Institut für Mathematische Optimierung
TU Braunschweig

WS 2005/2006

Prof. Dr. Sándor Fekete
Nils Schweer

Discrete Mathematics I
Assignment 9 (January 11, 2006)

(This assignment is due on January 18, 2006, 1.00 p.m., by dropping it into the wooden box **in front of** F 310)

Exercise 1 (Carmichael number):

A composite integer n is called a Carmichael number if it satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all integers a with $\gcd(a, n) = 1$.

Prove that 1105 is a Carmichael number.

(20 Points)

Exercise 2 (RSA system):

a) Encrypt the message MATH using the RSA cryptosystem with $p = 37$, $q = 43$ and $s = 13$.

b) Decrypt the encrypted message 09810461 which is encrypted using the RSA system with $n = 2537 = 43 \cdot 59$ and $s = 13$.

(Hint: The website http://www.math.umn.edu/∼garrett/crypto/a01/FastPow.html provides help for computing the integer $c \equiv b^e \pmod{m}$ where b, e and m are known integers.)

(20+20 Points)