незаинтересованных лиц:

- Протоколы с посредниками;
- Протоколы с арбитрами;
- Самодостаточные протоколы.

Лекция 13.09.23

1. Если с-ма содержит n пользователей, сколько возможных секретных связей потребуется?

Если с-ма имеет n пользователей, то для возможных секретных связей потребуется $C_n^2 = \frac{n(n-1)}{2}$ ключей.

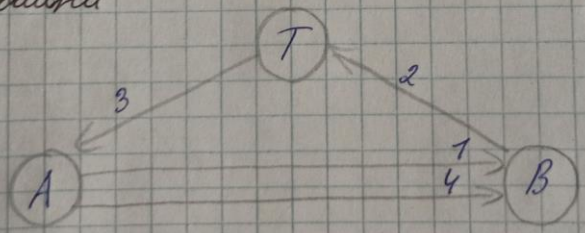
2. К какому типу протоколов относятся протоколы обмена ключами средствами симметрической криптографии?

Данный тип протоколов относится к протоколам с посредниками и решает задачу распределения ключей, а также состоит на основе симметричных криптосистем.

3. Назвите примеры этих протоколов

- Протокол „Лягушка с широкой глоткой" (Wide-mouthed-frog)
- Протокол Яхалом (Yahalom)
- Пр-кол Нидхема-Шрёдера (Needham-Schroeder conv. key)
- Пр-кол Отвея-Риса (Otway-Rees)
- Пр-кол Кербера (Kerberos)
- Пр-кол Нейлмана-Стабблбайна (Neuman-Stubblebine)

4. Нарисуйте общую схему проходов пр-кола Нейлмана-Стабблбайна



где A и B - пользователи сети,

T - ЦРК.

5. За счёт каких параметров осуществляется пр-кол

6. Сколько проходов содержит протокол Диффи и Хеллмана?

Данный протокол содержит 2 прохода.

7. Что такое примитивный корень по модулю p?

Примитивным корнем по модулю p называется число g такое, что каждое число от 0 до p можно представить как нек-рую степень числа g по модулю p. Например, число 3 является примитивным корнем по модулю 7, т. к.:

$3^1 \equiv 3 \pmod 7$,

$3^2 \equiv 2 \pmod 7$,

$3^3 \equiv 6 \pmod 7$,

$3^4 \equiv 4 \pmod 7$,

$3^5 \equiv 5 \pmod 7$,

$3^6 \equiv 1 \pmod 7$.