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

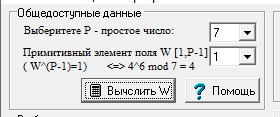
2023 г.

Цель работы:

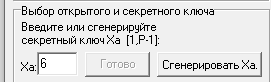
Практическая часть:

1. Запустить файл Gybrid.exe из 3-ей лабораторной работы.

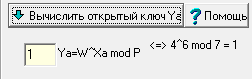
2. Выберите простое число Р из выпадающего списка, а затем выберите любое доступное число W. Желательно выбирать большие числа, т.к. это дает большую надежность закодированной информации и искажает ее сильнее, по сравнению с исходным текстом.



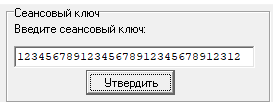
3. Далее необходимо сгенерировать секретный ключ Xa, который будет участвовать в шифровании сеансового ключа. Так же желательно чтобы это число было большим.



4. Затем нужно вычислить открытый ключ Ya.

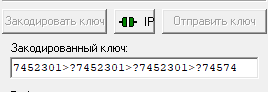


5. На следующем этапе необходимо ввести сеансовый ключ. Он должен быть длинной в 32 символа. Если будет введено выражение меньшей длинны, то ключ будет автоматически создан длинной в 32 байта, путем копирования введенных символов. После ввода ключа его нужно утвердить. Если вы, после того как уже утвердили ключ решили его поменять, то просто нажмите кнопку «Вычислить открытый ключ» и поле ввода сеансового ключа вновь станет доступным для редактирования.



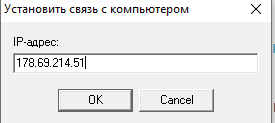
6. На данном этапе, в принципе, в данном приложении уже можно начинать кодирование и декодирование. Но если мы хотим передать ключ на другую машину, нужно приступать к следующему этапу.

7. Перед отправкой ключа по сети его, во избежание компрометации, необходимо закодировать. Для этого нужно нажать кнопку «Закодировать ключ». После этого вы увидите закодированный ключ, который будет передан на другую машину. Ключ закодирован по алгоритму Эль Гамаля с помощью ключа Xa.



7452301>?7452301>?7452301>?74574

8. На этом этапе требуется установить соедиенение с другим компьютером. Для этого нужно нажать кнопку «IP» или выбрать пункт меню «Установить соединение». Появится диалоговое окно, в котором нужно ввести IP-адрес компьютера, которому будет передаваться закодированный ключ. При этом необходимо, чтобы компьютер-приемщик находился в режиме ожидания (это показывается в строке состояния). Если это не так, то нужно установить флаг «Ожидание приема» в главном меню.



9. Теперь, после того как соединение установлено, можно отправлять ключ нажав соответствующую кнопку. При удачной передаче в приложении-сервере появится окно с результатом передачи.

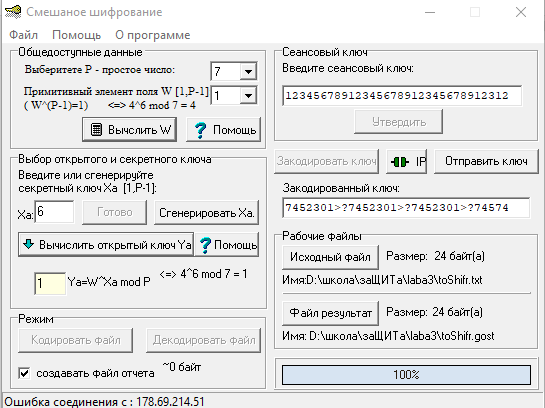


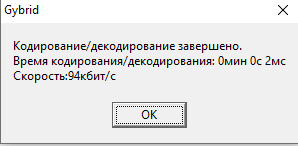
10. Теперь в приложении, которое получило закодированный ключ, появится кнопка «Декодировать ключ», нажав которую произведется декодирование ключа.

11. Далее оба приложения имеют один и тот же сеансовый ключ, с помощью которого можно шифровать данные.

12. Проделайте п.6-11, но при этом поменяйтесь ролями (сервер станет клиентом, клиент – сервером).

13. Выберите какой-нибудь сеансовый ключ и зашифруйте с его помощью текстовый файл.





14. Теперь закодируйте сеансовый ключ и передайте его на другую машину. Машина примет ключ, после чего его нужно будет декодировать. Теперь скопируйте файл, который получился в предыдущем пункте, по сети или с помощью дискеты на машину-сервер (которая приняла сеансовый ключ) и проделайте процедуру декодирования скопированного файла, при этом создав файл отчета. Сделайте вывод. Файл отчета сохраните.

15. Проделайте п.13, 14 поменявшись ролями. Сравните время кодирования и декодирования на разных машинах и сделайте по результатам сравнения вывод.

16. 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. Эта процедура равнозначна тому, что ключ по сети передался с ошибкой. Сделайте вывод.

17. Попробуйте закодировать файл большого размера, а декодировать его на другой машине, при этом желательно, чтобы быстродействие этих машин было различным. Сделайте вывод, как изменилась скорость преобразования.

18. Сделайте общие выводы по работе. В отчет должны быть вставлены файлы отчетов. Какие преимущества смешанного шифрования вы уяснили для себя?

Вывод: