Question 1 : À part une société de télécommunication, qu’est-ce que le ‘salt’ ajouté à un mot de passe et à quoi sert-il ?

Question 2 : Donner 1 exemple de mot de passe

1. Cracké instantanément
2. Cracké en quelque minutes / heures
3. Cracké en plusieurs années

Question 3 : Un mot de passe peut être hashé ou crypté. Quelle est la différence et comment peut-on dans les deux cas récupérer le mot de passe initial si cela est possible ?

Question 4 : Démontrez mathématiquement qu’un mot de passe composé de majuscules, minuscules, chiffres ainsi que les caractères spéciaux # ;! et d’une longueur de 12 symboles ne sera cassé qu’après plusieurs années avec une architecture multi-gpu (4x) et « ocl-hashcat-plus » pouvant tester 20'000 mot de passe à la seconde.

Réponse 1 : Il ajout des caractères en plus dans le mot de passe. EX : mdp-> admin, mdp+salt->admin12345.  
ça permet de sécuriser les mots de passe des utilisateurs s’il sont interceptés.

Réponse 2 :

1. 123456789
2. 11111111111111111111111
3. M0nmO7D3P@$s3E$t¢hi4NT

Réponse 3 :   
Crypté : les données cryptées peuvent être décrypter, les mdp crypter ne changer pas.  
Hashé : On ne peut pas récupérer un mdp depuis un hashage, chaque hash est unique et il est différant si on hash 2 fois un même mdp.

Réponse 4 :

Majuscule = 26  
Minuscule = 26  
Chiffre = 10  
Caractère spéciaux = 3  
65^12 = 5.688009063 \* 10^21  
5.688009063 \* 10^21 / 20'000 = 2.844004532 \* 10^17 seconde  
2.844004532 \* 10^17 seconde = 9’018’279’210 années