**Отчет по крипточасти мессенджера**

Составитель:

Макаренкова Марьяна

Участники команды:

Жаболенко Антон

Павлова Елена

Бажев Кантемир

Морозов Никита

**Алгоритм работы, соединение клиент-сервер.**

1. Клиент пересылает свой id + режим шифрования (англ/рус сюита) + запрос на аутентификацию сервера

*Режим шифрования – параметр, принимающий одно из 2 значений 0 или 1. В зависимости от этого параметра в дальнейшем буду использоваться или иностранные версии функций шифрования, хэш – функции и тп или функции, реализованные по российским ГОСТам.*

1. Контроль целостности осуществляется после выработки общего ключа между клиентом и сервером (после построения защищенного канала). Используемые алгоритмы для проверки описаны далее.
2. Аутентификация: Сервер перед клиентом через запрос-ответ.

Используем первый вариант

*Первый вариант: используем ассиметричное шифрование. Клиент использует открытый ключ сервера и зашифровывает какую-либо произвольную, всегда разную информацию (к примеру дата, время + случайное число) и отправляет сервер. Сервер используя ключ расшифровки, получает информацию и передает ее клиенту. Если она совпадает с тем, что было изначально, то аутентификация пройдена.*

*~~Второй вариант: аутентификации сервера ssl pining.~~*

*~~Третий вариант: используем ВКО - он же внешний ключевой обмен.~~*

*Используемый ассиметричный шифр: RSA*

1. Если сервер подтверждает, то отправляет клиенту id беседы.
2. После аутентификации сервера создается защитный канал, т.е. с помощью Диффи Хелмана создается общий ключ и далее происходит блочное шифрование этим общим ключом. Используемые алгоритмы далее.
3. С помощью алгоритма key diversification из общего ключа получаем два ключа. Первый используется для проверки целостности, второй для шифрования сообщений пользователя.
4. Для смены ключей для хэш-функции и шифрования используем CryptoPro Key Meshing (в rfc4357). Меняем раз в 1 Кб.
5. Аутентификация: Клиент перед сервером по паролю.

*Клиент отправляет серверу логин и хэшированный пароль. На сервере ранится таблица логин и хэш пароля. Сравнение хэшей.*

*Используемая хэш-функция : SHA-3 (Keccak) или BLAKE-256*

*Российский стандарт: ГОСТ Р 34.11-2012.*

1. Сообщение, которым заканчивается подтверждение связи («Finished»), содержит в себе хэш всех сообщений, которыми обменялись стороны в процессе подтверждения связи.
2. Для шифрования сообщений используем симметричный блочный шифр (если проблемы со скоростью используем поточный шифр). Генерация ключа по алгоритму Диффи-Хелмана.

*Используем режим шифрования:*

*Cipher block chaining (CBC);*

*Используемый блочный шифр:*

* *IDEA - возможно*
* *RC2 – вариант, если есть реализация; быстрее DES*
* *Rijndael(AES) – возможно*

*Реализация алгоритма Диффи-Хелмана :*

*Найти реализацию в openssl*

*Алгоритм случайного простого числа: Криптографически стойкий генератор псевдослучайных чисел(CSPRNG)*

*Найти реализацию в openssl*

1. Проверка целостности сообщений:

*Используем алгоритм HMAC с нашей используемой хэш-фнкцией. Если не будет найдена реализация то используем HMAC-RIPEMD-160 (или MAA )*

*Российский стандарт: ГОСТ Р 34.11­2012*

1. Групповой чат

*Аутентификация пользователей в групповом чате : протокол Шамира (доказательство с нулевым разглашением (информации))*

*Для выработки общего ключа: Схема разделения секрета Шамира*

Если не будет проблем с реализаций, в качестве иностранной сюиты будут использованы подчеркнутые алгоритмы.