Введение

В современном мире проблема защиты информации поставлена особенно остро. Сейчас практически невозможно найти передаваемую информацию, не закодированную тем или иным способом. Но, несмотря на возрастающие усилия по созданию различных технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой передачи данных и обеспечением информационной безопасности их обработки, все более усиливается. 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.

Как передать сообщения одним людям так, чтоб об этом не знали другие? Этот вопрос волнует людей с давних времен. Так, еще до нашей эры люди использовали нестандартные и необычные символы, а также активно использовали стеганографию, чтобы зашифровать важную информацию. Например, использовали деревянные дощечки и сообщение писали на дереве, потом заливали воском. Следовательно, дощечка выглядела пустой и не вызывала никаких опасений. С развитием письма усовершенствовались методы шифрования. Большинство из используемых шифров сводились к перестановке или подстановке в одном и том же алфавите. Одним из первых примеров является шифр Цезаря, в котором каждая буква заменяется другой, находящейся в алфавите на некоторое число позиций правее. С развитием вычислительной техники, такие алгоритмы стали не эффективны, так как все

возможные комбинации можно просчитать на машине за приемлемое время. Тогда пришло время различных математических алгоритмов, некоторые из них эффективны и в наше время. Криптографические алгоритмы применяются в различных областях, связанных с передачей, хранением и обработкой важной и конфиденциальной информации[1].

С развитием глобальной сети все больше пользователей стали общаться друг с другом на просторах интернета. Но в период, когда заинтересованные лица отслеживают интернет-контент и личные данные пользователей, возрастает интерес к приложениям, которые обеспечивают безопасность передачи сообщений. Это и есть так называемые крипто мессенджеры. Целью данной выпускной работы является написание крипто мессенджера, но с возможностью добавления своих алгоритмов шифрования.

Заключение

В результате выполнения вышеуказанных задач, была успешно достигнута основная цель работы, а именно, реализован программный комплекс, который соответствует предъявляемым к разработке требованиям. Был разработан и успешно реализован крипто-мессенджер, который предназначен для безопасного общения в сети Интернет как отдельным пользователем, так и какой-либо компании в корпоративной сети. Крипто-мессенджер реализован отдельными модулями, что позволяет без особых усилий добавлять в программу новые алгоритмы шифрования или стеганографические алгоритмы, или свои собственные алгоритмы.

Во время выполнения выпускной квалификационной работы были выполнены следующие задачи:

- изучены и реализованы два алгоритма стеганографии – это метод наименьшего значащего бита и метод встраивания цифрового водяного знака, с помощью которых производилось сокрытие факта отправки сообщения;
- произведен анализ аналогов, который показал, что одни мессенджеры не шифруют передаваемые данные, а другие создают иллюзию безопасности;
- изучена архитектура клиент-сервер, которая была реализована в данном программном продукте;
- разработан и реализован интуитивно понятный интерфейс пользователя.

Таким образом, поставленная цель выпускной квалификационной работы сделана в полном объеме.