Les fonctions de hachage

Les fonctions de hachage sont souvent utilisés pour chiffrer les mots de passe d'un site web avant de les sauver en base. Un haché ne doit pas pouvoir être déchiffré. En tant qu'étudiant de deuxième année en BUT informatique à l'IUT du Limousin, vous devez étudier quelques propriété des fonctions de hachage.

Rendez-vous sur le site : https://passwordsgenerator.net/sha1-hash-generator/ ou trouvez un générateur sha1.

Ecrivez lettre par lettre le message suivant « Unilim ». Que pouvez-vous observer sur la longueur du haché ?

A présent, nous allons changez le mot « Unilim » par « unilim ». Que constatez-vous sur l'ensemble du haché alors que nous avons seulement modifié une lettre ?

Il y a longtemps, vous vous êtes inscrit sur un site web, cependant vous vous souvenez plus de votre mot de passe. Le site vous pose la question secrète à laquelle vous avez répondu en vous inscrivant : « Quel est le nom de votre Avengers préféré ? ». Vous connaissez également le haché (sha1) de la réponse : B750BF91C273E4F3DDB4F320D7202FE3EC31F456. Retrouvez la réponse à la question. Pourquoi cette question secrète n'est pas pertinente ?

Chiffrement par substitution

Vous êtes à présent doctorant à l'institut XLim. Votre directeur de recherche vient de recevoir un appel du musée de la résistance de Limoges. Alors que l'équipe du musée faisait du rangement dans le sous-sol. Ils ont retrouvé un morceau de papier avec un cryptogramme dessus. Votre directeur de recherche vous proposes de résoudre cette énigme. Il vous précises que selon lui, il s'agirait d'une méthode de substitution, chaque lettre correspond à une autre et cela de manière arbitraire. Retrouvez la correspondance de chaque lettre en complétant le programme fournis.

Exemple de la méthode de substitution : A => C ; B => H ; …

RZCCB PBRPBNR BFDNK KIQ YFJKPYOBT, KJBR TZF RZNDBUB O'BQKPDKDYZF OKFT PB TZPBYP O'KGNYVIB, BFDNB YRY, MBKF CZIPYF, KJBR DZF DBNNYLPB RZNDBUB. KJBR RBIQ VIY TZFD CZNDT OKFT PBT RKJBT TKFT KJZYN XKNPB, RZCCB DZY, BD CBCB, RB VIY BTD XBID-BDNB XPIT KDNZRB, BF KWKFD XKNPB.

Aide : La longueur des mots, le contexte de la trouvaille et la fréquence d'apparition de certaines lettres peuvent vous être utile