1. Stallings, 10.1.

2. Stallings, 10.2.

3. Stallings, 10.5.

4. In class, we discussed the following key exchange protocol, based on Diffie-Hellman:

   (a) $A$ sends $B$: $g^x$, $\text{Sig}_A(g^x, B)$, $\text{Cert}_A$

   (b) $B$ sends $A$: $g^y$, $\text{Sig}_B(g^x, g^y, A)$, $\text{Cert}_B$

Suppose that the protocol is modified as follows: in the first flow, instead of $\text{Sig}_A(g^x, B)$, $A$ sends two separate signatures: $\text{Sig}_A(g^x)$ and $\text{Sig}_A(B)$. Discuss any potential vulnerabilities in this modified protocol.