**La protection des données à caractère personnel**

# Introduction à la cybersécurité

**🖉 Travail à faire**

**Q1.1** – Donner quelques exemples de données ou de systèmes informatiques qu’il faut protéger

Ce sont les données qui identifient ou peuvent etre utilisé afin d’identifier une personne spécifique

Nom, prénom, adresse postale, numéro de téléphone, adresee mail, numéro de sécurité sociale, coordonnées bancaires, informations médicales…

**Q1.2** – Donner quelques exemples de systèmes ou d’entreprises qui ont subi des piratages informatiques.

* Equifax en 2017 les données personnelles des clients ont été compromises (data breach)
* Yahoo en 2013, data breach
* Sony en 2014, data breach
* Rockstar games 2022, data breach
* Microsoft 2024, data breach
* (et cetera…)

Définition : la **cybersécurité**

C’est l’ensemble de pratique, technologies, processus mis en place afin de protéger les systèmes d’informations SI, les réseaux et les logiciels, contre les cybercriminels (ensemble d’acteurs malveillants).

Le but est d’assurer l’intégrité et la confidentialtié des données, et minimiser les risques d’attaques.

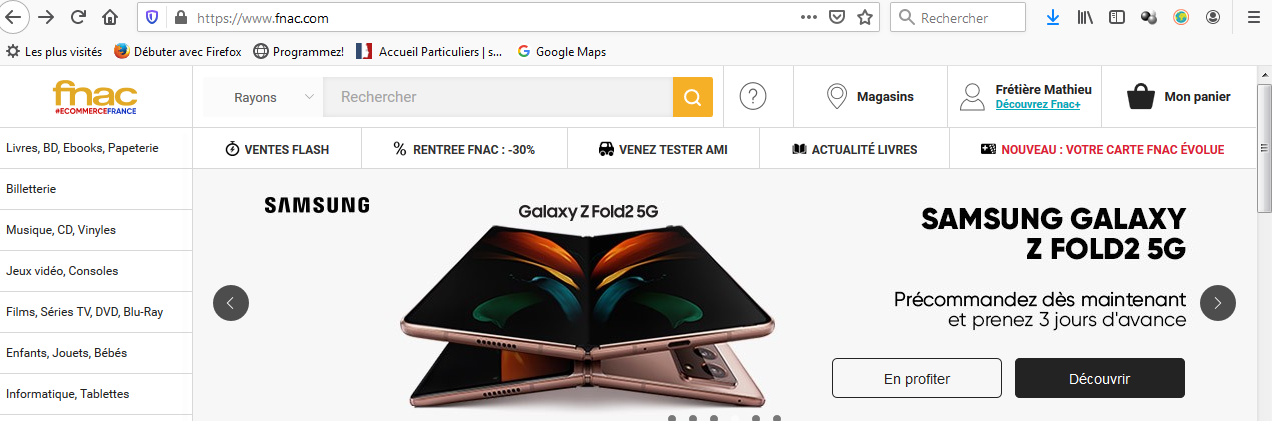
Exercice : la FNAC

## FNAC TernesPrésentation du contexte : la FNAC

La **Fnac** (appelée à l'origine « Fédération nationale d'achats des cadres ») est une chaîne de magasins française spécialisée dans la distribution de produits culturels (musique, littérature, cinéma, jeu vidéo) et électroniques (Hi-fi, informatique, télévision), à destination du grand public, dont la gamme s'est élargie en 2012 au petit électroménager. En 2016, la Fnac rachète Darty et prend le nom de Fnac Darty. (Source : Wikipedia.)

Fnac des Ternes à Paris

La Fnac possède plus de 230 magasins dans le monde et depuis plusieurs années elle fait du commerce en ligne sur le site internet fnac.com.



