Exercise 8

Benjamin Boudra

February 15, 2016

Contents

1 Prompt

Write up a careful example of the entire RSA process, including finding d, encrypting a, and decrypting c, with $p = 137$, $q = 241$, $e = 53$, and $a = 12345$. You will be expected to do all of this (including efficient modular exponentiation and the extended Euclidean algorithm) by hand during the test, so do the exercise that way, just using an ordinary calculator.

2 Solution