College of Computer and Information Science Fall 2004
Northeastern University
CSG252: Cryptography and Communication Security

Problem Set 1 (due September 27, 2004)
Due in class before start of lecture

Problem 1 [20 points]:

(a) Evaluate the following:

- 4657 mod 13 =
- (-4657) mod 13 =
- 3^{64} mod 19 =
  Notice that $64 = 2^6$.
- 3^{68} mod 19 =
  Notice that $68 = 2^6+4$.

(b) Devise an efficient algorithm for computing a^b mod c, where a, b, and c, are positive integers. Use the binary encoding $b_1 b_2 \ldots b_n$ for b.

Problem 2 [20 points]:
Textbook problem 1.29, page 43.

Problem 3 [20 points]:
Textbook problem 1.22, page 41.

Problem 4 [20 points]:
Textbook problem 1.25, page 42.

Problem 5 [20 points]:
Theorem 2.1 (page 9) states that if the prime power factorization of a number is $m = \prod_{i=1}^{n} p_i^{ei}$, where p_i's are distinct primes and $e_i > 0$, then the number of integers in Z_m that are relatively prime with m is: $\phi(m) = \prod_{i=1}^{n} (p_i^{ei} - p_i^{ei-1})$.

In class I have shown this theorem for m that is a power of a prime. Prove this theorem for the general case.