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 № 4**

Шифр RSA

Дисциплина: «Защита информации»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

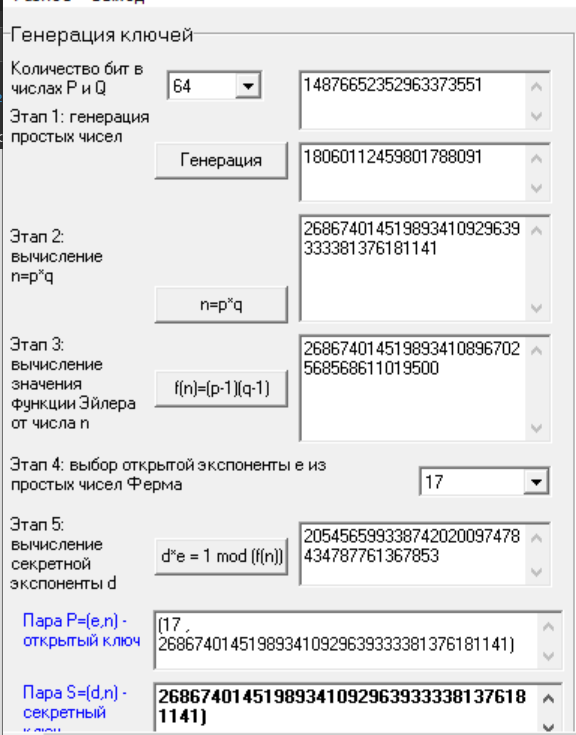
|  |  |
| --- | --- |
| Руководитель | Давыдова.Е.Н |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | 4Б09 ВМ-41 4 курс |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_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

Вологда

2023 г.

Практическая часть.

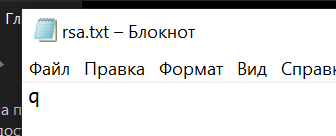
1. Генерация ключей



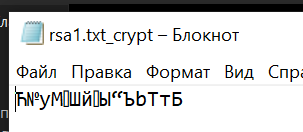
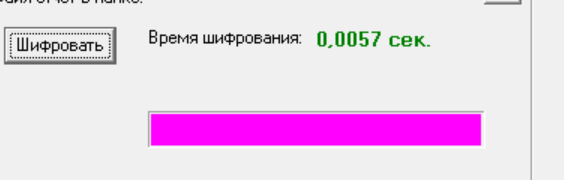
Открытый ключ P: (17 , 268674014519893410929639333381376181141)

Секретный ключ S: (205456599338742020097478434787761367853 , 268674014519893410929639333381376181141)

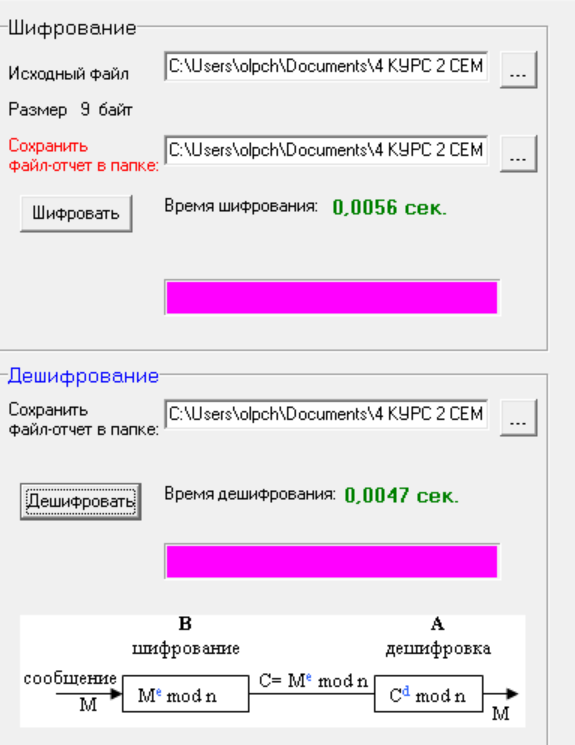
2. Выбрать текстовый файл размером 1 байт (то есть в файле должен быть один символ). Выбрать папку для сохранения зашифрованного файла.

