Распределение ключей

В криптографической практике при каждом сеансе связи принято пользоваться новым ключом шифрования. Этот ключ называют *сеансовым*. Такое ограничение на существование ключа является важным условием надёжности конфиденциальной связи, но в то же время создаёт дополнительную сложную задачу передачи сеансового ключа.

Если система имеет k пользователей, тогда для возможных секретных связей потребуется $C_k^2 = \frac{k(k-1)}{2}$ ключей. Но при этом мало вероятно, что все эти ключи или большинство из них будут востребованы. Чтобы уменьшить утечку информации о ключах и облегчить процесс генерации ключей создают протоколы распределения ключей только по запросу на очередной сеанс связи.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протоколы распределения ключей через ЦРК.

В этих протоколах пользователи сети Алиса и Боб получают свой сеансовый ключ от центра распределения ключей, ЦРК, роль которого исполняет посредник Трент. Для общения с Трентом пользователи должны получить от него ключи ещё до начала исполнения протокола. Простейший протокол такого типа имеет следующую графическую запись:

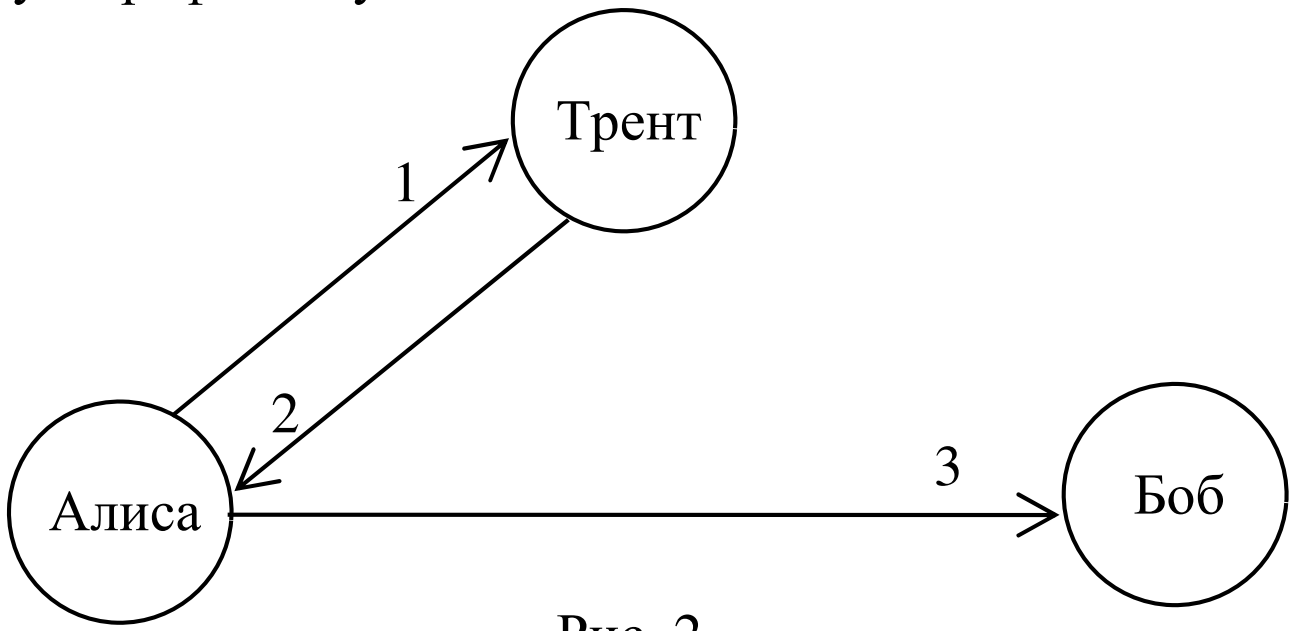

Рис. 2

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протоколы распределения ключей через ЦРК.

