Questions :

1. Lisez attentivement l'ensemble des documents fournis
2. Dans le document n°2, expliquez pourquoi le déchiffrement des mots de passe à 4 caractères est instantané. Vous justifierez votre réponse par les calculs appropriés.
3. Commentez alors l'article du document n°3. Vous fournirez au moins deux arguments en vous appuyant sur la question précédente et le document n°4.
4. Compléter le tableau du document n°3.
5. Expliquez les conseils fournis par la CNIL (document n°1).

Document n°1

Qu'est-ce qu'un « bon » mot de passe ?

Un bon mot de passe doit être **suffisamment long**, et faire **au moins huit caractères**. Il doit être composé d'**au moins 3 types de caractères différents** parmi les quatre types de caractères existants (majuscules, minuscules, chiffres et caractères spéciaux). Il ne doit **pas avoir de lien avec son détenteur** (nom, date de naissance...).

Source : cnil.fr

Document n°2

Il existe une myriade de programmes pour récupérer un mot de passe. Nous en avons utilisé un pour récupérer un mot de passe à 7 caractères sur une archive WinZip en 20 minutes. Ceci nous a rendu curieux : à quelle vitesse notre configuration essayait-elle les combinaisons ?

Toutes nos archives protégées par un mot de passe sont-elles vraiment à 20 minutes du premier venu ?

Concrètement, un Core i5-2500K peut retrouver un mot de passe à cinq caractères en quelques instants vu qu'il peut tenter environ 28 millions de combinaisons par seconde.

Plus que la capacité du processeur à tester les combinaisons, c'est surtout la résistance des mots de passe qui nous intéresse ici :

Durée de la recherche à 28 millions de combinaisons/seconde	Mot de passe à 4 caractères	Mot de passe à 6 caractères	Mot de passe à 8 caractères	Mot de passe à 12 caractères
Minuscules	***instantanée***			
Minuscules et chiffres	***instantanée***			
Minuscules et majuscules	***instantanée***			
Minuscules, majuscules et chiffres	***instantanée***			
Tous caractères ASCII	***9 secondes***			

Note : Il existe 128 caractères ASCII. Le tableau est volontairement incomplet.

Quand bien même on est en mesure d'essayer 28 millions de combinaisons par seconde, on voit que la probabilité de trouver la bonne finit par devenir infime lorsque l'on a un mot de passe long et complexe.

Source : Adapté d'un article du site Tom's Hardware

Document n°3

Mots de passe les plus utilisés : le top 25 demeure dominé par 123456

L'invincible et incassable 123456...

SplashData, éditeur d'une solution de gestion de mots de passe, vient de livrer son classement annuel des mots de passe les plus utilisés. Et malheureusement, en 2014 comme en 2013, le tandem "*123456*" et "*password*" fait la course en tête.

Basé sur un échantillon de 3,3 millions de mots de passe compromis et diffusés sur le Net, le classement de SplashData n'est pas un exemple de fiabilité et de précision — il se veut d'ailleurs un classement des "pires" mots de passe. En effet, il indique très clairement quels sont les modèles à ne pas suivre. Ainsi, si vous utilisez une des 25 suites alphanumériques présentées ci-dessous pour un service revêtant une quelconque importance, n'hésitez pas : changez-la. Ces mots de passe sont les premiers qu'un pirate en herbe essaiera de combiner avec votre adresse mail pour accéder à vos différents comptes.

Malheureusement, concernant le classement des mots de passe les plus rencontrés, les piratages ont beau faire l'actualité de manière toujours plus fréquente, les années passent et se ressemblent. Ainsi, en 2014, le roi des sésames demeure l'invincible "*123456*", ô combien pratique pour les pirates de tout poil. Dans son sillage, on trouve le tout aussi symbolique "*password*", qui ne retiendra pas très longtemps d'hypothétiques intrus. Quant à la suite, nous vous laissons le loisir de la découvrir ci-dessous.

Rank	Password	Change from 2013	Rank	Password	Change from 2013
1	123456	*No Change*	14	abc123	*Down 9*
2	password	*No Change*	15	111111	*Down 8*
3	12345	*Up 17*	16	mustang	*New*
4	12345678	*Down 1*	17	access	*New*
5	qwerty	*Down 1*	18	shadow	*Unchanged*
6	123456789	*No Change*	19	master	*New*
7	1234	*Up 9*	20	michael	*New*
8	baseball	*New*	21	superman	*New*
9	dragon	*New*	22	696969	*New*
10	football	*New*	23	123123	*Down 12*
11	1234567	*Down 4*	24	batman	*New*
12	monkey	*Up 5*	25	trustno1	*Down 1*
13	letmein	*Up 1*			

Vous l'aurez compris, les séries de chiffres basiques, les noms de superhéros, de sports et les fameux "*qwerty*", "*azerty*" et autres "*qwertz*" ne font pas des mots de passe particulièrement robustes. Pour éviter que n'importe qui puisse s'infiltrer sans grand effort, il est nécessaire de prendre la peine de réfléchir à un sésame à la fois personnel, mais peu évident (pas une date de naissance). Il est aussi souhaitable, dans la mesure du possible, d'ajouter des caractères spéciaux, même si ceux-ci ne sont pas plus "forts" qu'un autre caractère. Quant à réutiliser ce mot de passe sur plusieurs sites sans modification, cette démarche est fortement déconseillée, sous peine de subir un effet domino au moindre piratage. *Source : les numériques*

Document n°4

Attaque par force brute

L'**attaque par force brute** est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Cette méthode est en général considérée comme la plus simple concevable. Elle permet de casser tout mot de passe en un temps fini indépendamment de la protection utilisée, mais le temps augmente avec la longueur du mot de passe.

Optimisation de l'attaque par force brute

Le principe général de l'attaque par force brute reste toujours de tester l'ensemble des mots de passe possibles, cependant l'ordre de test peut être optimisé afin d'obtenir de meilleurs rendements qu'une attaque par ordre alphabétique.

Attaque par dictionnaire

Plutôt que d'utiliser des chaînes de caractère aléatoires comme mot de passe, les utilisateurs ont tendance à utiliser des mots courant plus faciles à retenir or, s'il existe un nombre important de combinaisons aléatoires pour une chaîne de longueur donnée, le nombre de mots présents dans un ou plusieurs langages est beaucoup plus faible (à titre d'exemple l'Académie française estime que les dictionnaires encyclopédiques comptent environ 200 000 mots). Connaissant ce phénomène culturel, il peut être judicieux de tester ces mots courants et leurs dérivés (y compris argot, dialectes, mots avec fautes d'orthographe courante…) en priorité.

Source : Wikipedia