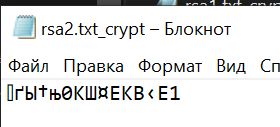
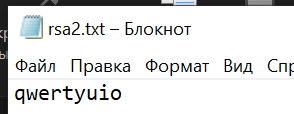


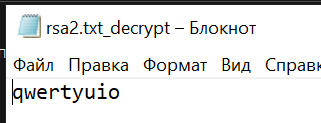
3. Нажмите на кнопку «Шифровать». Посмотрите размер зашифрованного файла.



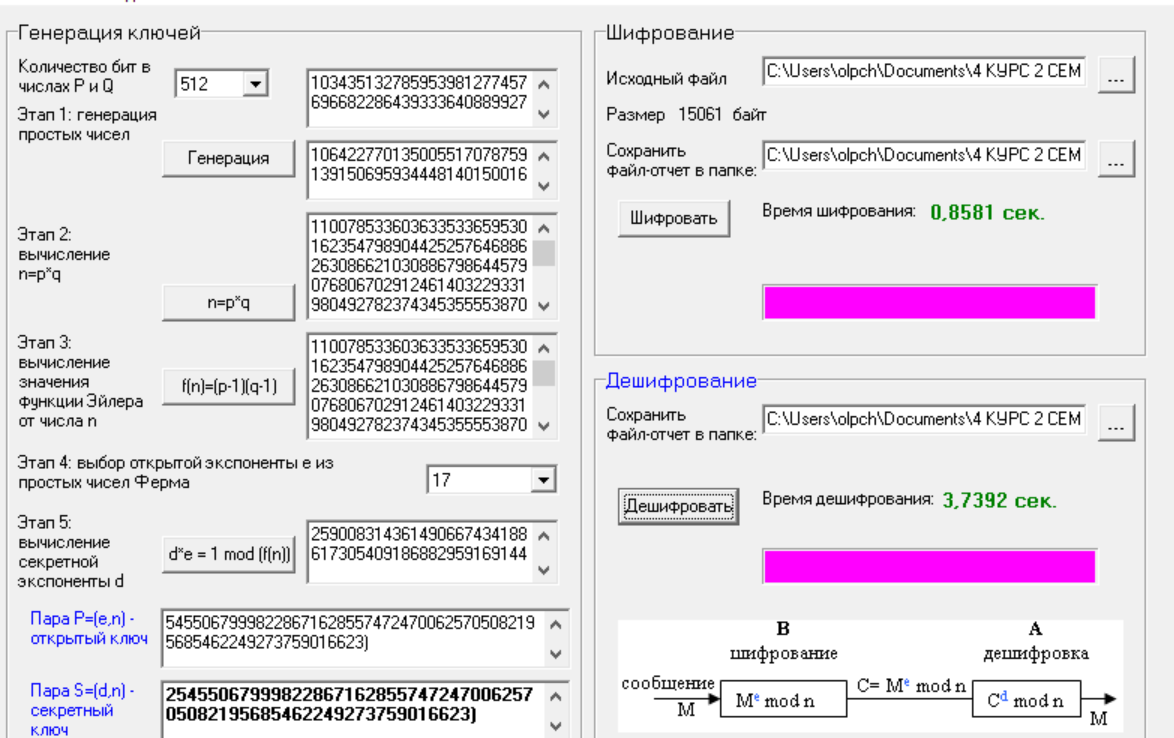
4. Зашифруйте файл размером от 8 до 16 байт, то есть 8-16 символов.

