HONS 195N: CRYPTOGRAPHY
HOMEWORK #8

Problem 1. Convert the top secret password

a6@1!*H

into a string of ASCII bytes. (See e.g. `http://ascii-table.com/`.)

Then encrypt the message Redtail using the above password as a one-time pad, and convert this back to sequence of symbols.

Problem 2. Use the Euclidean algorithm to find $\gcd(51, 113)$. Express 1 as a combination of 51 and 113. Then find $51^{-1} \pmod{113}$.

Problem 3. Encrypt the message $m = 9$ with public key 55 and encryption exponent $e = 3$.

Decrypt the message $m = 5$ with the same public key and encryption exponent.

Problem 4. In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user?

Problem 5. Find a nontrivial factorization of $n = 999999999999999919$ without using any technological aid.

Date: Due Wednesday, 9 December 2009.