Christian Schindelhauer Freiburg, 2010-06-21

Exercise No. 8

Peer-To-Peer Networks

Summer 2010

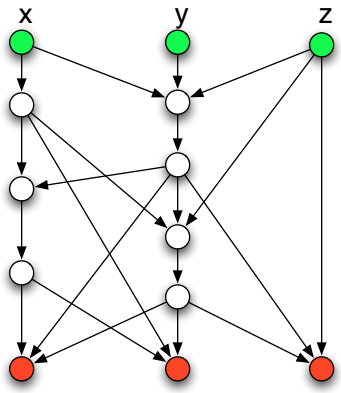
Exercise 1 *Onion routing*

Chaum's Mix Cascades can send a message anonymously from a peer A to a target peer B. Extend the algorithm such that the target peer B can send anonymously an answer to A without revealing A's identity (i.e. IP address) to B.

Design an Onion Routing algorithm where after sending and replying B does not know A and the send and reply messages cannot be distinguished by all other nodes (except A).

Exercise 2 *Network Coding*

Consider the following network:



1. What dataflow can be achieved in the network independently to each sink?
2. Find an optimal network coding for the network.
3. Compute the tables for the logarithm of $GF[2^3]$. Use the irreducible polynom $x^3 + x + 1$.
4. Calculate the following values in $GF[2^4]$
   (a) $8 \cdot 14$
   (b) $7/14$
   (c) $3/1$