NetSec Exam prep

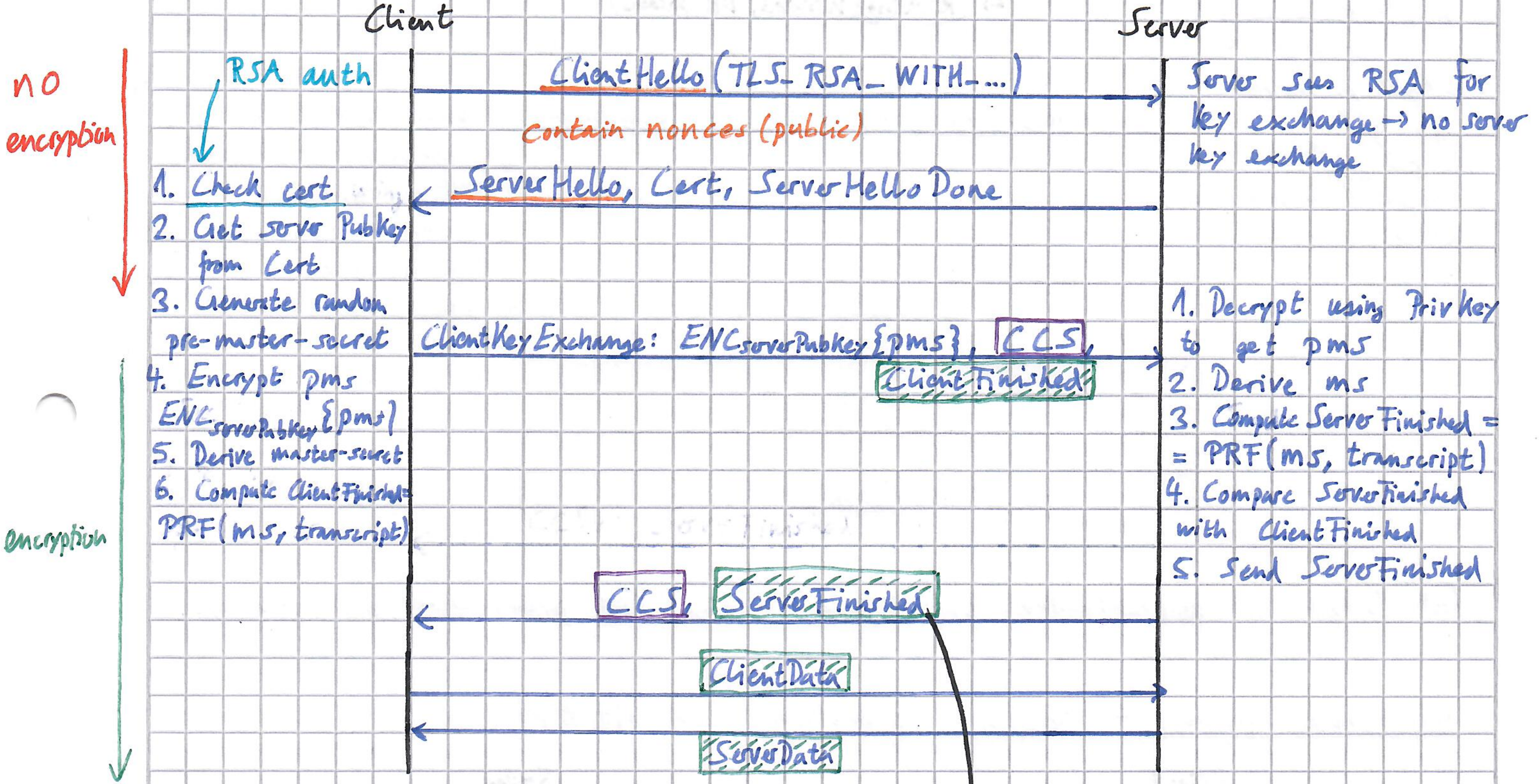
TLS

Handshake protocol

▨ encrypted with ms using record-layer crypto

□ indicate switch of cipher spec, says that I will now use the negotiated keys

- TLS_RSA_WITH_...



Server sees RSA for key exchange → no server key exchange

1. Check cert
2. Get server PubKey from Cert
3. Generate random pre-master-secret
4. Encrypt pms $ENC_{serverPubkey}\{pms\}$
5. Derive master-secret
6. Compute ClientFinished = PRF(ms, transcript)

1. Decrypt using PrivKey to get pms
2. Derive ms
3. Compute ServerFinished = = PRF(ms, transcript)
4. Compare ServerFinished with ClientFinished
5. Send ServerFinished

transcript: concatenation of all messages in the protocol as seen by the subject.

the ServerFinished message authenticates the server to the client by proving that it was able to decrypt pms using his PrivKey.

Logic behind ServerFinished authentication: You can only compute the correct ServerFinished message (PRF(ms, transcript)) if you have the mastersecret (ms). You can only know the ms if you know the pre-mastersecret (pms). You can only know pms if you can decrypt $ENC_{pubkeyServer}\{pms\}$. You can only decrypt if you have the server PrivKey.

Note: just sending a (valid) certificate does not yet authenticate a server → certificate could be replayed