Problem Set 8

Problem 1
Using the encryption keys $A = 77$ and $N = 221$, the following encrypted message of xs was sent:

72, 284, 49, 2, 83, 186, 82, 57, 184, 90, 50

Find *p, q, m, n,* and *B*. (You'll need to try a few values of *m* to see which makes *A* a factor of *n*.) Decrypt these numbers to find the numbers before encryption. Use the ASCII chart in Lecture 2 to find the letters corresponding to the decrypted numbers.

Problem 2
You intercept the encryption keys $A = 11941$ and $N = 16850989$. Find the decryption key *B*. To factor *N* you'll need a computer program to test the possible factors from 2 up to the square root of *N* (which is about 4105). Although this *N* seems large, it's no problem for a computer to factor. But it gives you some feel for the difficulty of factoring large numbers.

Problem 3
For $p = 5$ and $q = 13$, find the smallest *m* for which $n = m \cdot (p - 1)(q - 1)/2 + 1$ is not prime (which would prevent factoring *n* into *A* and *B*) and not the square of a prime (which would result in $A = B$).

Problem 4
Do for a friend what I did for you in Problem 1. Use the ASCII code to convert some message into numbers. Design your own encryption/decryption keys *A, B,* and *N*, and use *A* and *N* to encrypt the numbers. Then give *A*, *N*, and the encrypted numbers to friend, and have him figure out *B,* decrypt the numbers, and decode the message.