Attaque par force brute sur cryptage.
(FBA Force Brut Attac).

L'**attaque par force brute** est une méthode utilisée en cryptanalyse pour la clé de cryptage. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Cette méthode est en général considérée comme la plus simple concevable. En théorie la complexité d'une attaque par force brute est une fonction exponentielle de la longueur en bit du mot de passe.

Dans le cas des clés utilisées pour le chiffrement, la longueur est donnée en bits. Dans ce cas, le nombre de possibilités (si la clé est aléatoire) à explorer est de l'ordre de 2^N où *N* est la longueur de la clé en bits. Une clé de 128 bits représente déjà une limite impossible à atteindre avec la technologie actuelle et l'attaquant doit envisager d'autres solutions cryptanalytiques si celles-ci existent. (voir un ordinateur quantique). Il faut cependant prendre en compte que la puissance du matériel informatique évolue sans-cesse et un message indéchiffrable à un moment donné peut l'être par le même type d'attaque une dizaine d'années plus tard.

DES cryptage 56 Bits
AES cryptage 128 ou 256 bits.

Rappel :

Comment Alan Turing a pu casser le code produit par la machine de Cryptage allemande Enigma pendant la guerre de 39-45, codage pourtant réputé inviolable.

Tout ceci a l'aide d'un pré ordinateur qui utilisait des relais électromécaniques pour représenter un bit.

Dans un film on voit Alan Turing comprendre qu'il peut avancer dans ses travaux de cassage du code, si il sait, au par avant, que chaque message météo qu'il reçoit d'une station allemande de l'antarctique se termine par les mots « Heil Hittler » . Soit déjà traduit les 13 derniers mots du message.

Pour qu'un ordinateur puisse casser un cryptage avec FBA.

Il lui faut une information connue (mot et emplacement) pour donner une référence d'exactitude à l'ordinateur. Ce qui lui permettra de faire ses essaies et ses vérifications tout seul.

Exemple 1 :

Si on essaie de casser des lettres dactylographiques on part du principe que sur la première ligne en haut et justifié à droite se trouve le nom du lieu d'envoi, une virgule et la date du jour.

Exemple 2 :

Si on essaie de casser un cryptage sur des messages IP. (VPN Crypté)

On sait par exemple que sur l'entête de routage du message IP, l'adresse IP de l'envoyeur (que l'on connait) se trouve à partir de la position 54 de la trame IP. (Valeur inexacte).