**Atribuições da semana**

* Melhorar a apresentação da semana(construir mais analogias para o público mais leigo e posteriormente abordar assuntos mais técnicos).
* Conhecer melhor sobre os quadros PING, CRYPTO,PADDING.
* Como ocorre a criptografia ? É chave assimétrica ou simétrica ?
* Quando que as chaves são trocadas(em qual pacote e como) ?
* Utilizar analogias para melhorar a conceituação para leigos e comparações para não leigos(por exemplo, associar com o protocolo TCP)

**QUIC ASSOCIADO AO TLS(rfc 9001)**

Em relação à

<https://www.ibm.com/docs/pt-br/aix/7.3?topic=authentication-diffie-hellman-encryption>

QUADRO PING : Serve para saber se o endpoint está ativo.

QUADRO PADDING : Serve para completar o tamanho do datagrama

**É chave simétrica ou assimétrica ?**

É uma combinação dos dois. Inicialmente, é enviado uma chave assimétrica para iniciar o handshake e a troca de chaves, logo depois é enviado a chave pública e privada. Tudo isso acontece de uma maneira semelhante ao handshake QUIC.

1- Primeiro o cliente envia uma solicitação de handshake, com uma criptografia assimétrica(Ele envia uma chave criptografada para começar a troca de chaves)

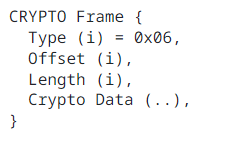
2-Depois o servidor irá começar a enviar a chave simétrica

3-Enquanto isso, paralelamente, o servidor irá enviar dados 0-rtt da aplicação criptografados(pela chave simétrica) para que depois que o handshake for concluído, o cliente possa ler as informações da aplicação guardadas em buffer

4-Handshake é concluído com um pacote handshake. s outros dados são trocados num rtt de 1 e criptografados, com header sendo curto. Tanto é que no wireshark pacote é identificado como protected payload .

**QUADROS CRYPTO:**

São quadros que levam informações criptográficas. Eles não são controlados por fluxo.



O campo type especifica o tipo de frame, no qual o bit identificador para o frame crypto é 0x06.

Perguntar o que é o campo offset, e se há alguma relação com a fragmentação de dados (MTU)

Length: É o tamanho do frame

Crypto data: é o dado criptográfico

**Quadro PING:**

É para identificar se o endpoint está ativo(para evitar o tempo de conexão limite), nesse quadro só há o bit identificador(0x01)

**Quadro Padding:**

É que nem outros protocolos, serve para aumentar o tamanho do pacote para um tamanho mínimo exigido.