Activité (déconnectée) - Créer un code secret vivant et inoubliable

TOUTES LES FICHES

par André Van der Linden et Hélène Desmulliers • Médiathèque de Roubaix

CC BY SA

PUBLIC	PARTICIPANTS	ANIMATEURS	NIVEAU	PRÉPARATION	ACTIVITÉ

Description

Avec cette activité, le public saura créer un code :
– vivant parce qu'il se métamorphose, varie et évolue ;
– inoubliable parce qu'aussi facile qu'une charade qu'on a inventée soi-même

Objectifs

Codes secrets
Mots de passe

Matériel

Papier, crayon,
En option : un tableau blanc et un vidéo-projecteur, broyeur (pour montrer qu'on ne laisse pas de traces .. écrites) !

Contenus utilisés

A quel point mon mot de passe est-il sûr?
https://howsecureismypassword.net/

Pré-requis

Savoir écrire, compter

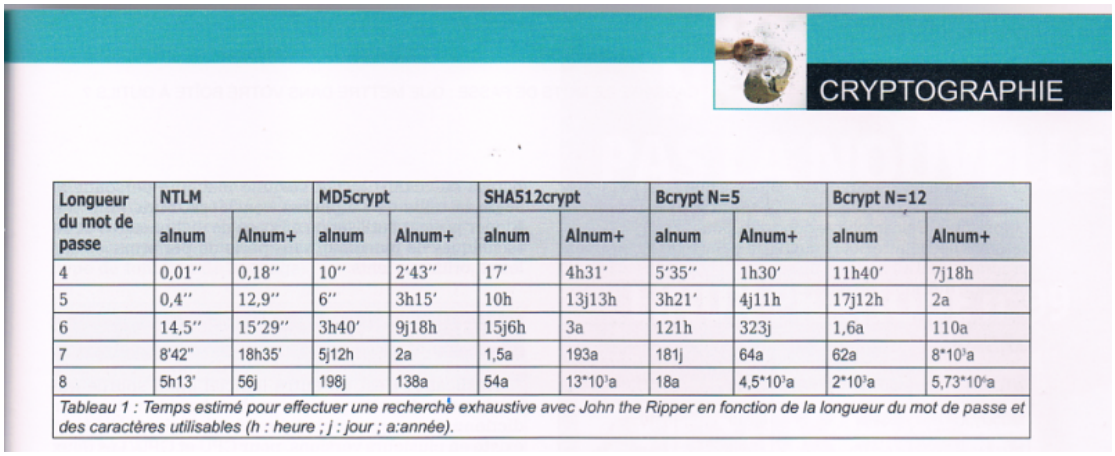
WORKFLOW

1 Faire deviner un chiffre entre 0 et 9

Dans cette première étape, chaque participant.e doit choisir dans sa tête un chiffre entre 0 et 9 et doit le faire deviner au groupe. Il ne faut pas oublier de mesurer le temps nécessaire pour trouver le code secret !

***Constat:* on trouve très rapidement le code secret de quelqu'un (en quelques secondes) !**

Donc, plus un code secret est long, plus le temps nécessaire pour le casser est grand !



Longueur du mot de passe	NTLM		MD5crypt		SHA512crypt		Bcrypt N=5		Bcrypt N=12	
	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+
4	0,01''	0,18''	10''	2'43''	17'	4h31'	5'35''	1h30'	11h40'	7j18h
5	0,4''	12,9''	6''	3h15'	10h	13j13h	3h21'	4j11h	17j12h	2a
6	14,5''	15'29''	3h40'	9j18h	15j6h	3a	121h	323j	1,6a	110a
7	8'42"	18h35'	5j12h	2a	1,5a	193a	181j	64a	62a	$8*10^3$a
8	5h13'	56j	198j	138a	54a	$13*10^3$a	18a	$4,5*10^3$a	$2*10^3$a	$5,73*10^6$a

Tableau 1 : Temps estimé pour effectuer une recherche exhaustive avec John the Ripper en fonction de la longueur du mot de passe et des caractères utilisables (h : heure ; j : jour ; a:année).

[MISC n°89] Références de l'article « Cassage de mots de passe : que mettre dans votre boîte à outils ? » ».

Ici temps mis par le logiciel "John the Ripper" pour casser un mot de passe.

2 Faire deviner un chiffre entre 0 et 999

Comme pour l'exercice présent, il s'agit à chacun.e de choisir un nombre, cette fois-ci entre 0 et 999 (plus complexe donc !)

***Constat:* on met plus de temps mais on trouve facilement quand-même. On**

estime que la longueur idéale d'un code secret est de *12 caractères et plus* !

La vitesse de calcul d'un ordinateur est infiniment plus grande que la vitesse de calcul du cerveau humain ! De plus, on estime que cette vitesse des microprocesseurs d'ordinateurs double tous les ans (loi de Moore). Il est intéressant d'expliquer cela aux participant.es.

Conseil médiation :

Pour en savoir un peu plus sur le sujet, ne pas hésiter à consulter la page Wikipedia dédiée.

3 Comprendre ce qu'il ne faut pas faire !

Pour ce troisième exercice, l'objectif est de commencer à faire comprendre la logique d'un mot de passe, et ce qu'il ne faut pas faire lorsque l'on créé son mot de passe.

