Skúška z predmetu Základy kryptografie

14.12.2016

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.

Úlohy:

1. 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	0
0	1	0	1
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	1

   (a) (6 bodov) Nájdite algebraickú normálnu formu funkcie f a určite jej nelineárny rád.
   (b) (8 bodov) Vypočítajte nelinearitu (t.j. stupeň nelinearity) funkcie f.
   (c) (1 bod) Určite, či je funkcia f balancovaná.
   (d) (7 bodov) Zistite, či je funkcia f úplná a či spĺňa kritérium SAC.

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

2. (10 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 101101101101 v móde OFB. Použite sub-kľúče $K_1 = 001$, $K_2 = 010$ a inicializačný vektor 111111.

3. Uvažujte E/D podobný šifrátor IV. typu, kde

   - počet kôl je 2;
   - šifrujú sa vstupy $x \in (Z_8, +)$;
   - involučná funkcia I je daná predpisom $I(x, k) = x \oplus k \oplus 010$ (prvky zo Z_8 tu reprezentujeme binárne);
   - involutórna permutácia P_I je daná predpisom $P_I(x) = 3x \bmod 8$
   - kľúče sú postupne $4, 5, 3, 1, 2$.

   (a) (2 body) Nakreslite schému šifrovania.
   (b) (2 body) Uvedeným šifrátorom zašifrujte správu $x = 7$.
   (c) (5 bodov) Zašifrovanú správu následne uvedeným šifrátorom dešifrujte.

4. Porovnajte šifrátory DES a GOST:

   (a) (2 body) AGP
   (b) (2 body) S-box
   (c) (1 bod) počet kôl
   (d) (4 body) načrtnite schémy

5. (Prémia) Nech X, Y, N, E sú náhodné premenné reprezentujúce otvorený text, zašifrovaný text, modulus a šifrovací exponent v kryptosystéme RSA 2048.

   (a) (2 body) Aká je entropia H(Y/N,E,X)? Oddôvodnite.
   (b) (2 body) Aká je entropia H(X/N,E,Y)? Oddôvodnite.