College of Computer Science
Northeastern University
COM 1721: Freshman Honors Seminar

Fall 2002
Handout 10
29 October 2002

Homework 6

1. Suppose my public key under the RSA system is $(n, b) = (1961, 5)$. In order to send me a message in English, you encrypt each letter of the message separately, using the RSA algorithm, with the letters ordered from 1 to 26. (Assume that the message only contains letters from the English alphabet, no spaces, periods and other punctuation marks.)

So the message "HEY" will be encrypted as follows. The letter H corresponds to 8, and 8^5 mod 1961 equals 1392. The letter E corresponds to 5, and 5^5 mod 1961 equals 1164. The letter Y corresponds to 25, and 25^5 mod 1961 equals 1806. So the encrypted message reads as follows.

1392 1164 1806

Encrypt any 5-letter (meaningful) word of your own choice using the above public key. Show your work.

2. Now suppose you want to decrypt a message that somebody else has sent to me, using the same public key as in the above question. The encrypted message is as follows.

1119 468 1609 243 1392 1

Can you decipher the message? For extra credit, determine my private key; that is, the exponent a? Again, show your work.