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 № 3**

**Исследование работы смешанной криптосистемы**

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

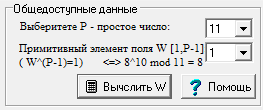
2023 г.

Цель работы:

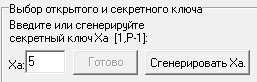
Практическая часть

1. Запустить файл Gybrid.exe из 3-ей лабораторной работы.
2. Передача ключа и закодированного файла

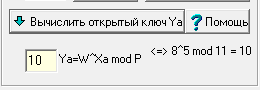
2.1 Выберите простое число Р из выпадающего списка, а затем выберите любое доступное число W.



2.2 Далее необходимо сгенерировать секретный ключ Xa, который будет участвовать в шифровании сеансового ключа



2.3 Затем нужно вычислить открытый ключ Ya.



2.4 На следующем этапе необходимо ввести сеансовый ключ. Он должен быть длинной в 32 символа.

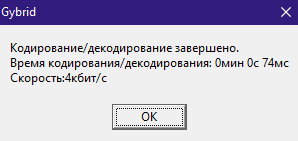
12345678912345678912345678912341

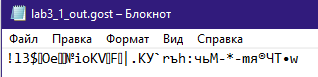
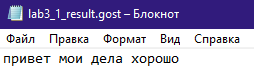
2.5 Закодировать ключ. Ключ закодирован по алгоритму Эль Гамаля с помощью ключа Xa.

4761032=<4761032=<4761032=<47614

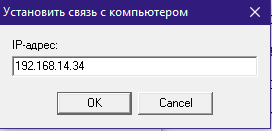


2.6 Закодировать файл





2.7 Ввести IP адрес и установить соединение с другим компьютером.



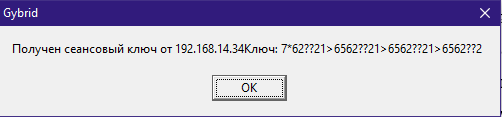


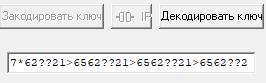
2.8 Отправить ключ, и закодированный файл.

3. Прием ключа и закодированного файла

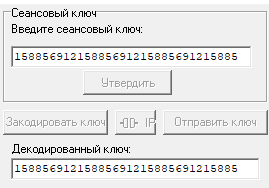
3.1 Получение закодированного файла

3.2 Получение закодированного ключа



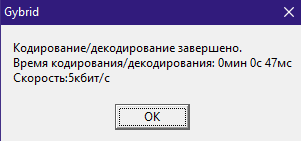


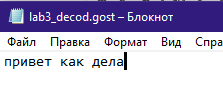
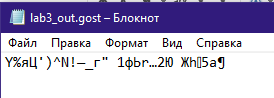
3.3 Декодирование полученного ключа.



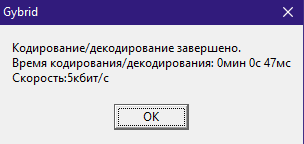
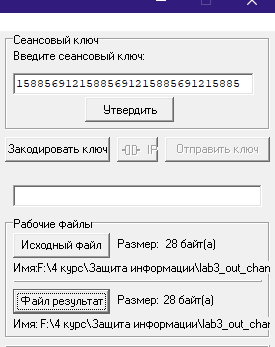
3.4 Расшифровать файл с помощью полученного ключа.

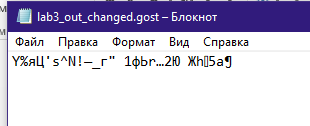
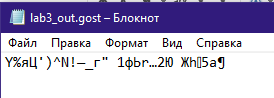
15885691215885691215885691215885

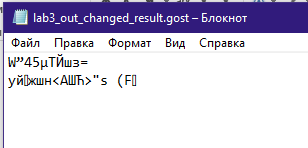
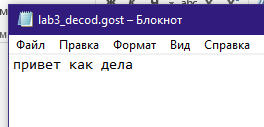




4. Измените 1 символ сеансового ключа в каком-нибудь из приложений (но только в одном) и закодируйте этим ключом файл. Затем скопируйте файл на другую машину и проведите декодирование с созданием отчета.







Вывод: