Sécurité par mot de passe

Durée : 2 heures

L'objectif de ce sujet est d'étudier certains aspects liés à la sécurité de l'accès par mot de passe à un espace client d'une entreprise.

Partie I. Bases de données

On considère une entreprise qui vend des produits par Internet. On suppose que cette entreprise stocke des informations sous la forme d'une base de données, contenant notamment deux tables, appelées respectivement `client` (chaque enregistrement de cette table représentant un client) et `vente` (chaque enregistrement de cette table représentant une vente).
La table `client` comporte, entre autres, comme attributs :

- `Idclient`, clé primaire, qui est un entier, représentant l'identifiant du client ;
- `Mdp`, qui est une chaîne de caractères, représentant le mot de passe du client permettant d'accéder à son espace client ;
- `Mail`, qui est une chaîne de caractères, correspondant à l'adresse mail du client ;
- `Adresse`, chaîne de caractère, représentant l'adresse postale du client ;
- `Pays`, chaîne de caractères qui représente le pays où vit le client (FR pour France, BE pour Belgique, LU pour Luxembourg, CH pour Suisse, ...).

Quant à la table `vente`, elle contient, entre autres, les attributs :

- `Idvente`, clé primaire, qui est un entier représentant l'identifiant de l'achat effectué ;
- `Client`, qui représente l'identifiant du client ayant effectué l'achat ;
- `Idproduit`, qui est un entier, et qui représente la référence du produit acheté ;
- `Annee`, qui est un entier, qui représente l'année d'achat du produit ;
- `Prix`, qui est un flottant, et qui représente le montant en euros correspondant à l'achat du produit considéré.

Question 1. Pour des raisons de calcul des frais de livraison, l'entreprise souhaite avoir la liste des clients habitants en Suisse. Écrire une requête SQL permettant de connaître les identifiants des clients concernés.

Question 2. Pour gérer ses stocks et commandes aux fournisseurs, l'entreprise souhaite connaître, pour chaque produit, le nombre de fois où il a été vendu. Écrire une requête SQL permettant d'avoir accès à cette information.

Question 3. L'entreprise souhaite contacter, afin de les récompenser, ses meilleurs clients de l'année, la « qualité » d'un client se mesurant à la somme totale qu'il a dépensée sur le site lors de l'année 2024.
Écrire une requête SQL permettant d'avoir les adresses mail et les sommes dépensées des dix meilleurs clients en 2024.

Question 4. Écrire une requête SQL permettant d'avoir les adresses mail et les sommes dépensées des clients ayant dépensé plus de 100€ sur le site Internet au cours de l'année 2024.

Question 5. L'entreprise souhaite connaître tous les clients qui sont dans leur base, mais qui n'ont effectué aucun achat en 2024. Écrire une requête SQL permettant d'avoir accès aux identifiants de ces personnes.

Question 6. Parfois, quand plusieurs personnes d'un même foyer souhaitent effectuer des achats, il arrive qu'ils renseignent la même adresse mail. L'entreprise souhaite connaître ces doublons. Écrire une requête SQL permettant d'obtenir les couples d'identifiants de clients différents ayant pourtant la même adresse mail dans la base de données.

Partie II. Conversion de données

L'identifiant d'un client, est, la plupart du temps, une chaîne de caractères. Or comme dans la partie I, il arrive qu'on souhaite que les identifiants clients soient stockés sous forme d'entiers. Pour cela, on souhaite pouvoir convertir de façon bijective une chaîne de caractères en un entier et réciproquement. Pour cela, il existe (entre autres) le code ASCII : le principe est d'associer à un caractère d'une liste prédéfinie regroupant les caractères les plus courants, un unique entier entre 0 et 127. Pour connaître le code correspondant à un caractère c, en Python, on utilisera la commande `ord(c)`. Par exemple, `ord('R')` renvoie l'entier `82`.
Réciproquement, étant donné un entier n entre 0 et 127, pour connaître le caractère correspondant, on utilise la commande `chr(n)`. Par exemple, `chr(82)` renvoie `'R'`.
Notons $\varphi : \mathrm{C} \mapsto [\![0, 127]\!]$ l'application qui à un caractère, associe son code ASCII.

Question 7. Écrire une fonction Python `str2int` d'argument une chaîne de caractères `s` constituée des caractères $c_0, \ldots, c_{n-1}$ et qui renvoie l'entier $\displaystyle\sum_{k=0}^{n-1} \varphi(c_k) \times 128^k$.

Question 8. Écrire une fonction Python `int2str` d'argument un entier, qui réalise l'opération réciproque à celle de la question précédente, et renvoie donc une chaîne de caractères.

Question 9. Il est couramment admis qu'un bon mot de passe comporte au minimum douze caractères comprenant au moins une majuscule (code ASCII compris entre 65 et 90), une minuscule (code ASCII compris entre 97 et 122), un chiffre (code ASCII compris entre 48 et 57) et un caractère spécial (code ASCII compris entre 33 et 47).

Rédiger une fonction Python `conforme(mdp)` qui prend en argument une chaîne de caractères `mdp` (le mot de passe choisi par le client) et renvoie le booléen `True` si ce dernier respecte les conditions ci-dessus, et `False` sinon.

Partie III. Une fonction de hachage cryptographique

Question 10. Expliquez les problèmes de sécurité que pourrait poser le stockage de l'attribut `Mdp` dans la table `client` de la base de données de la partie I.

Pour pallier à ce problème, on souhaite disposer d'une fonction ψ, appelée *fonction de hachage cryptographique*, définie sur l'ensemble des chaînes de caractères, et à valeurs dans $[\![0, 2^{128} - 1]\!]$. Ainsi, au lieu de stocker un mot de passe s sous forme d'une chaîne de caractères, on stockera plutôt dans la base de données la valeur $\psi(s)$.

Question 11. Expliquez les propriétés attendues pour que la fonction ψ soit efficace du point de vue de la sécurité du stockage des mots de passe des différents clients.

On considère la fonction $\mathrm{H} : \mathbb{N} \to [\![0, 2^{128} - 1]\!]$ définie par le fait que si $z \in \mathbb{N}$ se décompose sous forme $z = x + 2^{64}y$ avec $x \in [\![0, 2^{64} - 1]\!]$, alors $\mathrm{H}(z) = \displaystyle\sum_{k=0}^{127} \Big(f^k(x) \bmod 2\Big) \times 2^k$, où $f : u \mapsto \left\lfloor \frac{(2y+3)u}{2} \right\rfloor \bmod 2^{128}$, et où les puissances de f sont à comprendre pour la loi de composition entre les applications.
Avec les notations de la partie II, un candidat pour la fonction ψ sera la fonction $\mathrm{H} \circ$ `str2int`.

Question 12. Écrire une fonction `encrypte(s)` prenant en argument une chaîne de caractères s et qui renvoie l'entier $\mathrm{H} \circ$ `str2int`(s).