**CS426: Computer Security** **Fall 2010**

# Homework #4

**Due date & time:** 1:30pm on November 19, 2010. Hand in at the beginning of class (preferred), or email to the TA (twykoff@purdue.edu) by the due time.

**Late Policy:** You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 1:30pm the day after it is due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

**Additional Instructions:** (1) The submitted homework must be typed. Using Latex is recommended, but not required.

**Problem 1 (10 pts)** The quantum key agreement protocol we discussed in class requires two channels: one quantum channel that is subject to adversary and/or noises, and one public channel that must be authentic and unjammable.

- Explain how an adversary can break the protocol if the adversary can intercept, drop, and forge messages in the public channel. Describe what the adversary needs to do step by step, and what are the effects.
- Suppose that Alice and Bob want to agree on a key of 128 bits long. Estimate the minimal number of bits Alice needs to send to Bob to be able to do so, while detecting any eavesdropper with probability 0.999999999. Explain your answer. (You may want to refer to the wiki page *http://en.wikipedia.org/wiki/Quantum_key_distribution*)

**Problem 2 (10 pts)** Suppose Alice uses the RSA method as follows. She wants to send a message consisting of several letters, and assign $a = 1, b = 2, \ldots, z = 26$. She then encrypts each letter separately. For example, if her message is *cat*, she calculates $3^e \mod n$, $1^e \mod n$, and $20^e \mod n$. Then she sends the encrypted message to Bob. Explain how Eve can find the message without factoring $n$. In particular, suppose $n = 8881$ and $e = 13$. Eve intercepts the message

$$4461 \quad 794 \quad 2015 \quad 2015 \quad 3603$$

Find the message without factoring 8881.

**Problem 3 (10 pts)** Suppose Alice tries to implement an analog of the Diffie-Hellman key exchange as follows. Alice wants to send the key $K$ to Bob. Alice chooses a one-time pad key $K_a$ and XORs it with $K$ to compute $M_1 = K \oplus K_a$, and then sends $M_1$ to Bob. Bob chooses a one-time key $K_b$ and sends to Alice $M_2 = M_1 \oplus K_b$. Alice then sends to Bob $M_3 = M_2 \oplus K_a$.

- Show how Bob can recover $K$.

- Suppose Eve intercepts $M_1, M_2, M_3$. How can she recover $K$?

**Problem 4 (25 pts)** Read the article "New Directions in Cryptography" by Diffie and Hellman (available from the lectures & handouts page), and answer the following questions.

**a (6 pts)** The paper gives rationales for building encryption schemes that are secure against known plaintext attacks and chosen plaintext attacks, by discussing how such schemes remove restrictions that are placed on the ways of using them. Discuss these rationale in your own words.

**b (6 pts)** List all the limitations and shortcoming discussed in the paper about symmetric encryption schemes.

**c (6 pts)** List all the limitations and shortcoming discussed in the paper about symmetric message authentication schemes.

**d (7 pts)** The paper establishes the relationships among (1) public-key encryption, (2) public key distribution, and (3) digital signature (referred to in the paper as one-way authentication). By relationships, we mean using one scheme to implement another scheme. List these relationships, and explain the constructions involved to use one scheme to implement another.

**Problem 5 (20 pts)** Read the paper titled "Role-Based Access Control Models" by Sandhu et al. (available from the lectures & handouts page), and answer the questions below.

- Why is the notion of roles a useful concept? What are the differences between roles and groups?
- Briefly describe the four models in the paper: $\text{RBAC}_0$, $\text{RBAC}_1$, $\text{RBAC}_2$, and $\text{RBAC}_3$.
- Describe the constraints considered in the paper, and for each type of constraints discuss whether they are related to the "Separation of privilege" and "least privilege" principles identified by Salzer and Schroeder.

**Problem 6 (25 pts)** Read the paper by Boebert and Jain, titled "A Practical Alternative to Hierarchical Integrity Policies" (available from the lectures & handouts page), and answer the questions below.

- What are the differences between integrity policies and confidentiality policies (called compromise policies in the paper)? Why they cannot be viewed as duals of each other?
- Describe what are "Assured Pipeline" policies. Come up with an example that is not in the paper.
- Why did the authors conclude that enforcing assured pipeline policies using hierarchical integrity policies (such as those in Biba) is unsatisfactory?
- Describe how the Type Enforcement system proposed in the paper work.
- Do you agree that the proposed Type Enforcement system is a better alternative to the hierarchical integrity policies for enforcing assured pipeline policies? Give your reasons.