LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / I & C
CH-1015 Lausanne
Phone: ++41 (0) 21 693 76 03
Fax: ++41 (0) 21 693 68 79
URL: http://lasecwww.epfl.ch

Exercise A#2

A user who wants to receive messages and be sure to avoid error transmissions decides to use two RSA keys. Someone willing to send him a message should encrypt it using both keys and send both ciphertexts. We assume plain RSA or RSA with deterministic formatting rule. The (lazzy) user who do not want to generate too many prime numbers decide to use a single modulus for both keys. Show that an adversary can easily decrypt messages.
Hint: assume that the two encryption exponents are coprime and use the extended Euclid algorithm.