1. Explain three countermeasures for buffer overflow attacks; how were these disabled to mount a buffer overflow attack?
2. What is the role of a session key? Provide at least 2 real-world examples for session key negotiation, e.g., SSL-TLS, IPSec or SSH. Explain differences between the two approaches: RSA vs. DH.
3. How does salting prevents dictionary attacks? Argue on the size for the salting value that you would recommend for a real-world encrypted password-file?
4. For the protocol trace below, show an attack or argue that it is secure:

   A→B : {A, nA}pkB
   B→A : {B, A, nA, KAB}pkA
   A→B : {A}KAB

5. Explain the general structure of a zero-knowledge protocol and outline some advantages/disadvantages compared to challenge-response protocols.