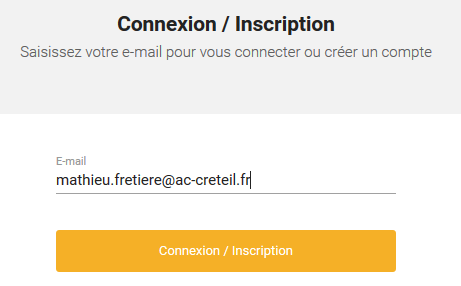
Extrait de la page d’accueil du site internet

## La création d’un compte Fnac par un internaute

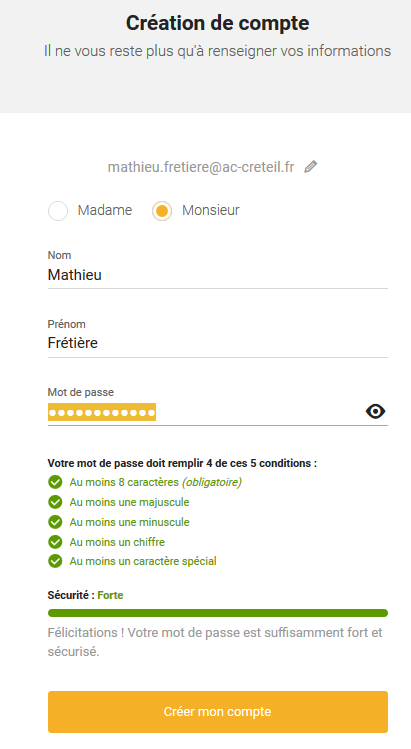
Lorsqu’un internaute arrive sur le site fnac.com il peut se créer un compte. Voici les différentes étapes de création d’un compte.

L’internaute clique sur le lien : 

Dans le formulaire de connexion/inscription il faut saisir son adresse de courriel (email) :



Il faut ensuite donner des renseignements personnels et choisir un mot de passe :



Le mot de passe saisi doit répondre à certaines exigences.

Il faut encore saisir d’autres renseignements :

|  |  |
| --- | --- |
|  |  |

Une fois qu’on est inscrit, le nom apparaît en haut de la page d’accueil :



**🖉 Travail à faire**

**Q2.1** - Le mot de passe saisi doit répondre à certaines exigences, citez les (au moins 5)?

* Le mot de passe doit être d’au moins 8 caractères, de préférences plus
* Le mot de passe doit etre complexe, composé de chiffres, lettres majuscules et miniscules, et de caractères spéciaux.
* Le mot doit de préférence etre ne pas avoir des mots courants qui sont en clair
* Le mot de passe doit etre renouveler régulièrement
* Avant de choisir le mot de passe il faut d’abord tester sa sécurité contre les attaques par force brute

**Q2.2** - Identifier les données personnelles qui sont collectées par le site web de la Fnac lors de la création de compte

Adresse email, genre, nom, prénom, mot de passe, statut (adhérent, professionnel), prénoms des enfant et leurs date de naissances, adresse postale, code postale, ville, numéro de téléphone

**Q2.3** – Pourquoi le mot de passe doit-il avoir une certaine complexité (voir l’image page précédente) ?

Un mot de passe plus long est plus sécurisé contre les attaques par force brute (tester tout les mots de passes possibles), ou les attaques par dictionnaire (on teste les pattern les plus fréquents que les gens utilisent en choisissnat leurs mots de passes)

Un mot de passe complexe a plus d’entropie (incertitude et désordre du mot de passe), ce qui le rend plus difficile à deviner ou à déterminer le mot de passe via les attaques malveillantes

Exemple de mot passe avec une grande entropie ! « F3{61@90#b2éd0&ec »

Une fois qu’il est inscrit, l’internaute reçoit par email le message suivant :

|  |  |
| --- | --- |
|  | Nous avons le plaisir de **vous confirmer que votre inscription sur Fnac.com a bien été prise en compte.**  Toute l’équipe Fnac.com est très heureuse de vous accueillir. Vous pouvez désormais commander, découvrir votre espace personnalisé, poster un avis, noter vos articles préférés... Bienvenue !  **Désormais pour vous connecter à** [**votre compte**](http://eultech.fnac.com/dynclick/fnac/?eml-publisher=Neolane&eml-name=70978647&eurl=http://fr.r.emails.fnac.com/r/?id=h2cce443f,632d7fcb,632d7fce&OriginClick=YES&Origin=mail_632d7fce&clientUid=1) **vous pouvez utiliser votre adresse email et votre mot de passe**  fleche-blanche-noire-20x20  [**Accedez à votre compte**](http://eultech.fnac.com/dynclick/fnac/?eml-publisher=Neolane&eml-name=70978647&eurl=http://fr.r.emails.fnac.com/r/?id=h2cce443f,632d7fcb,632d7fcf&OriginClick=YES&Origin=mail_632d7fcf&clientUid=1) |

L’internaute peut aussi s’insrire à la newsletter (lettre d’information) de Fnac et ainsi recevoir par email des informations sur les sujets qui l’intéressent, des promotions…

**🖉 Travail à faire**

**Q2.3** – Expliquer quel est l’intérêt pour l’internaute de créer un compte (plusieurs éléments à trouver).

Créer un compte à la Fnac rend tes achats en ligne plus sécurisés. Les informations personnelles sont cryptées avant d'être stockées dans la base de données, ce qui les protège contre les attaquants malveillants. de plus l’utilisateur est informé de toute anomalie ou de tout compromis de ses informations personnelles.

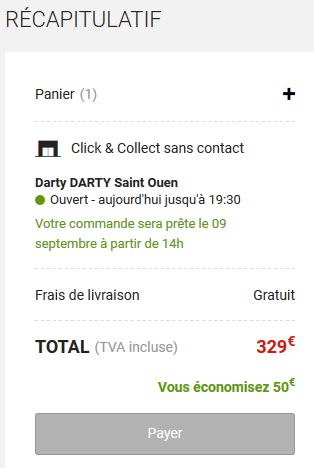
## Commande d’un produit en ligne

L’internaute qui s’est créé un compte décide de commander en ligne un smartphone Samsung Galaxy A51 :



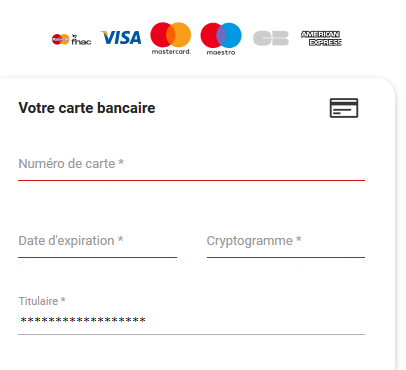
Il l’ajoute à son panier.

Comme l’internaute s’est connecté avec son compte Fnac, le site lui propose un retrait dans un magasin Darty proche de chez lui :



Adresse du magasin proche du domicile de l’internaute.

L’internaute n’a plus qu’à payer en saisissant les informations relatives à sa carte bleue :



**🖉 Travail à faire**

**Q2.4** – Quelles autres données personnelles sont fournies par l’internaute lors de la commande ?

Les coordonnées bancaires sont également fournies, le numéro de carte bancaire, la date d’expiration, le cryptogramme de 3 chiffres, et le nom du titulaire de la carte

**Q2.5** - Recenser les traitements faits avec toutes ces données personnelles par la Fnac

Adresse mail : envoi des mail de la newsletter (informations, nouveautés, promotions…)

Informations concernant les enfants : publicité personnalisé (prise en compte des anniversaires des enfants et prénoms dans les pub)

Adresse postale : déterminer les points de retraits les plus convenables

Coordonnées bancaires : traitement des paiements

**Q2.6** – Quel est l’intérêt pour la Fnac de collecter les données personnelles des internautes et des clients ?

La collecte des informations personnelles permet de personnaliser la publicité pour chaque utilisateur, de proposer des articles différents selon l’individu.

