Algorithmes de calcul du logarithme discret

Pas-de-bébé, pas-de-géant. (SHANKS)

Soit G un groupe cyclique d’ordre N et g un générateur. Etant donné un element x dans G, il s’agit de trouver l’entier n tel que x=g^n. On pose K=⌈rac(N)⌉. L’idée est de parcourir les éléments de G de deux façons. Lors du premier parcours, par pas-de-bébé, on établit la liste des puissances successives du générateur :

A={g^i | i=0,1,…,K-1}

Lors du second parcours, par pas-de-géant, on saute de K en K :

B={xg^(-Kj) | j=0,1,…,K-1}

Ces deux listes ont nécessairement un élémént commun g^i=xg^(-Kj), i.e. x=g^(i+Kj)=g^n qui correspond à la division euclidienne de n par K.

La complexité de l’algorithme est exponentielle puisqu’il nécessite le stockage de ⌈rac(N)⌉ éléments et en moyenne (½)\*⌈rac(N)⌉ calculs avant de trouver l’élément commun à A et à B.

Calcul de l’indice (index calculus)

Algorithme le plus efficace actuellement mais difficile à implémenter dont la complexité est sous-exponentielle.