Časovna zahtevnost algoritmov, RSA

1. Zaporedje 10101100 je generirano z linearno rekurzivno šifro reda 4. Izračunajte koeficiente ustrezne rekurzivne enačbe!

2. Dani sta praštevili $p = 11$ in q = 17 ter kodirni eksponent $e = 3$.

   (a) Preverite, da je (pq, e) veljaven javni ključ za RSA.

   (b) Izračunajte še ustrezen dekodirni eksponent d.

   (c) Z javnim ključem (pq, e) zašifrirajte kriptogram 107.

   (d) Z zasebnim ključem (pq, d) dešifrirajte kriptogram 6.

3. (Napad na skupni modul) Alenka ima javni RSA ključ (n, e_1), Boris pa javni ključ (n, e_2), pri čemer je $\gcd(e_1, e_2) = 1$. Cene sporočilo b zašifrira za obema javnima ključema in pošlje Alenki oziroma Borisu. Eva prestreže oba kriptograma, $c_1 = b^{e_1} \bmod n$ in $c_2 = b^{e_2} \bmod n$.

   - Pokažite, kako lahko Eva dešifrira kriptogram(a).
   - Napad ilustrirajte na primeru $n = 55$, $e_1 = 3$, $e_2 = 7$, $c_1 = 8$ in $c_2 = 18$. Napad, pri katerem faktorizirate n, ne velja!

4. Pokažite, da lahko razcepimo $n = p \cdot q$, če poznamo $\varphi(n)$.

5. Na prvih vajah smo ocenili število korakov pri Evklidovem algoritmu. Čim bolj natančno ocenite časovno zahtevnost Evklidovega algoritma.