Cryptography and Security — Retake Exam

Serge Vaudenay

27.2.2009

1 RSA Parameters

As a toy example we want to use RSA with modulus $N = 67 \times 71 = 4757$. We want to compute $x^e \bmod N$ using the square-and-multiply algorithm.

1. What is an eligible value for e?
2. How many eligible e's do we have?
3. Given an eligible e, compute how many multiplications are needed in this algorithm.
4. What is the best eligible e?