Lect. Dr. Sorin Iftene
Department of Computer Science
"Al.I.Cuza" University
E-mail: `siftene@info.uaic.ro`

Computational Number Theory, *Spring 2017*

Homework 4 (10 points)
April 28, 2017

1. Generate α, a primitive root modulo a prime p, where p is an odd prime, using one of the algorithms discussed in class (assume that the prime factorization of $p-1$ is known in advance - the simplest choice will be $p = 2q+1$, where p and q are odd primes). (2p)

2. For p and α generated as above and an arbitrary $\beta \in \mathbf{Z}_p^*$, compute the discrete logarithm $\log_\alpha \beta$ modulo p, using one of the algorithms discussed in class (Skanks or Pollard). Use moderate-sized primes (e.g., p is on 32 bits). (4p)

3. Implement the Silver-Pohlig-Hellman algorithm for computing discrete logarithms modulo a large prime p (e.g., p is on 1024 bits). Assume that $p-1$ has only small prime divisors and that its prime factorization is known in advance. (4p)

Due: May 16, 19