Skúška z predmetu Základy kryptografie

12.12.2014

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. Na prvú stranu tiež uveďte, koľko papierov odovzdávate. Zadanie si môžete nechať.

1. (14 bodov) Popíšte algoritmus Rijndael. (AGP popisovať nemusíte) Ako sa v algoritme Rijndael využíva aritmetika v poli $GF(2^8)$?

2. Uvažujme funkciu $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ danú nasledujúcou tabuľkou:

x_0	x_1	x_2	$f(x_0, x_1, x_2)$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	0
1	0	1	1
0	1	1	0
1	1	1	1

   (a) (4 body) Nájdite algebraickú normálnu formu funkcie f a určite jej nelineárny rád.

   (b) (4 body) Vypočítajte nelinearitu (t.j. stupeň nelinearity) funkcie f.

   (c) (2 body) Určite, či je funkcia f balancovaná.

   (d) (6 bodov) Zistite, či je funkcia f úplná a či spĺňa kritérium SAC.

   (e) (5 bodov) Predpokladajme, že vstupy do funkcie f sú rovnomerne náhodne rozdelené. Vypočítajte hodnotu $H(x_0|f(x_0, x_1, x_2))$.

   (Pozor, úlohy (b)-(e) môžete riešiť, aj keď neviete vyriešiť úlohu (a).)

3. 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)	2	3	4	5	6	7	0	1

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

   (a) (8 bodov) Pomocou takto definovanej šifry zašifrujte správu 101101 v móde OFB s dĺžkou bloku 3 bity. Použite kľúče $K_1 = 001$, $K_2 = 010$ a inicializačný vektor 111.

   (b) (2 body) 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 $Q(x) = x \ \forall x$.)

4. (5 bodov) Uvažujme nasledovný kryptosystém. Vstupom je dvojbitový blok M. Ten sa zašifruje prixorovaním dvojbitového kľúča K. Pre výsledný zašifrovaný blok C teda platí $C = M \oplus K$. Kľúč K je generovaný náhodne tak, že platí:

$$P(K = k_1k_0) = \begin{cases} \frac{1}{3} & \text{ak } k_1k_0 \neq 00 \\ 0 & \text{ak } k_1k_0 = 00 \end{cases}$$

   Predpokladajme, že vstupný blok je generovaný náhodne z rovnomerného rozdelenia. Určite hodnotu I(C;M). (Pozor, 0 nie je správna odpoveď!)