# Exercises on Modulo Arithmetic and RSA

Víctor Alcázar Kosmas Palios Albert Ribes

April 3, 2017

## Exercise 2

We first compute $x = b^c mod\phi(p)$
Then we compute $a^x modp$.

Why is this correct? Simply because for every p,a, as Euler tells us that$a^{\phi(p)} = 1modp$, we have the following $a^k = a^{k+\phi(p)*l}modp$.

This takes polynomial time, as modular exponentiation can be computed in polynomial time, with use of repeated squaring.