Exercise 1. Do Exercise 2 of Section 8.4 of the textbook.

Exercise 2. Do Exercise 8 of Section 8.4 of the textbook. (For the modular exponentiation in this problem, you may use software such as Maple or Wolfram Alpha)

Exercise 3. Do Exercise 14 of Section 8.4 of the textbook.

Exercise 4. Do Exercise 40 of Section 4.1 of the textbook.

Exercise 5. Do Exercise 18 of Section 6.2 of the textbook.

Exercise 6. Suppose that \( m = pq \), with \( p, q \) distinct odd primes. Suppose that for some \( a \) with \( 1 < a < m - 1 \), we have \( a^{m-1} \equiv 1 \pmod{m} \), but \( a^{(m-1)/2} \not\equiv \pm 1 \pmod{m} \). Show that \( (a^{(m-1)/2} - 1, m) \) is either \( p \) or \( q \).

The above exercise is the basic idea behind the fact that if we have both keys \( d, e \) of an RSA code, we can factor \( m \).