1. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 16. april 2009

1. (20 točk) Naj bo $\mathcal{S} = (\mathcal{B}, \mathcal{CK}, \mathcal{E}, \mathcal{D})$ simetričen kriptosistem in naj bodo B, C in K takšne slučajne spremenljivke z zalogo vrednosti $\mathcal{B}, \mathcal{C}$ oziroma $\mathcal{K}$, da ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti. Predpostavimo še, da za vsako besedilo b in vsak kriptogram c velja $P[B = b] > 0$ oziroma $P[C = c] > 0$. Dokaži ali ovrzi.

   (a) Za vsaka $b, b' \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ velja

   $$P[B = b|C = c] = P[B = b'|C = c].$$

   (b) Za vsaka $b, b' \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ velja

   $$P[C = c|B = b] = P[C = c|B = b'].$$

2. (30 točk) Naj bo $GF(16)$ končni obseg, konstruiran z nerazcepnim polinomom $f(x) = x^4 + x + 1$. Simetrični kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ definiramo takole:

   $$\mathcal{B} = \mathcal{C} = \mathrm{GF}(16) \text{ in } \mathcal{K} = \mathrm{GF}(16)^*,$$

   za ključ $p \in \mathrm{GF}(q)^*$ je kodirna funkcija definirana kot

   $$E_p(b) = b \cdot p \pmod{f}.$$

   (a) Pokažite, da za tako definirano kodirno funkcijo vedno obstaja tudi dekodirna funkcija s potrebnimi lastnostmi, in jo opišite.

   (b) Za dani kodirni ključ $p(x) = x^2 + 1$ dekodirajte kriptogram $c(x) = x^3 + x + 1$.

3. (25 točk) Poiščite LFSR najmanjše stopnje, ki generira zaporedje 01000010. Predpostavite lahko, da je LFSR izbran tako, da ima čim daljšo periodo. Ali je rešitev enolično določena?

4. (25 točk) Bojan ima javni ključ za RSA enak (n, e), kjer je n dovolj velik, da ga ne moremo faktorizirati v doglednem času. Anita mora Bojanu poslati šifrirano sporočilo. Da si delo malo poenostavi, vsaki od črk priredi številko med 0 in 24 ($A \leftrightarrow 0,\ B \leftrightarrow 1, \ldots, \check{Z} \leftrightarrow 24$) in potem šifrira vsako črko posebej z Bojanovim javnim ključem.

   Opišite, kako lahko napadalec takšno sporočilo čim bolj učinkovito dešifrira, ne da bi faktoriziral n. Ilustrirajte napad na kriptogramu $1, 25, 49, 0$, pri čemer je Bojanov javni ključ enak$(55, 17)$.

Vse odgovore je potrebno ustrezno utemeljiti!