

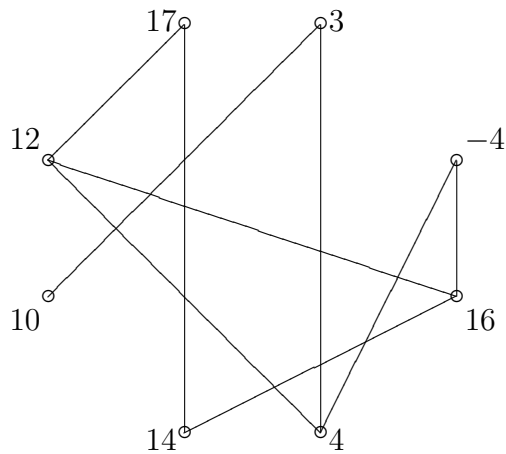
Cryptography I, homework sheet 1

Due: 12 September 2013, 10:45

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.