Resit Distributed Algorithms

Vrije Universiteit Amsterdam, 5 July 2023, 18:45-21:30

You may use (a hard copy or print-out of) the textbook Distributed Algorithms: An Intuitive Approach. *Use of solutions to exercises, slides, notes, laptop is* not *allowed.*

The exercises in this exam sum up to 90 points; each student gets 10 points bonus.

1. Explain how vector clock values can be computed at run-time. (12 pts)

2. Give an example where in the Peterson-Kearns rollback recovery algorithm a process must retrieve from one of its checkpoints a basic message it needs to resend to the crashed process. (12 pts)

3. Give an example run of the Dolev-Klawe-Rodeh election algorithm on a directed ring of seven processes to show that an active process can receive a message for two rounds ahead. (12 pts)

4. Propose an adaptation of the Itai-Rodeh election algorithm in which the Boolean fourth parameter in messages, to recognize whether another process selected the same random ID in the current election round, is omitted. (14 pts)

5. Consider a complete network of five processes. Apply the Chandra-Toueg 2-crash consensus algorithm, where initially four processes choose the value 0 and one process the value 1. Give a computation in which all correct processes decide for 1. (12 pts)

6. Suppose that in a run of the BB84 quantum key exchange protocol, Eve checks all bits sent from Alice to Bob. How many mistakes is she expected to introduce in the secret key computed by Bob? (9 pts)

7. Let Alice and Bob build a private key using the Diffie-Hellman key exchange protocol, with $p = 17$ and d the smallest positive integer that is a primitive root modulo 17. Moreover, let $a = 2$ and $b = 3$. Explain how Alice and Bob construct their private key. (10 pts)

8. In the Winternitz signature, why would the checksum $b_1 + \cdots + b_n$ be less effective against replay attacks than the actual checksum? (9 pts)