Tema 3

1. Verificaţi dacă următoarele sisteme de criptare sunt perfect sigure:

   (a) Cifrul Hill cu $n = 2$ şi $b = 0$ peste $\mathbb{Z}_2$ Pe spaţiul cheilor se consideră distribuţia uniformă, iar pe spaţiul textelor simple şi al celor criptate distribuţia probabilităţii este nenulă.

   (b) Se consideră $M = \mathbb{Z}_{26}^n = C$ iar $K = \mathbb{Z}_{26}$. Dacă $m = (m_1, \ldots, m_n) \in M$ atunci $E_k(m) = (m_1 + k, \ldots, m_n + k)$, mod 26, cu $k \in K$. Pe spaţiul cheilor se consideră distribuţia uniformă, iar pe spaţiul textelor simple şi al celor criptate distribuţia probabilităţii este nenulă.

2. Fie $M = \{0, 1\}$ spaţiul textelor simple, $K = \{A, B\}$ spaţiul cheilor, peste care sunt date probabilităţile: p_M definită prin $p_{_M}(0) = 1/4$, $p_{_M}(1) = 3/4$ şi p_K dată prin $p_{_K}(A) = 1/4$, $p_{_K}(B) = 3/4$. Fie $C = \{a, b\}$ spaţiul textelor cifrate. Funcţiile de cifrare sunt date prin
$$e_{_A}(0) = a, \;\; e_{_A}(1) = b, \;\; e_{_B}(0) = b, \;\; e_{_B}(1) = a.$$
   Calculaţi $p(\overline{0}|\overline{a})$ şi $p(\overline{0})$.

3. Alice observă că dacă un mesaj este criptat cu cifrul Vernam (One-Time Pad), folosind cheia nulă, mesajul este practic transmis în clar. Dorind o siguranţă şi mai mare, ea se gândeşte să definească cifrul Vernam fără cheia nulă. Este aceasta o idee bună? Explicaţi. Folosirea cheii nule poate fi considerată o slăbiciune a sistemului? Explicaţi.