Les informations peuvent également être utilisé afin d’améliorer les services qui sont dèjà existants

Le but général est d’améliorer l’expérience de l’utilisateur

# - Les données à caractère personnel

## Notions importantes à retenir

**Données personnelles**

Ce sont les données qui identifie ou qui peuvent être utilisé pour identifier une personne spécifique, cela inclut des éléments tels que (le nom, l’adresse, le numéro de téléphone, l’adresse e-mail, le numéro de sécurité sociale…) ces données doivent etre protégés

**Traitements faits avec les données personnelles**

Ces données peuvent utilisés pour plusieurs fins, communication marketing (publicité, newletter, offres promotionnelles ciblées…) Personnalisation des services, traiter les transactions bancaires, et afin d’améliorer le service client. Les données personnelles peuvent également etre utilisé afin d’améliorer les clients des fraudes « scam » probables

## Exercice 2

**🖉 Travail à faire**

Dans le tableau suivant, pour chaque information collectée, indiquer s’il s’agit d’une information à caractère personnel et/ou commercial (en cochant les cases).

|  |  |  |  |
| --- | --- | --- | --- |
| **Information collectée** | **Information personnelle** | | **Information commerciale (ou autre)** |
|  | identifie **directement** | identifie **indirectement** |
| Prénom et nom du client | X |  |  |
| Adresse du client | x |  |  |
| Prix du produit « Apple MacBook Pro Touch Bar 16" » |  |  | X |
| Nombre de smartphones vendus ce mois-ci |  |  | X |
| Numéro de carte bleue | X |  |  |
| L’historique des achats de M. Dumont |  | X |  |
| Nombre d’acheteurs en ligne pour le mois courant |  |  | X |
| Chiffre d’affaires réalisé en août 2020 |  |  | X |
| Nombre de produits en stock |  |  | X |
| La date et l’heure de la dernière connexion de Mme Chadli |  | X |  |
| L’adresse IP d’un client |  | X |  |
| Les données de géolocalisation |  | X |  |
| Une empreinte digitale | X |  |  |

# Données sensibles

## Définition selon la Cnil

Les **données sensibles** forment une catégorie particulière des données personnelles.

Ce sont des informations qui révèlent la **prétendue origine raciale ou ethnique**, les **opinions politiques**, les **convictions religieuses ou philosophiques** ou **l'appartenance syndicale**, ainsi que le traitement des **données génétiques**, des **données biométriques** aux fins d'identifier une personne physique de manière unique, des données concernant la **santé** ou des **données concernant la vie sexuelle ou l'orientation sexuelle** d'une personne physique.

Le règlement européen interdit de recueillir ou d’utiliser ces données, sauf dans certains cas (la personne a donné son consentement, ou il y a un intérêt public, ...).

(source : CNIL - https://www.cnil.fr/fr/definition/donnee-sensible)

**Qu.4.1.1 –** Pourquoi faut-il faire particulièrement attention aux données sensibles ?

Ces informations révèlent des éléments intimes aux personnes, comme leur origine ethnique ou leurs opinions politiques. Si ces informations sont divulguées ou utilisées de façon incorrecte, cela peut porter atteinte à la vie privée et causer des problèmes graves pour les personnes concernées. Il est donc très important de respecter les règles de protection des données et de s'assurer qu'elles sont traitées en toute sécurité et de manière appropriée.

## https://www.axl.cefan.ulaval.ca/asie/images/liban-smap.gifExercice 3

**Exercice 3 - Les Libanais découvrent l’anonymat religieux**

(source : liberation.fr, 18 février 2009)

Les Libanais peuvent désormais supprimer ou s’abstenir de mentionner leur religion sur leur fiche d’état civil.

Dans un pays où l’on pouvait, durant la guerre civile (de 1975 à 1990), se faire exécuter par des miliciens à un barrage pour une simple mention sur sa carte d’identité, c’est un progrès important.

Il s’agit d’une décision symbolique dans un pays riche de 18 confessions, où la mention de l’appartenance religieuse est requise dans la plupart des formalités administratives. Les citoyens ont le choix entre garder la mention de leur confession, s’abstenir de l’enregistrer ou la supprimer de la fiche d’état civil. L’ONG Human Rights Watch, qui salue cette décision, demande la création d’un véritable statut personnel civil au Liban.

Pour l’instant, le mariage et l’héritage y demeurent régis par la confession des intéressés.

**Qu.4.2.1 –** Quelles données sensibles étaient mentionnées sur la carte d'identité libanaise avant 2009 ?

La donnée sensible dans ce contexte est la croyance religieuse

**Qu.4.2.2 –** Quels problèmes cela a-t-il posé, et pourrait poser encore ?

Les habitants du liban se font arreté à des barrages par maliciens où on contrôle leur carte d’identité afin de voir leur croyance religieuse, les personnes arretées peuvent etre exécutés pour leur croyance religieuse

Sécurité et sûreté

## Distinction entre la sécurité informatique et la sûreté

Définition – La **sécurité**

La sécurité est la protection contre les menaces et les dommages potentiels. C’est la protection des SI, des données et des informations contre les accès non autorisés et les risques tels que les attaques, les virus et le vol de données.

Définition – La **sûreté**

La sûreté est un concept plus large qui englobe la sécurité, mais elle met davantage l'accent sur la prévention des accidents, des dommages ou des événements indésirables.

## Exercice - Datacenter de Global switch

Le site web et la base de données de la Fnac sont hébergés sur un serveur qui se trouve dans un **centre de données** (**datacenter**) situé à Clichy (92).

|  |  |
| --- | --- |
| Salle de serveurs | Vue extérieure |

Ce datacenter appartient à la société Global switch qui loue des serveurs à différentes sociétés comme la Fnac. Global switch est responsable de la sécurité et de la sûreté de ses installations afin que les serveurs fonctionnent 24 h / 24, de manière normale.

Pour cela, de nombreux dispositifs équipent les salles des serveurs :

* un dispositif anti-incendie,
* une alimentation électrique redondante, c’est-à-dire une alimentation en double : s’il y a une panne de courant, ou un problème d’alimentation électrique, l’alimentation de secours prend le relais.
* une climatisation qui maintient les salles à une température optimale pour le fonctionnement des serveurs.

Les salles des serveurs sont situées aux étages pour se prémunir contre les inondations.

Des logiciels anti-virus performants sont installés sur les serveurs.

Il faut aussi assurer la maintenance des serveurs. Pour cela les informaticiens chargés de la maintenance utilisent un logiciel qui permet une prise de contrôle des serveurs à distance, en s’identifiant avec un login et un mot de passe.

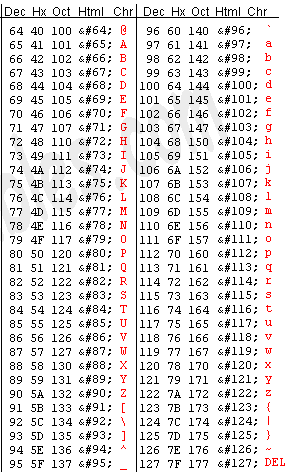
Mais pour certaines opérations de maintenance, comme le changement d’un disque dur en panne, il faut se rendre sur place. L’accès à la salle est règlementé et n’est permis qu’aux personnes autorisées.

Pencil-icon **Q.1.2.1** - A partir du texte, identifier les dispositifs qui relèvent de la sécurité et ceux qui relèvent de la sûreté.

|  |  |
| --- | --- |
| **sécurité** | **sûreté** |
| * Dispositif anti-incendie * Alimentation électrique redondante * Climatisation * Logiciels antivirus performants * Maintenance à distance avec identifiant et mot de passe | * Serveurs situés aux étages * Accès règlementé à la salle des serveurs |

1. **Principe du hachage**

**5.0 Donner la définition du hachage :**

Le hachage est un processus informatique qui transforme des données en une empreinte de taille fixe. Cette empreinte est unique. Le hachage permet la sécurité et l’intégrité des données

**Exercice 1 – Calcul d’empreintes avec un algorithme simple**

L’algorithme de hachage d’un mot que l’on va utiliser est le suivant :

il consiste à faire la somme de tous les codes ASCII (décimaux) des lettres d’un mot.

