Math 139 Problem Set #7 Due 25 April 2003

Exercises: Write your solutions clearly, remembering that they will be graded for presentation as well as correctness.

A1. Use the extended Euclidean algorithm to verify that $\gcd(427, 2818) = 1$ and to find the multiplicative inverse of 427 modulo 2818.

A2. Agent Jayne Bond encrypts a number a (with $0 \leq a \leq 2818$) by raising a to the power 427 and reducing the result modulo the prime 2819. She reports that the encrypted version of a is 1268. What was a?

A3. Agent Bond uses the same scheme to encrypt five more numbers between 0 and 2818 (inclusive), and reports the results: 468, 2685, 1088, 2684, and 2424. She claims that the six numbers she's sent us spell an *alphabetic* message. What is it?

B1. We are given that the numbers 2063 and 3779 are prime and that

$$2063 \times 3779 = 7796077.$$

Find the smallest exponent $e \geq 2$ such that

$$a^e \equiv a \pmod{7796077}$$

for every integer a.

B2. An important phone number has been encrypted for us by raising it to the power 4232091 and reducing the result modulo 7796077. The encrypted phone number is 2046049. What was the original phone number?

B3. Our adversary is encrypting numbers between 1 and 50 by raising them to some power k and reducing the result modulo some prime p. By interviewing one of the adversary's agents, we discover that he is using $p = 53$.

(a) What are the possible values for k?

(b) In an effort to discover k, we trick our adversary into encrypting a known number. He encrypts the number 23, and the result is 30. What can we deduce about k from this crib?

(c) Through a lucky accident, we get one more crib: our adversary encrypts the number 10 and gets the result 28. What do we know now about the number k?