РАЗРАБОТКА ПРИЛОЖЕНИЯ-МЕССЕНДЖЕРА С ПРИМЕНЕНИЕМ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Зданевич О. В.

Белорусский государственный университет, Минск, Беларусь,
e-mail: oleg.zdanevich@icloud.com

В наши дни очень трудно быть уверенным в конфиденциальности частной жизни, мобильные разговоры могут прослушивать мошенники, работодатели, конкуренты и другие. Поэтому в настоящее время все большую набирают сервисы, построенные на технологиях шифрования.

Результатом представленной здесь работы является безопасное приложение-мессенджер с применением криптографических алгоритмов шифрования.

В качестве основных инструментов для реализации сервиса были выбраны технологии Spring Boot и React.js.

Криптографический протокол Диффи-Хеллмана использован для получения двумя сторонами общего секретного ключа длинной 2048 бит. Сообщения мессенджера шифруются с помощью алгоритма симметричного блочного шифрования AES-256. В качестве функции формирования ключа использован алгоритм хеширования SHA-256. Использованные криптографические алгоритмы позволяют защитить передаваемую информацию от нежелательного просмотра злоумышленниками.

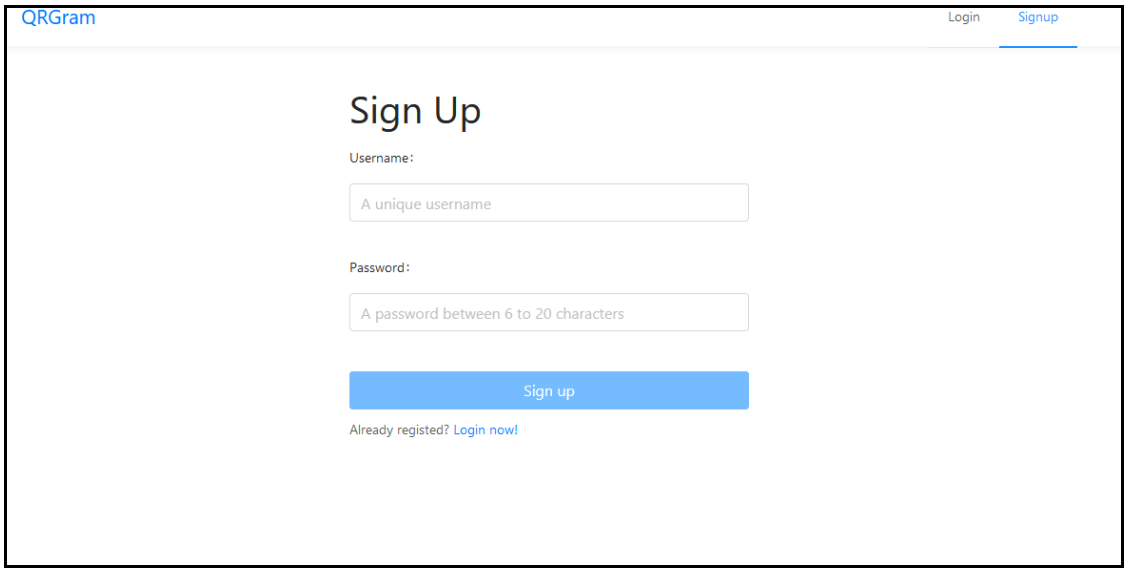

Рис. 1. Экран регистрации

Регистрация в приложении не требует ввода личных данных пользователя (номер мобильного телефона, адрес эл. почты). Для осуществления «входа» в приложение пользователю необходимо ввести свои логин и пароль (требуемой сложности). Такой подход к регистрации гарантирует полную анонимность пользователя.

