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**

**Шифр ELGAMAL**

Дисциплина: «Защита информации в автоматизированных системах»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

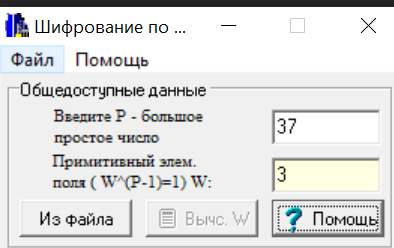
|  |  |
| --- | --- |
| Руководитель | Давыдова Е.Н. |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | ВМ-41 |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись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

Вологда

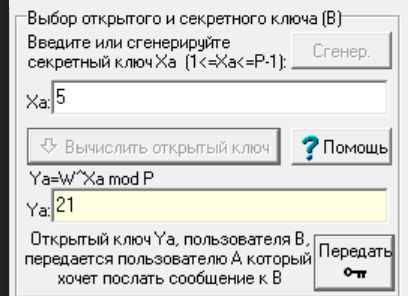
2023 г.

Практическая часть.

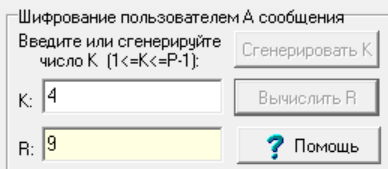
Ввести в Число Р=37. Программа автоматически сгенерирует и число W.



Вычисление открытого ключа.

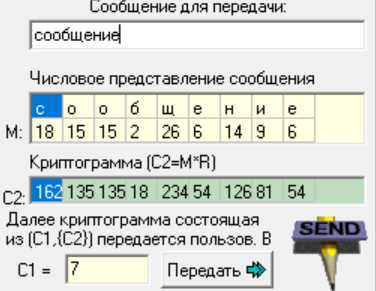


Ввод числа К=4 и вычисление числа R.

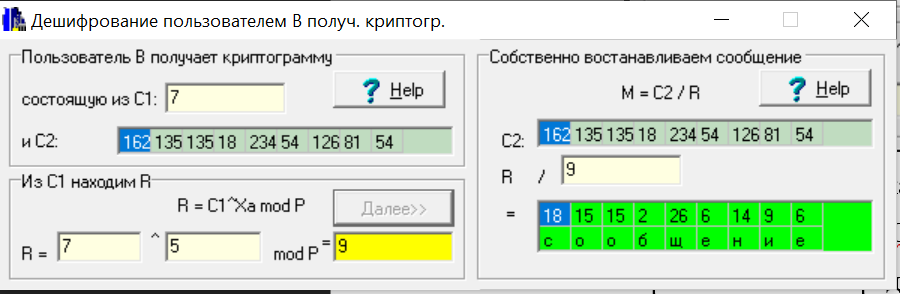


Ввод сообщения для передачи.

Автоматически сгенерировалась С1.



Передача сообщения пользователю В и прием криптограммы пользователем В.



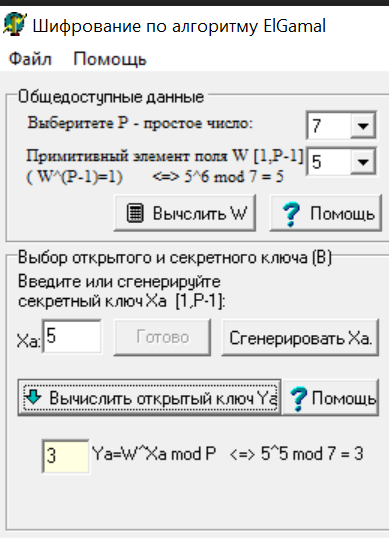
Задание 2.

Запустить программу ElGamal\_2.exe;

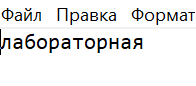
Выбрать в любое из представленных чисел Р = {5,7,11,13}.

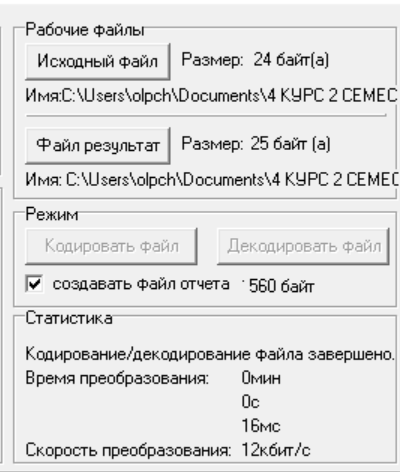
После того как выберите простое число Р нажмите кнопку «Вычислить W» и выберите любое число W (кроме W=1) из сгенерированного ряда.

