

Homework 2  
18-739: Foundations of Security and Privacy  
Due: Thu Oct 13, 2011

Course: 18739, Carnegie Mellon University  
Instructor: Professor Anupam Datta  
Teaching assistant: Divya Sharma

**Problem 1 [4pts]: Anonymous Communication**

In the lecture on September 8, we discussed the Dining Cryptographers protocol. In this problem, we will explore how to use that protocol as a building block to construct a general protocol for anonymous communication. Consider a group of  $n$  agents.

1. Describe a protocol using which one of the  $n$  agents can send an  $m$ -bit message. Explain informally why the protocol is *correct* (i.e., all agents receive exactly the message that was sent) and *anonymous* (i.e., none of the other agents have any clue who the real sender is).
2. State and prove rigorously that anonymity is preserved by the protocol for the case where  $n = 4$  and  $m = 1$ . (You need to show that from the point of view of any non-sender, the probability of any of the other agents being the sender is  $1/3$ ).
3. How many bits of randomness and how many message transmissions are needed to complete this protocol with  $n$  agents and an  $m$ -bit message?
4. How robust is this protocol to collusion, i.e., if  $k$  out of the  $n$  non-sender agents collude, what is the probability that they can figure out who the real sender is?

**Problem 2 [2pts]: Password Composition Policies**

In the lecture on September 13, we discussed password composition policies. This problem is intended to make you think about the effect of such policies on user behaviors and the challenges in evaluating the effectiveness of such policies.

1. Password composition policies that require passwords to adhere to many rules often cause users to behave in ways that may compromise security. State three such behaviors, and explain how each behavior can negatively impact security.
2. State four metrics that could be used to measure the usability of a password composition policy.

### Problem 3 [4pts]: Password Management

Suppose that Alice needs to create passwords for 15 sites: 0001.com, 0010.com, 0011.com, 0100.com, . . . , 1111.com. Alice has adopted the following password management scheme:

1. Alice picks 4 bit strings:  $x_1, x_2, x_3, x_4 \in \{0, 1\}^4$  uniformly at random. Alice has committed these 4 bit strings to memory.
2. For the site  $b_1b_2b_3b_4.com$  Alice uses the password  $(b_1x_1 \oplus b_2x_2 \oplus b_3x_3 \oplus b_4x_4)$ .

Suppose that each site has implemented a 3 strikes policy so that Mallory (the adversary) will get locked out after 3 incorrect guesses in an online attack. Furthermore suppose that Mallory is unable to try more than 97 guesses (per site) in an offline attack.

#### Part a

Suppose that Mallory is allowed to compromise two sites of her choosing (phishing) and learn the passwords at those sites. Show how Mallory can learn the password for a 3rd site.

#### Part b

Suppose that Mallory is allowed to compromise one site of her choosing (phishing) and learn the password at that site. Show that the probability that Mallory learns the password for any other site is less than 0.006.

#### Part c

Suppose that Mallory is allowed to compromise one site of her choosing (phishing) and learn the passwords at that site. Additionally suppose that Mallory can execute offline attacks against the other fourteen sites. Show that the probability that Mallory learns the password for any other site is less than 0.2.

#### Part d

Assume the same scenario as part C except that Alice has now picked :  $x_1, x_2, x_3, x_4 \in \{0, 1\}^{13+k}$  uniformly at random. Show that the probability that Mallory learns the password for any other site is less than  $0.2 * 2^{-k}$ .