Homework, April 4, due April 11

1. read chapters 13 and 14
2. (2 pts) Book problem 13-1
3. (2 pts) Book problem 13-2
4. (2 pts) Book problem 13-3
5. (2 pts) Book problem 13-4
6. (3 pts) Book problem 13-5
7. (2 pts) Compare the security properties of
   a) basic strong password protocols
   b) augmented strong password protocols
   c) Ford-Kaliski two-server protocol
8. (2 pts) Book problem 14-1
9. (1 pt) Book problem 14-4
10. (2 pts) Book problem 14-5
11. (2 pts) If the user has an RSA key pair, and the KDC knows the user's public key, can the client create her own TGT as with problem 13-1?
11. (2 pts) When the user's long term secret is the private key of a public key pair (and the KDC knows the user's public key), why is it necessary for the KDC to sign the response to a TGT request (in PKINIT or a similar protocol)?