1. $A \rightarrow T$: $X = E_{AT}(B)$. (Алиса обращается к Тренту и запрашивает сеансовый ключ для связи с Бобом. По сути, Алиса отправляет Тренту имя Боба B зашифрованное ключом Алисы и Трента $E_{AT}(B)$.)
2. $T \rightarrow A$: $\{Y_1 = E_{AT}(K_{AB}), \ Y_2 = E_{BT}(K_{AB})\}$. (Трент генерирует случайный сеансовый ключ K_{AB} и зашифровывает две копии ключа. Одна копия предназначена Алисе, вторая - Бобу. Затем Трент отправляет обе копии Алисе.)
3. $A \rightarrow B$: Y_2. (Алиса отсылает Бобу его копию сеансового ключа.)
4. Далее, Алиса и Боб расшифровывают свои копии сеансового ключа, $D_{AT}(Y_1) = K_{AB}$, $D_{BT}(Y_2) = K_{AB}$, и используют его для своего сеанса связи.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протоколы распределения ключей через ЦРК.

По схожей схеме построены следующие протоколы обмена ключами:

- Протокол «Лягушка с широкой глоткой» (Wide-mouthed-frog)
- Протокол Яхалом (Yahalom)
- Протокол Нидхема-Шрёдера (Needham-Schroeder conv. key)
- Протокол Отвея-Рииса (Otway-Rees)
- Протокол Цербера (Kerberos)
- Протокол Ньюмана-Стабблбайна (Neuman-Stubblebine)

Они различаются между собой в важных мелочах, как то: последовательность проходов между участниками; число проходов; дополнительные вложения в сообщения, например, метка времени (timestamp), и т.д. Все эти мелочи потому и очень важные, что призваны противостоять различным атакам на протокол.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протокол Ньюмана-Стабблбайна

Этот протокол является усовершенствованной версией протокола Yahalom. Его особенностью является отсутствие необходимости синхронизации часов у сторон, а также возможность повторной аутентификации без использования промежуточной стороны.

При десинхронизации часов большинство протоколов, использующих метку времени и время жизни (lifespan) сеансового ключа могут быть вскрыты. Если часы отправителя опережают часы получателя, Мэллори может перехватить сообщение отправителя и передать его повторно, когда на узле получателя метка времени сравняется с текущей. Такая атака называется *атакой повторной передачи* или *повторного воспроизведения*. Протокол Ньюмана-Стабблбайна (протокол Н-С) противодействует этой атаке.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

