Design and Analysis of Algorithms
Computer Science 45
Due: in class Friday, May 2, 1997

Neal Young

Problem Set 4

1. Prove that $\gcd(a, b)$ is the smallest positive element of $\{ai + bj : i, j \in \mathbb{N}\}$.

   (See CLR problem 33.2-7.)

2. Given primes p and q, integer $n = pq$, and integer e relatively prime to $\phi(n)$, show how to efficiently compute $d \equiv e^{-1} \pmod{\phi(n)}$.

   What does this have to do with RSA?

3. Exercise 33.7-3 (random self-reducibility of RSA).

4. Exercise 33.8-2 (Carmichael numbers).