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 № 1**

**Исследование симметричного алгоритма шифрования ГОСТ 28147-89**

Дисциплина: «Защита информации в автоматизированных системах»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

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

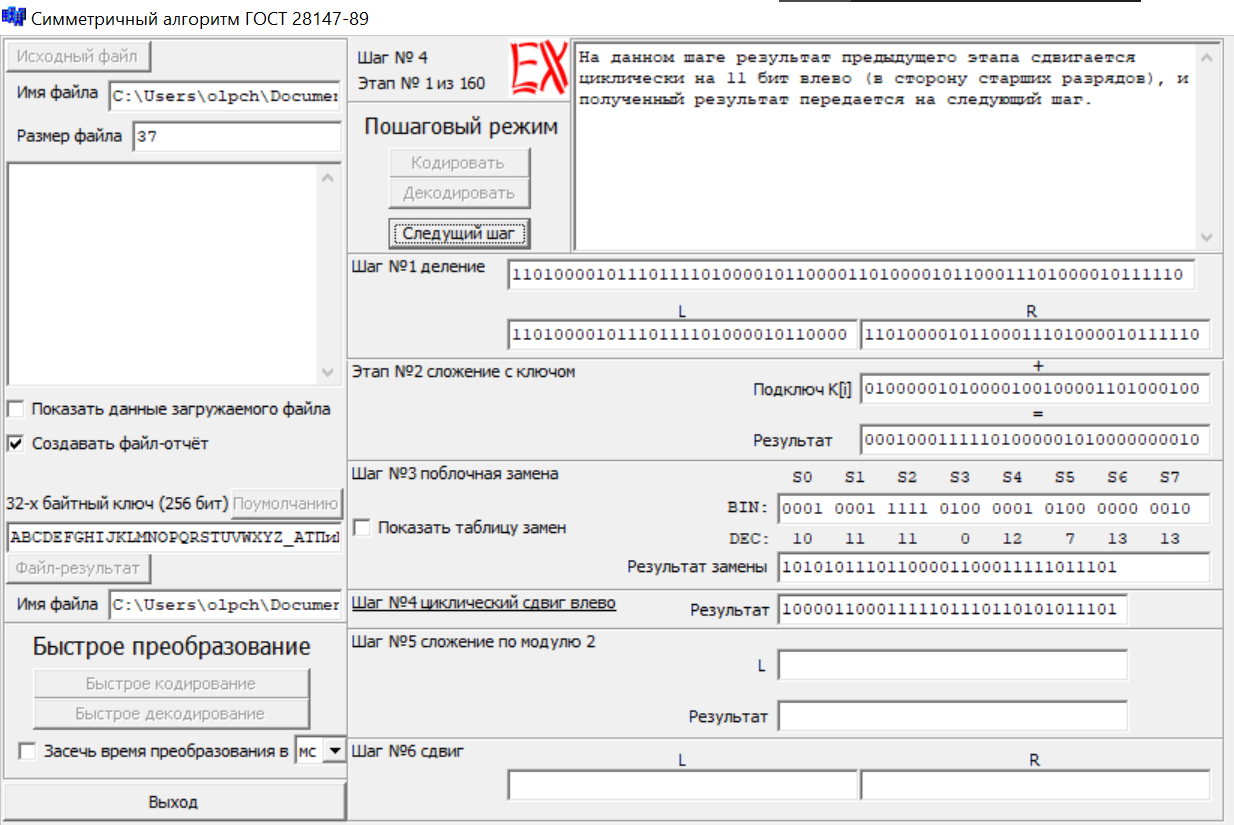
Вологда

2023 г.

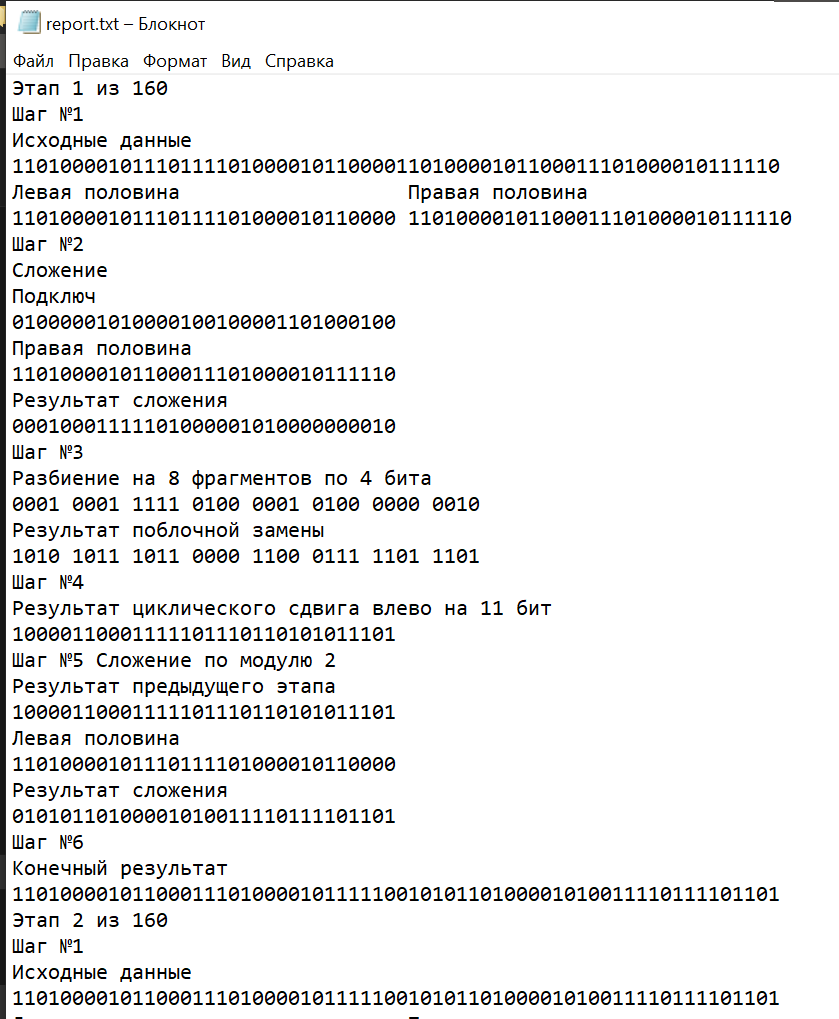
Цель работы:

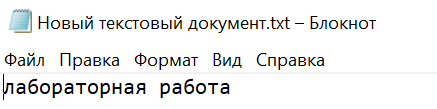
1. Загрузить ТХТ -файл небольшого размера (16-32 байт).

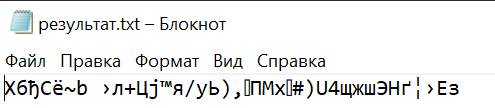
2. Выбрать выходной файл и запустить режим пошагового кодирования, предварительно установив флажок в поле «создавать файлы отчета». Выполнить процесс преобразования файла до конца, параллельно изучая комментарии на каждом шаге выполнения.



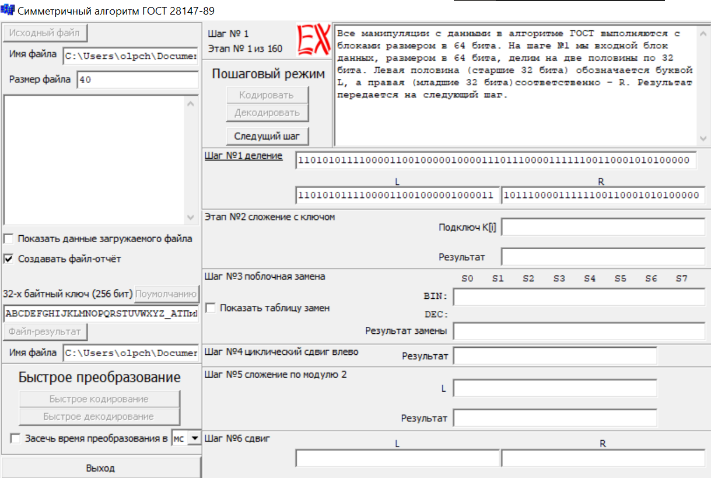
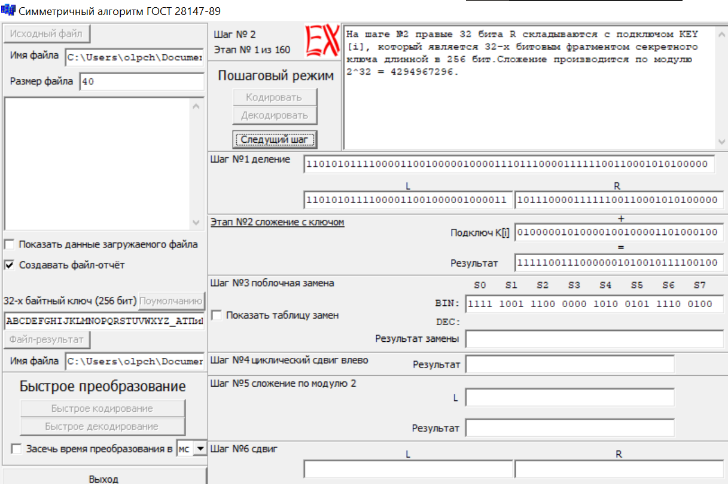
3. После выполнения предыдущего шага необходимо скопировать файл отчета report.txt в какую-либо другую директорию, т.к. при каждом новом кодировании/декодировании этот файл обновляется.

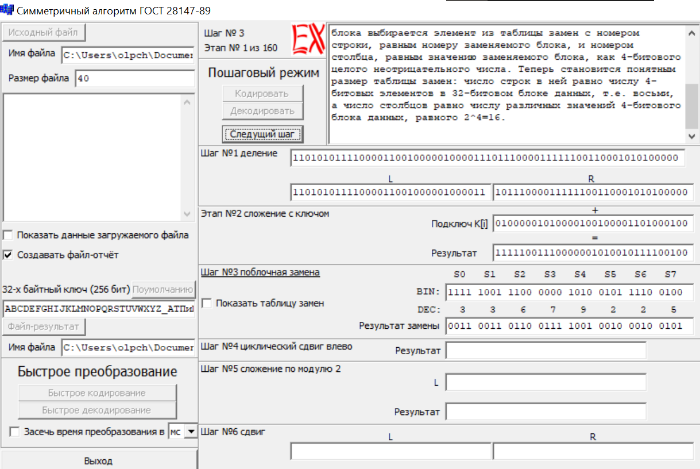
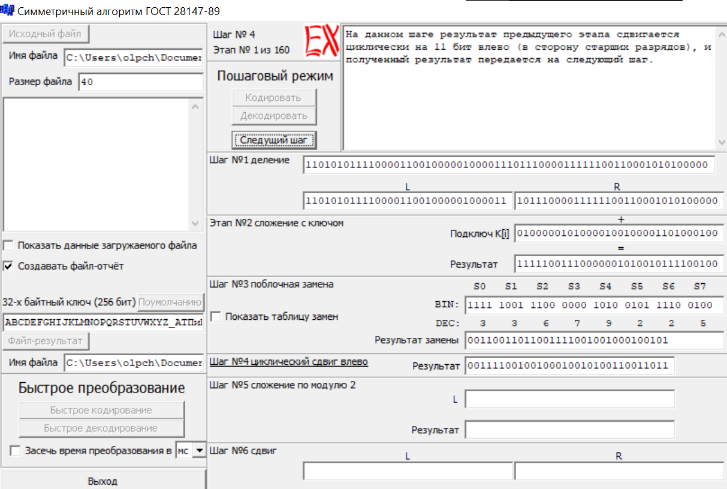


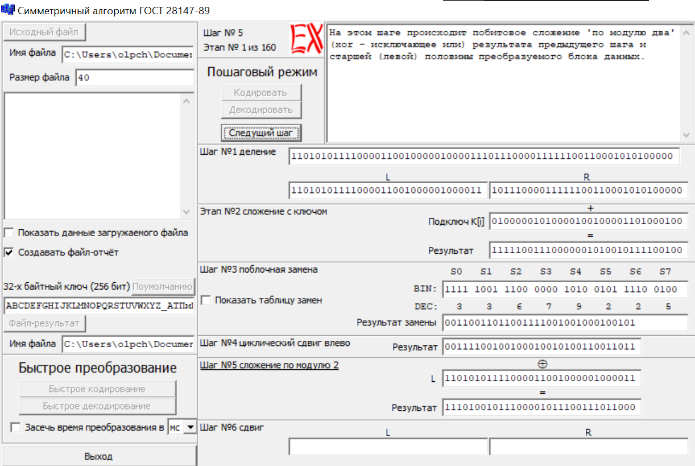
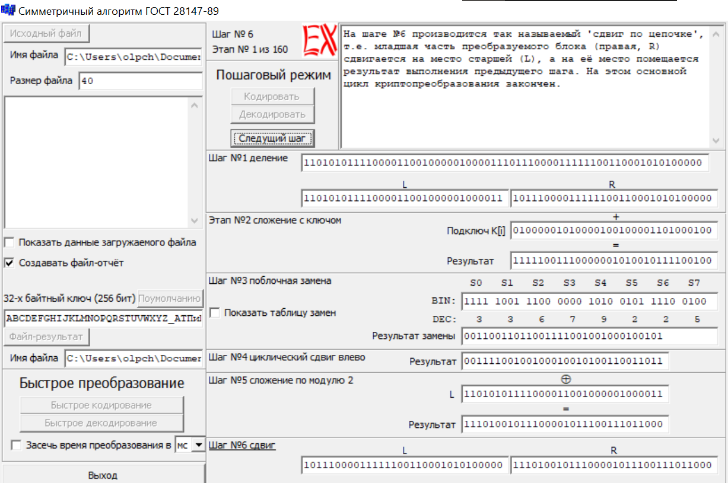




4. Запустить пошаговое декодирование файла, созданного на шаге 4.

