Протоколы обмена ключами: Merkle’s puzzles и немного о постквантовой криптографии

Концепт

- **Merkle’s puzzles** (Головоломки Меркла) были **одной из первых** описанных систем, позволяющей осуществлять **безопасную коммуникацию** посредством **НЕ безопасного** канала связи.

- Под **безопасной коммуникацией** здесь понимается тот факт, что мы можем **выработать общий секретный ключ**, даже если до этого **никогда не взаимодействовали**.

- **Преимуществом** такой системы является тот факт, что **даже если** наш общий ключ куда-то утек - мы всё равно можем относительно просто **поменять его** и продолжить **защищенный обмен**.

Теперь сам алгоритм по шагам

- Начинается всё с того, что Алиса хочет обменяться с Бобом сообщениями так, чтобы **никто другой не смог** их **прочитать**. Но **канал**, по которому идут сообщения **открытый**. Значит для начала Алиса и Боб должны выработать **общий секретный ключ**.

- Далее **порядок действий следующий**:

    1. Алиса создаёт **N штук** случайных **секретных ключей**, затем берет каждый ключ, добавляет к нему **индекс** и получает сообщение.

       То есть по сути дела она на выходе имеет ОГРОМНОЕ число сообщений, в каждом из которых есть **рандомный ключ Y** и **рандомный индекс X**.

       Да, очевидно, что они **не должны** при этом **повторяться**.

    2. Что будет дальше - можно уже догадаться. Алиса **сохраняет открытые копии** каждого сообщения где-то **у себя**, далее каждое сообщение **шифруется симметричным алгоритмом** со **случайным ключом.**

       Длина ключа не очень большая, потому что Бобу **потом** его **надо будет перебирать (обычный брутфорс)**.

    3. После этого Алиса получает уже готовые **Пазлы.** (Да, теперь они имеют право так называться - поскольку **передавать симметричный ключ** мы Бобу **не будем** и он будет вынужден просто брутфорсом их решить).

    4. Алиса отправляет все Пазлы Бобу - он случайным образом выбирает из них, а затем после брутфорса **достает из сообщения X и Y**.

5. Дальше дело за малым: Боб берёт сообщение, которое он хотел отправить, **шифрует** его этим **секретным ключом Y**, полученным после решения Пазла и отправляет обратно Алисе **вместе с индексом X** (индекс в открытом виде).

6. Алисе остается лишь получить зашифрованное сообщение и **индекс X.** А поскольку она **сохраняла** все сообщения **в открытом виде** - она спокойно может **найти** то самое **с индексом X** и **взять** оттуда **секретный ключ Y**.

7. Всё! Это **победа**, теперь у Алисы и Боба есть **общий секретный ключ Y**.

В чем сложность для Евы?

- Как обычно, в незащищенных системах мы **предполагаем наличие** в канале передачи третьего участника - **Евы**, которая **перехватывает всю проходящую** через нее **инфу**.

- Итак, Ева имеет на руках **все N пазлов**, но **вот какой именно** выберет Боб на своей стороне (если она не предсказала там рандом) - **она не знает**.

  Значит ей остаётся **единственно** возможное: **ломать вообще все :)**

- Даже когда она обратно от Боба перехватит **в открытом виде индекс X** - это ей никак не поможет, ведь она должна ещё **умудриться найти и решить** пазл, в котором был **зашифрован** этот **индекс**.

- Да, разумеется она может как-то с **первого раза угадать** и **решить нужный** пазл - но это **становится** всё менее и менее вероятнее **с увеличением числа N**.

- К слову, если у нас длина ключей (которым Алиса шифровала пазлы) тоже равна N - мы получим **оценку брутфорса** около ***O(N^2)* -** надо ломануть **каждый пазл** и у **каждого ключ длины N**.

- Для Боба же сложность линейная: ***O(N)*** - он выбирает одно сообщение и спокойно брутфорсит. Так что Ева уступает ему в разы.

А что насчет применения на практике?

- **На практике** Головоломки Меркла если где **используются**, то лишь в **учебных целях**.

- Причина достаточно банальна: у нас есть хотя бы тот же Диффи — Хеллман, **работающий в разы эффективнее**. В ***Merkle Puzzle*** **даже Бобу надо брутфорсить** сообщение и если длина ключа **равна 2 байтам** - то в худшем случае ему **надо совершить 2^16 переборов**.

- Так что это скорее **неплохая теоретическая идея**, но на практике она проигрывает. Несмотря на это, работа Меркла всё равно считается одной из первых работ, связанных с **криптографией с открытым ключом**.

- Даже сам Хеллман несколько раз **приписывал открытие** этой идеи Мерклу и называл протокол Диффи-Хеллмана **протоколом Диффи-Хеллмана-Меркла**..

Список источников:

1) Merkle’s Puzzles. The first of many
2) Day 75: Merkle’s puzzles

3) Merkle's Puzzles (Wiki)
4) number571: Cryptography and Golang: