подготовки: 09.03.01. Информатика и вычислительная техника

|  |  |
| --- | --- |
| Руководитель | Давыдова.Е.Н |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | 4Б09 ВМ-41 4 курс |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись преподавателя)* |

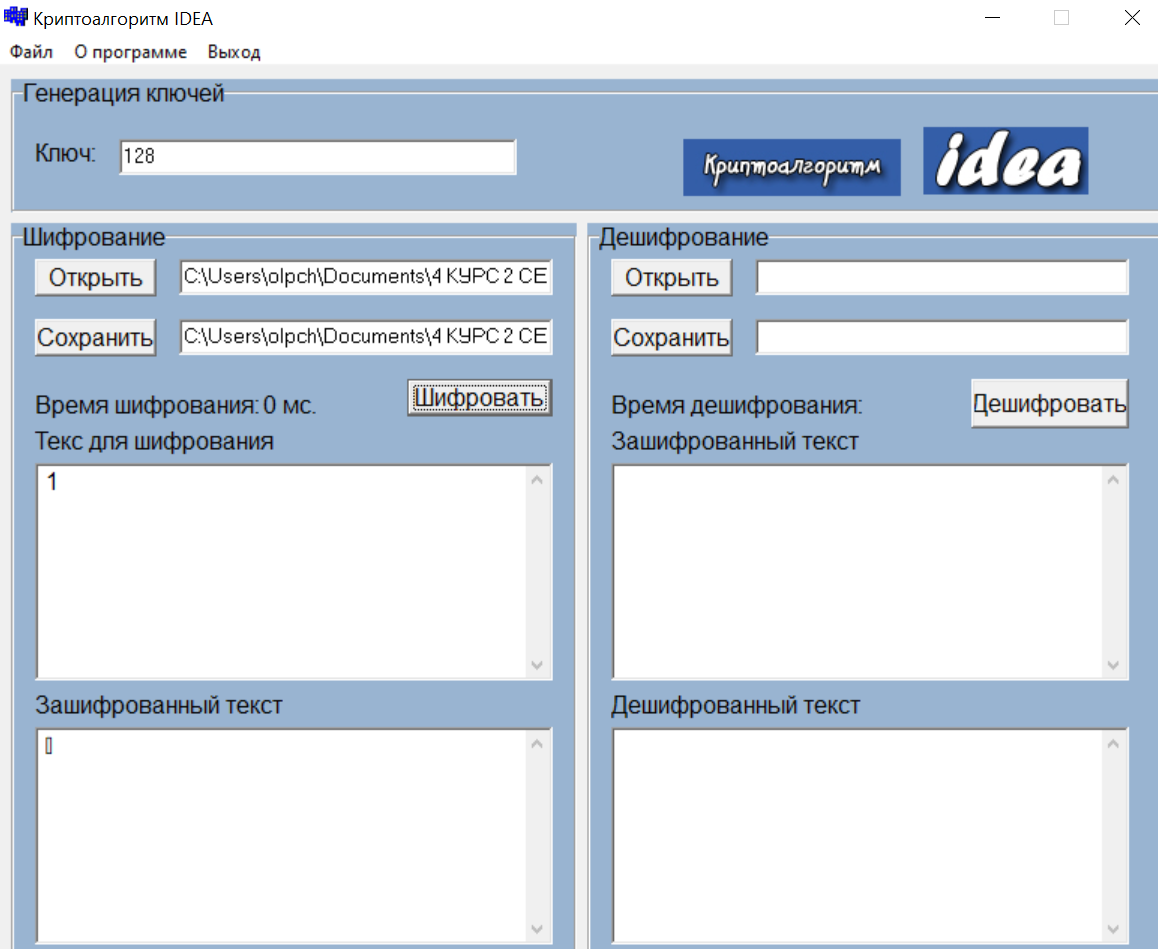
Вологда

2023 г.

