

Les nombres pseudo-aléatoires

<http://en.cppreference.com/w/cpp/numeric/random>

Un nombre aléatoire est un nombre dont la valeur est choisit au hasard. Ils sont utilisé dans de nombreux contextes, par exemple dans un jeu vidéo (pour avoir un comportement non prédictible), en cryptographie (pour encoder des informations), dans les tests (pour vérifier le comportement d'un programme avec des valeurs indéterminées). Vous verrez dans différents projets de ce cours des cas d'utilisation des nombres aléatoires.

En pratique, il est assez difficile d'obtenir un nombre réellement aléatoire avec un ordinateur, c'est-à-dire un nombre dont aucune caractéristique ne sera prédictible. La théorie de la génération des nombres aléatoires est très complexe et sort de ce cours, c'est un domaine de recherche des mathématiques. On utilisera en général des nombres pseudo-aléatoires, c'est-à-dire des nombres qui sembleront aléatoires, même si ce n'est pas réellement le cas formellement.

Ces nombres pseudo-aléatoires seront en fait le résultat d'un algorithme complexe. Cet algorithme sera initialisée avec une valeur quelconque (graine ou *seed*) et produira une suite de nombres pseudo-aléatoires à chaque appel.