Coduri şi Criptografie (2012–2013)
Prof.dr. F. L. Ţiplea
Lect.dr. S. Iftene
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 7.02.2013

Examen [1]

1. Fie $\mathcal{S} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ criptosistemul dat prin:
   - $\mathcal{P} = \{a, b\}$;
   - $\mathcal{C} = \{1, 2, 3, 4\}$;
   - $\mathcal{K} = \{K_1, K_2, K_3\}$;
   - $\mathcal{E}$ şi $\mathcal{D}$ sunt date în următorul tabel

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

   ($e_{K_1}(a) = 1$, $d_{K_2}(2) = a$ etc.).

   Considerăm distribuţiile de probabilitate:
   - $p_{\mathcal{P}}(a) = 1/4$, $p_{\mathcal{P}}(b) = 3/4$;
   - $p_{\mathcal{K}}(K_1) = 1/2$, $p_{\mathcal{K}}(K_2) = p_{\mathcal{K}}(K_3) = 1/4$.

   Determinaţi distribuţia de probabilitate $p_{\mathcal{C}}$ pe spaţiul $\mathcal{C}$. Asigură acest criptosistem secret perfect? **4p**

2. Construiţi structura de access asociată formulei booleene monotone

$$\varphi = (x_1 \wedge x_2) \vee ((x_3 \wedge x_4) \vee x_5)$$

2p

3. Fie Γ o structură de acces peste $U = \{1, 2, 3, 4, 5\}$ dată prin

$$\Gamma_0 = \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{4, 5\}, \{1, 2, 3\}, \{1, 3, 5\}\}.$$

   Construiţi circuitul boolean atasat si apoi o schemă de partajare perfectă care să realizeze Γ. Justificaţi răspunsul. **3p**

[1] Baza de notare: 1p