2. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 3. september 2010

1. (20 točk) Na primeru pokažite, da Vernamova šifra nima lastnosti popolne tajnosti, če ključ dolžine n uporabimo dvakrat na sporočilu dolžine $2n$.

2. (25 točk) Anita in Bojan bi se rada dogovorila za skupen ključ po ne-varnem kanalu s pomočjo Diffie-Hellmanovega algoritma. Izbrala sta praštevilo $p = 227$ in bazo $g = 5$.

   (a) Preverite, da je g generator grupe $\mathbb{Z}_{227}^*$.

   (b) Anita je izbrala naključno število $a = 4$ in Bojanu poslala $A = g^a$. Bojan je izbral naključno število b in Aniti poslal $B = g^b = 200$. Izračunajte skupni ključ!

3. (30 točk) Bojanov javni ključ za sistem RSA je (n, e), kjer je $n = 899$ in $e = 23$.

   (a) Poiščite dekodirni eksponent d (pri predpostavki, da poznate razcep števila n, $n = 29 \cdot 31$).

   (b) Ali bi Bojan za kodirni eksponent lahko izbral sodo število, na primer $e = 4$?

   (c) Bojan pošlje svoj javni ključ Aniti po elektronski pošti. Oskar pismo prestreže, spremeni kodirni eksponent e v $e' = 17$ in pismo posreduje Aniti. Anita zašifrira besedilo b s ključem (n, e') in ga pošlje Bojanu. Bojan sporočila seveda ne more razvozlati in zopet pošlje Aniti svoj javni ključ. Anita še enkrat zašifrira sporočilo b, tokrat s ključem (n, e) in ga pošlje Bojanu. Oskar je prestregel obe Anitini pismi. Natančno opišite, kako lahko izračuna besedilo b (pri predpostavki, da ne pozna razcepa števila n oziroma dekodirnega eksponenta d).

4. (25 točk) Naj bo $\mathcal{C}$ dvojiški linearen kod z generatorsko matriko

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

   Poiščite generatorsko matriko za $\mathcal{C}$ v standardni obliki. Poiščite nadzorno matriko za kod $\mathcal{C}$. Kolikšna je razdalja koda $\mathcal{C}$? Koliko napak lahko popravi? Ali je kod $\mathcal{C}$ cikličen?

Vse odgovore je potrebno ustrezno utemeljiti!