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 № 2**

**Исследование работы алгоритма шифрования с открытым ключом Эль Гамаля**

Дисциплина: «Защита информации в автоматизированных системах»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

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

Вологда

2023 г.

Цель работы:

Практическая часть:

1. Ознакомиться с теоретической частью работы.

2. Запустить файл ElGamal\_1.exe и изучить интерфейс программы.

3. В меню «Помощь» основного окна выбрать строку «Оглавление» и ознакомиться с примером, разобранным в пункте 4 помощи. При необходимости можно прочитать и остальные разделы, в которых рассмотрены принципы работы алгоритма.

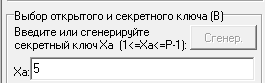
4. Постараться реализовать разобранный пример и проверить получается ли тот же результат. Для этого необходимо выполнить:

4.1 Ввести в Число Р=37. Программа автоматически сгенерирует и число W. Проверьте, действительно ли соблюдаются условия для числа W (диапазон, W^P-1 mod P = 1);

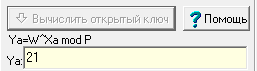




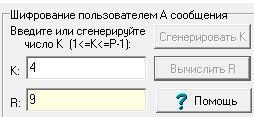
4.2 Введите секретный ключ Xa = 5;



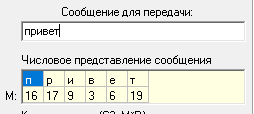
4.3. Вычислите открытый ключ и затем нажмите кнопку «Прердать». На этом этапе закончились действия пользователя В. Далее начинает работать пользователь А;



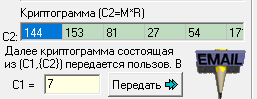
4.4 Введите число К=4 и вычислите число R. Проверьте, действительно ли соблюдаются условия для числа R;



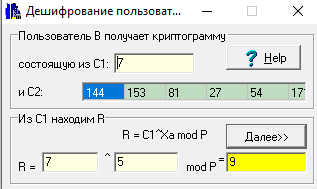
4.5 Введите сообщение для передачи, но учтите, что в сообщении должны использоваться только русские строчные буквы;



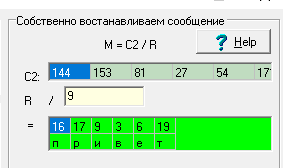
4.6 Автоматически сгенерируется С1. Проверьте, соблюдается ли равенство C1=W^K mod P;



4.7 Нажмите кнопку «передать». На этом этапе пользователь А снова передает инициативу действий пользователю В. Проследите за тем, как эмулируется прием криптограммы пользователем В, а по завершении нажмите кнопку «Далее»;



4.8 Теперь вы видите как восстанавливается исходное сообщение.

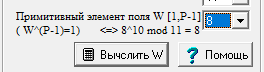


5. Запустить программу ElGamal\_2.exe;

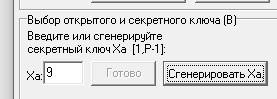
6. Выбрать в любое из представленных чисел Р = {5,7,11,13}.



7. После того как выберите простое число Р нажмите кнопку «Вычислить W» и выберите любое число W (кроме W=1) из сгенерированного ряда.

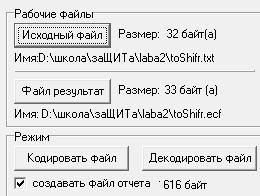


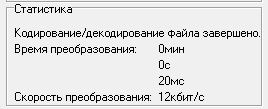
8. Сгенерируйте или введите секретный ключ Xa и по его значению вычислите открытый ключ Ya, причем значения W и Xa должны быть такими, чтобы Ya не равнялось 1.

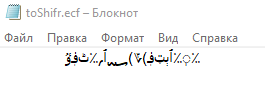
 

9. Сгенерируйте число К и вычислите R, причем R не должно равняться единице.

