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

Computational Number Theory, *Spring 2020*

Homework 2 (10 points)
March 9, 2020

1. Implement `multi-prime RSA` decryption (i.e., computing $y^d \, mod \, n$, for $n = p \cdot q \cdot r$, where p, q, and r are distinct 512-bit primes) using the Chinese remainder theorem algorithm discussed in class. Perform time comparisons between this modular exponentiation algorithm and the regular modular exponentiation algorithm (the one that is implemented in your large integers library). (4p)

2. Implement `multi-power RSA` decryption (i.e., computing $y^d \, mod \, n$, for $n = p^2 \cdot q$, where p and q are distinct 512-bit primes) using the Chinese remainder theorem algorithm and Hensel's lifting lemma discussed in class. Perform time comparisons between this modular exponentiation algorithm and the regular modular exponentiation algorithm (the one that is implemented in your large integers library). (4p)

3. Combine (1) with constructing short addition chains for the elements $d \, mod \, (p-1)$, $d \, mod \, (q-1)$, $d \, mod \, (r-1)$ (2p)

Due: March 30, 31, April 2, 3