

What to turn in: Submit hardcopy answers to the questions below. Please include your name, e-mail address, and the number of hours you spent working on the assignment.

1. True or False

Indicate the appropriate answer.

- a. T F A good password for human authentication should contain about 64 bits of random information, as provided by a typical mixed-case, alphanumeric, 8-character ASCII string.
- b. T F Digital signatures require the property of *nonrepudiation*, which says that a principal should not be able to spoof another principal's signature.
- c. T F Kerberos is an example of an arbitrated protocol.
- d. T F Good protocol design suggests that message formats be kept as uniform as possible to simplify the end hosts and reduce the trusted computing base.
- e. T F It is infeasible in practice to arrange for users of a computer system to authenticate using one-time passwords.
- f. T F For shared-key protocols that employ a trusted third party (like Needham-Schroeder and Kerberos), it is necessary to distribute $O(n^2)$ keys before any session keys may be generated. (Here, n is the number of principals.)
- g. T F Under mandatory access controls, the creator of a file may grant permissions to any users of their choice.
- h. T F Sequence numbers, timestamps, and nonces are used to prevent replay attacks.
- i. T F If there are n subjects and m objects in an access control matrix, it can take $O(n)$ time to revoke all rights of a given subject when the matrix is represented as capabilities

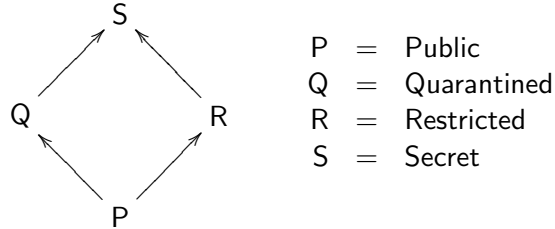
2. Cryptographic Protocols

Find a flaw in the following authentication protocol that establishes a session key k for use by two principals A and B . In this scenario, A and B want to authenticate to each other using an existing shared (symmetric) key K_{AB} . N_A and N_B are nonces generated by A and B , respectively, and the session key k is freshly created by B . Assume nonces and keys have the same number of bits.

1. $A \xrightarrow{A, N_A} B$
2. $A \xleftarrow{K_{AB}\{N_A\}, N_B} B$
3. $A \xrightarrow{K_{AB}\{N_B\}} B$
4. $A \xleftarrow{K_{AB}\{k\}} B$

5. Multilevel Security (15 points)

Consider a Bell & LaPadula style multilevel security setting in which all data is labeled with one of four security levels drawn from the following hierarchy (higher is more confidential):



Consider the following program that calculates output variables v , w , x , y , and z from input variables p , q , r , and s . Assume that the input variables have security labels that correspond to their names (i.e. variable p has label P , etc.). Assume that all output variables are initially set to 0.

```
v = p + q;  
if (r > 0) then {  
    w = 1;  
    if (v > 0) then {  
        x = 1;  
    }  
} else {  
    y = 1;  
}  
z = s - s;
```

For each output variable indicate the *minimal* security label it can be given so that system is secure according to the information-flow policy. Each answer should be one of $\{P, Q, R, S\}$.

- label of v = _____
- label of w = _____
- label of x = _____
- label of y = _____
- label of z = _____