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.

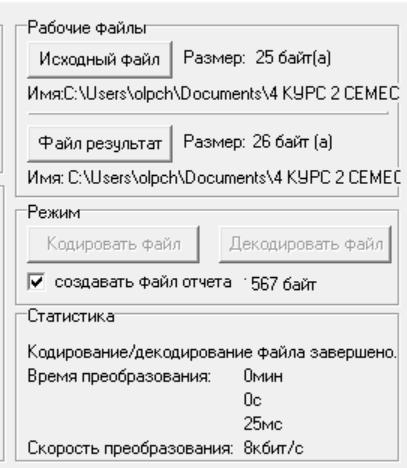


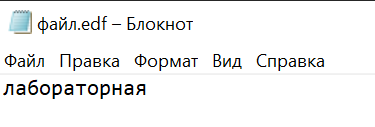
Кодировка файла.





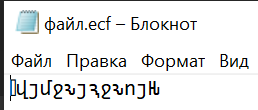
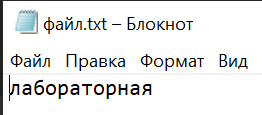
Декодирование файла.



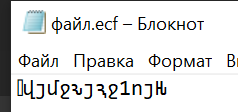
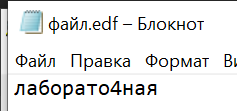


Проверка алгоритма Эль Гамаля на помехоустойчивость:

Загрузить текстовый файл небольшой и выполнить кодирование.

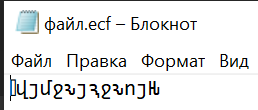
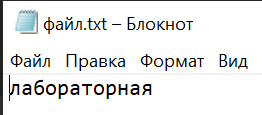


Изменить в любом текстовом редакторе 1 символ (кроме первых трех) в закодированном файле и провести декодирование измененного файла.

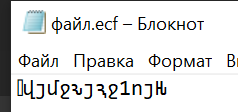
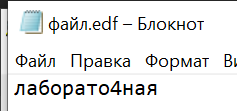
 

Проверка алгоритма на криптостойкость:

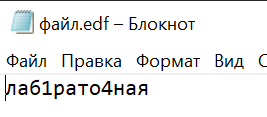
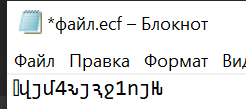
Закодировать текстовый файл.



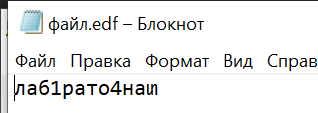
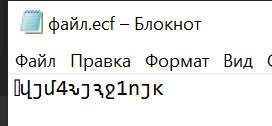
Изменить любой из символов в закодированном файле и провести декодирование.

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

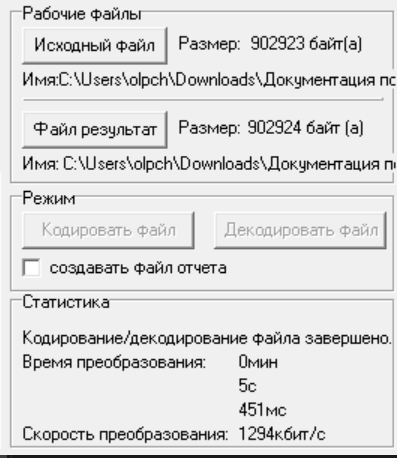


Изменить в закодированном файле 3-й байт на другое значение. Это равносильно изменению простого числа Р. Провести декодирование

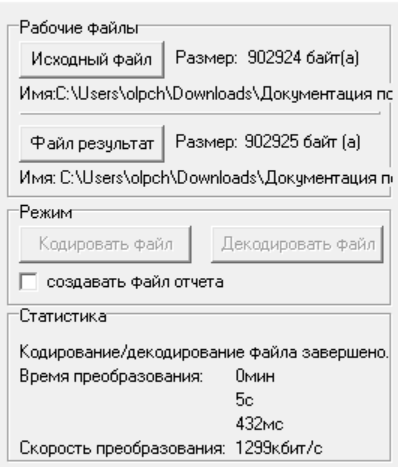


Проверка скорости работы алгоритма:

Закодировать большой файл (500 - 1000 кбайт).



Декодировать закодированный файл и провести замер времени декодирования.



Файл был раскодирован корректно. Скорость работы алгоритма по сравнению с алгоритмом ГОСТ быстрее.

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