Журавлев К. В. ПИ20-1

При запуске клиент и сервер генерируют каждый свою пару ключей. При подключении клиент посылает серверу свой открытый ключ. В ответ сервер посылает клиенту открытый ключ сервера. Клиент посылает сообщение серверу, шифруя его своим закрытым ключом и открытым ключом сервера. Сервер принимает сообщение, расшифровывает его сначала своим закрытым ключом, а потом - открытым ключом клиента. Обратное сообщение посылается аналогично. Для шифровки - расшифровки используем функции симметричного шифрования из предыдущей работы по симметричному шифрованию по Unix. Изображение выглядит как текст

Автоматически созданное описание

Далее в функции get\_keys() читаем уже существующие ключи, если их нет - создаются новые.

1. Модифицируйте код клиента и сервера так, чтобы приватный и публичный ключ хранились в текстовых файлах на диске и, таким образом, переиспользовались между запусками.

Реализовано в коде, можно убедиться что между запусками ключи в файлах не меняются.

Csv файл с ключами клиента:

Изображение выглядит как стол

Автоматически созданное описание

Csv файл с ключами сервера:

Изображение выглядит как стол

Автоматически созданное описание

Сервер хранит ключи для каждого из клиентов (по IP).

1. Проведите рефакторинг кода клиента и сервера так, чтобы все, относящееся к генерации ключей, установлению режима шифрования, шифрованию исходящих и дешифрованию входящих сообщений было отделено от основного алгоритма обмена сообщениями.

Можно увидеть в коде:

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст, монитор, снимок экрана

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

1. Реализуйте на сервере проверку входящих сертификатов. На сервере должен храниться список разрешенных ключей. Когда клиент посылает на сервер свой публичный ключ, сервер ищет его среди разрешенных и, если такого не находит, разрывает соединение. Проверьте правильность работы не нескольких разных клиентах. Важно! данный пункт предполагает, что ключи уже существуют, поэтому в репозитории приложены файлы с уже созданными ключами.

Разрешенные открытые ключи клиентов хранятся в файле allowed.csv

Изображение выглядит как стол

Автоматически созданное описание

1. Модифицируйте код клиента и сервера таким образом, чтобы установление режима шифрования происходило при подключении на один порт, а основное общение - на другом порту. Номер порта можно передавать как первое зашифрованное сообщение. Также можно увидеть в коде, и сервер и клиент выводят сообщение о подключении к конкретному порту. Изначально сервер подключился на порте 10101

После подключения клиента они переключились на новый (случайный) порт и продолжают общение на нем

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

1. Модифицируйте код FTP-сервера таким образом, чтобы он поддерживал шифрование.