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 due iterazioni) agli interi $n_1 = 15841$ e $n_2 = 1103$.

2. Sapendo che una versione di RSA ha $N = 10573$, esponente di cifratura $e = 11$ e di decifratura $d = 8483$, 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.

4. Usando l'attacco di Wiener (delle frazioni continue) trovare la chiave privata del crittosistema RSA che ha $N = 1868077, e = 1356611$.

5. Lo stesso messaggio m è stato cifrato per i tre utenti A_1, A_2, A_3 che hanno chiavi pubbliche RSA rispettivamente $(161, 3)$, $(209, 3)$, $(221, 3)$. I tre testi cifrati ottenuti sono $y_1 = 6, y_2 = 113, y_3 = 177$. Decifrare il messaggio, senza fattorizzare i moduli.

6. Consideriamo un cifrario di Rabin con chiave $N = 4601 (= 107 \cdot 43)$. Decifrare il messaggio $y = 798$ (trovando i quattro possibili testi in chiaro).