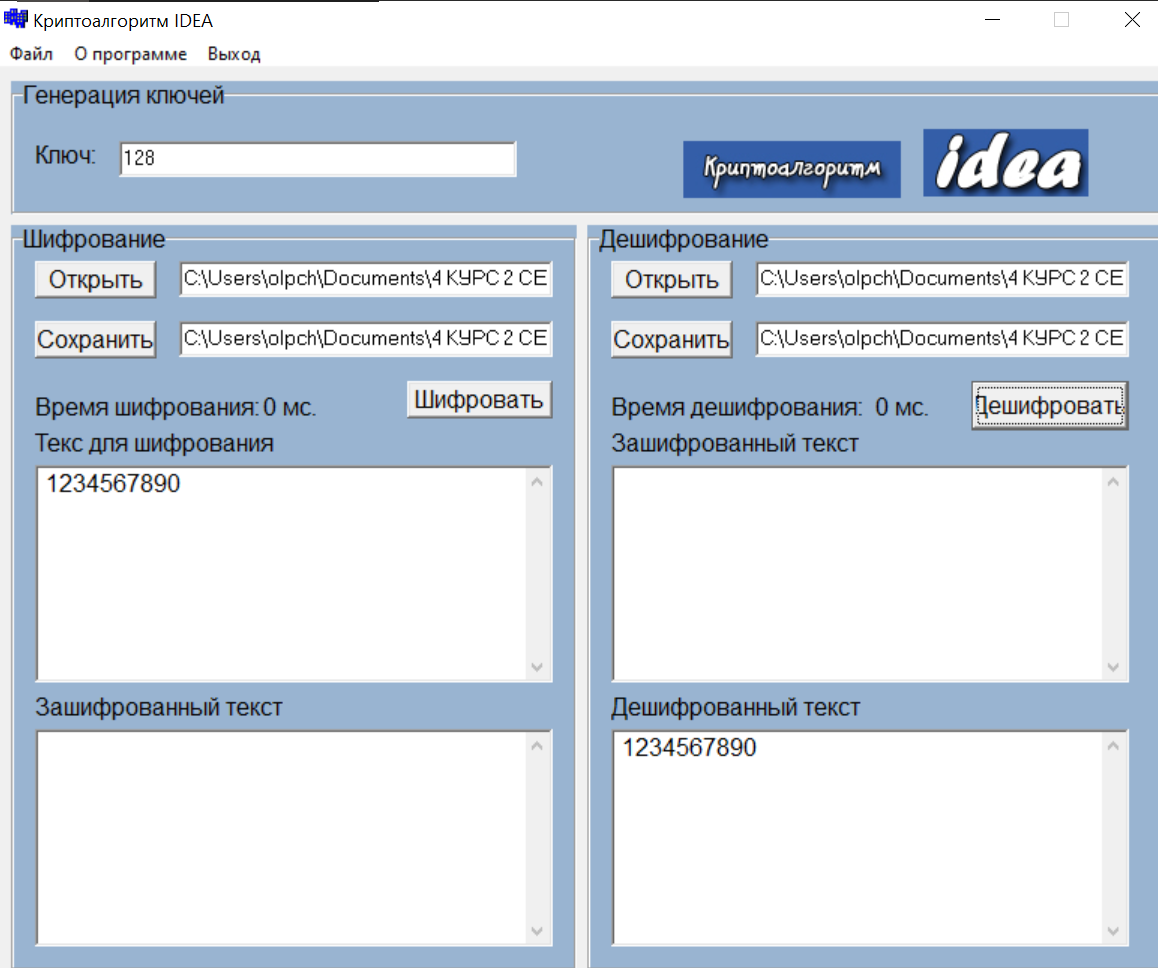
Постараться реализовать разобранный пример:



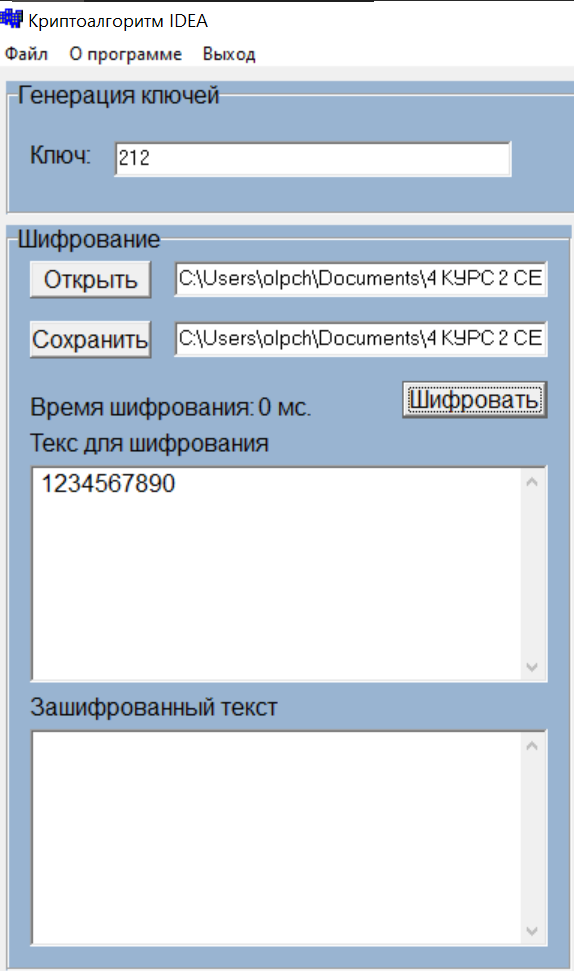


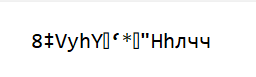


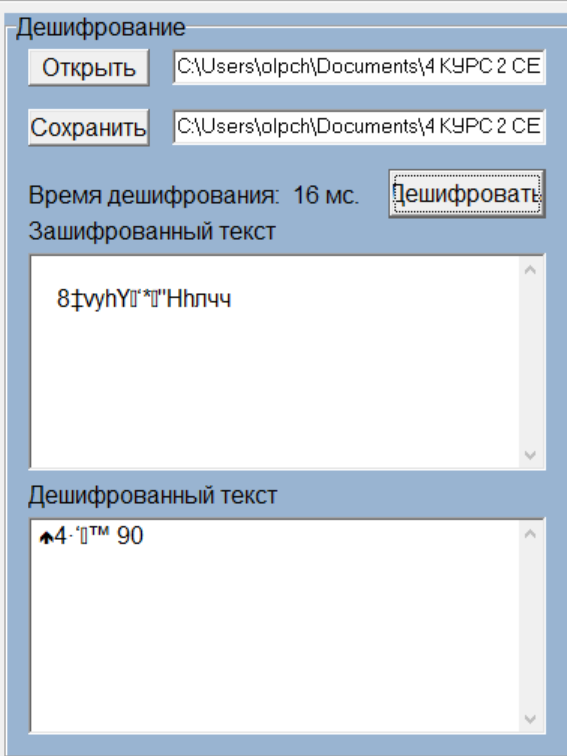




