КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В ПРИЛОЖЕНИИ TELEGRAM

С.В. Недбайлик, П.Б. Гусаков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Основное отличие криптосистемы Telegram от стандартных криптосистем заключается в применении ряда уникальных методов шифрования данных.

1. Сквозное шифрование – шифрование, которое подразумевает генерацию ключей на устройствах клиентов в системе «клиент-клиент», ключи генерируются на устройствах клиентов.

2. Шифр RSA – алгоритм шифрования данных в ассиметричных криптосистемах. Суть заключается в генерировании случайных открытых ключей и последующая генерация закрытых ключей, на основе открытых (вычисления закрытого ключа производится при помощи функции mod).

3. Алгоритм SHA-256 – алгоритм обращения (шифрования) данных в крипто текст при помощи хэш-функции. Использует слово длиной 32 бит, 256 – размер хэш-сообщения.

4. Алгоритм AES-256 – симметричный алгоритм блочного шифрования.

5. Алгоритм Диффи-Хеллмана – алгоритм шифрования, позволяющий получить секретный ключ, используя незащищенный от прослушивания канал связи.

Шифрование происходит по следующей схеме:

1.Создание закрытого ключа посредством алгоритма DH.

2.Разбиение пакета на случайно 64 бит число меняющееся каждые 30 минут, случайного 64 бит числа, используемого для однозначной идентификации сообщения в сеансе, текста сообщения, добавление (12–1024 бит) «пустых» битов информации с целью повышения криптостойкости.

3.Далее ключ и текст шифруются алгоритмом SHA-256, ключ переписывается и сохраняется в виде хэш-функции.

4.Ключ переформируется на основе SHA – 256 на основе секретного значения.

5.Формирование ключей и создание шифрование сообщение AES-256 алгоритмом.

6.Разбиение сообщения на (64 бит) хеша SHA-1 и используется для идентификации ключа. 128 бит хеша SHA-256. Зашифрованного сообщения.

Особенность заключается в применении как симметричного, так и ассиметричного шифрования информации. Так же важной составляющей является применение сквозного шифрования данных, при котором ключи, как открытые, так и закрытые генерируются и хранятся на устройствах клиентов, что делает невозможным их перехват (за исключением случаев, в которых устройство клиента является скомпрометированных, но в таком случае нарушитель столкнется с проблемой, так как ключ хранится в виде хэша).

Список литературы

1. Шо там по MTProto в Telegram-то? [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/590667/. – Дата доступа: 07.05.2024.

2. Практическая криптография / под. ред. Н. Фергюсона, Б. Шнайера. – М.: Издательский дом «Вильямс», 2004. – 420 с.