**Travail à faire :** calculer l’empreinte des mots suivants :

**Hello , Hellp, Hella**

Codes ASCII des lettres de l’alphabet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Mot** | **H** | **e** | **l** | **l** | **o** |  |
| code ASCII | 72 | 69 | 76 | 76 | 79 | Empreinte  (Total) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Mot** | **H** | **e** | **l** | **l** | **p** |  |
| code ASCII | 72 | 69 | 76 | 76 | 80 | Empreinte  (Total) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Mot** | **H** | **e** | **l** | **l** | **a** |  |
| code ASCII | 72 | 69 | 76 | 76 | 65 | Empreinte  (Total) |

**Q.1.1** – Est-ce qu’on obtient bien trois empreintes différentes ? . . .

Oui car le mots d’origine sont différents

**Q.1.2** – Est-ce qu’à partir de l’empreinte on peut retrouver le mot d’origine ? . . .

Oui, il suffit de remplacer les chiffres par les lettres correspondantes

1. **Un algorithme de hachage : SHA-2**

L’algorithme de hachage SHA-256 permet d’obtenir une empreinte de 256 bits.

**Exemples :**

|  |  |
| --- | --- |
| **Message** | **Empreinte SHA-256** |
| le renard court sur la glace | 3418d07f1c8b593990fe55308b05f1014d5dfae1fc074d1da50fc02633646779 |
| l**a** renard court sur la glace | 943f6b28942250ad4eb5d2240648b51e39cc97f177af4066b82797ac2f97f5a1 |
| **L**e renard court sur la glace | 5465d1ddd4aed92734361e3f88982b29ef21650a4946a48c7d0b81e5dd111587 |
| le renard court sur la glace**!** | 85250dea86637bd7d39a23ebece0e7cf8bdee897d0322f248e7e493030781a8e |

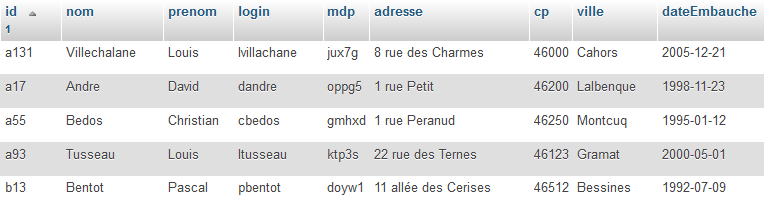
**Q.2** – Que constatez-vous ?

Malgrès que la différence est minimale, les empreintes sont différentes

1. **Utilité du hachage pour le stockage des mots de passe**

**Exercice 2**  : le laboratoire pharmaceutique GSB dispose d’une application en intranet utilisée par ses salariés, qui donne accès à la messagerie électronique, à l’agenda et divers utilitaires.

Les utilisateurs sont enregistrés dans la table ***utilisateur*** d’une base de données. En voici un extrait :



**Qu.2.1** – Quel est le problème de sécurité qui apparaît dans cette table ?

Les informations personnelles des utilisateurs ne semble pas etre cryptés avant d’etre stockés dans la base de données, ceci est un problème

**Qu.2.2** – S’il y a une divulgation de données de cette table, ou si un pirate accède à la base de données, quels sont les risques pour les utilisateurs ?

