1) (5 pts) Use the Miller-Rabin test to show that \( n = 30227 \) is composite. Do the calculation on a separate piece of paper. Write down the smallest \( a \) for which the test works as well as the numbers (modulo \( n \)) \( a^q, a^{2q}, \ldots \) where \( n - 1 = 2^k q \).
2) (5 pts) Use the Pollard $p - 1$ algorithm to factor 30227. Do the calculation on a separate piece of paper. Write down here only the smallest $a$ for which the test works as well as all $a_i \equiv a^i \pmod{n}$ needed to factor $n$, and $\gcd(a_i - 1, n) \neq 1$ for the last $i$. 
3) (5 pts) The composite number $n = 30227$ with the encryption exponent $e = 7$ is used to produce - using the RSA cypher - a secret message:

$$4110.$$ 

Use the factorization of $n$ obtained in the previous exercise to compute the decryption exponent $d$ and to decipher the message. Express the final answer using the replacement table:

<table>
<thead>
<tr>
<th>A</th>
<th>O</th>
<th>H</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Write down here the answer for $d$ and (detailed) computation of $4110^d$ modulo $n$ using the method of consecutive squares.
4) (5 pts) Using the quadratic sieve method factor
   a) $n = 26123$
   b) $n = 64777$
   c) $n = 7097$

   Recall that you need to use $x_i = \lceil \sqrt{n} \rceil + i$, $i = 1, 2, \ldots$ and compute $x_i^2 \equiv y_i \pmod{n}$. Do these calculations on a separate piece of paper. Write down here only the congruences needed to construct a congruence $x^2 \equiv y^2 \pmod{n}$. Then calculate $GCD(x \pm y, n)$ to find the factors of $n$. 
5) (5 pts) Let $R$ be the ring of numbers $a + b\sqrt{3}$ where $a$ and $b$ are integers. We say that

$$a + b\sqrt{3} \equiv c + d\sqrt{3} \pmod{n}$$

if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. The set of equivalence classes modulo $n$ is denoted by $R/nR$. This is a ring with $n^2$ elements. The group of invertible elements, with respect to multiplication, is denoted by $(R/nR)^\times$. Consider $2 + \sqrt{3}$. Note that $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$. It follows that $2 + \sqrt{3}$ is invertible modulo any integer $n$. Let $\ell$ be an odd prime and $m_\ell = 2^\ell - 1$ the corresponding Mersenne number. Prove that if

$$(2 + \sqrt{3})^{\frac{m_\ell + 1}{2}} \equiv -1 \pmod{m_\ell}$$

then $m_\ell$ is a prime. Hint: the order of the group $(R/nR)^\times$ is less than $n^2$. Then use this test to show that $127 = 2^7 - 1$ is prime.