Введение

В современном мире проблема защиты информации поставлена вызывает большой интерес не только со стороны военных или государственных деятелей, но и обычных людей. С развитием интернет все больше пользователей стали общаться друг с другом в сети. Но в период, когда некоторые лица отслеживают интернет-контент и личные данные пользователей, возрастает интерес к приложениям, которые обеспечивают безопасность передачи сообщений. Это и есть так называемые крипто мессенджеры. Цель этих крипто мессенджеров зашифровывать сообщения так, что прочитать их могли только те, кому они предназначаются.

Сейчас в интернете практически всю передаваемую информацию кодирую тем или иным способом. Но, несмотря на огромные усилия по созданию различных технологий защиты данных, их уязвимость постоянно возрастает, так как находятся все более новые способы взламывать шифры. Поэтому актуальность проблем, связанных с защитой передачи данных растет. Одним из путей решения проблемы защиты информации, а точнее - решения небольшой части вопросов, является криптографическое преобразование информации, или шифрование. В этом случае, отправитель зашифровывает сообщение по какому-то алгоритму и ключу, а получатель его расшифровывает, причем для потенциальных захватчиков сообщение не будет иметь никакого смысла. Есть еще способ защищенной передачи сообщения, а именно сокрытие существования этого сообщения, которая называется стеганографией. Но если сообщение будет перехвачено, его содержимое сразу же станет известно. По этой причине методы стеганографии и шифрования используются совместно [1].

Таким образом, необходимо создать такой крипто мессенджер, чтобы он мог отправлять зашифрованные определенным алгоритмом данные, а также сделать возможным добавление собственных алгоритмов.

Заключение

В данной пояснительной записке описана выпускная квалификационная работа по созданию программного продукта для безопасного обмена сообщениями в сети Интернет.

Актуальность поставленной задачи обусловлена возросшим интересом общественности к безопасному общению в сети, безопасности хранения своих личных данных.

Был проведен сравнительный анализ имеющихся аналогов, а именно: Telegram, WhatsApp, Tox, Ricochet. Одним из главных недостатков является отсутствие у данных мессенджеров модульной архитектуры.

Для реализации данного программного продукта был выбран .Net, так как обладает большим набором компонент, необходимых для разработки, таких как: WPF,Entity Framework и другие.

В ходе выполнения выпускной квалификационной работы были выполнены следующие задачи:

- изучена предметная область, а именно изучены и реализованы алгоритмы симметричного шифрования AES и алгоритмы асимметричного шифрования RSA, а также алгоритм PGP, с помощью которых производилось шифрование сообщений;
- изучена и реализована клиент-серверная архитектура программного продукта, то есть реализован сервер, клиент и настроено взаимодействие между ними.

Таким образом, работа выполнена в полном объеме, все поставленные задачи выполнены.