Test 3
Math 105: Topics in Mathematics
Cryptology, the Science of Secret Writing
Rhodes College
20 April 2002

Instructions: Start each numbered problem on a new page. Show your work, explain when requested, and be as neat as possible. Don't spend too much time on any one problem. Turn in your test sheet along with your work, making sure that you have pledged your work.

1. (14 points)
   (a) Use the Euclidean Algorithm to find the greatest common divisor of 28 397 and 1 167.
   (b) With the aid of the Table of Primes, find the factorization of 24345.

2. (15 points)
   (a) Explain what a linear feedback shift register is supposed to simluate.
   (b) Explain briefly where the security of the RSA cryptosystem lies.
   (c) Distinguish between a *public key* cryptosystem and a *private key* cryptosystem.

3. (14 points)
   (a) Compute the first 14 output bits of the linear feedback shift register with initial configuration 1 0 1 0 0 1 and feedback equation

$$b'_6 \leftarrow (b_5 + b_3 + b_1) \mod 2.$$

   (b) Use these bits as the binary Vigenère key to decipher the message `1 0 0 1 1 1 1  1 0 0 1 1 0 1`.

4. (14 points) Prove that there are infinitely many prime numbers.

5. (14 points)

   (a) State the corollary to Fermat's Little Theorem.

   (b) Use the corollary to aid in computing $4^{362} \text{ MOD } 143$ (*Hint:* 143 is divisble by 11.)

6. (15 points) Consider an implementation of RSA with $p = 11$, $q = 23$, and encryption exponent $e = 17$.

   (a) Find the decryption exponent d.

   (b) Encipher the message $x = 19$.

   (c) Decipher the message $y = 24$ to obtain numerical plaintext.

7. (14 points) Consider an implementation of RSA where the public modulus is $pq = 5429$. Suppose you have discovered also that $(p-1)(q-1) = 5280$. Find p and q.

Bonus Rumor has it that one of the factors of the RSA modulus $m = 99799811$ has five digits and one has four. Break this implementation of RSA.
