|  |  |
| --- | --- |
| Gerb-BMSTU_01 | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ Информатики и систем управления

КАФЕДРА ИУ8 «Информационная безопасность»

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

***К КУРСОВОМУ ПРОЕКТУ***

***НА ТЕМУ:***

***Разработка сетевого чата для мобильных устройств с шифрованием трафика***

Студент ИУ8-35 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. С. Блинов**

(Подпись, дата) (И.О.Фамилия)

Студент ИУ8-35 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. П. Пожуев**

(Подпись, дата) (И.О.Фамилия)

Руководитель курсового проекта **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И. В. Мацак**

(Подпись, дата) (И.О.Фамилия)

Консультант **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись, дата) (И.О.Фамилия)

*2018 г.*

Оглавление

[Цель 4](#_Toc532853827)

[Задачи 5](#_Toc532853828)

[Основные определения 6](#_Toc532853829)

[Введение 8](#_Toc532853830)

[Требования к проекту 8](#_Toc532853831)

[Архитектура 9](#_Toc532853832)

[Firebase 9](#_Toc532853833)

[Android приложение 9](#_Toc532853834)

[Выбор технологий 11](#_Toc532853835)

[Выбор языка программирования 11](#_Toc532853836)

[Выбор языка разметки 11](#_Toc532853837)

[Описание технический решений 12](#_Toc532853838)

[Заключение 13](#_Toc532853839)

[Список используемых источников 14](#_Toc532853840)

# Цель

Реализовать систему мгновенного обмена зашифрованными сообщениями между пользователями в сети через мобильное приложение для операционной системы Android. Выработку общего секретного ключа реализовать с помощью протокола Диффи-Хеллмана. Шифрование трафика реализовать с помощью одного из современных криптографически стойких симметричных алгоритмов шифрования. Разработанное ПО должно иметь удобный и интуитивно понятный интерфейс.

# Задачи

1. Изучить алгоритм Диффи-Хеллмана.
2. Изучить язык программирования Java.
3. Изучить работу с базой данных Firebase.
4. Изучить язык разметки XML.
5. Реализовать мобильное приложение на android.
6. Реализовать обмен сообщениями с помощью сервера.
7. Выбрать алгоритм симметричного шифрования для сообщений.
8. Реализовать алгоритм шифрования сообщений в приложении.
9. Реализовать обмен сессионными ключами между Администратором и Пользователем по алгоритму Диффи-Хеллмана в приложении.
10. Реализовать хранение сессионных ключей на устройстве.
11. Создать простой и понятный интерфейс приложения

# Основные определения

* AES - также известный как Rijndael — симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США.
* Android - операционная система для электронных устройств, основана на ядре Linux c собственной реализацией виртуальной машины Java от Google.
* Firebase - облачная СУБД класса NoSQL, позволяющая хранить и синхронизировать данные между несколькими клиентами. Поддержаны особенности интеграции с приложениями под операционные системы Android и iOS, реализовано API для приложений на JavaScript, Java, Objective-C и Node.js.
* XML - расширяемый язык разметки. Рекомендован Консорциумом Всемирной паутины (W3C).
* Алгоритм Диффи-Хеллмана - криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.
* БД - представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).
* Бэкэнд - программно-аппаратная часть сервиса.
* Интерфейс - общая граница между двумя функциональными объектами, требования к которой определяются стандартом; совокупность средств, методов и правил взаимодействия (управления, контроля и т.д.) между элементами системы.
* Сессионная пара - представляет собой две строки по 128 бит (16 символов), 1-я строка - ключ для AES шифрования, 2-я строка - параметры шифрования.

# Введение

Каждый из нас, пользуясь интернетом, хочет быть уверен в том, что его информация надежно защищена, и любой посторонний не сможет её получить. Поэтому мы решили реализовать проект, который попробует решить вопрос безопасного хранения сообщений на сервере в сети интернет.

Благодаря формированию общего секрета по алгоритму Диффи-Хеллмана и алгоритму симметричного шифрования AES, будет происходить шифрование сессионной пары и её передача от администратора чата новому пользователю. Таким образом, сессионная пара будет храниться на устройстве пользователя, а зашифрованные сообщения на сервере.

## Требования к проекту

* Простой и понятный интерфейс.
* Относительно быстрая генерация приватного и публичного ключа для алгоритма Диффи-Хеллмана на устройстве пользователя в отдельном потоке.
* Возможность авторизации с любого устройства.