Pour cela, il suffit d'imprimer les différentes étiquettes ci-dessous (ou de les créer à la main sur des bouts de papier) et de demander aux participant.es de relier chaque personnage connu à son mot de passe.

Relier chaque personnage à son mot de passe

Personnages

Mario
Iron Man
La Reine des Neiges
Paul Pogla
Grand Schtroumpf
Kilan Mbappé
Sacha Ketchum
Aladin
Shrek
Astérix

Mots de Passe disponibles

Lib'Délivrée
Jasmine

Mots de Passe disponibles

Rougra99
Champion2018
ChamiMoustache
RoisManc006
T.Stark
Gaul.-50.Gos-Ude
Pok151Bourg
OgreVert

***Constat:* si on tombe sur une liste de mots de passe, il est assez facile de deviner à qui elle appartient et quel est l'usage de mots de passe qu'elle contient !**

Les logiciels utilisés pour "craquer" les mots de passe utilisent des dictionnaires de mots …. il vaut toujours mieux inventer des codes sans signification numérique ou littéraire et qui ne peuvent donc pas être présents dans les dictionnaires … –> en inventer soi-même !

4 Créer un mot de passe grâce à une charade

Maintenant que les participant.es ont compris ce qu'il ne faut pas faire, il est temps de leur donner une astuce pour créer un code secret qu'ielles n'oublieront pas.

Il est bien de rappeler qu'un mot de passe dit "fort" doit contenir au moins 8 caractères, des minuscules, des majuscules, des chiffres et au moins un signe spécial.

Où en sommes-nous ? il faut inventer un code secret *long* et que personne ne peut deviner. Il ne faut pas le laisser traîner sur un bout de papier (*ne pas l'écrire*), le retenir facilement et ne l'utiliser que pour *un seul usage* (pas utiliser le code d'une autre cachette).

***Solution:* Inventer une charade personnelle qui permettra de retenir un ou des**

codes secrets impossibles à trouver sans elle.

Voici comment nous allons procéder:

	Proposition	**Règle**	**Exemple**
Mon premier	mon surnom à l'école / au collège , mon personnage préféré, etc	les 3 premières lettres, une en majuscule	**Man**
Mon second	le numéro de l'adresse de la maison de mes parents / le numéro du bâtiment où je travaille / l'année de naissance de mon animal préféré, etc	les 3 premiers chiffres	**28 ? 028**
Mon troisième	le lieu où je me sers de ce code	les 3 premières lettres, une en majuscule	Médiathèque ? **Med**
Mon séparateur	caractère ou chiffre entre chaque partie	caractères spéciaux:* ou = ou + ou , etc	, puis ; puis :
Mon tout		Code secret que j'utiliserai à la Médiathèque	**Man,028;Med:**
Mon tout		Code secret que j'utiliserai au travail	**Man,028;Ovh:**
Mon tout		Code secret que j'utiliserai à l'école	**Man,028;Ana:**
Option	Mon mot de passe doit changer tous les …	je change mon mot de passe pour le 1er trimestre 2019	**Man,028;Med:1T19!** **Man,028;Ovh:1T19!** **Man,028;Ana:1T19!**

5 Mise en application

Pour celle.eux qui ont une carte médiathèque, on propose de remplacer le mot de passe d'accès à leur compte par leur code secret.
Cela peut bien évidement être fait avec tout autre accès, ou site nécessitant un mot de passe.

En effet, tout ce que nous venons de découvrir pour fabriquer un code secret très

solide peut être utilisé pour fabriquer des mots de passe pour les sites Internet.

6 Consignes concernant la charade pour un code plus complexe

Constat:

- Mon code secret doit être composé d'environ 13 caractères ;
- Mon code secret doit être composé de 3 parties, de différents types de caractères (numériques, alphabétiques en minuscules, alphabétiques en majuscule), dont 1 partie variable en fonction du lieu (site sur lequel nous créons le mot de passe), séparée par un même caractère de ponctuation (au choix)
- Dans mon code secret, je dois éviter des suites de lettres comme celles contenues dans mon prénom, mon nom ou ma ville d'habitation ou de naissance ainsi que des suite de chiffres contenus dans ma date de naissance, mon code postal de ville d'habitation ou natale
- Plus il y a de types de caractères différents, plus il est difficile de craquer un mot de passe : utiliser des chiffres, des lettres (majuscules et minuscules), des caractères spéciaux comme * ou = ou + ou , etc …. mais attention aux déplacements à l'étranger ?)
- Plus souvent on change de code secret pour une même cachette, plus il sera difficile pour un hacker ou un logiciel de "craquer" ce code … il faut donc prévoir une partie qui varie avec le temps (qui passe).
- Un code ne doit servir que pour une seule cachette; si mon code est dévoilé pour une de mes cachettes, il serait très facile et rapide de pénétrer dans toutes mes autres cachettes.
- Il ne faut jamais laisser de trace écrite d'un code secret: moins on écrit ailleurs le mot de passe ou moins on en parle autour de soi, plus le secret sera facile à garder : le code secret idéal se trouve uniquement dans notre cerveau.

7 Pour aller plus loin

Cassage de mots de passe : que mettre dans votre boîte à outils ?

[MISC n°89] Références de l'article « Cassage de mots de passe : que mettre dans votre boîte à outils ? »