Introduction to Cryptography: *Homework 2*

Submission date: April 8, 2008

Solve all questions. (you also get 1 point for free)
Note: If you cannot solve an item which is part of a question (for example, item (b) in question 3), you can still solve the rest of the question (e.g. items (c) and (d) of question 3) and assume in your answer that the first 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 $g^{(p-1)/pi}\neq 1 \mod p$. (33 points)

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 $x=b_{n-1}2^{n-1}+ b_{n-2}2^{n-2}+\ldots+b_1 2^1+b_0$ be the binary representation of x.

   a. Show how to find the least significant bit (b_0) of x (given g,y). (7 points)
   b. Set $z=y\cdot g^{-b0}$, and show how to use it to find the bit b_1. (10 points)
      Hint: there is an integer i such that $z=g^{4i+2\cdot b1}$. Recall also that $e=p\text{-}1=2^n$ 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. (10 points)
   d. Explain why this method is only good for a prime modulo p that satisfies $p=2^n+1$. (6 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. Consider a public-key encryption scheme where the public information is $<p,H\subset Z_p^*,g>$ (where H is a subgroup of Z_p^* which has q elements in it, and g is a generator of H). The private key is a value a which is chosen at random in the range $[0,q]$, and the public key is a pair $<g,h>$, where $h=g^a$.
   The system is used to encrypt a bit x in the following way:
   - If $x=0$ then the ciphertext is the pair $<g^b,h^b>$, where b is chosen at random in the range $[0,q]$.
   - If $x=1$ then the ciphertext is the pair $<g^b,g^c>$, where b and c are each chosen at random in the range $[0,q]$.

   Show that knowledge of the private key enables to decrypt efficiently. (13 points)
   Prove also that this encryption is secure if the DDH assumption holds in H. (20 points)