T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 10
Tue 15.4.2003 12–14 T3 or Wed 16.4.2003 18–20 T1

1. In the withdrawal phase of the Chaum-Fiat-Naor protocol, what is the probability that a user is able to generate a completely faked bill that does not contain the user's identity at all?

2. What is the probability that the user manages to reuse a valid bill in the payment phase without getting caught?

3. Why cannot the seller deposit the bill twice and claim that the buyer is cheating?

4. Can the user cheat with higher probability if she creates a bill where some of the messages contain her identity while others do not?