Тема: **Создание приложения для расширенного обмена информацией в общих сетях с мобильных устройств с алгоритмом двойного шифрования передаваемой информации**

Выполнил: Алпатов Артём Вадимович
ученик 10 «А» класса
Самарского лицея информационных технологий (МАОУ СамЛИТ)

Научный руководитель: Кудряшова Екатерина Максимовна
учитель информатики
Самарского лицея информационных технологий (МАОУ СамЛИТ)

Наша работа посвящена созданию приложения для расширенного обмена информацией между мобильными устройствами пользователей с повышенной надёжностью, безопасностью и сохранностью конфиденциальной информации.

Цель работы: Создание приложения для расширенного обмена информацией между мобильными устройствами, работающими на операционной системе Android, с повышенной надёжностью, безопасностью и сохранностью конфиденциальной информации.

Задачи:

1. Обзор методов передачи данных.
2. Обзор протоколов, средств шифрования, выбор. Анализ архитектур серверной части.
3. Проектирование API. Разработка серверной части. Разработка клиентской части.

Новизна работы заключается в следующем:

1. Создание авторской hash-функции.
2. Создание алгоритма двойного шифрования, заключающегося в отдельные шифровки передаваемой части информации, заключённой в малый блок и положения блока в общей структуре передаваемой информации.
3. Написание авторского программного кода, реализующего двойное шифрование на мобильном устройстве и на сервере отдельно.
4. Создание нового приложения для расширенного обмена информацией в общих сетях с мобильных устройств

Значимость исследования заключается в повышении надёжности передачи информации за счет двойного шифрования.

В отличие от известных криптографических протоколов (SSL и TLS) мы используем двойное шифрование. При шифровании по SSL и TLS шифруется только передаваемая информация. Поэтому, имея скрытый ключ, можно расшифровать всю зашифрованную этими способами информацию. В нашем случае, отдельному шифрованию подвергается и сама передаваемая информация, разбитая на малые блоки, и порядковый номер, указывающий на положение блока к общей информации. Это позволяет увеличить надежность шифрования, потому что получить ключ и расшифровать информацию, содержащуюся в блоках будет недостаточно для понимания общего смысла расшифрованной информации. Необходимо дополнительно угадать правильное положение блоков в исходной информации.

На данный момент в приложении создана возможность передачи текстовых и голосовых сообщений, а также любых видов файлов, представлена возможность осуществления звонков и видео-звонков. Все передаваемые данные шифруются с помощью описанного ранее алгоритма.

Заключение и выводы.

Сознано новое защищенное от потери информации приложение для обмена любыми видами данных через мобильные устройства, в том числе звонки и видео-звонки.

Разработанный нами алгоритм передачи подверженной двойному шифрованию информации позволяет значительно повысить защищённость информации.

При передаче информации по предлагаемой авторами схеме, информация шифруется каждый раз в момент ее отправки. Шифрование происходит при передаче от Мобильного устройства №1 (источник) к корпоративному Серверу. Шифрование выполняется при передаче с Сервера на Мобильное устройство №2 (приемник). Само шифрование каждый раз выполняется по двойному алгоритму. Все отмеченное выше позволяет повысить защищённость передаваемой информации.

Новизна работы заключается в следующем:

1. Создание авторской hash-функции.
2. Создание алгоритма двойного шифрования, заключающегося в отдельные шифровки передаваемой части информации, заключённой в малый блок и положения блока в общей структуре передаваемой информации.
3. Написание авторского программного кода, реализующего двойное шифрование на мобильном устройстве и на сервере отдельно.
4. Создание нового приложения для расширенного обмена информацией в общих сетях с мобильных устройств

Значимость исследования заключается в повышении надёжности передачи информации за счет двойного шифрования.