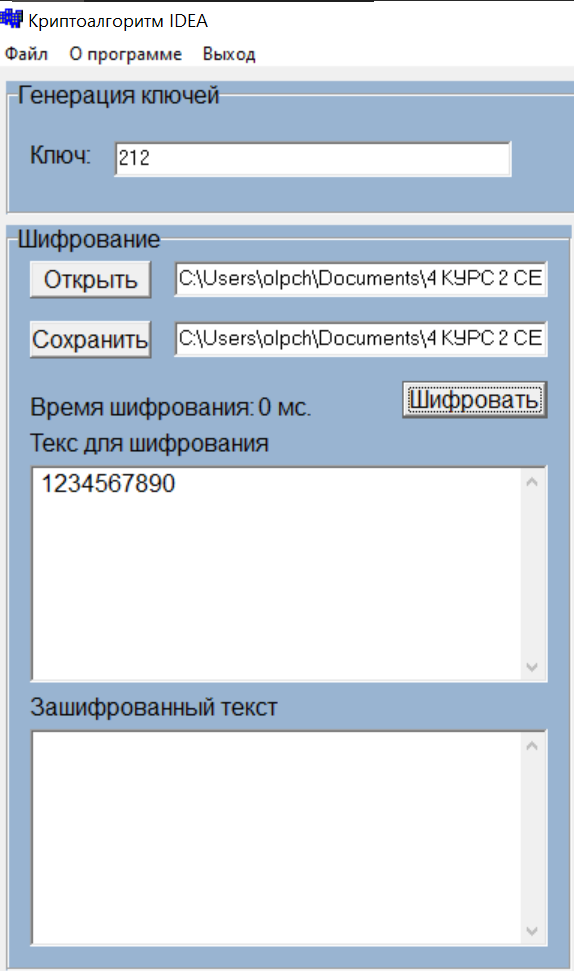


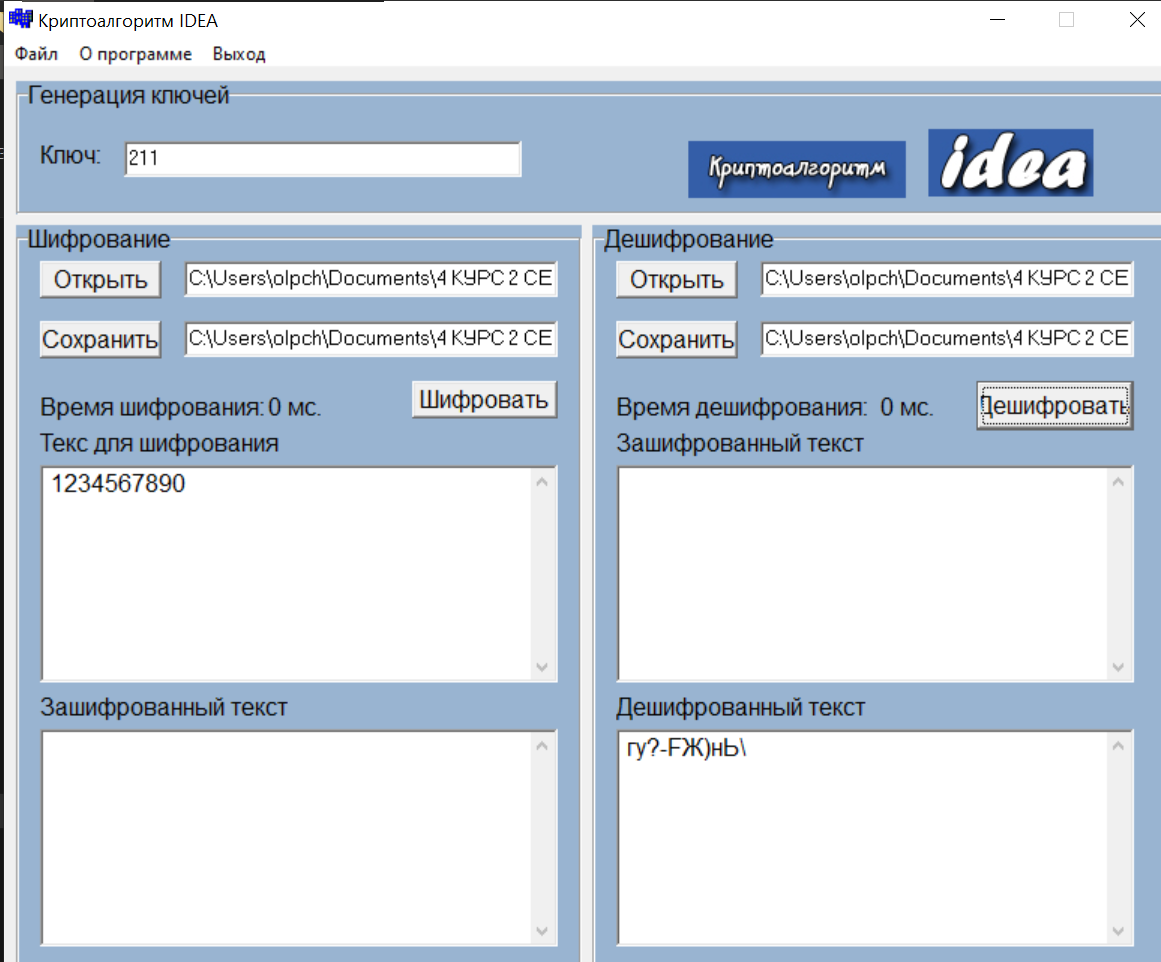
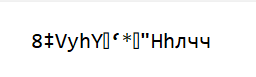
Проверка алгоритма на помехоустойчивость: 



