

# 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  $p-1 = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$  ( $\forall i, p_i$  is prime and  $e_i \geq 1$ ). Prove that  $g \in \mathbb{Z}_p^*$  is a generator if and only if for all  $1 \leq i \leq m$  it holds that  $g^{(p-1)/p_i} \neq 1 \pmod p$ . (30 points)

2. The purpose of this exercise is to find an efficient algorithm for computing discrete logarithms in  $\mathbb{Z}_p^*$ , where  $p$  is prime and  $p = 2^n + 1$ .

The discrete logarithm problem is the following:

Input: a prime  $p$ , a generator  $g$  of  $\mathbb{Z}_p^*$ , and a value  $y$  in  $\mathbb{Z}_p^*$ .

Output:  $x$  s.t.  $g^x = y \pmod p$ .

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

- a. Show how to find the least significant bit ( $b_0$ ) of  $x$  (given  $g, y$ ). (6 points)
- b. Set  $z = y \cdot g^{-b_0}$ , and show how to use it to find the bit  $b_1$ . (10 points)  
Hint: there is an integer  $i$  such that  $z = g^{4i+2 \cdot b_1}$ . Recall also that  $e = p-1 = 2^n$  is the smallest exponent s.t.  $g^e = 1 \pmod p$ . Use these facts to find  $b_1$ .
- c. Show how to find the complete binary representation of  $x$ . (9 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  $\mathbb{Z}_p^*$  for which  $p-1 = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ , all  $p_i$  are small primes, and the factorization of  $p-1$  is known. (There is not need to prove this fact.)

3. Let  $p$  be a prime number. Suppose that  $g$  is a generator of  $\mathbb{Z}_p^*$  and let  $b = g^i$  for an exponent  $0 \leq i \leq p-2$ .
  - a. Show that the order of  $b$  is  $(p-1)/\gcd(p-1, i)$ . (20 points)
  - b. Show that the number of generators in  $\mathbb{Z}_p^*$  is  $\phi(p-1)$ . (20 points)