Elemente de Securitate si Logica Aplicata, modulul 1

3 martie 2023

1. Fie COMP multimea acelor cuvinte $w \in \{0,1\}^*$ care incep cu litera 1 si reprezinta binar numere naturale compuse. Un numar natural n se numeste compus daca exista $x, y \in \mathbb{N}$ astfel incat $n = (x+2)(y+2)$.

   (a) Folosind definitia, aratati ca multimea COMP este in NP.

   (b) Folosind un rezultat de la curs, aratati ca multimea COMP este in P.

2. Pe planeta Mondoshiva se folosesc diferite sisteme de codare, criptare, transmisie, etc. O divizie ultrasecreta a SIE a facut un stagiu pe Mondoshiva si a luat cunostiinta de un singur sistem mondoshivan de criptare, numit Leeloo.

   - Leeloo este un sistem de criptare simetric si determinist. Determinismul inseamna ca $c = Enc_k(m)$ are aceeasi valoare de fiecare data cand este calculat.

   - Mesajele clare, mesajele criptate si cheile sunt cuvinte din $\{0,1\}^*$.

   - Cheile au o lungime fixa j, iar valoarea lui j este cunoscuta de SIE.

   - Lungimea mesajului criptat este intotdeauna egala cu lungimea mesajului clar, si poate fi orice numar natural.

   SIE stie ca la un moment dat un mafiot galactic de pe Mondoshiva ii va trimite magnatului pamantean Jean-Baptiste Emanuel Zorg semnalul 0^n si ca semnalul va fi transmis criptat. SIE cunoaste numarul n si constata ca $n > j$. Azi SIE a depistat un mesaj criptat de lungime n de pe Mondoshiva, iar din alte surse stie ca acesta este semnalul pentru Zorg. Fie p probabilitatea ca semnalul sa NU fi fost criptat cu Leeloo, ci cu un alt sistem mondoshivan de criptare, pe care SIE nici nu-l cunoaste.

   Aratati ca:

$$p \geq 1 - \frac{1}{2^{n-j}}$$