Università degli Studi Roma Tre
Corso di Studi in Matematica
CR410 – Crittografia a chiave pubblica
Esercizi
Foglio 4

1. Usando l'algoritmo $p-1$ di Pollard, fattorizzare $n_1 = 18\,923$ e $n_2 = 115\,147$.

   Sol. $18\,923 = 127 \cdot 149$, $115\,147 = 113 \cdot 1019$

2. Usando l'algoritmo ρ di Pollard, fattorizzare $n_1 = 1649$, $n_2 = 24\,911$, $n_3 = 96\,637$.

   Sol. $1649 = 17 \cdot 97$, $24\,911 = 29 \cdot 859$, $96\,637 = 41 \cdot 2357$.

3. Usando il metodo di Fermat, fattorizzare $n_1 = 18\,896\,309$ e $n_2 = 192\,404\,497$

   Sol. $18\,896\,309 = 4337 \cdot 4357$, $192\,404\,497 = 13859 \cdot 13883$.

4. Usando il metodo delle basi di fattorizzazione, fattorizzare $n_1 = 540\,143$.
   Sol. $540\,143 = 421 \cdot 1283$.

5. Fattorizzare:

$$8\,926\,861; \quad 24\,458\,477$$

$$1\,313\,303; \quad 6\,791\,173;$$

$$157\,954\,399; \quad 298\,217\,461.$$

Sol.

$$8\,926\,861 = 2521 \cdot 3541; \quad 24\,458\,477 = 1601 \cdot 15277 :$$

$$1\,313\,303 = 101 \cdot 13003; \quad 6\,791\,173 = 541 \cdot 12553;$$

$$157\,954\,399 = 12553 \cdot 12583; \quad 298\,217\,461 = 17239 \cdot 17299.$$