ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Жемойтяк Наталья Павловна

Содержание

Введение

В этом документе будет описываться техническое задание для выполнение задач данного проекта. Тут будет кратко описаны комноненты Signal Protocol и как их описывать. Также будет описан по каким критериям сравниваем Signal Protocol и MTProto(telegram).

Главные задачи

- Изучить и описать Signal Protocol
- Сравнить Signal Protocol и MTProto
- Описать алгоритм сквозного шифрования
- Реализоватъ приложение с криптосистемой протокола

Изучить и описать Signal protocol

Изучить и ознакомится

В интернете достаточно ресурсов, чтобы прочитать об этом протоколе. Также у самого Signal есть документация и репозиторий на гитхабе, которыми можно воспользоваться.

В документации и википедии указаны следующие составляющие элементы:

- Двойной храповик(double ratchet algorithm)
- Расширенный тройной Диффи-Хеллман(extended triple Diffie-Hellman)
- Ключи двух пользователей
- Эллиптические кривые
- AES
- Sha256

  Каждый из этих пунктов нужно изучить. Есть много статей в интернете

Описать алгоритмы

Каждый алгоритм необходимо описать таким образом:

- Что на вход
- Что на выход
- Шаги
- Краткое описание что делает и для чего

Дополнительно: вставить диаграммы где это уместно(3DH, двойной храповик)

Signal vs MtProto

Требуется сравнить два протокола по следующим пунктам:

- Генерация ключей
- Примитивные простые числа
- Алгоритм шифрования ключей
- Алгоритм обмена ключей
- Приватность ключей
- Функция хеширования
- Применение

Мессенджер

Написать мессенджер с приминением протокола:

- Написать базу: два пользователя
- Подключить к серверу
- Наложить двойной храповик