Introduction to Cryptography

Homework 2

Note: If you can't solve an item which is part of a question (for example, item (b) in question 2), you can still solve the rest of the question (e.g. items (c) and (d) of question 2) assuming that this item holds.

1. Let p be a prime number such that $p\text{-}1=p_1^{e1}p_2^{e2}\ldots p_m^{em}$ ($\forall i$, p_i is prime and $e_i \geq 1$). Prove that $g \in Z_p^*$ is a generator if and only if for all $1 \leq i \leq m$ it holds that $g^{(p-1)/pi} \neq 1 \mod p$.

2. The purpose of this exercise is to find an efficient algorithm for computing discrete logarithms in Z_p^*, where p is prime and $p=2^n+1$.
   The discrete logarithm problem is the following:
   Input: a prime p, a generator g of Z_p^*, and a value y in Z_p^*.
   Output: x s.t. $g^x=y \mod p$.

   Let $x=b_{n-1}2^{n-1}+ b_{n-2}2^{n-2}+\ldots+b_12^1+b_0$ be the binary representation of x.

   a. Show how to find the least significant bit (b_0) of x (given g,y). (4 points)
   b. Set $z=y\cdot g^{-b0}$, and show how to use it to find the bit b_1. (8 points)
      Hint: there is an integer i such that $z=g^{4i+2\cdot b1}$. Recall also that $e=p-1=2^n$ is the smallest exponent s.t. $g^e=1 \mod p$. Use these facts to find b_1.
   c. Show how to find the complete binary representation of x. (8 points)
   d. Explain why this method is only good for a prime modulo p that satisfies $p=2^n+1$. (5 points)

   Note: this algorithm can be generalized for any Z_p^* for which $p\text{-}1=p_1^{e1}p_2^{e2}\ldots p_m^{em}$, all p_i are small primes, and the factorization of p-1 is known. (There is not need to prove this fact.)

3. Let p,q be prime numbers, and $n=pq$. *For a number* $m \in [0,1,2,\ldots,n-1]$ we can use the representation $[a,b]$, where $a=m \mod p$, and $b=m \mod q$.
   a. Show that for $m_1,m_2,m \in [0,1,2,\ldots,n-1]$, if the representation of m_1 is $[a_1,b_1]$ and the representation of m_2 is $[a_2,b_2]$, then the representation of $m= m_1+m_2$ is $[a,b]$, where $a=a_1+a_2 \mod p$, and $b=b_1+b_2 \mod q$. (6 points)
   b. State and prove a similar claim for multiplication. (6 points)
   c. For $x,y \in [0,1,2,\ldots,p-1]$, how is it possible to *efficiently* compute $z=x/y \mod p$? I.e., compute a number $z \in [0,1,2,\ldots,p-1]$ that satisfies $yz=x \mod p$. (6 points)
   d. State and prove a claim (similar to (a) and (b)) for division modulo n. (7 points)

4. Let $n=pq$. Define $\lambda(n)=\mathrm{lcm}(p-1,q-1)$, i.e., $\lambda(n)$ is the least common multiplier of $p-1$ and $q-1$.
    a. Show that if $a=1 \bmod \lambda(n)$ then for all $m \in Z_n^*$ it holds that $m^a = m \bmod n$. (Hint: use the CRT.) (15 points)
    b. Show that in the RSA cryptosystem one can choose e,d to satisfy $ed=1 \bmod \lambda(n)$. (Instead of satisfying $ed=1 \bmod \phi(n)$.) (10 points)