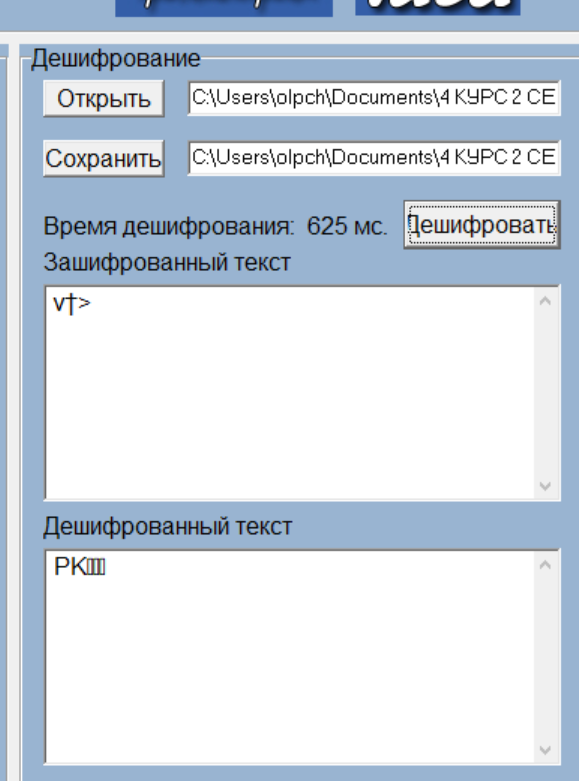
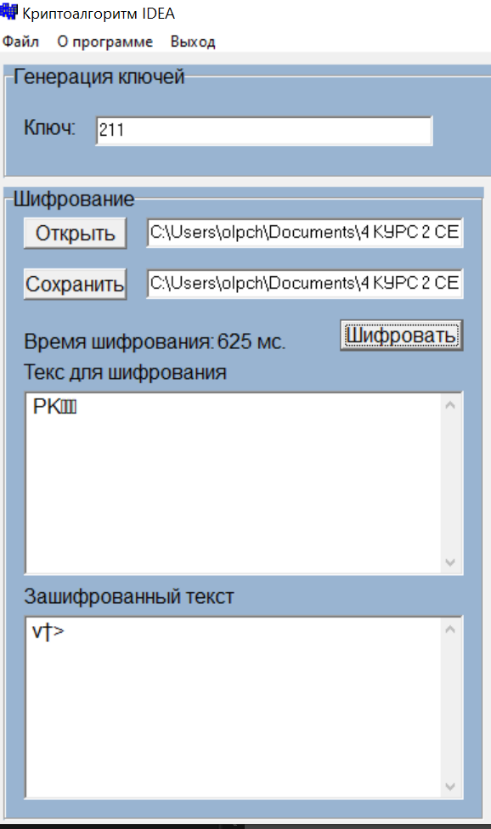


Проверка алгоритма на криптостойкость:

