CS325 Assignment 2 (Due date: 6th April)

Practice RSA with the following parameters: e = 23 and n = 233 ×241.

A. Encrypt message m = 2, i.e. compute $c = m^e \bmod n$ using "repeated squaring algorithm". Write down all steps; or write a program implementing the algorithm and print out the steps.

B. Self-study "Extended Euclidean algorithm" and use it to compute private key $d=e^{-1} \bmod (n)$ corresponding to the given above public key (e, n), and write down all steps.

C. Decrypt the ciphertext and get message $m= c^d \bmod n$ using "repeated squaring algorithm" in slides. Write down all

steps; or run the program you write for Question A to print out the steps.