МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Определение наличия внесенных изменений в изображение

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Карпова Глеба Игоревича

Научный руководитель
к.п.н., доцент _____ А. С. Гераськин
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

Благодаря быстрому темпу развития технологий 20-го века, люди задумались о новых способах передачи информации, что значительно бы ускорило обмен знаниями, тем самым давало бы толчок к новым открытиям. Такой способ был найден – передача информации в цифровом виде.

В 60-х годах прошлого столетия, благодаря трудам Ликлайдера была разработана детальная концепция компьютерной сети. В ней предлагалось использовать связанную между собой систему компьютеров, которая даже при отказе работы одного из них была работоспособна и поддерживала связь с остальными компьютерами. Благодаря данной концепции решалось две немаловажные задачи – обеспечение работоспособности системы и невозможность уничтожить данные, так как они хранились в сети, на удаленных друг от друга компьютерах, а не на жестком диске определенного компьютера.[1]

В 1984 году Национальный фонд науки США (National Science Foundation Network) основывает широкую межуниверситетскую сеть, которая включает в себя более мелкие сети. Данная сеть строится по принципу ARPANETсети, но имеет пропускную способность 56 Кбит/с. Целью данного объединения сетей была передача информации между исследовательскими центрами страны. Она росла очень быстро и уже к 92-му году было подключено более семи тысяч мелких сетей и более двух тысяч находились за пределами США. Вскоре правительство Америки принимает важное решение о передаче большей части каналов в общедоступное пользование.[2]

В наши дни сеть Интернет объединяет более сотни миллионов людей по всему миру. Большую часть информации мы получают благодаря различным информационным ресурсам, мессенджерам и многому другому. Каждый день

[1]Блау, М. Г. Удивительный интернет/ М. Г. Блау, А. М. Меламед // ЭНАС-КНИГА. – 2016. – С.25–28. – Яз. рус.

[2] Karen, D. F NSFNET: A Partnership for High-Speed Networking Final Report 1987-1995 / D. F. Karen, G. Caviness, E. Hoffman // D. F. Karen. – 1995. – С. 40–44. – Яз. англ.

сотни миллионов людей используют различные сайты для передачи и поиска информации. Интернет стал не только местом, где люди могут получить или обменять информацию, но и важным инструментом воздействия на жизнь людей в каждой стране.

Сегодня все наши данные о кредитных картах, фотографиях с отдыха, списков покупок на завтра и многое другое люди привыкли сгружать в сеть, чтобы оставить место в своих гаджетах свободным,либо сами того не зная оставляют след данных в Интернете. Также человеческое общение переместилось в сеть Интернет, что не могло сказаться на личной безопасности каждого. Для сохранения и защиты данных в любых сервисах используются различные методы и инструменты, которые с большой долей вероятности помогают нам доверить им информацию о себе и защититься от будущих хакерских атак.

На сегодняшний день мессенджеры активно развиваются и применяются в различных сферах деятельности, также в государственных структурах, где необходима определенная секретность. Использование SSLсертификатов – отличное решение для поддержки внутреннего документооборота государственной структуры с учетом его относительно невысокой цены.

Всем известно, что сертификаты обеспечивают безопасное соединение клиента с сервером, в данной дипломной работе я хочу разобраться в том, как именно это происходит, а также разработать программное обеспечение шифрования на сокетах в сетях с помощью SSL сертификата, использующего отечественный метод симметрического шифрования.[3]

Целью данной дипломной работы является разработка приложения с защитой персональных данных с помощью SSLсертификата, осуществляющего отправку мгновенных сообщений.

[3]Что такое SSL-сертификат – определение и описание [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate (дата обращения: 13.04.2021). – Загл. с экрана. – Яз. рус

Таким образом в рамках дипломной работы решаются следующие задачи:

1. познакомиться со структурой SSL сертификатов;
2. рассмотреть принцип работы данных сертификатов;
3. рассмотреть и проанализировать существующие методы передачи секретного ключа и на основе анализа определить наиболее подходящий метод в данной задаче;
4. описать алгоритмы шифрования, применяемые при разработке SSL сертификатов;
5. разработать «мессенджер» по отправке мгновенных сообщений с защитой персональных данных с помощью SSL сертификата.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Технологии SSLсертификата» рассматривается технология SSL сертификата, а именно его значение и принцип работы.В программной части будет использована данная технология, а также выбранные в ходе исследования преддипломной практики метод передачи секретного ключа и алгоритмы шифрования, которые будут подробно описаны в следующих главах.

В разделе 2 «Методы передачи секретного ключа» рассматривается сравнение пороговых схем разделения секрета.

В ходе сравнения пороговых схем разделения секретабыла выбрана наиболееэффективная пороговая схема разделения секрета Асмута-Блума. Эта схемабыла выбрана для разработки программного продукта.

Рассмотрим преимущества схемы Асмута-Блума:

- схема Асмута-Блума является совершенной, так как злоумышленник, имея $k - 1$ данных, не получит никакой информации;

- так как часть данных выбирается как остаток от целочисленного деления на ряд взаимно простых чисел, которое больше исходной информации, то эта схема является идеальной;

- схема разделения секрета называется совершенной, если запрещенное подмножество участников не получает никакой дополнительной информации о секрете, кроме априорной. Другими словами, распределение секрета остается равномерным и при наличии частичных секретов участников из запрещенного подмножества. Схема Асмута-Блума в отличие от других схем может быть совершенной;

- схема Асмута-Блума имеет над остальными схемами преимущество в вычислительной сложности примерно в 2,28-2,99 раза.

В разделе 3 «Алгоритмышифрования» рассмотрены основные симметричные алгоритмы шифрования. Выбраны конкретно симметричные

шифры по той причине, что асимметричные шифры имеют низкую скорость работы и требуют сложных вычисления.

В разделе 4 «Обзор популярных мессенджеров и методов из шифрования» рассматриваются методы шифрования популярных мессенджеров.Конкурируя междусобой, мессенджеры вынуждены «наращивать» свой функционал, предлагать пользователям новые услуги и возможности. Ниже представлена таблица с плюсами и минусами популярных мессенджеров.

Таблица 6 - Плюсы и минусы популярных мессенджеров

Мессенджер	Плюсы	Минусы
Telegram	• Сквозное шифрование. • Алгоритмы шифрования: MTProto, собственный протокол. • Приложения с открытым исходным кодом и Telegram Database Library. • Самоуничтожающиеся сообщения. • Можно входить в учётную запись с разных устройств одновременно. • Поддержка двухфакторной авторизации. • Отвечает требованиям GDPR.	• При регистрации нужно указывать номер телефона. • Сквозное шифрование применяется только при голосовых звонках и в секретных чатах. • Серверы без открытого исходного кода. • Отсутствие публикации официальных сторонних аудитов. • Записываются IP-адреса и другие метаданные.
WhatsApp	• Клиентские приложения для iOS, Android, Windows, macOS и web-версия для общения в браузере. • Синхронизация списка контактов с телефонной	• Отсутствует надежный алгоритм шифрования. • Номера телефонов людей видны другим пользователям, даже если их нет в списке контактов.

	книгой вашего устройства. • Бесплатные аудио- и видеозвонки через сеть (3G или Wi-Fi), то есть вы оплачиваете только услуги вашего интернет-провайдера. • Обмен фото, видео, PDF-файлами, слайд-шоу и другими документами, но размер файла не должен превышать 100 Мб. • Медиафайлы сначала отправляются на специальный HTTP-сервер, а конечному получателю передаются в сжатом виде, что позволяет снизить потребление трафика.	• Приложение копирует все телефонные номера из вашей книги контактов на свой сервер. • Чтобы начать переписку, необходимо сохранить контакт в телефонной книге.
Viber	• Сквозное шифрование для всех бесед; • Удаление сообщений; • Секретные чаты, защищенные паролем; • Исчезающие сообщение; • Отсутствие предварительного просмотра секретных сообщений на экране “Домой” и в списке переписок; • Доступность на всех платформах.	• Реклама, которую невозможно отключить; • Отслеживание интересов пользователя; • Большие различия функционала безопасных сообщений между клиентскими приложениями для разных платформ; • Трудности при создании публичного аккаунта; • Приложение устанавливается на компьютер только при условии, что оно уже есть на вашем смартфоне.
Signal	• Сквозное шифрование.	• Для регистрации нужно

	• Алгоритмы шифрования: протокол передачи сигналов с Perfect Forward Secrecy (PFS) для текстовых сообщений, голосовых сообщений и видеозвонков. • Открытый исходный код. • Самоуничтожающиеся сообщения. • Публикация отчётов прозрачности и проверок безопасности. • Запись минимального объёма информации. • Отсутствие записи IP-адреса. • Может заменить СМС-приложение на вашем устройстве. • Акцент на частных пользователей. • Бесплатный.	указать номер телефона. • Не поддерживает двухфакторную аутентификацию.

В разделе 5 «Программная часть» было разработано клиент-серверное приложение, в программном обеспечении Windows 10 x64 с помощью языка программирования Python 3.7 – версии.

Используемые библиотеки:

- socket – установление связи через сокеты;
- threading – для возможности использовать выполнение в потоке, используется для прослушивания сервера и клиента;
- tkinter – для графического интерфейса;
- random – генерация случайных чисел;
- math –для использования различных математических функций.

В разработанном программном продукте данный подход был реализован следующим образом. Существует сервер, который генерирует секрет (большое число 256 бит) с помощью отдельной написанной функции которая в последствии будет использоваться для шифра RSA и делит его на n частей (N – частей зависит от количества клиентов в чате), и отправляет части этого секрета, разделенного по схеме Асмута-Блума клиентам.

Для работы приложения нужно запустить сервер, реализованный в консольном режиме, как показано на рисунке 1.

Рисунок 1 – Запуск сервера

Далее клиент №1 отправляет запрос на сервер для соединения, как показано на рисунке2.

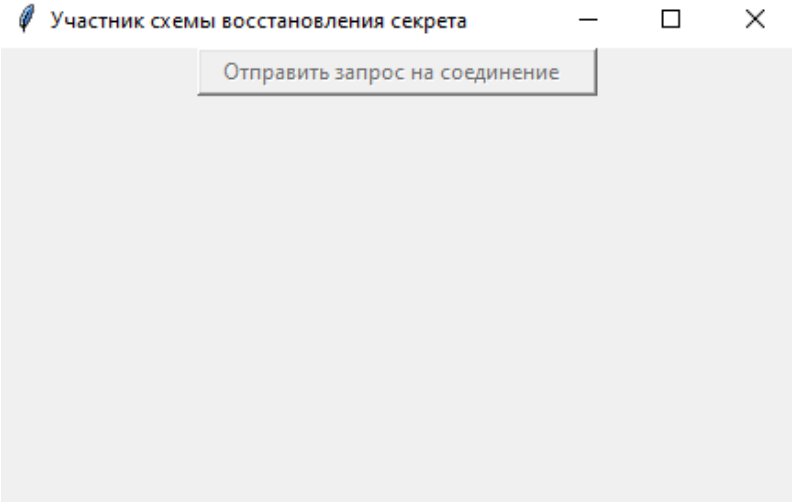

Рисунок 2 – Оконный интерфейс клиента

После этого клиент вводит количество участников будущего чата, как показано на рисунке 3, данное число участников является числом $K = N$, это нужно для того, чтобы общение происходило только тогда, когда в сборе все участники, иначе общение невозможно.

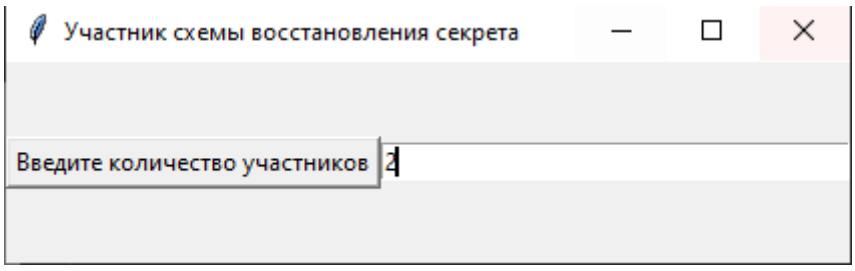

Рисунок 3 – Ввод количества участников

Успешно подключив всех остальных участников – в примере их количество равно двум – мы увидим сообщение об этом, как показано на рисунке 4.

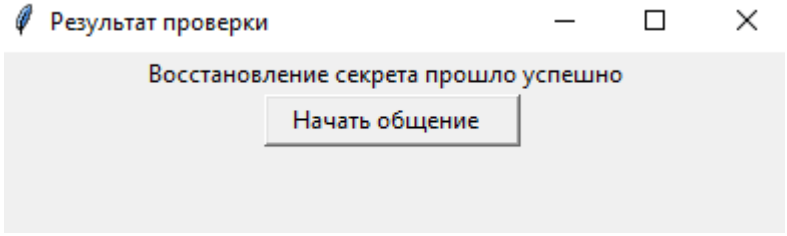

Рисунок 4 – Результат проверки

Теперь пользователи могут начать общение, нажав соответствующую кнопку. В новом окне они указывают свое имя и могут увидеть себя в сети, что демонстрирует рисунок 5.

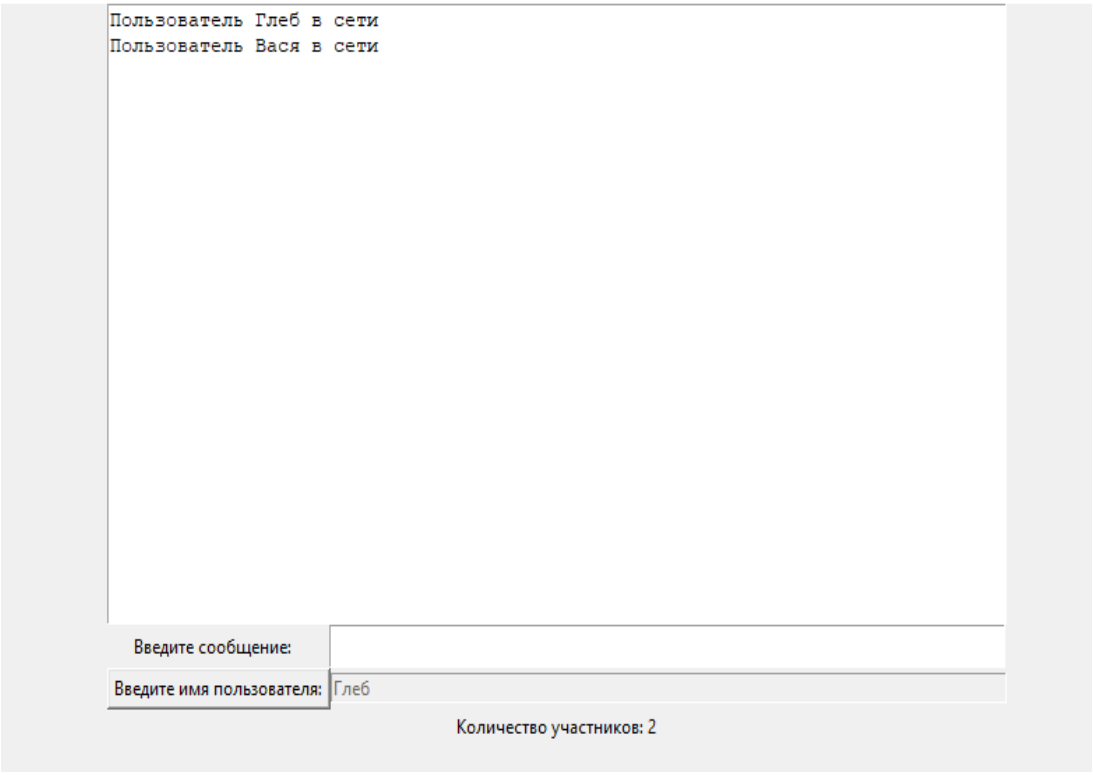

Рисунок 5 – Интерфейс мессенджера

Начнем общение между клиентами для разбора механизма выбора шифра, как показано на рисунке 6.

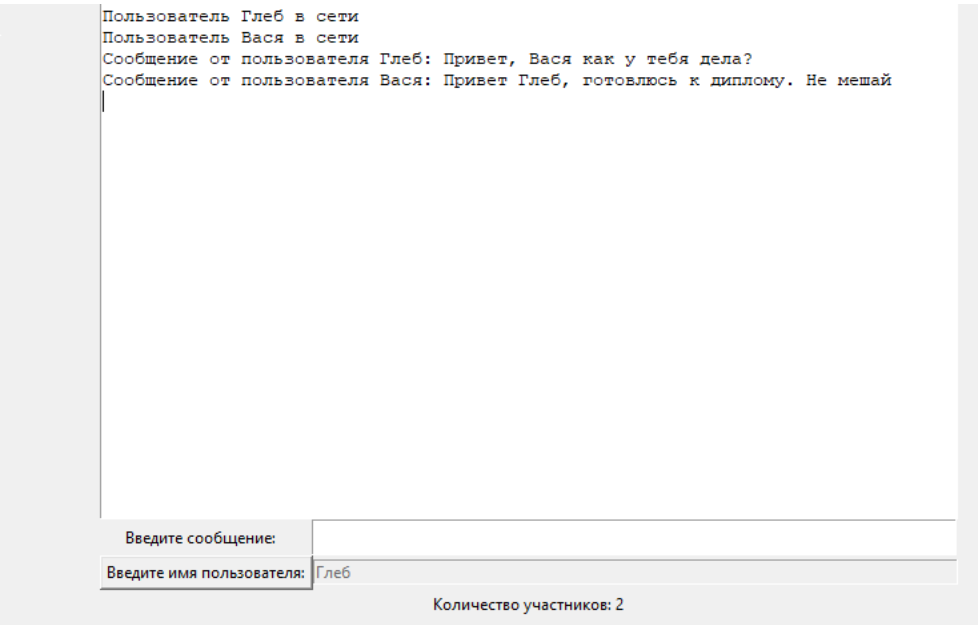

Рисунок 6 – Общение пользователей

ЗАКЛЮЧЕНИЕ

В результате работы проекта были рассмотрены основные этапы работы SSLсертификата на примере входа на сайт с сети, такие как проверка сертификата у сервера, а также проверка клиента.

Структура сертификата состоит из асимметричного и симметричного шифрования. В асимметричном шифре применяется шифр RSA. RSA ключи имеют длину 256 бит. В симметричном шифровании используются шифр МАГМА, имеющий длину 256 бит, которые разбиваются на 8 ключей по 32 бита.

В результате работы были решены следующие задачи:

- изучены структура SSL сертификатов и принципы их работы;
- рассмотрены и проанализированы существующие методы передачи секретного ключа и выделен наиболее подходящий метод в данной задаче – шифр МАГМА с режимом простой замены и самым распространённым алгоритмом при ассиметричном шифровании - RSA для общения с сервером;
- разработан программный продукт по отправке мгновенных сообщений с защитой персональных данных с помощью схемы Асмута-Блума.

В результате теоретических исследований был разработано клиент-серверное приложение, который осуществляет обмен мгновенными сообщениями между двумя пользователями на основе SSLсертификата.

Таким образом цели и задачи дипломной работы были достигнуты.