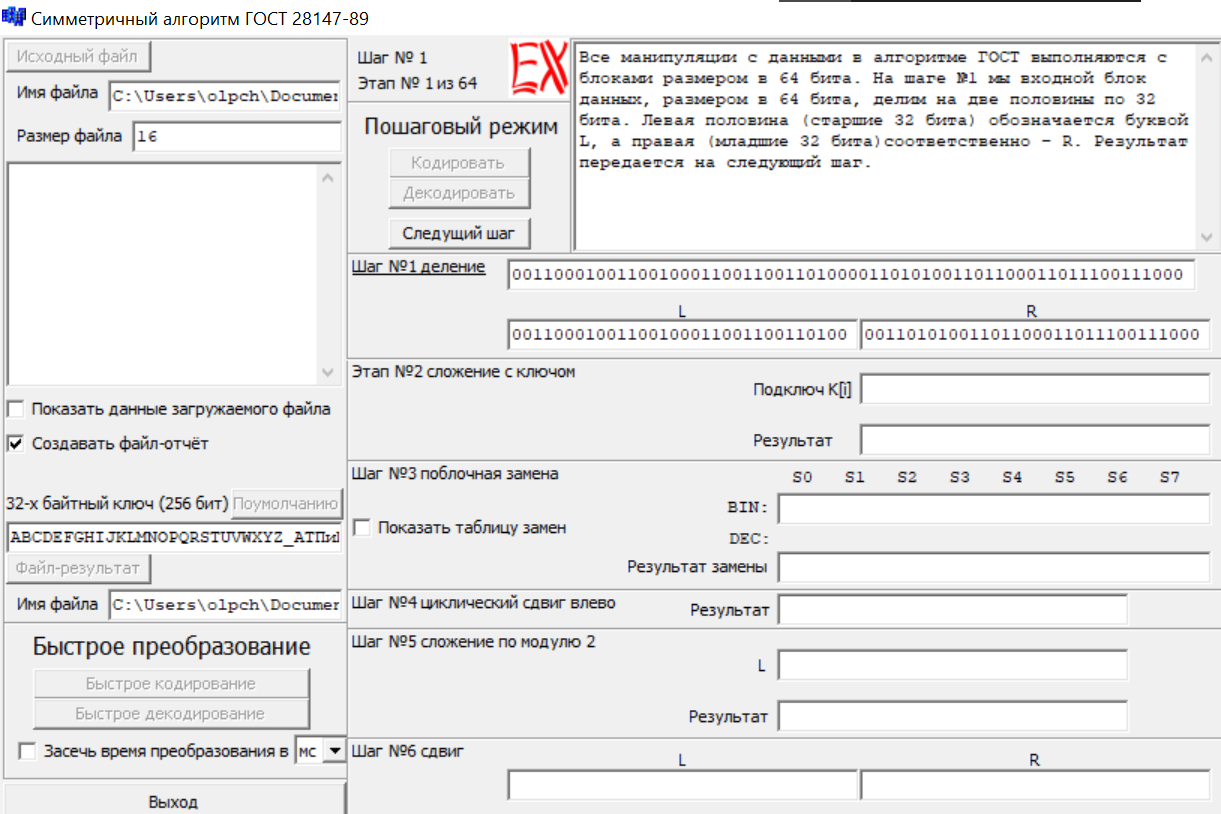
 

5. Скопировать файл отчета.

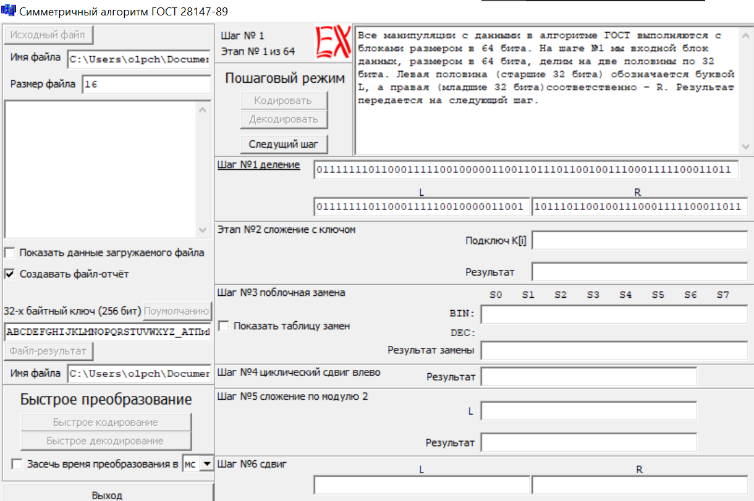
6. На данном этапе проводится проверка алгоритма ГОСТ на помехоустойчивость:

6.1 Загрузить текстовый файл длинной в 16 байт и выполнить пошаговое кодирование. Для этого может подойти и файл из шага №4. Сохранить файл отчета.



6.2 Изменить в любом текстовом редакторе 1 байт(символ) в закодированном файле и провести пошаговое декодирование измененного файла. Проанализировать результаты и сделать вывод, как повлияло изменение 1 бита на файл в целом. Сохранить файл отчета.





6.3 Изменить первые 8 символов в файле, полученном в п. 8.1 и запустить пошаговое декодирование. Проанализировать результаты и сделать вывод, как повлияло изменение на файл в целом. Сохранить файл отчета.



6.4 Проделать тоже самое, изменив 4 символа с позиции 7 по 12 (т.е. с 7 по 12-й байты файла). Проанализировать результаты и сделать вывод, как повлияло изменение на файл в целом. Сохранить файл отчета.



7. Проверка алгоритма на криптостойкость:

7.1 Можно использовать закодированный файл из п. 4 или п. 8.1 или же вновь пошагово закодировать файл.

7.2 Изменить любой из первых 4-х символов ключа и провести пошаговое декодирование. Как изменился файл по сравнению с п.4 или 6.1?



7.3 Проделать тоже самое, но изменить в ключе один из последних символов. Сделать вывод.



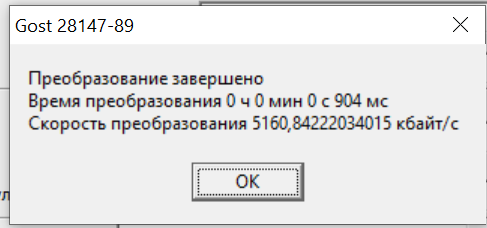
7.4 Пошагово закодировать файл из п. 9.1 с измененным ключом (ключ нужно запомнить) и сравнить полученный файл и файл из п.7.1

Ключ: ABCDEFGHIJKLMNOPQRSTUVWXYZ\_АТПэП

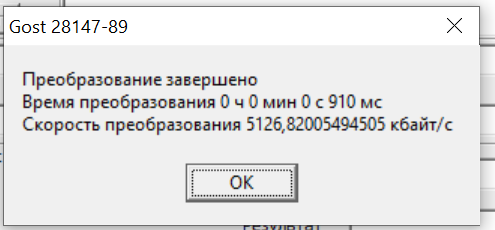


8. Проверка скорости работы алгоритма:

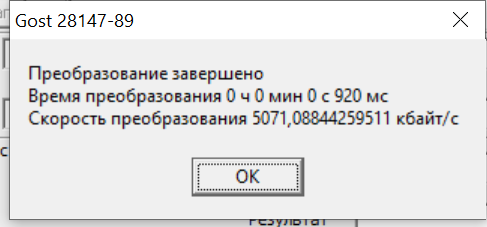
8.1 Закодировать большой файл (5-10 Мбайт) в ускоренном режиме, предварительно убрав флаг в поле «создавать файлы отчетов» (т.к. файл отчета может получиться огромных размеров), и провести замер времени, которое потребуется для кодирования. В качестве файлов для кодирования желательно использовать ZIP или RAR архивы, чтобы затем можно было проверить их работоспособность.

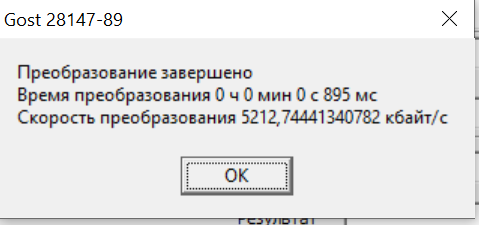


8.2 Декодировать закодированный файл и провести замер времени декодирования. Сравнить время кодирования и декодирования. Сделать вывод. Проверить на работоспособность и корректность преобразования раскодированый файл.



8.3 Выполнить п.10.1 – 10.2 с измененным ключом.





Вывод: