Skúška z predmetu Základy kryptografie

10.12.2015

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. Uvažujme funkciu $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ danú nasledujúcim predpisom:

$$f(x_0, x_1, x_2) = x_0 \oplus x_0x_2 \oplus x_1x_2$$

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

   (b) (5 bodov) Vypočítajte nelinearitu (t.j. stupeň nelinearity) funkcie f.

   (c) (7 bodov) Zistite, či je funkcia f úplná a či spĺňa kritérium SAC.

2. (12 bodov) Popíšte algoritmus Rijndael. Uveďte:

   - veľkosť bloku
   - veľkosť kľúča
   - počet kôl
   - ako vyzerá jedno kolo
   - ako vyzerá posledné kolo
   - ako sú reprezentované medzivýsledky v priebehu šifrovania

   AGP popisovať nemusíte.

3. (8 bodov) Uvažujme dvojkolovú feistalovskú šifru s veľkosťou bloku 6 bitov. V šifre sa používa funkcia $f : \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$, $f(\mathbf{x}, \mathbf{k}) = \mathbf{x} \oplus \mathbf{k}$. Pomocou takto definovanej šifry zašifrujte správu 101101. Použite kľúče $K_1 = 001$ a $K_2 = 010$.

4. 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	0	3	2	5	4	7	6

   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 CFB s dĺžkou bloku 3 bity. Použite kľúče $K_1 = 001$, $K_2 = 010$ a inicializačný vektor 111.

   (b) (8 bodov) Obdržali ste zašifrovanú správu 101101. O správe viete, že bola zašifrovaná hore uvedenou šifrou v móde CBC. Tiež viete, že boli použité kľúče $K_1 = 001$, $K_2 = 010$ a inicializačný vektor 111. Dešifrujte správu.