   Протокол Ньюмана-Стабблбайна

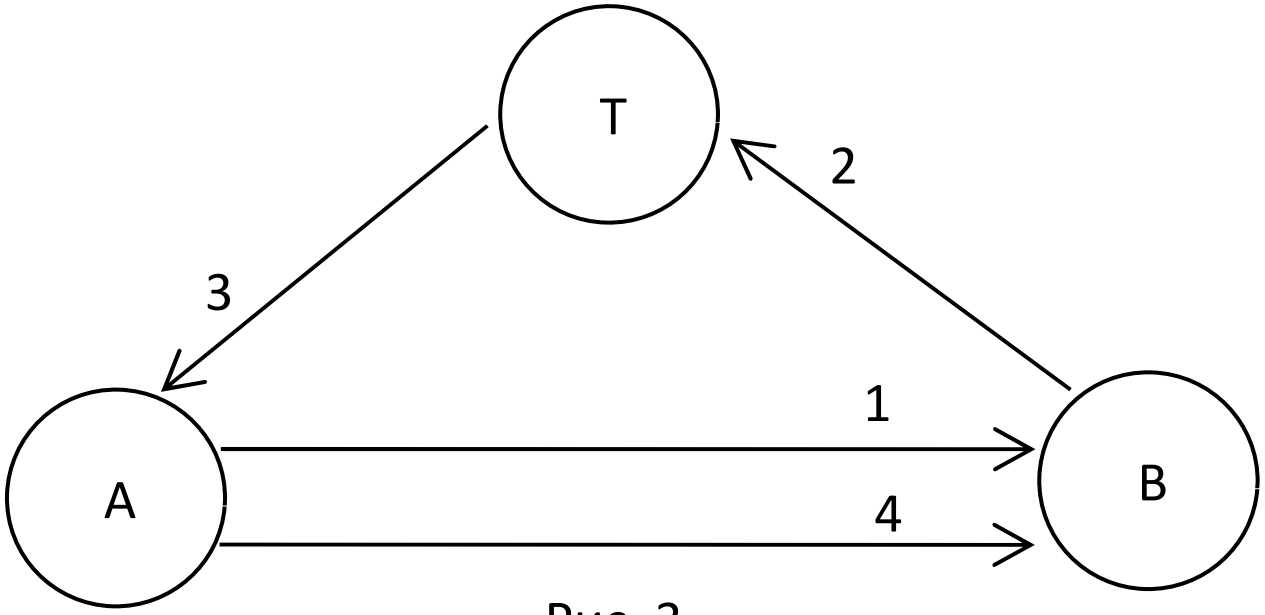

Рис. 3

1. $A \rightarrow B$: $\{A, R_A\}$, где A — имя Алисы, R_A — случайное число Алисы.
2. $B \rightarrow T$: $\{B, R_B, E_{BT}(A, R_A, T_B)\}$, где B — имя Боба, R_B — случайное число Боба, T_B — метка времени Боба.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии
   Протокол Ньюмана-Стабблбайна

3. $T \to A$: $\{E_{AT}(B, R_A, K_{AB}, T_B), E_{BT}(A, K_{AB}, T_B), R_B\}$.
4. A: $D_{AT}(E_{AT}(B, R_A, K_{AB}, T_B)) = B, R_A, K_{AB}, T_B$. (Алиса расшифровывает первое сообщение, если R_A совпадает со значением, посланным на этапе 1, то протокол продолжается.)
   $A \to B$: $\{E_{BT}(A, K_{AB}, T_B), E_{AB}(R_B)\}$, где $E_{AB}(R_B)$ — это R_B зашифрованное ключом K_{AB}.
5. B: $D_{BT}(E_{BT}(A, K_{AB}, T_B)) = A, K_{AB}, T_B, D_{AB}(E_{AB}(R_B)) = R_B$, (Боб расшифровывает последовательно оба сообщения соответствующими ключами, если T_B и R_B совпадают со значениями, посланными на этапе 2, то протокол заканчивается).
   Далее, Алиса и Боб используют K_{AB} для своего сеанса связи.

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протокол Ньюмана-Стабблбайна

И так как метка времени устанавливается только по часам Боба, и только Боб проверяет собственную метку времени, синхронизация часов не нужна.

Протокол имеет возможность в течение заранее заданного интервала времени после его проведения Алисе и Бобу повторно проверить подлинность друг друга (провести повторную аутентификацию) без обращения к Тренту, проведя следующий трёхпроходный протокол с новыми случайными числами.

