Druhý test z predmetu Základy kryptografie

8.11.2017

Inštrukcie:

- 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, číslo z AIS a meno fakulty, ktorú navštevujete (FEI alebo FIIT). Na prvú stranu tiež uveďte, koľko papierov odovzdávate.
- Zadanie si môžete nechať.

Úlohy:

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

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
1	0	0	1
0	1	0	0
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) (1 bod) Určite, či je funkcia f balancovaná.
   (d) (4 body) Zistite, či je funkcia f úplná a či spĺňa kritérium SAC.

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

2. Uvažujme dvojkolovú feistalovskú šifru s veľkosťou bloku 6 bitov. V šifre sa používa funkcia $f : \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$, $f(\mathbf{x}, \mathbf{K}) = \mathbf{x} \oplus \mathbf{K}$.

   (a) (4 body) Pomocou takto definovanej šifry zašifrujte správu 101101101101 v móde CBC. Použite sub-kľúče $\mathbf{K}_1 = 001$, $\mathbf{K}_2 = 010$ a inicializačný vektor 111111.
   (b) (4 body) Zašifrovanú správu z prvej časti následne dešifrujte.

3. (a) (1 bod) Čo znamená, že šifra je perfektne bezpečná?
   (b) (1 bod) Uveďte tvrdenie Shannonovej pesimistickej vety.
   (c) (2 body) Popíšte Vernamovu šifru. Ako súvisí Vernamova šifra so Shannonovou pesimistickou vetou?

4. (Prémia 1) Nech X, Y sú náhodné premenné s pravdepodobnostným rozdelením daným nasledujúcou tabuľkou:

P(X=x,Y=y)	X=0	X=1
Y=0	1/5	1/5
Y=1	1/5	2/5

   (a) (1 bod) Vypočítajte H(Y).
   (b) (1 bod) Vypočítajte H(X,Y).
   (c) (1 bod) Vypočítajte H(X/Y).

5. (Prémia 2) (2 body) Vypočítajte nelinearitu funkcie z príkladu 1 pomocou Walsh-Hadamardovej transformácie. Využite, že pre nelinearitu funkcie f platí $N_f = min_{u \in Z_2^n} \frac{1}{2}\{2^n \pm \hat{f}(u)\}$, kde $\hat{f}$ je definovaná vzťahom $\hat{f}(u) = \sum_{v \in Z_2^n} (-1)^{u.v+f(v)}, \quad u \in Z_2^n$.