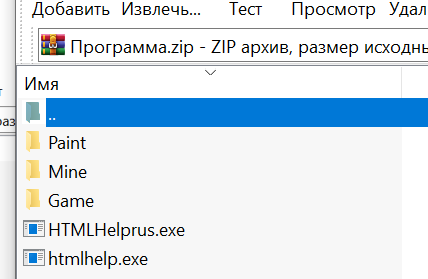


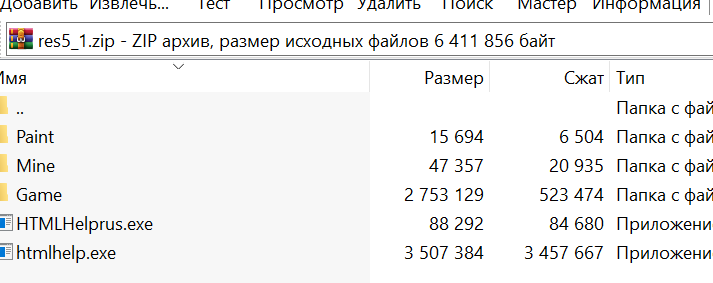


Сгенерировать ключи произвольной длины. Для шифрования выбрать любой нетекстовый файл, например, с расширением .zip. Зашифровать и дешифровать его. Убедиться, что он полностью идентичен исходному.



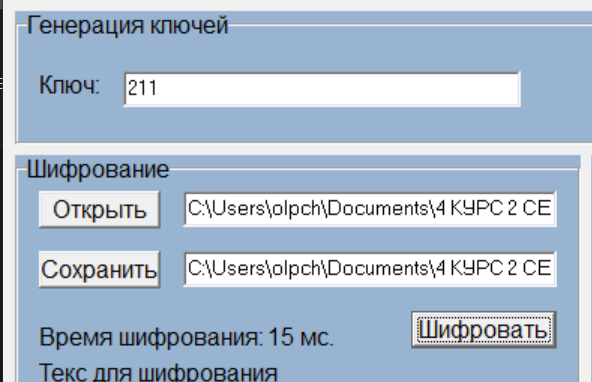
Архив до:



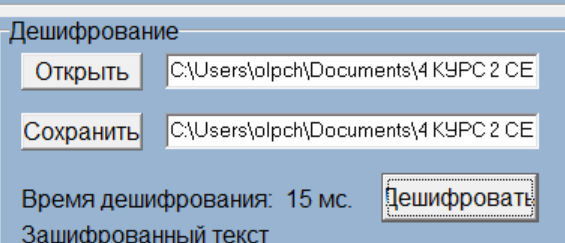
архив после:

Проверка скорости работы алгоритма:

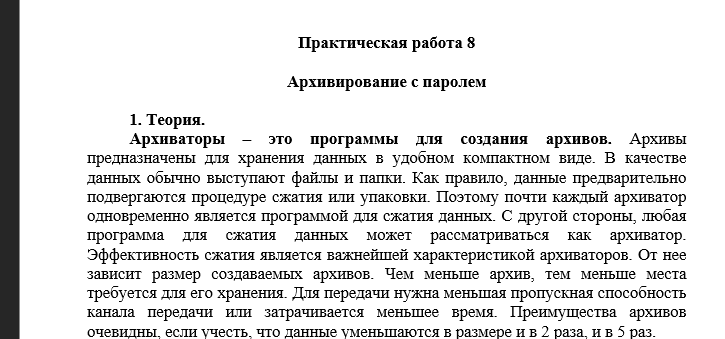
Зашифровать небольшой файл (1 Кбайт - 100 Кбайт). 



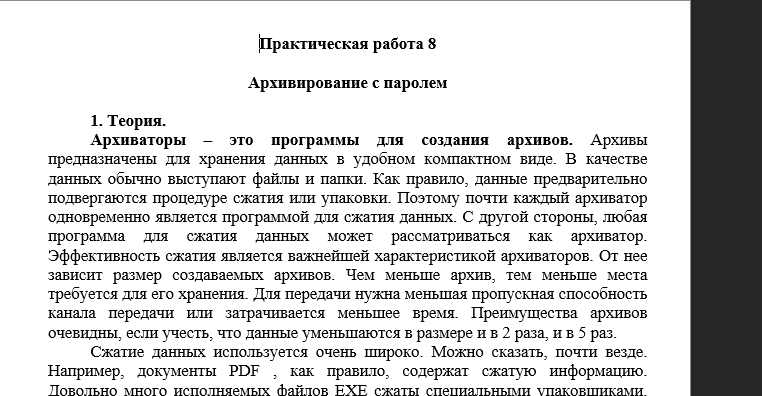
Дешифровать закодированный файл и посмотреть время дешифрования.



