

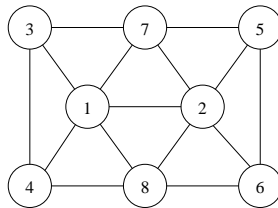
## DM69 — Lecture 10

### Lecture 10 — April 13

- The RSA public-key cryptosystem (Cormen 31.6–31.8).  
The material of Sections 31.1–31.5 is covered in DM72. If you are not familiar with this material, please read it and ask any questions you may have.

### Problems for April 15

1. Run the  $O(V^3)$  version of Edmonds' Blossom Algorithm on the graph below. Use BFS in the search for the next augmenting path, and whenever there is a choice as to which vertex to choose next (e.g., the vertex to search from in the next iteration, or the next vertex to visit in the search), choose the one with the lowest number.



2. Problem 3.74 in Bang-Jensen and Gutin
3. Explain the example on pages 154–158 in Bang-Jensen and Gutin.
4. Problem 3.77 in Bang-Jensen and Gutin.
5. Problem 3.73 in Bang-Jensen and Gutin.

### Exam questions

For the material we have covered so far, the following are the possible main questions.

1. Shortest paths in weighted graphs
2. The maximum  $(s, t)$ -flow problem and the minimum  $(s, t)$ -flow problem
3. Polynomial algorithms for maximum flows
4. Minimum cost flows
5. Matchings: characterizations and algorithms
6. The primal-dual algorithm for the transportation and the assignment problem