Homework 3

Due: Lesson 19

(50 pts)

Help Policy

AUTHORIZED RESOURCES: Any, except another cadet's program.

NOTE:

- Never copy another person's work and submit it as your own.
- Do not jointly create a program.
- You must document all help received from sources other than your instructor or instructor-provided course materials (including your textbook).
- **DFCS will recommend a course grade of F for any cadet who egregiously violates this Help Policy or contributes to a violation by others.**

1. [5] Use the Euclidean Algorithm to compute GCD(2310, 173). Use that fact to help prove 173 is prime. Hint: 2310 = 2*3*5*7*11. (Interesting fact: if you want to know whether any small primes divide a number, this is often a faster way to check, rather than dividing by lots of small primes).

2. [5] Evaluate the following expressions:
   a. $x \equiv 3^{97} \pmod{17}$
   b. $x \equiv 5^{74} \pmod{28}$

3. [5] Find the last five digits of $3^{1200567}$

4. [5] Suppose p and q are distinct primes, and gcd(m, pq)>1. Prove that m is a multiple of p or a multiple of q, or both. (Hint: What are the factors of pq?)

5. [5] The ciphertext 5377 came from RSA with modulus n=8989=101*89 and e=4889. Find the plaintext. Show all work.

6. [5] Bob decides to make RSA stronger by double encrypting his messages. So he first encrypts his message with key e_1, and then encrypts that ciphertext with e_2. Alice decrypts with d_2 then d_1. Is this more secure than single encryption? Why or why not? Assume all keys are the same size (i.e. same number of bits) and that n is unchanged.

7. [5] A toy public key cryptosystem called "Kid Krypto" works in this fashion: To be able to receive enciphered messages from others elsewhere, Ursala chooses four positive integers *a*, *b*, *A*, and *B* and calculates

$$M = ab - 1$$
$$e = AM + a$$
$$d = BM + b$$
$$n = \frac{ed - 1}{M}$$

She then publicizes *e* and *n* with instructions that a numerical message *x* in the range 0 to *n*-1 is to be enciphered as

$$y = e \cdot x \bmod n$$

Ursala deciphers a received message *y* by computing

$$x = d \cdot y \bmod n$$

(a) If Ursala chooses *a*=47, *b*=22, *A*=11, and *B*=5, calculate her values of *M*, *e*, *d*, and *n*.

(b) Suppose that Ursala had used other choices of *a*, *b*, *A*, and *B* to generate the values of *n*=25123 and *e*=2273. Further, suppose that Eve intercepts an enciphered PIN 9982 belonging to another bank customer, Walter, and would like to decipher it to gain access to his account. If all Eve knows is the relationship among *e*, *d*, and *n*, what can she do to find *d*? What alternative approach might she take to find an encrypted PIN without applying the standard decrypt formula? Find Walter's PIN.

8. [5] Use the quadratic formula to determine the existence of roots of the polynomial $2x^2 + 8x + 6 \pmod{997}$. If there are roots, give them and show that your answers are correct (ie: evaluate the expression and show it is equivalent to 0 mod 997). If there are no roots, explain why. Remember that to answer this question, *all* the mathematical operations in the quadratic formula must be performed modulo 997.

9. [10] Write a small program that uses Fermat's Little Theorem to print out the numbers from 1 to *n* (input by the user) that are "probably" prime. Check each number using brute force and indicate when Fermat's is wrong. Output should look similar to the following:

```
Find primes up to what number? 500
  …
  328
  329
  330
  331 Prime! & Fermat Prime
  332
  333
  334
  335
  336
  337 Prime! & Fermat Prime
  338
  339
  340
  341 ***** NOT PRIME but Fermat Prime *****
  342
  343
  344
  345
  346
  347 Prime! & Fermat Prime
  348
  349 Prime! & Fermat Prime
  350
  351
   …
```