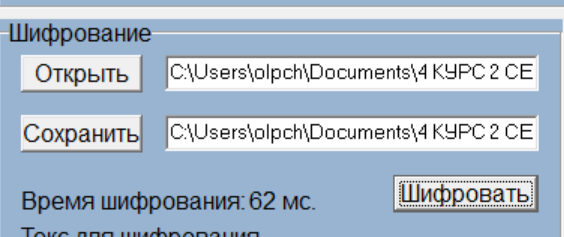
Файл до:



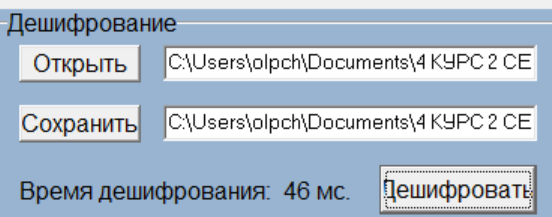
Файл после:



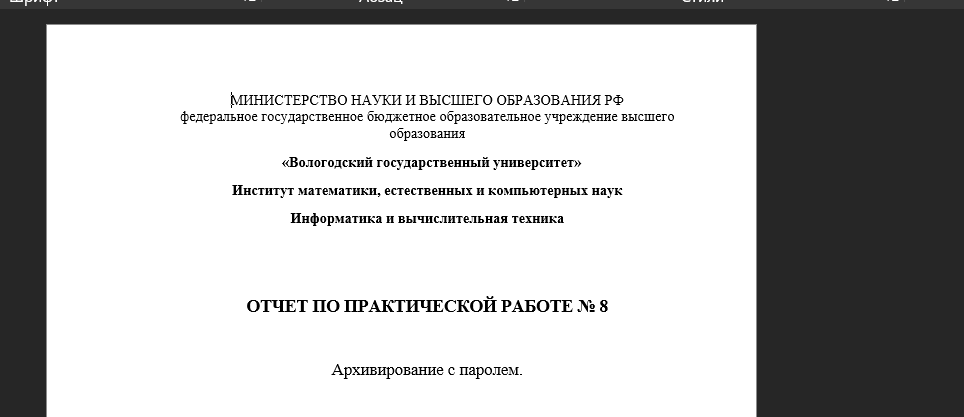
Зашифровать большой файл (100 Кбайт - 350 Кбайт), и посмотреть время шифрования. 



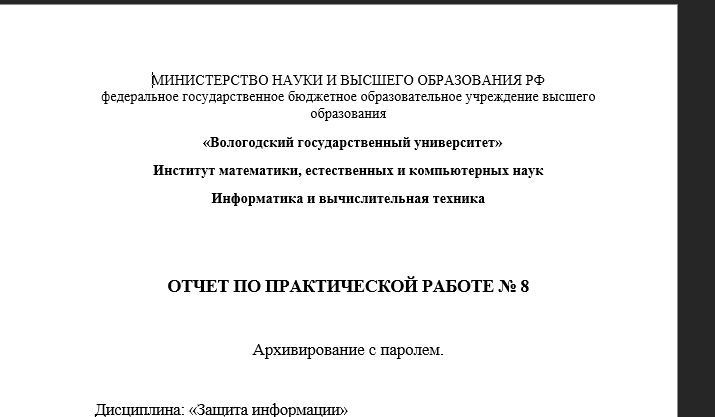
Дешифровать закодированный файл и посмотреть время дешифрования. Сравнить время шифрования и дешифрования.



Файл до:



Файл после:



Вывод: в ходе лабораторной работы зашифровали и дешифровали выбранные файлы, проверили алгоритм на помехоустойчивость и криптостойкость, а также проверили скорость работы алгоритма небольшого и большого файлов.