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 ?

La longueur du haché ne change pas, peu importe la longueur de l'entrée de la fonction.

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 ?

Le fait de changer une lettre ne change pas une partie du haché mais l'entièreté

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 ?

Le nom de l'Avengers est Thor (attention à la majuscule). L'ensemble de départ disponible est trop petit, donc facile à deviner

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 ; …

> *Comme Leclerc entra aux Invalides, avec son cortège d'exaltation dans le soleil d'Afrique, entre ici, Jean Moulin, avec ton terrible cortège. Avec ceux qui sont morts dans les caves sans avoir parlé, comme toi, et même, ce qui est peut-être plus atroce, en ayant parlé.*

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

A	K	G	U	M	C	S	T	Y	W
B	L	H	A	N	F	T	D	Z	E
C	R	I	Y	O	Z	U	I		
D	O	J	M	P	X	V	J		
E	B	K	S	Q	V	W	H		
F	G	L	P	R	N	X	Q		