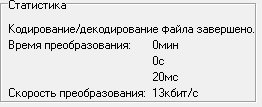
10. Выберите исходный файл (желательно текстовый, чтобы было явно видно преобразование) размером примерно до 1 кбайта и закодируйте его, предварительно установив флаг в поле «создать файл отчета». По завершении кодирования переименуйте или скопируйте файл отчета report.txt

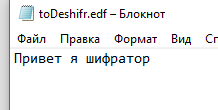






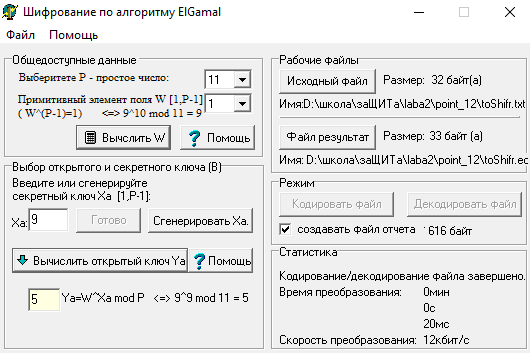
11. Выберите в качестве исходного файла только что закодированный файл и проведите процедуру декодирования. Сохраните файл отчета.



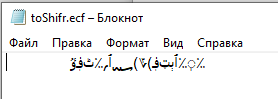
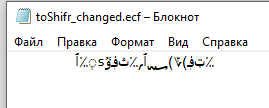


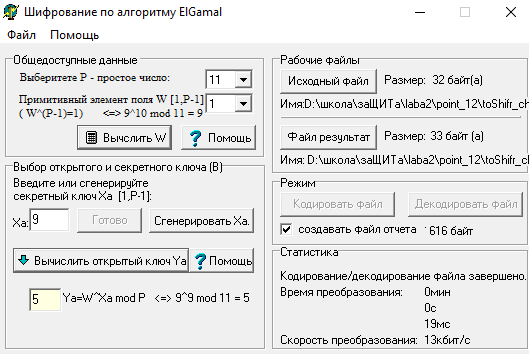
12. Проверка алгоритма Эль Гамаля на помехоустойчивость:

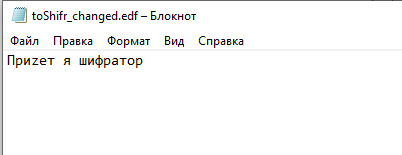
12.1 Загрузить текстовый файл небольшой и выполнить кодирование. Сохранить файл отчета.



12.2 Изменить в любом текстовом редакторе 1 символ (кроме первых трех) в закодированном файле и провести декодирование измененного файла.

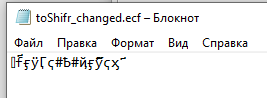
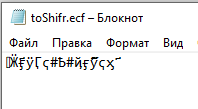


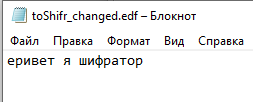
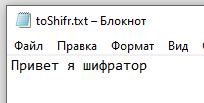


13. Проверка алгоритма на криптостойкость:

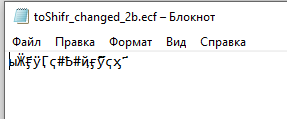
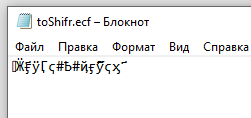
13.1 Закодировать текстовый файл.

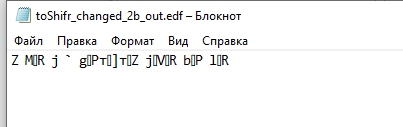
13.2 Изменить любой из символов в закодированном файле и провести декодирование.



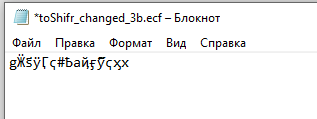
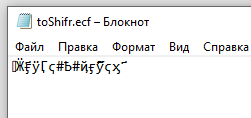


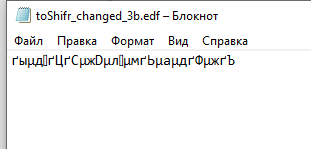
13.3 Изменить в каком-нибудь закодированном файле 2-й байт на другое значение. Это равносильно изменению секретного ключа Xa.





13.4 Изменить в закодированном файле 3-й байт на другое значение. Это равносильно изменению простого числа Р.

