CMSC 414: HW 3

1. (text 11.3) In section 11.3.1, we discuss various ways for forming a session key. Remember that R is the challenge sent by Bob to Alice, and A is Alice's secret, which Bob also knows. Which of the following are secure for a session key?
    - $A \oplus R$
    - $\{R + A\}_A$
    - $\{A\}_A$
    - $\{R\}_{R+A}$

2. (text 11.4) Design a variant of Otway-Rees that only has one nonce generated by Alice and one nonce generated by Bob. Explain why it is still as secure.

3. (text 11.8) Design a two-message authentication protocol that achieves both mutual authentication and establishment of a session key, assuming that Alice and Bob know each other's public keys.

4. (text 11.10) Section 11.4 *Mediated Authentication (with KDC)* describes several protocols. For each of those protocols, describe which nonces have to be unpredictable (i.e., cannot be sequence numbers).

5. (text 16.1) Which of the above properties does protocol 16-2 have: perfect forward secrecy (PFS); escrow foilage against passive attacks; escrow foilage against active attacks; identity hiding; perfect forward secrecy for identity hiding. Assume private encryption keys are escrowed and private signature keys are not escrowed.

6. (text 16.1) Repeat problem 5 for a modified form of protocol 16-2 in which the first two messages are encrypted with the other end's public key rather than signed by the transmitter's private signature key. So in message 1, Alice sends {"Alice", g^a mod p} encrypted with Bob's public key,and Bob in message 2 sends {"Bob", g^b mod p} encrypted with Alice's public key.

7. (text 16.1) Repeat problem 5 for protocol 16-4.

8. (text 16.1) Repeat problem 5 for protocol 16-9, where Alice and Bob share a secret key S.

9. (text 16.1) Repeat problem 5 for the protocol where each side sends a nonce encrypted with the other's public encryption key, and the resulting session key is the $\oplus$ of the two nonces.

10. (text 16.4) Referring to section 16.6 *Endpoint Identifier Hiding*, modify protocol 16-4 to hide the initiator's identity rather than the target's identity.

11. (text 16.5) Referring to section 16.6 *Endpoint Identifier Hiding*, show a protocol that hides both identifiers from an active attacker, assuming that Alice (the initiator) already knows Bob's public key.

12. (text 16.7) Devise a protocol based on a pre-shared secret key that hides identities and gives PFS for identity hiding. Make two variants, one in which an active attacker can learn only the initiator's identity, and one in which an active attacker can learn only the target's identity.