# Архитектура

Проект состоит из двух модулей:

1. Firebase - сервер, БД, предоставляет бэкэнд.
2. Android приложение - предоставляет интерфейс пользователя.

## Firebase

## Android приложение

Позволяет пользователю получить учётную запись, секретные ключи (сессионную пару), доступ к базе данных с зашифрованными сообщениями и возможность самому отправлять зашифрованные сообщения.

Экран авторизации содержит два поля ввода данных (для ввода email и пароля), а также три кнопки ("Авторизация", "Регистрация", "Авторы"). Присутствует проверка корректности введённых данных.

При успешной регистрации, авторизации без сессионной пары на устройстве и авторизации на новом устройстве, происходит генерация приватного и публичного ключа на устройстве пользователя в отдельном потоке, в главном потоке отображается подсказка для пользователя. Дальше происходит отправка публичного ключа на сервер. Обмен информацией с сервером происходит посредством передачи строковых переменных. На данном этапе пользователь может покинуть приложение.

В момент, когда администратор заходит в приложение, автоматически начинается проверка базы данных на наличие публичных ключей и их обработка. Администратор генерирует собственный публичный и приватный ключ, на основе публичного ключа пользователя и приватного ключа администратора формируется общий секрет, с помощью которого генерируется ключ AES, которым зашифровывается сессионная пара (находится на устройстве администратора). Затем Администратор отправляет на сервер собственный публичный ключ, зашифрованную сессионную пару и параметры AES шифрования, а также удаляет с сервера публичный ключ пользователя.

Когда Пользователь снова входит в приложение, автоматически проверяется наличие сессионной пары на устройстве, если её нет, он проверяет БД на наличие строк, которые отправил Администратор. Забирает эти строки себе, формирует общий секрет, пользуясь публичным ключом администратора. Генерирует AES ключ на основе общего секрета и параметров шифрования, расшифровывает сессионную пару.

Далее происходит переход на экран чата, где отображаются уже расшифрованные сообщения, присутствует поле для ввода сообщений, кнопка для их отправки.

Список сообщений представляет собой набор объектов, в каждом из которых содержится:

1. почта автора сообщения
2. текст сообщения
3. дата отправки сообщения.

Получая из БД зашифрованные строки, приложение пользователя расшифровывает сообщения с помощью сессионной пары на устройстве. Также происходит шифрование сообщений на устройстве и их отправка в данном виде на сервер.

# Выбор технологий

## Выбор языка программирования

Выбранным языком программирования стал Java, так как:

1. Java известный язык программирования.
2. Java безопасен по сравнению со многими другими языками программирования. Все приложения выполняются виртуальной Java-машиной, при любой попытке несанкционированного доступа или соединения программа просто прерывает свою работу.
3. Он работает на виртуальной машине, поэтому нет необходимости перекомпилировать его для каждого телефона и легко защищать.
4. Большое количество инструментов для разработки Java.

## Выбор языка разметки

Выбранным языком разметки стал XML. Он является распространенным форматом для обмена информацией в Интернете, поэтому велика вероятность, что он понадобится для доступа к данным в Web. Кроме того, XML может потребоваться для передачи данных, например, Web-сервису. Другими словами, чтобы приложение для Android работало через Интернет, придется иметь дело с XML. Cама платформа Java уже долгое время поддерживает множество различных способов использования XML, причем большинство API для Java, ориентированных на XML, доступны в Android.

# Описание технический решений

Во время разработки проекта нам пришлось столкнуться с несколькими проблемами. (как хранить ключи Shared Preference)()

# Заключение

В результате было реализовано Android приложение позволяющее быстро и безопасно обмениваться зашифрованными сообщениями между пользователями в сети, используя выработку общего секрета по алгоритму Диффи-Хеллмана. Приложение обладает понятным интерфейсом, с подсказками.

В дальнейшем возможно расширение проекта. Добавление нового функционала:

1. возможность создания новых комнат для чата.
2. прикрепление новых типов данных к сообщениям.
3. редактирование профиля пользователя.

# Список используемых источников

1. API specification for the Java™ Platform, Standard Edition: [Электронный ресурс]. URL: https://docs.oracle.com/javase/7/docs/api/.
2. Документация Android Studio: [Электронный ресурс]. URL: https://developer.android.com/studio/intro/.