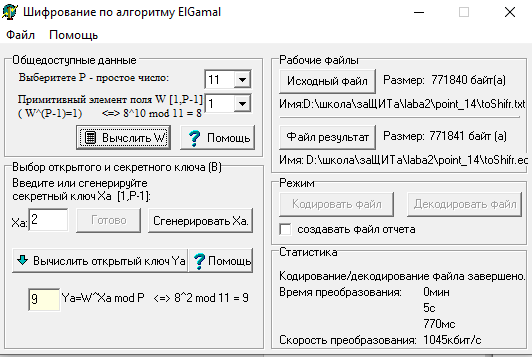


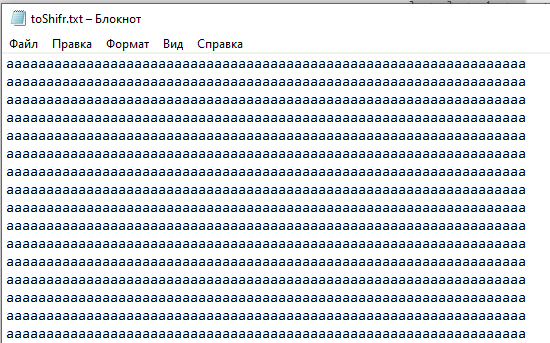


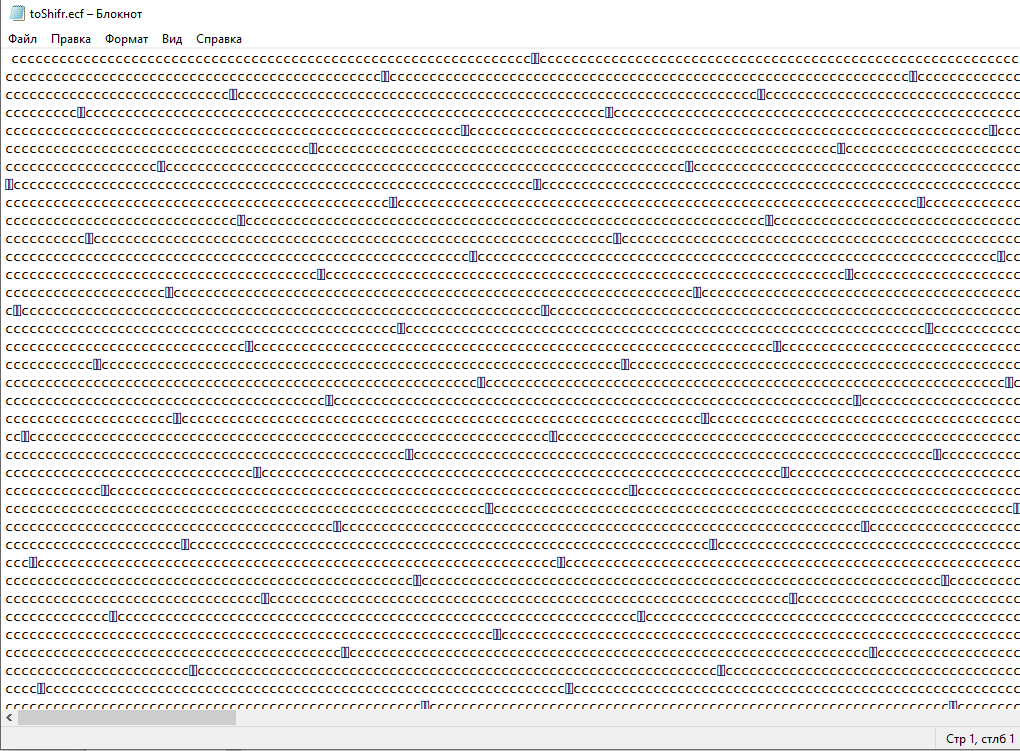
14. Проверка скорости работы алгоритма:

14.1 Закодировать большой файл (500 - 1000 кбайт), предварительно убрав флаг в поле «создать файл отчета» (т.к. файл отчета может получиться огромных размеров), и замер времени, которое потребуется для кодирования.

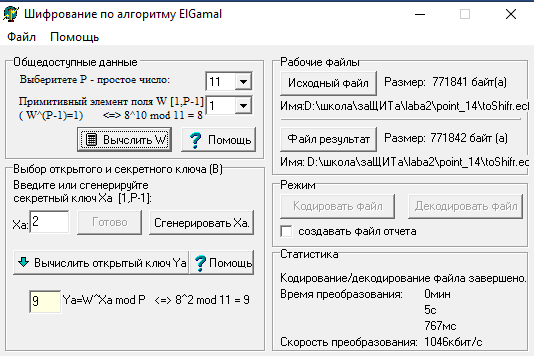








14.2 Декодировать закодированный файл и провести замер времени декодирования.





Вывод: