T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 7
Tue 25.3.2003 12–14 T3 and Wed 26.3.2003 18–20 T1

1. Suppose that you have shamanistic powers and you can control the local weather to the extent that you can make it a) rain or b) not rain on the following day. How could you interactively prove this to a understandably suspicious scientist (without revealing your secret magical methods) so that he can be 99.9% sure about this – and how long would it take ?

2. Discuss a *bit commitment scheme* using a collision-resistant hash function – say SHA-1.

3. Design a practical protocol for flipping an k-sided dice fairly, where k is a small integer. You may use the commitment scheme from previous problem.

4. Design a protocol for a zero-knowledge proof of factorization (which we assume to be equivalent to QR problem) of $n = pq$, where the verifier only knows one quadratic non-residue modulo n (but not the factorization).