

### Homework 3                      ICS 247 Security Algorithms

Due: Monday, February 3, 2003, in class

Please answer the following questions, each of which is worth 10 points.

1. A dishonest dealer in the Shamir secret-sharing scheme might choose to deal some wrong shares to certain users, so that some  $t$ -sized groups would evaluate to the wrong key. We could test all  $t$ -sized subsets to check this, but such a test would be inefficient. Design an efficient test to check the honesty of the dealer.
2. In the LKH group key scheme, there is no imposed order on the group members. Describe how we could easily perform insertions and deletions in this scheme, so that the height of the LKH tree is at most  $\lceil \log n \rceil$  (not big-oh), where  $n$  is the total number of insertions we have seen (starting from an empty group).
3. Suppose the tree in the LKH group key scheme is actually the computer network itself. Moreover, suppose that internal nodes can receive and send secret messages to/from each of their children. Suppose further that each node  $v$  can perform computations and broadcast in a single step a message to all of  $v$ 's descendents. Show how to initialize all the keys needed in the LKH scheme in  $O(\log n)$  communication rounds in this model.
4. In the RSA accumulator scheme, suppose we use as our hash function,  $h(x) = 2x + 1 \pmod{17}$ . What would be prime representatives for the elements 6, 10, and 13?
5. Suppose that George uses the RSA accumulator directly on the elements in the set  $\{3, 5, 7\}$ , using  $N = 85$ , and  $a = 3$ . What is the accumulated value the source will sign? Show how to forge the membership of element 9 in this set.