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

Fall 2002
Handout 12
12 November 2002

Quiz 3

Name: _____

1. RSA

(a) Suppose we choose the two primes p and q to be 5 and 7, respectively. So $n = 5 \cdot 7 = 35$. Choose suitable values for the other parts of the RSA keys, that is, the numbers a and b, to complete the RSA key generation. Recall that b is a number that does not share any prime factors with $(p-1)(q-1) = 24$ and a is selected so that $a \cdot b$ is 1 modulo $(p-1)(q-1)$.

(b) Suppose we have an RSA scheme with $p = 53$, $q = 37$, $n = 1961$, $b = 5$, and $a = 749$. In the decryption process, we need to compute the ath power of a number. The naive algorithm will take $a - 1 = 748$ multiplications. How many multiplications will the fast algorithm take? (Recall that the fast algorithm works by repeatedly squaring and using the binary representation of the power.)

(c) In the general RSA scheme studied in class we studied in class, we set (n, b) as the public key and (n, a) as the private key. Will the RSA scheme still work if we instead set (n, b) as the private key and (n, a) as the public key? Briefly justify your answer.

2. Give a brief definition (at most 2 sentences) of the term *certificate authority*, used in the context of digital signatures.