Что хотим? Обезопасить передачу данных для случая когда сеть не защищена.

Два вида атак:

1. Перехват пакетов левым устройством в сети
2. Получатель думает что общается с одним, на самом деле с другим

Чтобы защитить данные зашифровав их и установить аунтификацию (проверка идентичности того с кем мы общаемся)

1. Шифрование

Виды

Симметричное, ассиметричное

Симметричное

Идея есть функция

Encrypt(data, key) -> crypto

Decrypt(crypto, key) -> data

Key – секретный ключ

Data & crypto имеют одинаковый размер

Задача – передать ключ

Один из вариантов - сгенерировать его и отправить по безопасному каналу

Другой вариант – использовать алгоритм DHE позволяет с помощью мат приемов путем передачи сообщения по небезопасному каналу доставить ключ получателю. Левый наблюдатель не сможет этот ключ получить. Но это защищает только от просмотра.

Ассиметричное

Также имеется набор функций

Endcrypt(data, public key)->crypto

Decrypt(crypto, private key)->data

Идея: если кто-то хочет зашифрованные данные, то он публикует свой public key и каждый может зашифровать данные свои, но расшифровать их сможет только тот у кого есть приватный для этого конкретного публичного.

Своя проблема: надо проверить что публичный ключ именно от того, от кот мы хотим

Решение 1: сеть доверия. Проверяете корректность ключа путем спрашивания этого у тех кому доверяете. Недостаток: нет централизованной организации для этой сети.