1. Explicati ce se intelege prin coliziune pentru o functie hash. Exista functii hash fara coliziuni? Argumentati raspunsul.

2. Care este diferenta dintre o functie hash si o functie de criptare.#

3. Ce informatii poate oferi modul de criptare ECB unui hacker? Dintre modurile de criptare CFB si OFB pe care l-ati alege. Argumentati.

4. a. Explicati urmatoarele setari (drepturi) pentru programul "passwd"

```
-rwsr-xr-x 1 root root 30768  Sep 22  2019 /usr/bin/passwd
```

b. Explicati cum verificati daca programul "passwd" are bitul SUID setat.
c. Daca nu, cum il setati?
d. Explicati urmatoarele setari pentru fisierul "shadow":

```
-rwxr-sr-x 1 root shadow 54968 Sep 25  2019
```

5. Se da urmatorul sistem de protectie C = {α0, α1, α2}, unde

```
command α0(X,Y)    //X, Y ∈ S
        if e in (X,Y) then
         enter t into (X,Y)
end α0

command α1(X, Y, Z) // X, Y∈ S,  Z ∈ S∪O
        if t in (X,Y)  and r in (Y, Z) then
         enter r into (X,Z)
end α1

command α2(X, Y, Z)  // X, Y∈ S,  Z ∈ S∪O
         if t in (X,Y)  and t in (Y, Z) then
         enter t into (X,Z)
end α2
```

Se considera starea Q = {S, O, A} unde S = {p_1, p_2, p_3}, O = {p_1, p_2, p_3, f_1 , f_2 } si A este matricea de control al accesului definita prin:

A	p_1	p_2	p_3	f_1	f_2
p_1	-	e	-	-	r, w
p_2	-	-	e	-	-
p_3	-	o	-	r, w	-

Este starea Q sigura pentru dreptul r relativ la sistemul de protectie C? Justificati.