* L'**attaque par force brute** est une méthode utilisée en [cryptanalyse](https://fr.wikipedia.org/wiki/Cryptanalyse) pour [trouver un mot de passe](https://fr.wikipedia.org/wiki/Cassage_de_mot_de_passe) ou une [clé](https://fr.wikipedia.org/wiki/Cl%C3%A9_de_chiffrement). 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

L’efficacité peut varier considérablement en fonction de plusieurs facteurs :

* Longueur et complexité du mot de passe : Plus le mot de passe est long et complexe (c'est-à-dire qu'il contient des lettres majuscules et minuscules, des chiffres, des symboles, etc.), plus il est difficile à deviner par force brute.
* Espace de recherche : Le nombre de combinaisons possibles dépend de la longueur et de la complexité du mot de passe. Par exemple, un mot de passe de 8 caractères alphanumériques peut avoir 62^8 (environ 218 trillions) combinaisons possibles.
* Temps de traitement : La vitesse à laquelle les combinaisons sont testées dépend de la puissance de calcul de l'ordinateur utilisé pour mener l'attaque.

Reference :

-"Cryptography and Network Security: Principles and Practice" par William Stallings.

-"Applied Cryptography: Protocols, Algorithms, and Source Code in C" par Bruce Schneier.

* MD5 (Message Digest Algorithm 5) est un algorithme de hachage largement utilisé pour produire une empreinte numérique (hash) d'un message ou d'une donnée. Il prend en entrée un message de longueur quelconque et produit en sortie une empreinte numérique de 128 bits (généralement représentée sous forme hexadécimale comme une chaîne de 32 caractères).
* SHA-1 (Secure Hash Algorithm 1) est un algorithme de hachage cryptographique qui produit une empreinte numérique de 160 bits (20 octets).