Algorithms – CS-27200/37000 Homework – March 1, 2004
Instructor: László Babai Ry-164 e-mail: laci@cs.uchicago.edu

ADVICE. Take advantage of the TAs' office hours Monday, Tuesday and Thursday 5–6pm in the Theory lounge (Ry–162).

DATES TO REMEMBER. Mon Mar 8: Midterm 2. Fri Mar 12: **Last class. ATTENDANCE REQUIRED.** Review for final exam. Mon Mar 15, 10:30–12:30: Final Exam

READING. Floyd-Warshall algorithm (all pairs shortest path, transitive closure.) (Text, pp. 629-635.)

GRADUATE READING. Depth-first search (DFS). (Classification of the edges by DFS. The "white-path theorem.") Topological sort.

17.1 (3 points each) Recall that x is a multiplicative inverse of t mod m if $tx \equiv 1 \pmod{m}$. The notation $x = (t^{-1} \pmod{m})$ refers to the value of the multiplicative inverse between 0 and $m-1$. (m is a positive integer, t, x are integers.) Calculate the following multiplicative inverses (give the result as an integer between 0 and the modulus minus 1) or prove that they do not exist. Show all your work.

(a) $15^{-1} \pmod{70}$; (b) $15^{-1} \pmod{71}$; (c) $15^{-1} \pmod{72}$.

17.2 (2+5 points) Two parties, Alice and Bob, use the following cryptosystem in their confidential communication over a public channel. They first agree on a large prime number p. The message (plaintext) Alice wants to send to Bob is an integer m, where $1 \le m \le p-1$. Next, Alice privately selects an integer x ($1 \le x \le p-1$) and keeps it secret. Similarly, Bob privately selects an integer y ($1 \le y \le p-1$) and keeps it secret. Now Alice sends the value $a := (mx \bmod p)$ to Bob; then Bob sends $b := (ay \bmod p)$ to Alice; finally, Alice sends $c := (bx^{-1} \bmod p)$ to Bob. (a) Show how Bob can find out in polynomial time what the message m is. (b) Assume that Chuck, the eavesdropper, monitors the communication and gets each of the numbers p, a, b, c. Show how Chuck can compute the message m in polynomial time. (So this cryptosystem is not secure.) Perform Chuck's calculations with the following data: $p = 71$, $a = 29$, $b = 15$, $c = 61$. Show all your work.

17.3 (G only, 6 points) Prove: if FACT $\in$ NPC then NP = coNP. Here FACT is the decision version of the factoring problem, defined as FACT$=\{(a, x) : (\exists d)((2 \le d \le a) \text{ and } d \mid x)\}$.