Task 1

Алгоритм Диффи-Хеллмана (DH)

Обмен ключами с помощью протокола Диффи-Хеллмана (DH) — это метод безопасного обмена криптографическими ключами по общедоступному каналу. Это один из первых протоколов с открытым ключом, который изначально был концептуализирован Ральфом Мерклем и назван в честь Уитфилда Диффи и Мартина Хеллмана. DH является одним из первых практических примеров обмена открытыми ключами. Сегодня DH используется для многих приложений, таких как, например, Proton Mail, SSH, GPG и так далее

Диффи-Хеллман работает по принципу неполного обмена ключом шифрования по сети. У каждой стороны есть открытый ключ (который может видеть каждый, включая злоумышленника) и закрытый ключ (его может видеть только пользователь компьютера)

Пример: Пользователи Ник и Майк обмениваются информацией. Генерируются закрытые и открытые ключи, установленные на компьютерах. В реальной жизни обычно используются большие простые числа.

Теперь им нужно создать частичный ключ шифрования, используя 3 доступные единицы информации: закрытый и открытый ключи Ника, и открытый ключ Майка. Алгоритмически они согласились использовать открытый ключ Ника в качестве базы и открытый ключ Майка в качестве модуля. Далее они обмениваются частичными ключами.

После обмена, к полученным частичным ключам применяется операция, описанная выше (частичный ключ Майка возводится в степень закрытого ключа Ника и берется остаток от деления на открытый ключ Майка, с Ником аналогично). Должен получиться одинаковый результат. Причина заключается в следующем математическом соотношении:

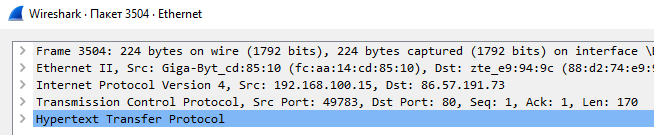
[](https://media.tproger.ru/uploads/2019/05/keys-exchange-formula.png)

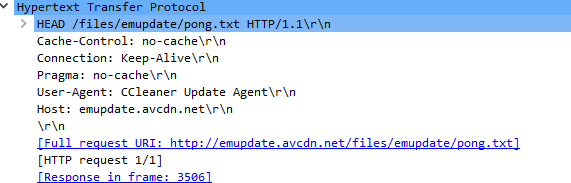
Здесь a и b — закрытые ключи, а g и p — открытые. Нам удалось обменяться друг с другом по сети достаточным количеством информации, чтобы сгенерировать общий ключ шифрования, не ставя под угрозу наши закрытые ключи.

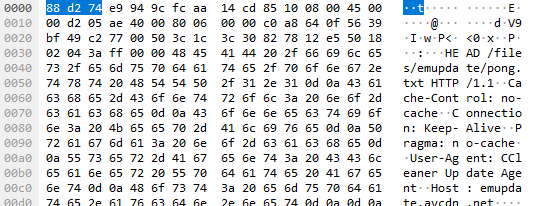
Далее создается алгоритм шифрования, например шифр простой замены(не рекомендуется) и тд.

Task 2

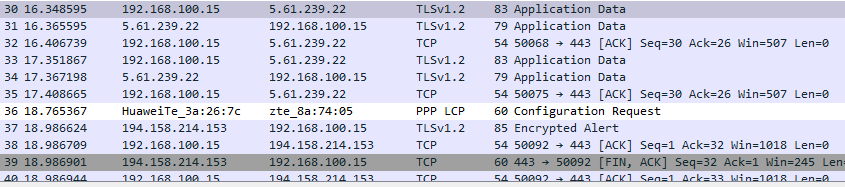
Протокол HTTP:

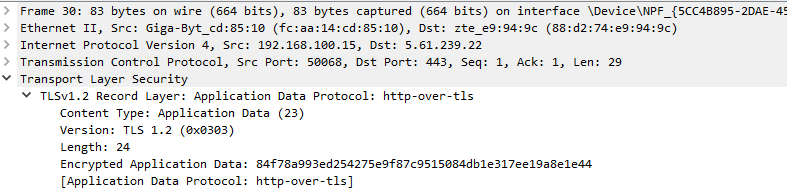


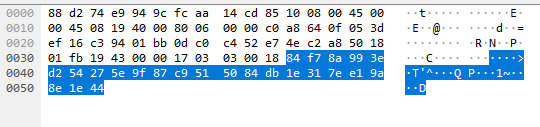




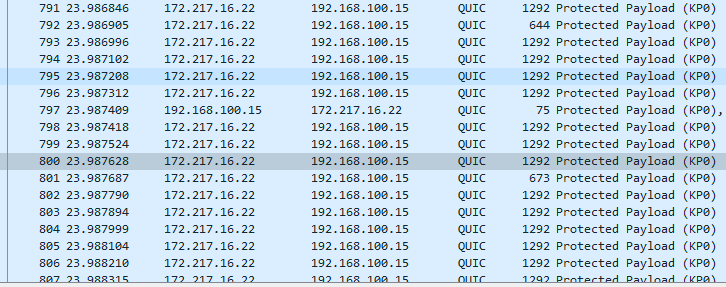
Протокол HTTPS:

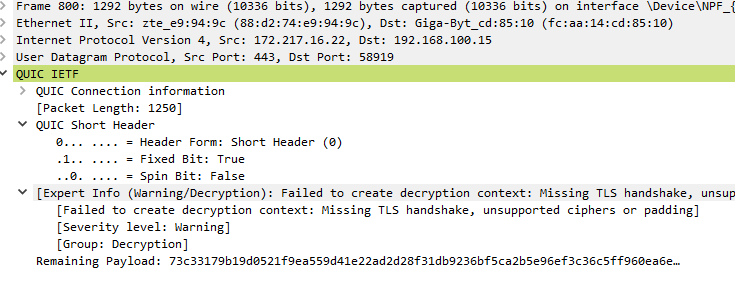


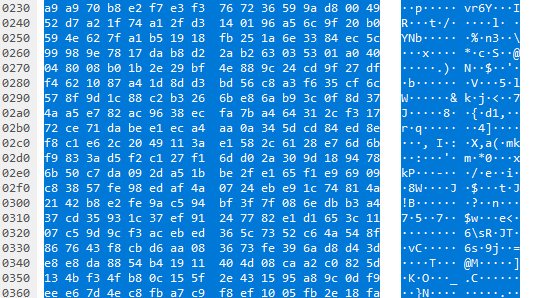




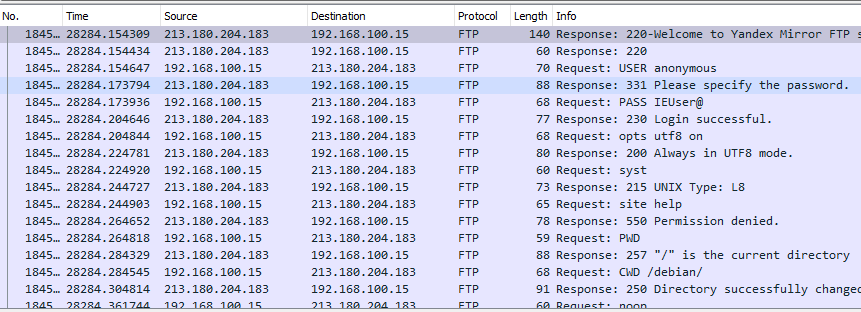
При работе в хром с youtube используется протокол QUIC:

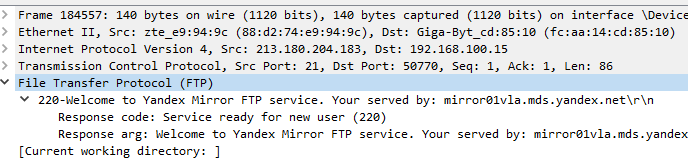


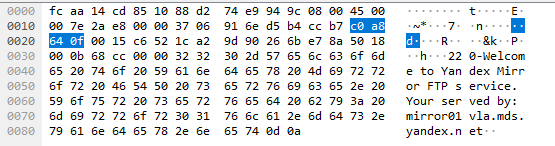




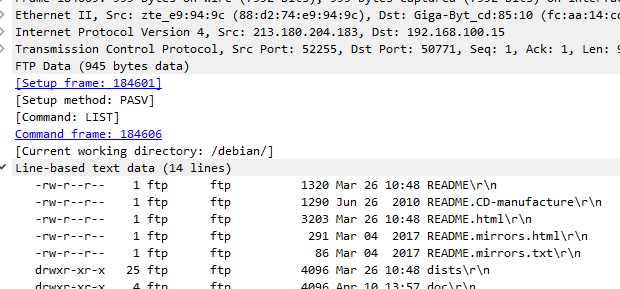
Task 3

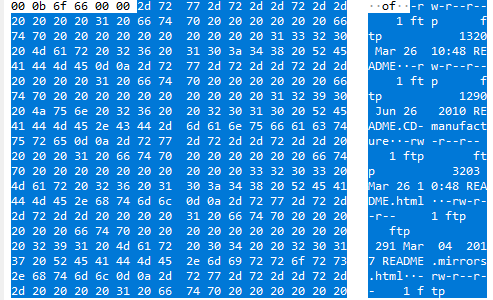












Через FTP можно передать данные на сервер. Например с помощью Total Commander или программы FileZilla и тд.