CALCULER LA "FORCE" D'UN MOT DE PASSE

QU'EST-CE QUE LA « FORCE » D'UN MOT DE PASSE ?

Par abus de langage, on parle souvent de "force" d'un mot de passe pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles.

Cette "force" dépend de la **longueur L** du mot de passe et du **nombre N** de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire. Elle se calcule aisément par la formule N^L.

COMMENT ESTIMER LA "FORCE" D'UN MOT DE PASSE ?

La force d'un mot de passe peut être estimée par comparaison avec les techniques cryptographiques. Une taille de clé cryptographique de 64 bits est aujourd'hui considérée comme non sûre car les capacités de calcul actuelles permettent de retrouver cette clé en énumérant toutes les clés possibles. Or, une telle clé, peut être vue comme un mot de passe de **64 caractères** où les **2** seuls caractères sont **0** et **1**. La "force" d'un tel mot de passe est donc 2^{64}.

Les règles édictées par l'ANSSI en matière de mécanismes cryptographiques imposent par exemple une taille de clé minimale de 100 bits. Il est même recommandé une taille de clé de 128 bits pour des clés dont l'usage présumé est de longue durée. Il est par ailleurs communément admis que des tailles de clé de 80 bits sont désormais exposées à des attaques utilisant des moyens techniques conséquents.

QUELQUES RÉSULTATS TYPIQUES

Longueur mot de passe [L]	Nombre de caractères à disposition [N]		Taille de clé équivalente [bits]
4	10	0 à 9	13
4	26	Alphabet "A Z" ou "a z"	19
8	26		28
8	52	Alphabet MAJ & min	46
8	62	Alphabet MAJ & min + Chiffres	48
12			71
16			95
20			119
8	70	Alphabet MAJ & min + Chiffres + € ! # $ * % ?	49
12			74
16			98
20			123
25			153
8	90	Alphabet MAJ & min + Chiffres + < € ! # $ * % ? [(: -)] @ ^£ § ° >	52
12			78
16			104
20			130
25			162

Force du mot de passe

64 | Très faible

Taille usuelle

64 < 80 | Faible

80 < 100 | Moyen

Taille minimale recommandée

100 <128* | Fort

Adresses courriels

> 128** | **Très fort**

Navigateurs

* 128 bits est la plus petite taille de clé de l'algorithme de chiffrement standard AES.

** Chiffrement par la carte de visite disponible sur **Partager.biz**

*Source **A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation : https://www.ssi.gouv.fr/*

LE CHIFFREMENT

QUE FAUT-IL POUR PARVENIR À LE CONTOURNER ?

Article complet (mars 2017) : https://www.ontrack.com/fr/blog/chiffrement-que-faire-pour-contourner/

L'histoire de la confidentialité des informations commence dès l'antiquité, la première preuve datant d'environ 4000 ans. À cette époque, les scribes égyptiens utilisaient des hiéroglyphes spéciaux pour encoder certains textes. Des légions romaines aux première et seconde guerres mondiales, les armées ont régulièrement utilisé le chiffrement des ordres. Bien évidemment quand y a chiffrement, c'est qu'il y des informations à préserver et en parallèle des personnes qui veulent avoir accès à ces données confidentielles pour les exploiter à leur profit.

De nos jours, non seulement les mathématiciens et les cryptologies, mais également les hackers et les malfaiteurs essaient de trouver de nouvelles façons de "craquer" les codes de chiffrement pour s'introduire dans des systèmes ou réseaux informatiques protégés.

Comme aux époques les plus anciennes, la seule solution possible pour "craquer" un lot de passe et de tester toutes les combinaisons possibles, chaque combinaison est appelé "clé". Grâce aux ordinateurs, qui peuvent essayer des centaines de milliards de "clés" par seconde cette méthode "brutale" est appelée "force brute".

Plus la "clé" est longue et composée à partir d'une base d'un grand nombre de type de caractères, plus le décodage sera difficile. La "force" d'une "clé" se mesure en bits. Jusqu'à l'an 2000 un chiffrement de 56 bits était considéré comme impossible à craquer. En 1998, un ordinateur d'une valeur de 250 000 € parvint à craquer une clé 56 bits pour la première fois en 56 heures. En 2006, deux universités allemandes parvinrent à construire un ordinateur qui ne coûtait que 10 000 € et qui était capable de craquer une "clé" 56 bits en seulement 6 jours et demi.

Il existe de très nombreuses méthodes de chiffrement possibles. Mais la procédure pour craquer les "clés" reste cependant la même : la ''force brute" doit être utilisée. C'est ce que fait la NSA, l'une des organisations des services secrets américains, qui est leader mondial en matière de déchiffrement.

Un super ordinateur est utilisé à chaque besoin pour tenter la méthode de la "force brute". Toutefois, s'il apparaît clairement que cette méthode ne fonctionne pas, le problème est mis de côté en attendant que la technologie progresse suffisamment pour que le déchiffrement puisse être fait avec un coût financier et un délai d'exécution raisonnables. S'il apparaît à nouveau que cela n'aboutira pas, le problème est à nouveau mis de côté en attendant que la technologie soit au point et rende le déchiffrement faisable ; tant d'un point de vue financier que du temps nécessaire.

La standard mondial, admis même par la NSA, depuis les années 2000 en matière de chiffrement s'appelle Advanced Encryption Standard ou AES (soit "norme de chiffrement avancé" en français). Il existe trois degrés de sécurité de référence : 128, 192 et 256 bits.

Le gouvernement américain a annoncé en juin 2003, à propos de la norme AES et suivant une analyse de la NSA : *L'architecture et la longueur de toutes les tailles de "clés" AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau "SECRET ". Le niveau "TOP SECRET" nécessite des clés de 192 ou 256 bits*.

Source : https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

En 2011, des chercheurs de Microsoft indiquent pour la première fois avoir pu trouver la clef d'un chiffrement d'AES 128 en m 2^{128} opérations par une attaque par "force brute".

POUR TESTER LA FORCE DE VOTRE MOT DE PASSE

https://howsecureismypassword.net/ & https://password.kaspersky.com/fr/

Durée pour craquer un MdP par deux approches différentes ; avec 12 caractères on est déjà en sécurité !