Лекция 27.09.23

1. Какой протокол противостоит атаке „человек по середине"?

Данной атаке противостоит протокол „станция-станция", в котором пользователи осуществляют подпись сообщений.

2. В какие протоколы можно встроить протокол „станция-станция"?

Данный протокол можно встроить в протоколы, которые ~~устойчивы~~ уязвимы к атаке „человек посередине". Примерами таких протоколов являются протоколы Диффи-Хеллмана и Хьюза.

3. Какие вам известны протоколы распределения ключей, построенные на основе открытого канала?

На основе открытого канала построены протоколы:

- ~~RSA,~~
- протокол DASS,
- протокол Деннинга-Сакко,
- протокол Ву-Лама,
- трехпроходный протокол Шамира.

4. Какая из коммутативная криптосистема подходит для трёхпроходного протокола Шамира?

Для данного протокола не подходит криптосистема, в которой используются одноразовые блокноты, т.к. при их использовании шифртексты будут выглядеть:

$C_1 = K \oplus A;$

$C_2 = K \oplus A \oplus B;$

$C_3 = K \oplus B$

Взяв операцию XOR над всеми, можно восстановить сообщение:

$C_1 \oplus C_2 \oplus C_3 = (K \oplus A) \oplus (K \oplus A \oplus B) \oplus (K \oplus B) = K.$

$C_2 \oplus C_3 = (K \oplus A) \oplus (K \oplus A \oplus B) \oplus (K \oplus B) = K.$

5. Назовите примеры криптосистем, подходящих для трёхпроходного протокола Шамира

Криптосистема RSA вполне удовлетворяет требованиям этого протокола при условии, что пользователи используют один и тот же модуль n, а свои пары открытый/закрытый ключ держат в секрете.

Криптосистема Шамира-Сильвера подходит для данного протокола только при условии секретности обоих (открытый и закрытый) ключей.