CS182 **Homework 6** **Spring 2011**

In all of the following questions, show the details of your work (it is not enough to just give the answer).

Question 1. (10 points) Use the Euclidean algorithm to find

(a) $\gcd(1529, 14039)$,

(b) $\gcd(1111, 11111)$.

Question 2. (10 points) Compute 615^{31} **mod** 713.

Question 3. (10 points) Prove that 937 is an inverse of 13 modulo 2436.

Question 4. (10 points) Solve $4x = 5 \bmod 9$.

Question 5. (10 points) Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers (where $A = 00$, $B = 01, \ldots Z = 25$) and grouping pairs of integers, as we did in class.

Date due: March 29, 2011