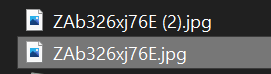
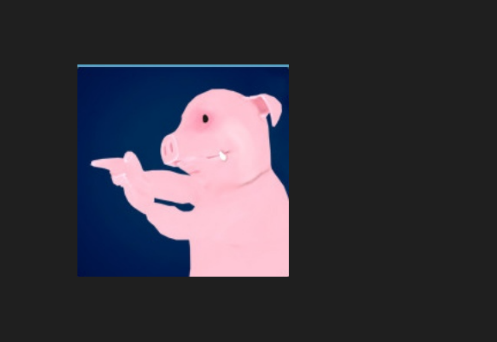


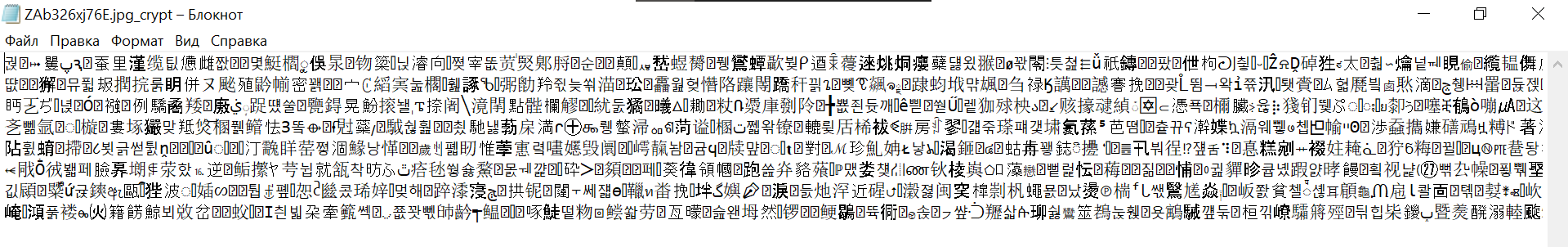


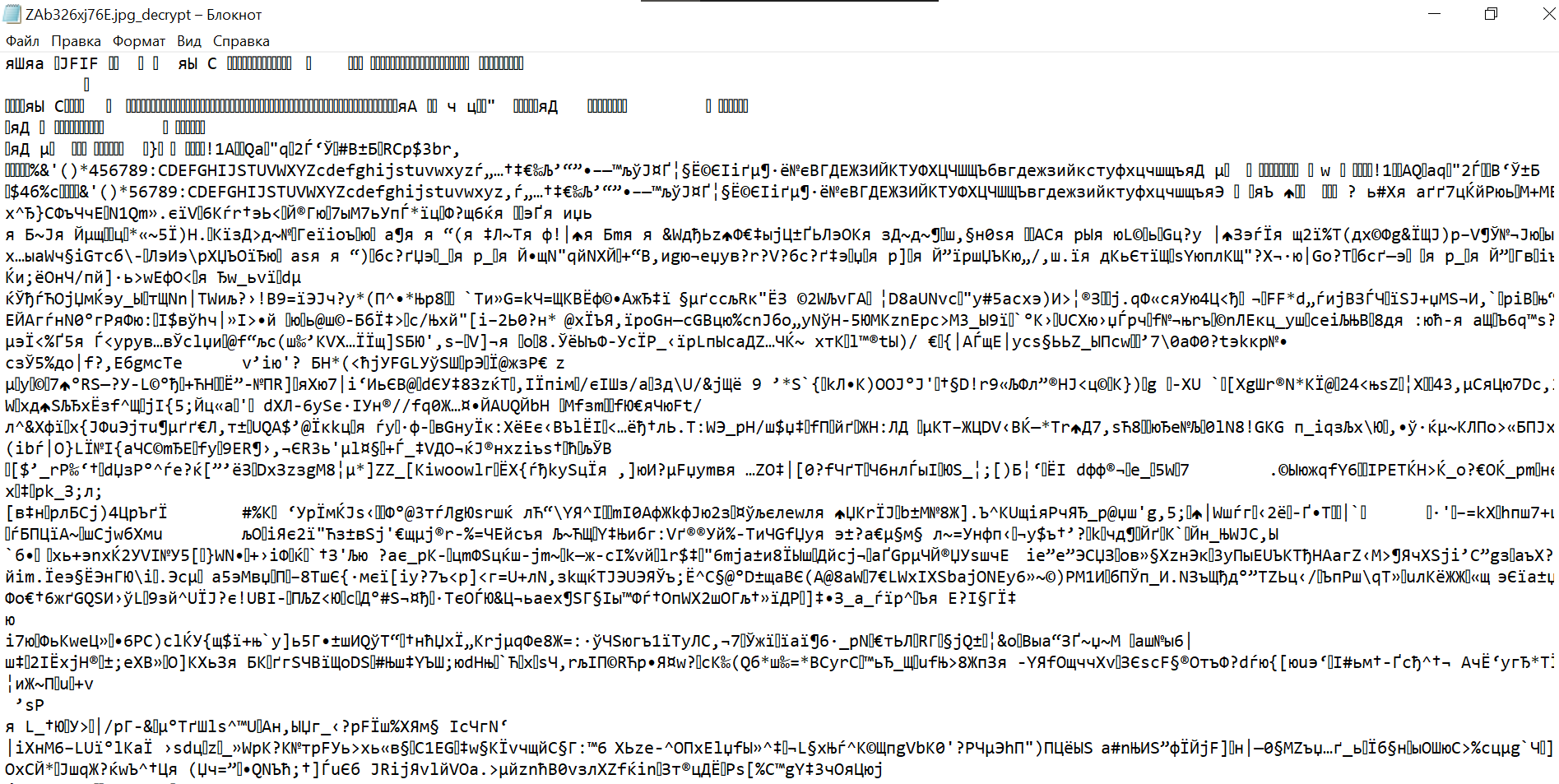


5. Проделать все действия, описанные в пункте 4, для ключа размером 1024 бита. Для этого выбрать размерность чисел p и q 512 бит. В отчет вставить выводы по пунктам, а также ключи и содержимое исходного, зашифрованного и дешифрованного файлов.







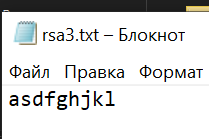
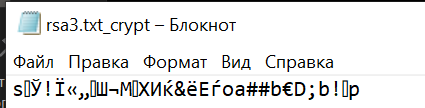


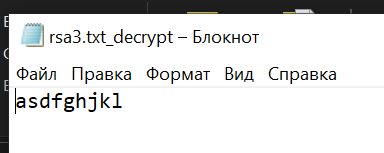
Открытый ключ P: (17 , 110078533603633533659530162354798904425257646886263086621030886798644579076806702912461403229331980492782374345355553870712800060069247020732275328084227871361970095007030395511059548198137753621867783882749793745516190165627869298623247825689492545506799982286716285574724700625705082195685462249273759016623)

Секретный ключ S: (25900831436149066743418861730540918688295916914414843910830796893798724488660400685285036053960465998301735140083659734285364720016293416642888312490406553029689365390842484679853168211741264810297362224683340118464661782594274577850201553511482562155913878207947214800405188698407986215754779214585687610033 , 110078533603633533659530162354798904425257646886263086621030886798644579076806702912461403229331980492782374345355553870712800060069247020732275328084227871361970095007030395511059548198137753621867783882749793745516190165627869298623247825689492545506799982286716285574724700625705082195685462249273759016623)

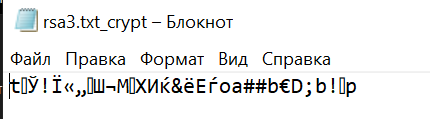
7. Проверка алгоритма на помехоустойчивость:

