

ALGORITMI U TEORIJI BROJEVA

zadaca 4.46

1. Odredite proste brojeve p i q te tajni eksponent d u RSA kriptosustavu ako je poznato da je $n = 3834247$, $\varphi(n) = 3830256$ i $e = 17$.

2. U RSA kriptosustavu s javnim ključem (n, e) i tajnim eksponentom d , gdje je

$$n = 11312143, \quad e = 5, \quad d = 3014669$$

odredite najmanji prirodan broj k takav da za broj $m = (ed - 1)/2^k$ postoji neki prirodan broj a takav da je $\text{nzd}(a, n) = 1$ i $a^m \not\equiv 1 \pmod{n}$. Odredite i najmanji pripadni prirodni broj a .

3. Neka je $(n, e) = (17673661, 8367643)$ javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{1}{3}\sqrt[4]{n}$. Odredite d pomoću Wienerovog napada.