Homework 4

Due: December 10, 2014 **Points:** 100

Questions

1. (*20 points*) Consider the RSA cipher with $p = 5$ and $q = 7$. Show that $d = e$ for all choices of public key e and private key d.

2. (*20 points*) Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not.

3. (*20 points*) In the ISO model, peer processes communicate without regard for precise implementation of activities at other layers. For example, the application does not know or care what specific routing has been chosen by the network layer. What is the security effect of an application program's not knowing the routing selected for a particular message, or even a particular session?

Do one of the following problems

4. (*40 points*) The year 2038 will pose a problem for most 32-bit UNIX systems because of the way time is represented. What specific aspect of the representation makes that year a problem? When during the year does the problem occur? Give a specific date and time. Show how you got it. What is the date with the same effect on a 64-bit system?
Hint: You will need to write a small program to find the specific date and time.

5. (*40 points*) Needham and Schroeder suggest the following variant of their protocol:

   1. $\text{Alice} \rightarrow \text{Bob} : \text{Alice}$
   2. $\text{Bob} \rightarrow \text{Alice} : \{ \text{ Alice} \mid\mid rand_3 \ \}k_{Bob}$
   3. $\text{Alice} \rightarrow \text{Cathy} : \{ \text{ Alice} \mid\mid \text{Bob} \mid\mid rand_1 \mid\mid \{ \text{ Alice} \mid\mid rand_3 \ \}k_{Bob} \ \}$
   4. $\text{Cathy} \rightarrow \text{Alice} : \{ \text{ Alice}, \text{Bob} \mid\mid rand_1 \mid\mid k_{session} \mid\mid \{ \text{ Alice} \mid\mid rand_3 \mid\mid k_{session} \ \}k_{Bob} \ \}k_{Alice}$
   5. $\text{Alice} \rightarrow \text{Bob} : \{ \text{ Alice} \mid\mid rand_3 \mid\mid k_{session} \ \}k_{Bob}$
   6. $\text{Bob} \rightarrow \text{Alice} : \{ \ rand_2 \ \}k_{session}$
   7. $\text{Alice} \rightarrow \text{Bob} : \{ \ rand_2 - 1 \ \}k_{session}$

   Show that this protocol solves the problem of replay as a result of stolen session keys.

Extra Credit

1. (*40 points*) Do the other one of the last two problems.

2. (*40 points*) Show that, under the Yaksha security scheme, Alice can obtain the session key by computing

$$(C_{Alice})^{d_{AliceA}} \bmod n_{Alice}$$