Exerciţiul 1. *(5p)*

Fie $m = m_1 \dots m_k$ un mesaj format din k blocuri. Utilizând AES-128-CBC, construim criptotextul $c = c_0 c_1 \dots c_k$, unde:

- *$c_0 = iv$ (vectorul de iniţializare);*
- *c_i = blocul de criptotext corespunzător blocului m_i, pentru fiecare $i \in \{1, \dots, k\}$.*

Criptotextul c este transmis intre două noduri intr-o reţea, iar la destinaţie, un octet din c_0 este corupt (modificat).

Câţi octeţi din mesajul iniţial m vor fi corupţi la decriptarea mesajului? Argumentaţi.

Exerciţiul 2. *(5p)*

Fie $h : \{0,1,2,3\}^2 \times \{0,1,2,3\}^2 \times \{0,1,2,3\}^2 \to \{0,1,2,3\}^2$,
$h(x, y, z) = 3x + 2y + z$, unde:

- *$x = x_1 x_2$, $y = y_1 y_2$, $z = z_1 z_2$, cu $x_i, y_i, z_i \in \{0,1,2,3\}$;*
- *operaţia de adunare este definită astfel:*

  pentru $a = a_1 a_2$, $b = b_1 b_2$, $a + b = s_1 s_2$, unde

  $s_i = ((a_i + b_i) \bmod 4)$, pentru fiecare $i \in \{1, 2\}$.

De exemplu $h(01, 13, 21) = 3 \cdot 01 + 2 \cdot 13 + 21 = (01 + 01 + 01) + (13 + 13) + 21 = 03 + 22 + 21 = 02$.

Este funcţia h rezistentă la coliziuni? Argumentaţi.

Exerciţiul 3. *(5p)*

Considerăm un director myDir, deţinut de root, cu următoarele drepturi asociate:

$d\underbrace{rwx}_{u}\underbrace{--x}_{g}\underbrace{--x}_{o}$.

Care dintre următoarele comenzi pot fi executate cu succes de către un utilizator obişnuit (aflat in categoria others relativ la permisiunile asociate directorului myDir)?

a) `sudo setcap cap_dac_override=p /bin/ls; ls myDir`

b) `touch myDir/myFile` (`touch` *creează un fişier obişnuit cu numele specificat);*

c) `cd myDir`

d) `ls myDir/myExtraFile` *(presupunând că myExtraFile este un fişier obişnuit in directorul myDir).*

Alegeţi varianta/variantele corectă/corecte.

Exerciţiul 4. *(5p)*

Fie $Q = (S, O, A)$ o stare a matricii de control, $\mathcal{R} = \{r, w, x, o\}$ o mulţime de drepturi, unde:

- *$S = \{p, q\}$; $O = \{p, q, f, g\}$,*
- *matricea A este dată astfel:*

A	p	q	f	g
p	r, w, x	x	r, w	r, x
q	r	r, w, x, o	$-$	r, x

Se dă următoarea comandă:

```
command  spawn_process_file(X, Y, Z)   X, Y ∈ V_sub, Z ∈ V_obj
         if o in (X, X)
         if x in (X, Z)
         then
             create subject Y
             enter x into (Y, Z)
end
```

Explicaţi efectele aplicării comenzii `spawn_process_file(q, s, g)`.

Exerciţiul 5 (TG 2)**.** *(5p)*

Se dă următorul graf Take-Grant (Figura 1):

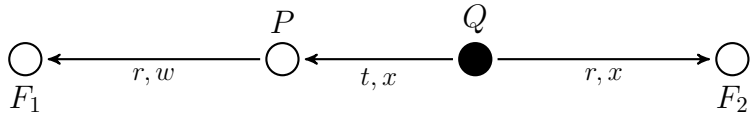

Figure 1: Graf Take-Grant

Scrieţi toate regulile de tranziţie necesare pentru a crea un nou subiect S, care să obţină dreptul w asupra lui F_1.

Observaţie*: scrieţi regulile de tranziţie necesare, numerotate, şi desenaţi un singur graf Take-Grant, pe care arătaţi aplicarea regulilor prin etichetarea arcelor după următorul model:* `număr_regulă_aplicată : drepturi_arc`.