FMI, Anul III
Elemente de securitate şi logică aplicată

Examen

Nume: _____

Prenume: _____

Grupa: _____

Modulul 3: Teoria Complexitatii si Criptografie

(P1) [1 punct] Intr-o tara sunt 4.000.000 de angajati iar salariul mediu lunar este de 1.000 euro. Sa se arate ca numarul angajatilor care castiga cel putin 4.000 de euro pe luna este strict mai mic decat 1.000.000.

(P2) [1 punct] Sa presupunem ca pentru orice sistem determinist de criptare (Enc, Dec) in timp polinomial in lungimea inputului (x, k), se intampla urmatorul lucru. Pentru orice algoritm determinist A in timp polinomial, si pentru orice pereche de mesaje $x_0, x_1 \in \{0,1\}^m$, cu $x_0 \neq x_1$:

$$Pr[A(Enc_k(x_b)) = b] < \frac{3}{4},$$

unde probabilitatea se calculeaza relativ la toti $b \in \{0,1\}$ si toate cheile $k \in \{0,1\}^n$.

1. Ce concluzie se poate trage despre existenta unor algoritmi deterministi care opresc in timp polinomial in lungimea inputului si decid satisfiabilitatea formulelor din logica propozitionala?

2. Ce concluzie se poate trage despre existenta unor algoritmi deterministi care opresc in timp polinomial in lungimea inputului si pentru inputul $x = pq$, unde p si q sunt numere prime, calculeaza $\min(p, q)$?