Laboratorul 8

1

1. A (nu putem recupera ingredientele daca descompunem prajitura)
2. F (exista posibilitatea de a crea coliziuni la cerere
3. A
4. A
5. F(nu avem o cheie de criptare)
6. F (un atacator poate incerca multe variante)
7. F (parola123)

3

1. Daca dorim sa verificam parola, nu stim carui utilizator ii corespunde
2. Username-ul trebuie retinut in text clar
3. Ar trebui sa se adauge salt la hash-uirea parolelor
4. Se foloseste acelasi salt pentru toate parolele
5. Se foloseste md5 care nu este sigur pentru stocarea parolelor