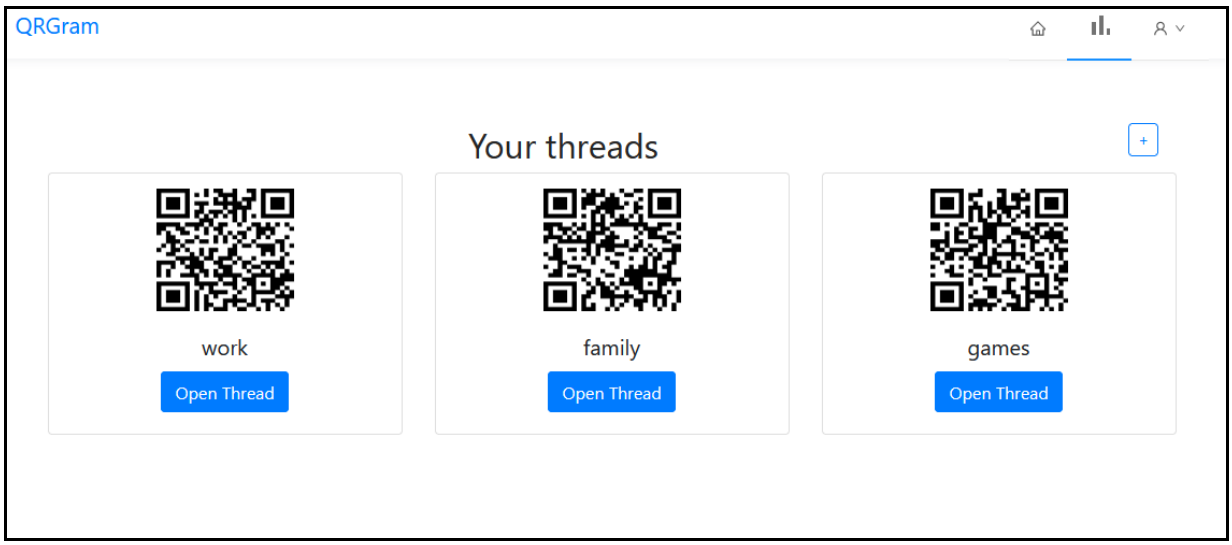

Рис. 2. Экран выбора потоков

Главной особенностью мессенджера является разделение чатов на различные потоки (threads). При создании пользователем нового потока генерируется QR-код (Код быстрого реагирования, Quick Response Code), по которому другие пользователи мессенджера могут начать чат с пользователем в созданном потоке. Потоки позволяют разделить чаты под разные задачи, например, один поток можно создать для общения с друзьями и семьёй, другой поток – для общения с коллегами, еще один поток – для продажи товаров на онлайн площадках объявлений. Если поток больше неактуален для пользователя (например, товар больше не продается), его можно удалить. Преимуществом такого подхода (разделение чатов на потоки) состоит в том, что пользователь может в открытом доступе разместить QR-код потока и получать сообщения от незнакомых пользователей с возможностью прекратить поток входящих сообщений, сохраняя анонимность.

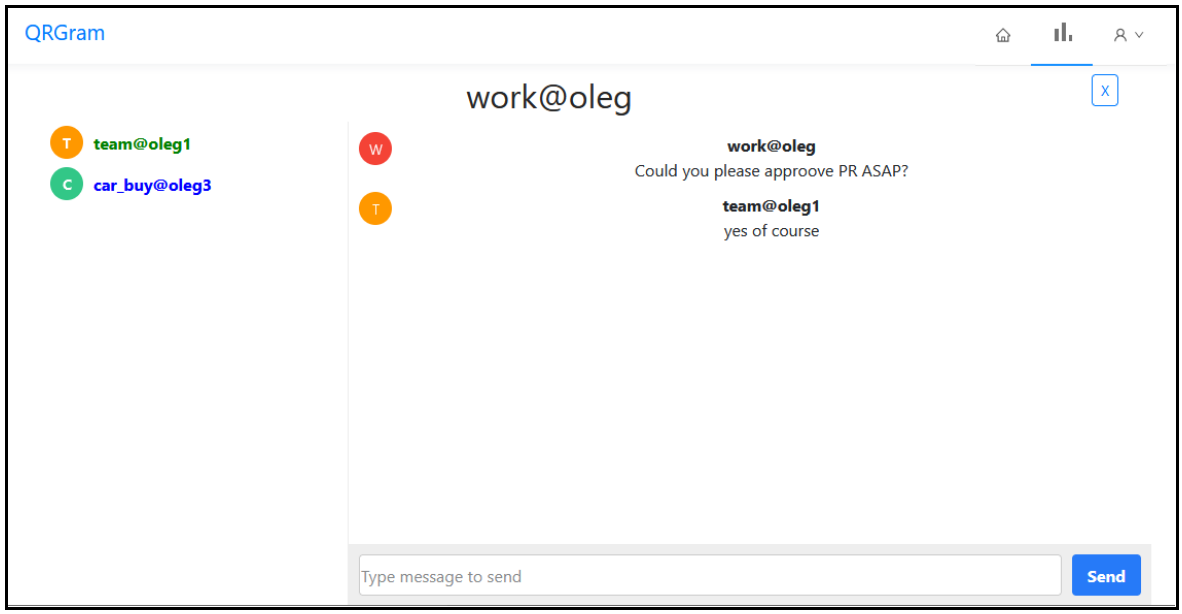

Рис. 3. Экран чата

Приложение позволяет обмениваться только текстовыми сообщениями с неограниченным числом пользователей в любом браузере. Пользователь получает уведомления обо всех новых сообщениях и ошибках регистрации/входа.

Важно отметить, секретные ключи чатов хранятся на пользовательских устройствах, что защищает данные пользователя в случае хищения логина и пароля. Также реализована возможность восстановления секретных ключей на другом устройстве пользователя путём подтверждения синхронизации ключей на авторизованном устройстве.

Современная криптография является основным средством защиты информации, которая, в свою очередь, является одной из самых ценных вещей в современной жизни. Защищая должным образом свою личную информацию, вы защищаете не только себя, но и своих близких от таких рисков как: воровство, утрата, искажение, несанкционированное распространение важной для вас информации.

Литература

1. Мао, В. Современная криптография: теория и практика, пер. с английского. М.: Издательский дом «Вильямс», 2005. – 768 с.

2. Баричев, С. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - 3-е изд., стер. – Москва : Горячая линия-Телеком, 2016. – 175 с.

3. Фергюсон, Н. Практическая криптография = Practical Cryptography / Нильс Фергюсон, Брюс Шнайер: [пер. с англ. Н. Н. Селиной ; под ред. А. В. Журавлева]. – Москва: Диалектика, 2005. – 422 с.

4. Тиленс Томас Марк, React в действии. – СПб.: «Питер», 2019. – 368 с.

5. Spring 5 для профессионалов = Pro Spring / Ю. Козмина, Р. Харроп, К. Шефер, К. Хо. – СПб.: Диалектика, 2019. – 1120 с.