3. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 16. september 2010

1. (20 točk) Poiščite linearno rekurzivno šifro najmanjše stopnje, ki generira izhodno zaporedje $(1101001)^\infty$. Poiščite linearno rekurzivno šifro najmanjše stopnje, ki generira izhodno zaporedje $(0110110)^\infty$.

2. (20 točk) Naj bo $\mathcal{S} = (\mathbb{Z}_2^{128}, \mathbb{Z}_2^{128}, \mathbb{Z}_2^{128}, \mathcal{E}, \mathcal{D})$ nek "dober" simetričen kriptosistem. Z E_k označimo kodirno funkcijo, ki uporablja ključ k. Sedaj definiramo zgoščevalno funkcijo, ki poljubnemu besedilu $b = (b_1, \ldots, b_n)$ priredi izvleček $h = E_{b_1}(IV) \oplus \ldots \oplus E_{b_n}(IV)$, kjer je IV nek vnaprej izbrani element $\mathbb{Z}_2^{128}$.

   Katere od lastnosti naslednjih ima takšna zgoščevalna funkcija: odpornost praslik, odpornost drugih praslik, odpornost na trke?

3. (30 točk) V velikem podjetju želijo zagotoviti, da bosta vsak dokument digitalno podpisala dva verodostojna uslužbenca (Anita in Bojan), eden za drugim. Podpis je veljaven le, če dokument podpišeta oba. V ta namen so prilagodili podpis s pomočjo RSA: zasebna ključa Anite in Bojana sta (n, a) oziroma (n, b), kjer je $n = p \cdot q$ produkt dveh velikih praštevil in a, b tuji s $\varphi(n)$. Javni ključ za preverjanje podpisa je (n, e), kjer je e izbran tako, da velja $a \cdot b \cdot e \equiv 1 \pmod{\varphi(n)}$. Besedilo m najprej podpiše Anita, ki izračuna $s_1 = m^a \pmod{n}$, nato pa Bojan izračuna še $s = s_1^b \pmod{n}$. Digitalni podpis za besedilo m je potem s. Podpis s besedila m je veljaven, če je $s^e \equiv m \pmod{n}$. Da Anita ali Bojan ne bi sama generirala podpisov, vse ključe generira certifikatna agencija, ki jo imajo v podjetju, Anita in Bojan pa dobita le zasebne ključe.

   (a) Naj bo $m \in \mathbb{Z}_n^*$ besedilo. Preverite, da zgornja shema zadošča zahtevam za digitalni podpis.

   (b) Ali je vrstni red podpisovanja pomemben?

   (c) Naj bo $n = 17 \cdot 23$, $a = 9$ in $b = 15$. Izračunajte e in preverite, da je $s = 144$ veljaven podpis za besedilo $m = 100$.

   (d) Ali lahko Bojan s pomočjo javnega ključa in svojega zasebnega ključa (hitro) izračuna Anitin zasebni ključ (pri predpostavki, da ne pozna razcepa števila n)?

4. (30 točk) Pokažite, da množica vseh dvojiških vektorjev dolžine 8 s težo sode dolžine sestavlja linearen bločni kod. Poiščite generatorsko matriko in nadzorno matriko za ta kod. Kolikšna je njegova razdalja?

Vse odgovore je potrebno ustrezno utemeljiti!