Exercise 4. Using the Fermat factorization method, factor each of the following positive integers.

(b) 73  
(c) 46,009  
(d) 11,021

Exercise 27. Use the Pollard $p-1$ method to find a divisor of 7,331,117. (For this exercise, you will need to use either a calculator or computational software.)

Exercise 2. Decrypt the ciphertext message $LFDPHLVDZLFQTXHUHG$, which has been encrypted using the Caesar cipher

Exercise 6. Decrypt the message $RTOLKTOIK$, which has been encrypted using the affine transformation $C \equiv 3P + 24 \pmod{26}$

Exercise 8. The message

$$KYVMR\ CLFW\ KYVB\ PZJJ\ MVEKV\ VE$$

was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use frequencies of letters to determine the value of $k$. What is the plaintext message?

Exercise 10. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \pmod{26}$, are $X$ and $Q$, respectively, then what are the most likely values for $a$ and $b$?

Exercise 12. The message

$$MJMZK\ CXUNM\ GWIYR\ VCPUW\ MPRRW\ GMIOP$$

$$MSNYS\ RYRAZ\ PXMCD\ WPRYE\ YXD$$

was encrypted using an affine transformation $C \equiv aP + b \pmod{26}$. Use frequencies of letters to determine the values of $a$ and $b$. What is the plaintext message?
Section 8.3

Exercise 6. With modulus $p = 29$ and unknown encryption key $e$, modular exponentiation produces the ciphertext 04 19 19 11 04 24 09 15 15. Cryptanalyze the above cipher, if it is also known that the ciphertext block 24 corresponds to the plaintext letter $U$ (with numerical equivalent 20). (Hint: First find the logarithm of 24 to the base 20 modulo 29, using some guesswork.)

Section 8.4

Exercise 2. Find the primes $p$ and $q$ if $n = pq = 4,386,607$ and $\phi(n) = 4,382,136$.

Exercise 8. If the ciphertext message produced by RSA encryption with the key $(e, n) = (5, 2881)$ is

$$0504\ 1874\ 0347\ 0515\ 2088\ 2356\ 0736\ 0468,$$

what is the plaintext message?

Exercise 14. Show that if the encryption exponent 3 is used for the RSA cryptosystem by three different people with different moduli, a plaintext message $P$ encrypted using each of their keys can be recovered from these resulting three ciphertext messages. (Hint: Suppose that the moduli in these three keys are $n_1, n_2$ and $n_3$. First find a common solution to the congruences $x_i \equiv P^3 \pmod{n_i}$ for $i = 1, 2, 3$.)

Exercise 16. Suppose that two people have RSA encryption keys with encryption moduli $n_1$ and $n_2$, respectively, where $n_1 \neq n_2$. Show how you could break the system if $(n_1, n_2) > 1$. 