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#1

Show that plain RSA signatures are easily broken by a universal forgery under a chosen message attack. How to solve this in practice.