Elemente de Securitate si Logica Aplicata, modulul 3

25 martie 2022

1. Trei zaruri corecte A, B, C sunt marcate in urmatorul mod:

$$\begin{aligned} A &= \{1,2,5,6,7,9\} \\ B &= \{1,3,4,5,8,9\} \\ C &= \{2,3,4,6,7,8\} \end{aligned}$$

   (a) Aratati ca:
$$Pr[\,A > B\,] = Pr[\,B > C\,] = Pr[\,C > A\,]$$

   (b) Aratati ca:
$$Pr[\,A = B\,] = Pr[\,B = C\,] = Pr[\,C = A\,]$$

2. Pentru $m \geq 2$ se considera urmatoarea criptare One Time Pad. Mesajele x si cheile k sunt siruri de elemente din $\mathbb{Z}_m$ de lungime n. Considerand adunarea si scaderea pe litere,

$$Enc_k(x) = x + k,$$

$$Dec_k(y) = y - k.$$

   Printr-o bresa de securitate, adversarul obtine textul $c = Enc_k(k)$.

   (a) Pentru $t \geq 1$ aratati ca elementul 2 este multiplicativ inversabil in inelele $\mathbb{Z}_{2t+1}$ dar nu este multiplicativ inversabil in inelele $\mathbb{Z}_{2t}$. ($\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ iar operatiile sunt modulo m)

   (b) Pentru $m = 2t + 1$ dati un algoritm determinist in timp polinomial care primeste c si calculeaza cheia k.

   (c) Pentru $m = 2t$, dati un algoritm probabilist in timp polinomial care primeste c si calculeaza cheia k cu probabilitate $1/2^n$.