Kriptografija in teorija kodiranja – 3. domača naloga

(do srede, 21. aprila 2010 – oddaja na predavanjih)

Naloge rešujte samostojno. Odgovori in rešitve naj bodo jasne, pregledne in dobro utemeljene!

1. RSA-podpis, ki je opisan v [5], je za razliko od Elgamalovega deterministične.
   Kako bi ga lahko spremenili v nedeterminističnega?
   Varnostno analiziraj svoj predlog.

2. Kakšne lastnosti naj ima zgoščevalna funkcija, da ne bo ogrožena varnost podpisa?

3. Predlagaj čim več načinov s katerim bi iz dokumenta poljubne dolžine z bločno šifro skonstruiral izvleček fiksne dolžine, nato pa svoje predloge analiziraj.

4. Predlagaj novo varianto Elgamalovega podpisa, kjer ne bomo več potrebovali računanja inverza (k^{-1}), ki ga ponavadi izračunamo z razširjenim Evklidovim algoritmom.