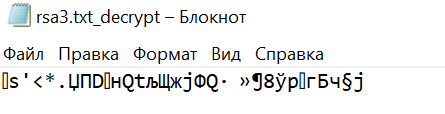


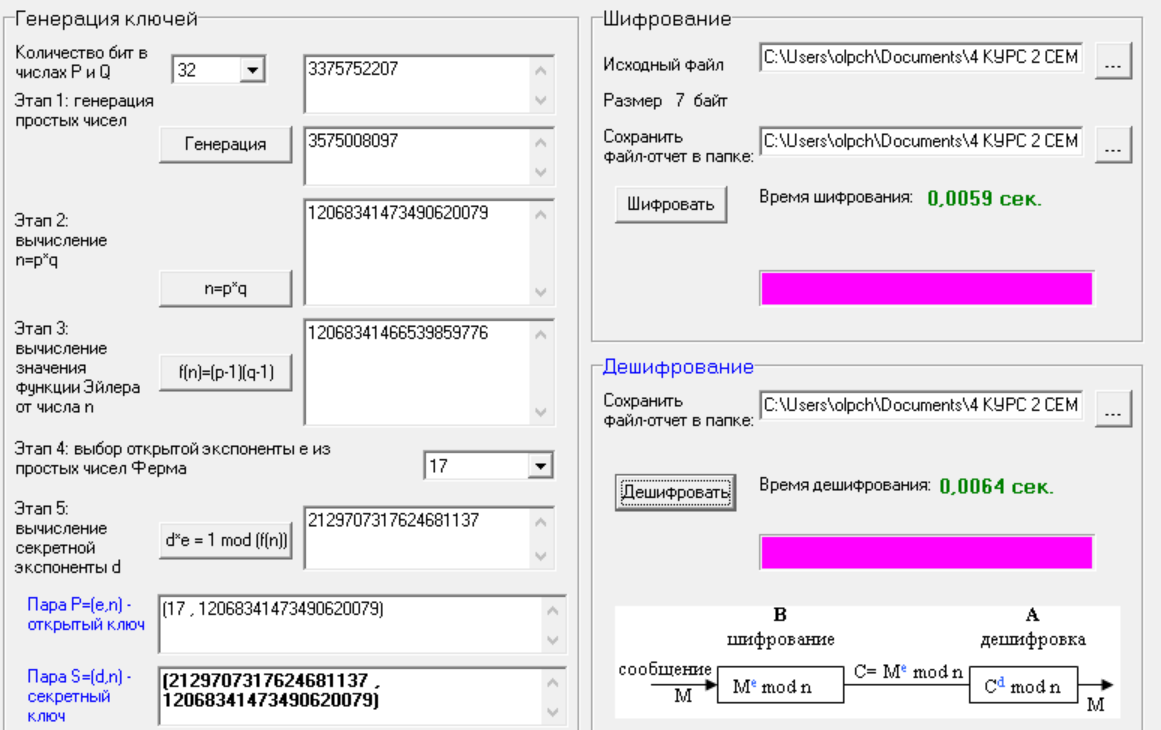


Меняем один символ:



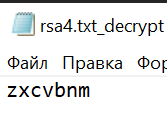
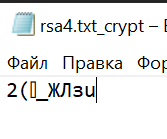
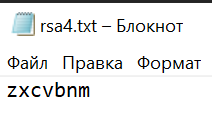


8. Проверка алгоритма на криптостойкость:

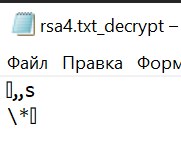


Открытый ключ P: (17 , 12068341473490620079)

Секретный ключ S: (2129707317624681137 , 12068341473490620079)

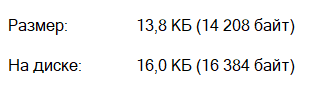


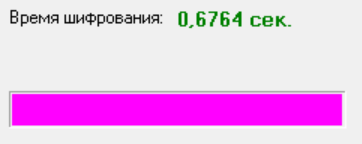
Измененный секретный ключ S: (3129707317624681137 , 12068341473490620079)



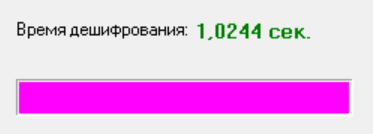
9. Проверка скорости работы алгоритма:

9.1. Зашифровать небольшой файл (1 Кбайт - 100 Кбайт), и посмотреть время шифрования.



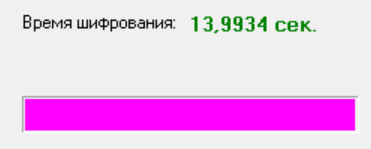


9.2. Дешифровать закодированный файл и посмотреть время дешифрования.

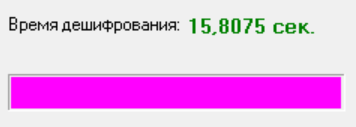


9.3. Зашифровать большой файл (100 Кбайт - 350 Кбайт), и посмотреть время шифрования.





9.4. Дешифровать закодированный файл и посмотреть время дешифрования.



Вывод: в ходе лабораторной работы мы ознакомились с шифром RSA на примере программы, проверили его на крипто устойчивость и скорость работы.