MATH/CS 295: CRYPTOGRAPHY
HOMEWORK #8 ADDITIONAL PROBLEMS

Problem 3.A*. Bob chooses the RSA modulus

$n = 1069524788729186444521284099154989216238375870617122680021373334588065126734368 7$

and

$e = 1857308780599082935579426134526996671022161384368318177549870987520554825439779$

and because he is short for time chooses a small decryption exponent. Alice sends the secret message

$b = 5876903442995476139711640244861982014547608694076473777226913452306949807294092$

to Bob by converting her codeword of seven letters into ASCII bytes, interpreting this as the binary expansion of an integer, and encrypting it using RSA. Decrypt the message and recover the plaintext codeword.

Problem 3.B. Let n be an RSA modulus, e_1 an encryption exponent, d_1 the corresponding decryption exponent, and e_2 a second encryption exponent. Given the data n, e_1, d_1, e_2, exhibit a fast and certain algorithm that determines the corresponding decryption exponent d_2 which does *not* using random choices, the factorization of n, or exponentiation modulo n. Illustrate your algorithm on $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 7$ and $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 11$.