Créer un code secret vivant et inoubliable

- vivant parce qu'il se métamorphose, varie et évolue
- inoubliable parce qu'aussi facile qu'une charade qu'on a inventé soi-même

Objectifs pédagogiques de l'activité

- donner une technique pour penser et retenir ses codes secrets (ses mots de passe) comme un jeu
- évoquer la relation entre longueur du mot de passe et difficulté pour les hommes et les machines de la deviner
- évoquer la nécessaire multiplicité des mots de passe sans difficulté de mémorisation
- faire prendre conscience de la vitesse de calcul d'un ordinateur

Durée de l'activité

30 à 40 minutes peut être moins ?

Nombres de participants maximum

10 / 12 personnes

Tranche d'âge du public (âge minimum)

de 7 à 107 ans

Pré-requis

→ savoir écrire, compter

Matériel nécessaire durant l'activité

papier, crayon, broyeur (pour montrer qu'on ne laisse pas de traces .. écrites) !

Déroulement de l'activité

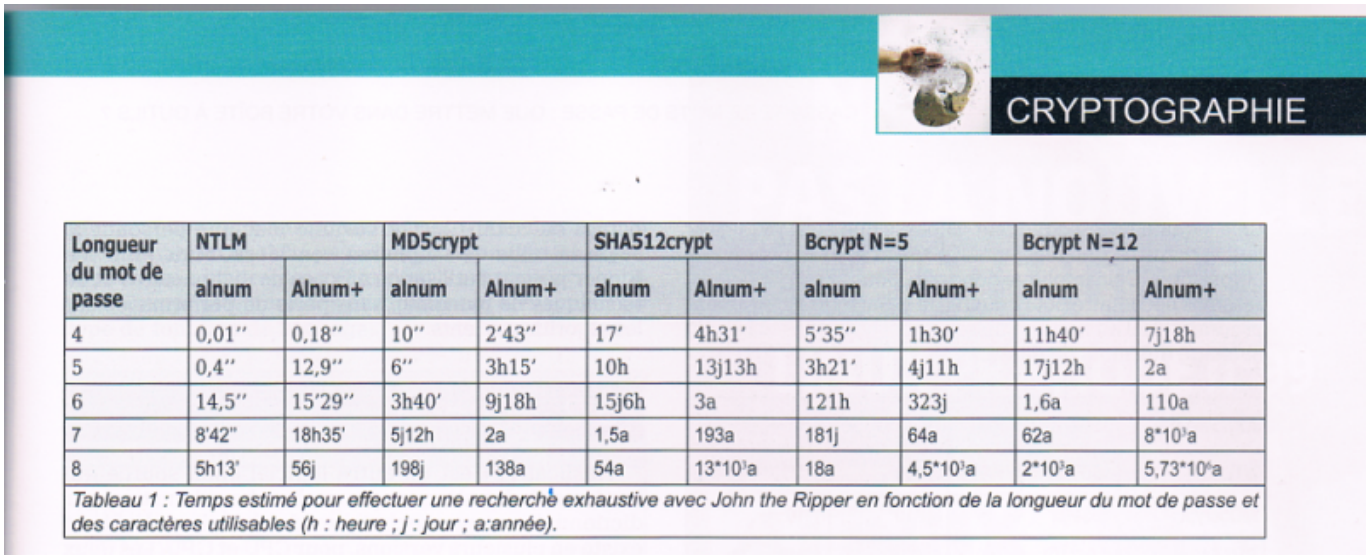
Chaque participant met un badge avec son prénom

Vous êtes traqué par la mafia japonaise et les yakuza veulent découvrir le code secret de votre cachette. S'ils vous trouvent, vous êtes mort !

Étape 1: choisir dans sa tête un chiffre de 0 à 9

et le faire deviner au groupe, 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.

Étape 2: choisir un chiffre de 0 à 999

et le faire deviner (réponse + / -) au groupe ..... plus long mais facile quand-même ... donner à réfléchir à la rapidité de calcul d'un ordinateur !
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)

Étape 3: proposer des couples « Personnage connu / Mots de passe » à deviner

Relier chaque personnage à son mot de passe

Personnages	**Mot de passe ?**
Mario	
Iron Man	
La Reine des Neiges	
Paul Pogla	
Grand Schtroumpf	
Kilan Mbappé	
Sacha Ketchum	
Aladin	
Shrek	
Astérix	

Liste de mots de passe: **Lib'Délivrée**, **Jasmine**, **Rougra99**, **Gaul.-50.Gos-Ude**, **ChamiMoustache**, **Champion2018**, **T.Stark**, **Pok151Bourg!**, **RoisManc006**, **OgreVert**.

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

Étape 4: créer une charade

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).

<note important>

Solution: Inventer une charade personnelle qui permettra de retenir un ou des codes secrets impossible 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 majuscules	**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 majuscules	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!

Étape 5: Du code secret au mot de passe

Pour ceux qui ont une carte médiathèque, on propose de remplacer le mot de passe d'accès à leur compte par leur code secret.
En effet, tout ce que nous venons de découvrir pour fabriquer un code secret très solide peut être utiliser our fabriquer des mots de passe pour les sites Internet.

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 composée de 3 parties, de différents types de caractères (numériques, alphabétiques en minuscules, alphabétiques en majuscules), 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
- au plus il y a de types de caractères différents, au plus c'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 ?)
- au plus souvent on change de code secret pour une même cachette, au 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 cachette, 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: au moins on écrit ailleurs le mot de passe ou au moins on en parle autour de soi, au plus le secret sera facile à garder : le code secret idéal se trouve uniquement dans notre cerveau

---

Allez plus loin

évaluer son mot de passe
évaluer son mot de passe

— André Vanderlynden 2019/02/20 22:13 — Hélène Desmulier pour les scénario d'animation