Recall the topics covered on role of nonces (one each from Alice and Bob) and sequence number counters (one each for Alice and Bob) and answer the following queries in crisp (5-10 lines). Alice is a web browser whereas Bob is a web server with Digital Certificate signed by a root CA using RSA. Also assume that RSA is used for key exchange between Alice and Bob.

Q1. Assume that TLS does not use any nonces. Explain how Trudy can be successful in launching session/connection replay attacks by capturing all the messages exchanged between Alice and Bob a while ago. You can assume Alice and Bob used TLS for securing their communication related to say ordering an item for e-commerce, online payments, secure file transfers, etc. Can Trudy replay Alice's previous messages with Bob for successfully launching session/connection relay attack with Bob? Explain your answer. Can Trudy replay Bob's previous messages with Alice for successfully launching session/connection replay attack? Explain your answer.

Q2. Explain how nonces employed in TLS help in preventing session/connection replay attacks in Q1.

Q3. How does Alice derive PreMaster Secret (PMS) which she wants to send to Bob? Refer RFC 5246.

Q4. Why can't Bob derive PMS and share it to Alice?

Q5. Think of a scenario in which it's possible for Bob to derive PMS and share it to Alice. Refer TLS 1.2 handshake message protocol and explain how it can be extended (say, by adding new messages) to achieve this behaviour.

Q6. Note that MS is derived by feeding PMS and nonces of Alice and Bob as inputs to a PRF (that is known to all) by both Alice and Bob independently. Similarly, MS and nonces of Alice and Bob, and key_block size are fed as inputs to a PRF to derive key material which are split into MAC keys, session keys and IVs (IVs for AES-CBC only) by both Alice and Bob independently. To lessen the burden(!) on Bob out of her love for Bob, Alice said that she would generate MS from PMS and nonces of Alice and Bob and directly share the MS to Bob by encrypting it with Bob's public key. Trudy captured messages exchanged between Alice and Bob in this modified handshake protocol. Do you think Trudy can succeed in launching session/connection replay attacks on Bob? Justify your answer.

Q7. More love from Alice. Extension to Q6. Alice said that she would generate key material from MS and nonces of Alice and Bob, and key_block size and share the key material directly to Bob by encrypting it with Bob's public key. Trudy captured messages exchanged between Alice and Bob in this modified handshake protocol. Do you think Trudy can succeed in launching session/connection replay attacks on Bob? Justify your answer.

Q8. Sequence number counter (initially set to 0) is used by Alice to input the current value of the sequence number counter while calculating MAC for inclusion into TLS records for integrity protection. Assume that Alice has been sending 10 TLS records carrying application data (each of size 500 Bytes) to Bob. Trudy being Woman-in-the-Middle between Alice and Bob, deletes record numbered 7th. She wants to fool TCP's insequence delivery mechanism so that TCP receiver at Bob thinks everything is perfect and forwards the received TLS records to TLS layer. How could she get away and pass through TCP checks? Hint: Trudy has to manipulate TCP segments numbered 8th, 9th and 10th. How?

Q9. Having successfully fooled TCP receiver of Bob in Q8, do you think Trudy can fool TLS receiver of Bob? Explain.

Q10. Assume that Trudy captured application data messages exchanged between Alice and Bob using TLS 1.2. Alice is a web browser where as Bob is a web server with Digital Certificate signed by a CA using RSA. After a year from this correspondence between Alice and Bob, Trudy hacked into the webserver and stolen Bob's private key. Explain how Trudy can decrypt all of the old application data exchanged between Alice and Bob? This means there is no forward secrecy. It's indeed possible when TLS_RSA_WITH_AES_256_CBC_SHA256 is used as the cipher suite.

Q11. You are tasked with providing perfect forward secrecy by fixing the issue described in Q10. What tweaks you make to TLS_RSA_WITH_AES_256_CBC_SHA256 for that? Hint: You can't replace RSA with any other algorithm.

Q12. Does TLS_ECDH_RSA_WITH_AES_256_CBC_SHA offer perfect forward secrecy? Explain.

Q13. Refer RFC 5246 on Cipher Suites of TLS 1.2 and list down the ones that offer perfect forward secrecy

Q14. Refer RFC 8446 on Cipher Suites of TLS 1.3 and list down the ones that offer perfect forward secrecy

Q15. Privacy issues with TLS 1.2: Does any 3rd party like ISPs/enterprises profile their users (i.e., browsing patterns) even though their application data is encrypted? Explain!

Deliverables: A Google Doc listing down Q&As. Write crisp answers (5-10 lines) based on your own understanding of the concepts. Copying from any sources will be dealt with seriously.

References:

- **Slide deck on TLS**
- https://tools.ietf.org/html/rfc5246
- https://www.coursera.org/learn/crypto/lecture/WZUsh/case-study-tls-1-2

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources *used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.*

Name:
Date:
Signature: <keep your initials here>

Late Policy:

10% cut in marks for each late day