IS2935 Introduction to Computer Security
Final Examination
Thursday, December 11, 2003

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

The questions have been grouped into four parts. These parts roughly correspond to the different sets of chapters as I had indicated in the class.

Part 1: (Total Score 20)
Part 2: (Total Score 20)
Part 3: (Total Score 30)
Part 4: (Total Score 30)

Note that scores for each question may be different – *so spend time accordingly on each question*. Be precise and clear in your answers.

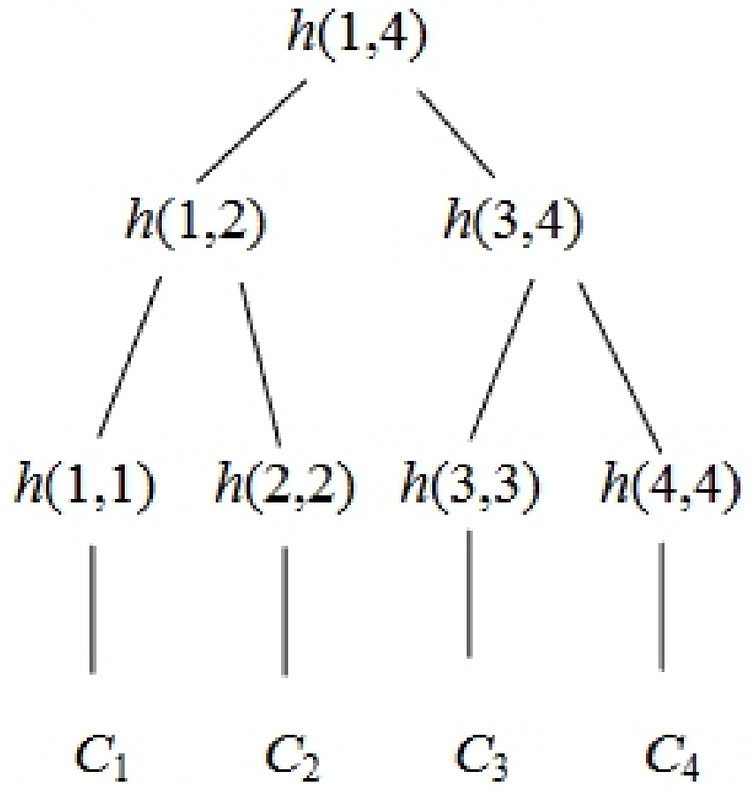
Score

Part 1 (20)	Part 2 (20)	Part 3 (30)	Part 4 (30)
Total =			

***Best of Lucks*!!**

Part I: Certificates, Authentication and Identity (Total Score 20)

1. Refer to the Merklee's tree shown below. [1, 3]
   a. Indicate the hash values that need to be *computed* (use *circles*) and that need to be *obtained* (use *rectangular* boxes) to validate C_3



   b. At the time C_3 is being evaluated, suppose that C_1 gets corrupted. How does it affect the validation of C_3? Assume that the hash values are all available in the same file, but the certificates are not. Provide enough arguments to substantiate your point.

2. Recall that *X*<<*Y*>> represents *Y*'s certificate signed by *X*. Consider the following certificates and answer (a) and (b) below. [2, 2]
   - *Dan*<<*Alice*>>
   - *Cathy*<<*Bob*>>
   - *Dan*<<*Cathy*>>
   - *Cathy*<<*Dan*>>

   (a) Show steps (or just write the *signature chain*) that Alice takes to validate Bob's certificate:

(b) Show steps (or just write the *signature chain*) that Bob takes to validate Alice's certificate:

3. What is a *dictionary* attack? Briefly describe the two types of *dictionary* attacks. [4]

4. Provide argument(s) *for* or *against* the following statement: [2]
"*Use of salt increases the effort needed to launch a dictionary attack on passwords.*"

5. For the *S/Key* scheme for password authentication, write the following: [2, 2].
   a. If h is the hash function used,
      (i) the n keys, $k_1, k_2, .., k_n$ are generated as follows:

      _____

      (*ii*) the keys are used in the following sequence:

      _____

   b. Assuming that h cannot be inverted, the attacker cannot determine the next password the user will use because of the following reason:

6. Identify two *biometric* authentication systems and give examples of attacks on them. [2]
(*Provide answer on the back of the adjacent page*)