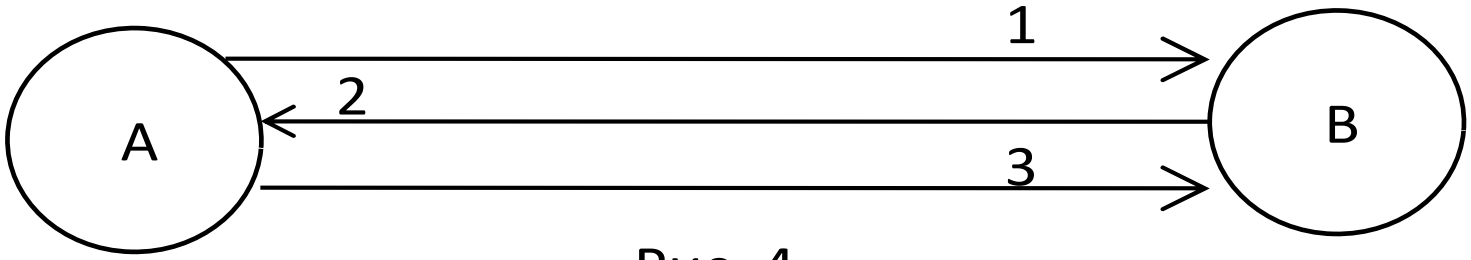

Рис. 4

Распределение ключей

1. Обмен ключами средствами симметричной криптографии

Протокол Ньюмана-Стабблбайна

1. $A \rightarrow B$: $\{E_{BT}(A, K_{AB}, T_B), R'_A\}$. (Алиса отправляет Бобу одно из сообщений Трента из прохода 3 протокола Н-С, и новое случайное число.)
2. $B \rightarrow A$: $\{R'_B, E_{AB}(R'_A)\}$. (Сверяя расшифрованное $E_{AB}(R'_A)$ с отправленным R'_A на первом проходе Алиса убеждается в подлинности Боба.)
3. $A \rightarrow B$: $\{E_{AB}(R'_B)\}$. (Сверяя расшифрованное $E_{AB}(R'_B)$ с отправленным R'_B на втором проходе Боб убеждается в подлинности Алисы.)

Новые случайные числа предотвращают атаку с повторной передачей.

Распределение ключей

2. Протоколы открытого распределения ключей

Алгоритм Диффи и Хеллмана

Безопасность протокола основывается на трудоемкости вычисления дискретных логарифмов в конечном поле, в сравнении с легкостью возведения в степень в том же самом поле. Он предполагает предварительный выбор некоторых начальных параметров, которые должны быть доступны всем участникам протокола и сети. Такие параметры будем называть *общими параметрами*.

Это двухпроходный протокол, схема которого имеет следующий вид.

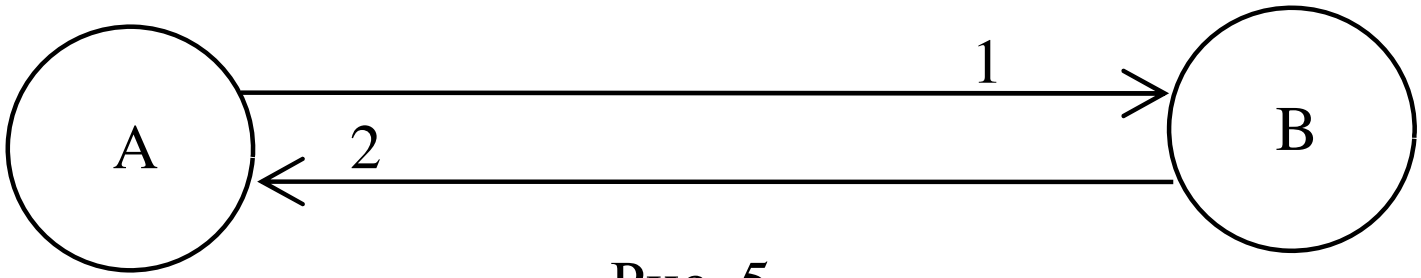

Рис. 5

Распределение ключей

2. Протоколы открытого распределения ключей

Алгоритм Диффи и Хеллмана

Общие параметры: p — большое простое число, g — примитивный корень по модулю p.

Протокол:

1. $A \rightarrow B$: $\{X = g^x \bmod p\}$, где x — случайное секретное целое число Алисы из интервала $1 < x < p$.
2. $B \rightarrow A$: $\{Y = g^y \bmod p\}$, где y — случайное секретное целое число Боба из интервала $1 < y < p$.
3. A: $K = Y^x \bmod p$, B: $K = X^y \bmod p$ (Алиса и Боб не зависимо друг от друга вычисляют их сеансовый ключ K).

Мэллори известны только значения p, g, X и Y. Ей нужно вычислить дискретный логарифм $\log_g Y = y$ или $\log_g X = x$, чтобы раскрыть x или y.