Signal Protocol

# Введение

В этом документе будет описываться Signal Protocol и его основные алгоритмы. Здесь будут много отсылок к документации самого сигнала, а также на теорию примитивов, которые использует данный протокол.

Данный протокол является документаций и пояснением к шифрованию сообщений в мессенджере Signal. Сейчас Facebook и Skype утверждают, что они тоже используют данный протокол в своих секретных(или приватных)чатах.

Так как этот протокол используется для сквозного шифрования, в этом документе так же будет описан алгоритм сквозного шифрования

# Главные компоненты:

* Двойной храповик(double ratchet algorithm)
* Расширенный тройной Диффи-Хеллман(extended triple Diffie-Hellman)
* Ключи двух пользователей
* Эллиптические кривые
* АЕS
* Sha256
* Ключи с подписью

# Базовые понятие и алгоритмы

## Криптосистема RSA

Самая простая и известная криптосистема по обмену сообщений это криптосистема RSA. Она приведена в пример чтобы проще было понять отдельные компоненты данного протокола и как они работают вместе.

RSA состоит из трех частей:

* Генерация ключей
* Шифрование
* Дешифрование

### Генерация ключей

Вход: Зависит от задачи. Может быть нулевой

Выход: Ключ = [public key(e,n), private key(d)]

Шаги:

1. Выбираются два простых числа p и q
2. n = p\*q
3. ϕ(n) = (p-1)(q-1)
4. Выбрать 1 <e < ϕ(n) && GCD(e, ϕ(n))==1
5. d = e-1(modϕ(n))
6. return [ e,n,d]

Определение: Публичная часть – эта та, которой пользователь может делится и/или она в открытом доступе. Она используется другим пользователем для шифровки сообщения

Определение: Приватная часть – эта та, которую пользователь не должен распространять, потому что он ее использует для расшифровки сообщения

### Шифрование

Вход: e,n,m

Выход: c – зашифрованное сообщение

Шаги:

1. Return[c = me(mod n)]

### Дешифрование

Вход: c,d,n

Выход: m – расшифрованное сообщение

Шаги:

1. Return[m = cd(mod n)]

### Зачем нужно понимать RSA

Данный протокол работает так же, как и RSA. Есть ключи, финкции, которые шифруют и расшифруют. Они гораздо сложнее и поэтому в качестве базы мы рассматриваем RSA.

## Эллиптические кривые и Диффи-Хеллмана

### Диффи-Хеллман

На этом алгоритме основывается весь обмен.

Обмен ключами:

1. Bob генерирует простое число p и число g, такое, что GCD(g,p-1) = =1. Она отправляет их Alice
2. Alice выбирает секретное число a.
3. Alice считает А = ga(mod p) и посылает Bob
4. Bob считает B = gb(mod p) и посылает Alice
5. Alice считает P = Ba(mod p) и Bob считает Q = Ab(mod p)
6. P==Q

Доказательство:

P = Ba(mod p) = (gb(mod p))a(mod p) = gba(mod p)

Q = Ab(mod p) = (ga(mod p) )b(mod p) = gab(mod p)

### Эллиптические кривые

Это тоже является одной из основ данного протокола.

Определение: Эллиптической кривой называется множество точек (x,y), удовлетворяющих уравнению:

y2 + a1xy + a3y = x3 + a2x2 + a4x + a6

Они используются как альтернатива огромным простым числам.

### Эллиптические кривые Диффи-Хеллмана

Выбирается заранее:

E – эллиптическая кривая

G – точка, принадлежащая кривой E, которая используется как начальная

1. Alice генерирует рандомное a – ее секретный ключ
2. Alice считает A = aG– публичный ключ
3. Bob выбирает b – его секретный ключ
4. Bob считает B = bG – публичный ключ
5. Alice и Bob обмениваются публичными ключами
6. Alice считает K = aB
7. Bob считает K = bA
8. K == K

Доказательство:

K = aB = abG

K = bA = baG

# Генерация ключей

В данном протоколе используют эллиптические кривые и подписи для генерации ключей, которые состоят из двух частей, как и в RSA, который описан выше.

# Список литературы

<https://www.elprocus.com/communication-protocols/>

<https://en.wikipedia.org/wiki/Signal_Protocol>

<https://signal.org/docs/>

<https://ru.wikipedia.org/wiki/Криптографический_протокол>

<https://qvault.io/cryptography/very-basic-intro-to-elliptic-curve-cryptography/>

<https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Operation>

<https://ru.wikipedia.org/wiki/Эллиптическая_криптография#Шифрование/расшифрование_с_использованием_эллиптических_кривых>

<https://en.wikipedia.org/wiki/Elliptic-curve_Diffie–Hellman>