Si le hacker accède à la base données, il pouura voir toutes les informations en clair, et il pourra voler les identifiants des utilisateurs afin de les utiliser pour des fins malveillantes

Pour remédier à ce problème, désormais les mots de passe ne sont plus stockés en clair. C’est l’empreinte SHA-256 du mot de passe qui est stockée :

|  |  |
| --- | --- |
| **…**  **…**  **…**  **…**  **…**  **…**  **…** | **Qu.2.3** – Si un pirate vole les données ci-contre, peut-il retrouver les mots de passe ?  Généralement non, car les fonctions de hachage ne sont pas révérsibles |

**???** Mais alors si les mots de passe ne sont plus stockés dans la base, comme va-t-on s’identifier ? Exemple :

L’utilisateur *lvillachane* saisit sont login et mot de passe :

login : **lvillachane** mdp : **jux7g**

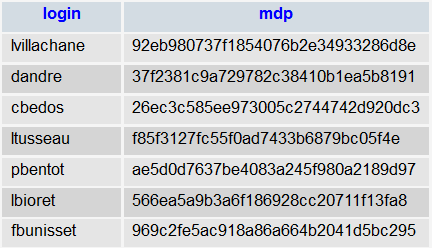
SHA-256

L’application calcule l’empreinte du mot de passe :



**…**

L’application va chercher ce login et cette empreinte dans la table des utilisateurs, et va les trouver :



**…**

L’utilisateur sera donc identifié.

Remarques :

* si l’utilisateur saisir un mauvais mot de passe, comme « tux7g », l’empreinte sera différente et l’application ne la trouvera pas, l’identification ne marchera pas.
* si un pirate dérobe les données et saisit l’empreinte comme mot de passe, le programme calculera l’empreinte de l’empreinte et l’identification ne marchera pas.

1. **Les attaques des mots de passe**
   1. ***Attaque par dictionnaire***

**Exercice 3**

En profitant d’une faille d’un serveur de bases de données, un pirate arrive à voler le mot de passe haché d’un utilisateur : 792fa9c36154572541124a7e06f3f6fea955b5c7f54bc599804b439cfe53f11d

**Q.3.1**. Expliquer en détail par quelle attaque simple le pirate peut essayer de retrouver le mot de passe original ? Et quelles sont les limites de cette attaque ?

Par dictionnaire, est sa limite est, si le vrai mot de passe recherché n’est pas dans la liste des possibilités, l’attaque est inefficace

* L’attaquant doit générer une liste des mots passes,
* puis calculer le haché de mot de passe générés
* Ensuite comparer les mots de passes hachés au mot de passe obtenu s’ils correspondent

Le pirate peut avoir une liste de mots de passe prédéfinie (obtenus grâce à des vols de données) avec leurs empreintes précalculées :

|  |  |
| --- | --- |
| Mot de passe | Empreinte SHA-256 |
| azerty  azerty1  azerty2023  bonjour  bonjour1  bonjour2023  etc. | f2d81a260dea8a100dd517984e53c56a7523d96942a834b9cdc249bd4e8c7aa9  46b995e8e8bf0834e93936de450a6eea38fd0f356e24c8fadb00fc2bb2695fc9  7703f9226b7a9be40089ae8ee3c2c7a00ce057fe41b0ccb372c9f446d500623e  2cb4b1431b84ec15d35ed83bb927e27e8967d75f4bcd9cc4b25c8d879ae23e18  65954a20fd6a9259ef594e93fd32719325e6b6fef22ab992ae33b641e2db4df1  792fa9c36154572541124a7e06f3f6fea955b5c7f54bc599804b439cfe53f11d |

**Attaque par dictionnaire** : si un pirate dispose d’une empreinte d’un mot de passe, il peut rechercher l’empreinte dans la liste et s’il la trouve il obtient immédiatement le mot de passe correspondant.

**Q.3.2.** Quel est l’avantage (pour le pirate) de l’attaque par dictionnaire par rapport à une attaque par force brute ?

L’avantage de l’attaque par dictionnaire par rapport à l’attaque par force brute

* Le nombre d’essaie est réduits car la liste des mots de passes potentiels est déjà prédéfinie.
* Au lieu d’utiliser toutes les combinaisons possibles on essaie seuelemnt une liste de mots de passes potentienls, c’est donc plus efficace.
* La liste contient généralment les mots de passes les plus utilisés