Introduction to Cryptography: *Homework 2*

Submission date: December 25, 2012. In Class.

Solve and submit the answers to questions 1 and 3.
Make sure that you know how to solve all of the other questions.

1. (CBC-MAC)
   Consider the CBC-MAC construction. Show that for any n>2, an adversary can forge a MAC of a message of length n, by asking for MACs of shorter messages.

2. 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.

3. 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.)

4. Let p be a prime number. Suppose that g is a generator of Z_p^* and let $b=g^i$ for an exponent $0 \leq i \leq p\text{-}2$.
   a. Show that the order of b is $(p\text{-}1)/gcd(p\text{-}1,i)$. (17 points)
   b. Show that the number of generators in Z_p^* is ϕ(p-1). (16 points)

5. Let g and h be any two generators of Z_p^*. Show that
   a. If $x=g^{2i}$ (that is, the discrete log of x to the base g is even), then there exists a value j such that $x=h^{2j}$. (13 points)
   b. If $x=g^{2i+1}$ (that is, the discrete log of x to the base g is odd), then there exists a value j such that $x=h^{2j+1}$. (20 points)

In your proof do not use the fact that if $x=g^{2i}$ then x must be a QR and therefore its discrete log to the base of any generator must be even.