Druhý test z predmetu Základy kryptografie

22.11.2013

Na vypracovanie písomky máte 90 minút. Príklady vypracujte aj s postupom, aby bolo jasné, ako ste dané výsledky dostali. Na každom papieri na odovzdanie uveďte svoje meno a číslo z AIS. Zadanie si môžete nechať.

1. (2 body) Opíšte princíp konfúzie a princíp difúzie v zmysle Shannonovej teórie.

2. (3 body) Opíšte, ako prebieha šifrovanie a dešifrovanie vo feistelovskej šifre.

3. (5 bodov) Stručne popíšte algoritmus Rijndael. (AGP popisovať nemusíte)

4. (5 bodov) Uvažujme funkciu $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ danú predpisom:

$$f(x_1, x_2) = x_1 \oplus x_2 \oplus x_1 x_2$$

   Zistite, či je f balancovaná, či spĺňa kritérium SAC a vypočítajte jej nelinearitu (t.j. stupeň nelinearity).

5. (5 bodov) Uvažujme blokovú šifru (dĺžka bloku je 3 bity) s dvomi kľúčmi K_1 a K_2 fungujúcu nasledovne: Otvorený text sa najprv zoXORuje s kľúčom K_1. Na výsledok sa potom aplikuje permutácia $P : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$ daná nasledujúcou tabuľkou:

x	0	1	2	3	4	5	6	7
P(x)	1	2	3	4	5	6	7	0

   Výstup z permutácie sa nakoniec zoXORuje s kľúčom K_2 a takto dostaneme zašifrovaný text.

   (a) Pomocou takto definovanej šifry zašifrujte správu 101101 v móde CBC. Použite kľúče $K_1 = 001$, $K_2 = 010$ a inicializačný vektor 111.

   (b) Uvedená šifra nie je E/D podobná. Ak by sme ale v šifre nahradili permutáciu P inou vhodne zvolenou permutáciou $Q : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$, dosiahli by sme E/D podobnosť uvedenej šifry. Uveďte príklad takej permutácie Q a svoju voľbu zdôvodnite. (Ako príklad sa neuznáva identická permutácia $Q(x) = x$ $\forall x$.)

6. (Prémia za 3 body)
   Uvažujme vrece s 1 červenou a 3 modrými guličkami. Z vreca sa náhodne vytiahne 1 guličk a. Pravdepodobnosť, že vytiahneme konkrétnu guličku je rovnaká pre všetky guličky. Ak sa vytiahne červená guličk a, náhodná premenná X nadobudne hodnotu 1. Inak bude hodnota náhodnej premennej X rovná 0. Vypočítajte entropiu náhodnej premennej X. Koľko bitov informácie získame, ak sa dozvieme, že z vreca bola vytiahnutá červená guličk a? Koľko bitov informácie získame, ak sa dozvieme, že bola vytiahnutá guličk a modrej farby? Odpovede môžete ponechať v tvare s logaritmami, nemusíte ich vyčíslovať.