ONLINE EXAM - Exercises

1. **True of False**

   Respond with true or false. If the claim is false, make it true by enforcing a minimal change (keep the same context, but do not simply negate).

   Example: RC4 is used as a building block in CCMP.
   Expected answer: False. AES is used as a building block in CCMP.

   (a) If an AP has been tampered with so that it always sends the same random challenge within the Auth Challenge to any station that initiates a WEP Auth Request, an adversary can eavesdrop on an Auth Response, replay it and gain access into the network. **(2p)**

   (b) In WEP, the reuse of the IV is a source of vulnerability. **(2p)**

   (c) Only the transmitter address is used in the computation of the Message Integrity Code (MIC) in TKIP. **(2p)**

   (d) In CCMP, OFB block cipher mode of operation is used for confidentiality. **(2p)**

   (e) Subscriber authentication is a security feature present in 2G, 3G, 4G, and 5G mobile networks. **(2p)**

   (f) In LTE, K_{eNB} is the key that is used for user data integrity protection. **(2p)**

   (g) Implementing diversity in algorithms, such that if one algorithm is vulnerable to a specific attack not all necessary are, is a good security practice. **(2p)**

   (h) In 5G, it is the visitor network that makes the final decision on UE authentication. **(2p)**

   (i) Network slicing assumes usage of shared physical resources, which can lead to DoS attacks if not properly implemented. **(2p)**

   (j) SUPI is the encryption of the SUCI in 5G networks. **(2p)**

2. **Trainer position**

   You apply for a security trainer position. To prove your knowledge, at the interview you are asked to explain some security aspects related to WPA2/CCMP (in relation to its predecessors and successors).

   (a) Briefly explain why WPA2 Enterprise provides better security than WPA2 Personal. Give at least one specific reason. **(5p)**

   (b) Refer to the 4-way handshake. Explain which messages are encrypted and why (why not). **(5p)**

   (c) Explain a difference in the key hierarchy of WPA2/CCMP vs WPA. **(5p)**

   (d) WPA3 brings in the *Wi-Fi Enhanced Networks*. Explain what it means and which are the security benefits of such a solution. **(5p)**

3. **SSL/TLS**

   You are asked to reason about the security of SSL/TLS. For this, refer to the video available at [1] and the screenshot below (minute 10:08):

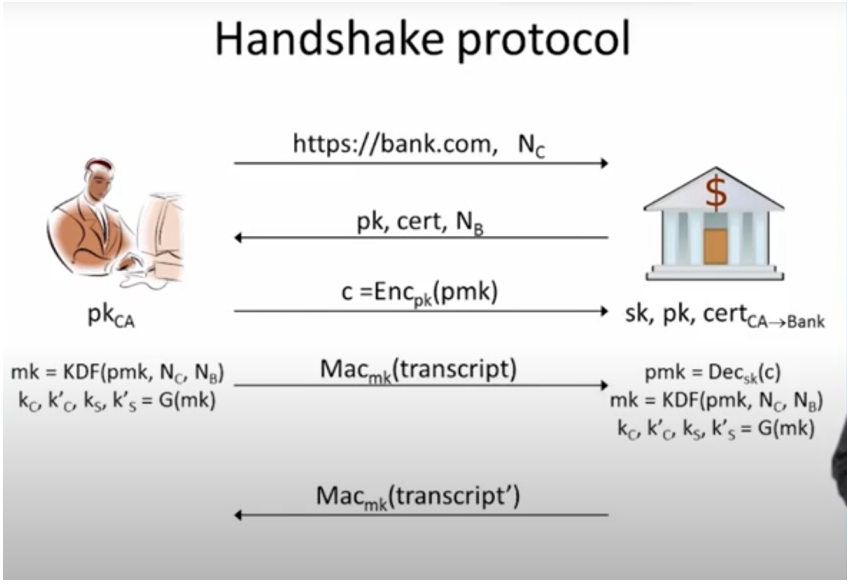

Figure 1: SSL/TLS Handshake [1]

(a) Briefly explain why there are used 2 nonces N_C and N_B and not only one (either N_C or N_B) **(5p)**

(b) Name and explain one general security principle that holds for the SSL/TLS handshake. For example, the Kerckhoffs's principle holds because the handshake protocol is public (standardized) and its security only relies in the security of the (private) keys. **(5p)**

(c) Starting from the protocol given in the figure, illustrate the handshake protocol when mutual authentication takes place. **(5p)**

(d) Briefly explain how padding can help security. Refer to the IETF RFC of the current TLS version for hints. **(5p)**

[1] J.Katz, Cryptography - Putting it all together, SSL/TLS. Available at: `https://youtu.be/AZKTwTn8szE`. Last accessed: January, 2022.

TOTAL available: 60p