Prvý test z predmetu Základy kryptografie

25.10.2013

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. (2body) Použite Euklidov algoritmus na nájdenie multiplikatívne inverzného prvku k 6 v $\mathbb{Z}_{13}$.
2. (2body) Nájdite všetky celočíselné riešenia kongruencie $16x \equiv 24 \pmod{88}$ z intervalu $[0, 88]$.
3. (2body) Nájdite riešenie sústavy:

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

   v intervale $[0, 140)$.
4. (3body) Nájdite všetky celočíselné riešenia kongruencie $x^2 \equiv 1 \pmod{77}$ z intervalu $[0, 77)$.
5. (2body) Nájdite najmenšie kladné celé číslo n také, že pre každé nepárne číslo a platí:

$$a^n \equiv 1 \pmod{128}$$

   Svoju odpoveď zdôvodnite.
6. (2body) Nech $M = \{0, 1, \ldots, 26\}$. Nech $a, b \in M$. Definujme funkciu $\alpha : M \to M$ nasledujúcim predpisom:

$$\alpha(x) = ax + b \pmod{27}$$

   Akú podmienku musí spĺňať a, aby bola funkcia α permutáciou? Ako v takom prípade vyzerá inverzná permutácia?
7. (2body) Definujte, čo je jeden bit informácií. Koľko bitov informácií získame, ak sa dozvieme, že pri hode dvoma kockami padol súčet 4 ?
8. (5bodov) Nech M je n-bitová otvorená správa. Správu zašifrujeme pomocou Vernamovej šifry. Zašifrovaný text označíme ako C a kľúč označíme ako K. Nakreslite schému dávajúcu do súvisu $H(M)$, $H(C)$, $H(K)$, $H(M/K, C)$ atď. a určte hodnoty všetkých oblastí v schéme. Aká je hodnota $I(C; K)$?