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#3

A trusted company want to sell RSA key pairs to users but want to limit the number of prime integers to generate. For this, it creates a pool of prime numbers p_1, ..., p_n. Every time a new customer wants a new key, his modulus becomes $n = p_i \times p_j$ for random i and j and his exponent is randomly drawn. Discuss the security.