# Introduction to mathematical cryptography
# Homework problems
# Week 9

17. Let $p$ be an odd prime and let $g$ be a primitive root modulo $p$ i.e. for any $a \in \mathbf{F}_p^\times$ there exists a solution to the discrete logarithm problem $g^x \equiv a \bmod p$, denote the smallest such (positive) $x$ by $\log_g a$. Suppose $a \in \mathbf{F}_p^\times$ is given. Assume there is a machine which does the following. You can give any number $1 \leqslant y \leqslant p-1$ as an input. Then if $\log_g a < y$, the machine returns the message `TOO LARGE`, if $\log_g a > y$, the machine returns the message `TOO SMALL`, while if $\log_g a = y$, the machine returns the machine `EXACT`. Prove that using this machine, $\log_g a$ can be computed in polynomial time.

18. Alice publishes her RSA cryptosystem (i.e. a number $N$ which is the product of two secret prime numbers, and an encrypting exponent $e$ coprime to $\varphi(N)$). Assume Eve has a machine which can solve the discrete logarithm problem in the multiplicative group $\mathbf{Z}_N^\times$ with any base (i.e. the machine does the following: for any input $1 \leqslant g, a \leqslant N$, if $\gcd(g,N) > 1$ or $\gcd(a,N) > 1$ or no power of $g$ is congruent to $a$ modulo $N$, the machine returns `ERROR`; otherwise, it returns the smallest positive number $x$ satisfying $g^x \equiv a \bmod N$). Prove that Eve can decrypt any cipher which she can intercept.

**Note:** Please provide complete arguments everywhere.