Cryptography I, homework sheet 1

Due: 11 September 2014, 10:45

Please check the webpage for how to submit. Please hand in your homework in groups of two or three.

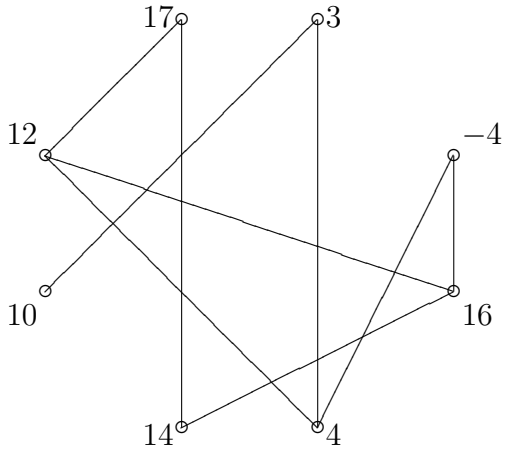
Please write the names and student numbers on the homework sheet. Please indicate your home university and study direction.

1. A *perfect code* is a set of nodes in a graph so that each node is in the neighborhood of exactly one selected node (a selected node is in its own neighborhood.) Not every graph contains a perfect code.

   Show that the public key in the cryptosystem on the slides of today's class contains a perfect code.

2. Explain why decryption works for this system.

3. Decrypt the following message



4. Describe how you can break the system for 10 000 nodes.