1. Чем отличается шаг от прохода протокола?

Шаг протокола – это элементарное законченное действие в протоколе с точки зрения его описания, а проход протокола – это последовательность протокола, непрерывно выполняемая одной из сторон.

2. Назвать основные хар-тики крипт-ких протоколов

• Прозрачность: каждый участник протокола должен знать протокол и всю последовательность его действий;

• Однозначность: действие каждого участника в протоколе д.б. однозначно определено;

• Полнота: протокол д.б. полным – в нём д.б. указаны точные действия любой возможной ситуации.

3. Назвать осн-ные задачи крипт-ких протоколов

• Конфиденциальность (секретность какой-либо части информации);
• Аутентичность (подтверждение подлинности или авторства);
• Неотделимость предметов и субъектов протокола.

4. Когда и кем был создан крипт-кий протокол, с к-го принято считать появление теории крипт-ких протоколов?

Появление собственной теории криптографических протоколов связывают с появлением протокола распределения ключей Диффи (Бейли Уитфилд Диффи) и Хеллмана (Мартин Эдвард Хеллман) в 1976 году.

5. Какие выделяются протоколы по степени участия незаинтересованных лиц?

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