Università degli Studi Roma Tre
Corso di Studi in Matematica, a.a. 2016/2017
CR410 – Crittografia1
Esercizi
Foglio 3

1. Applicare il test di Miller-Rabin (per max quattro iterazioni) agli interi $n_1 = 15841$ e $n_2 = 1103$.

2. Sapendo che una versione di RSA ha $N = 17473$, esponente di cifratura $e = 11$ e di decifratura $d = 4691$, fattorizzare N.

3. Provare che, se n è uno pseudoprimo di Eulero in base b e se $\left(\frac{b}{n}\right) = -1$, allora n è uno pseudoprimo forte in base b.