Génération de nombres Pseudo-aléatoires

"La génération de nombres aléatoires est trop importante pour la confier au hasard"

Cas d’usage des nombres aléatoires

- les jeux
- l'analyse
- la simulation
- l'échantillonnage
- la prise de décision

Le hasard des ordinateurs

Les nombres pseudo-aléatoires en python

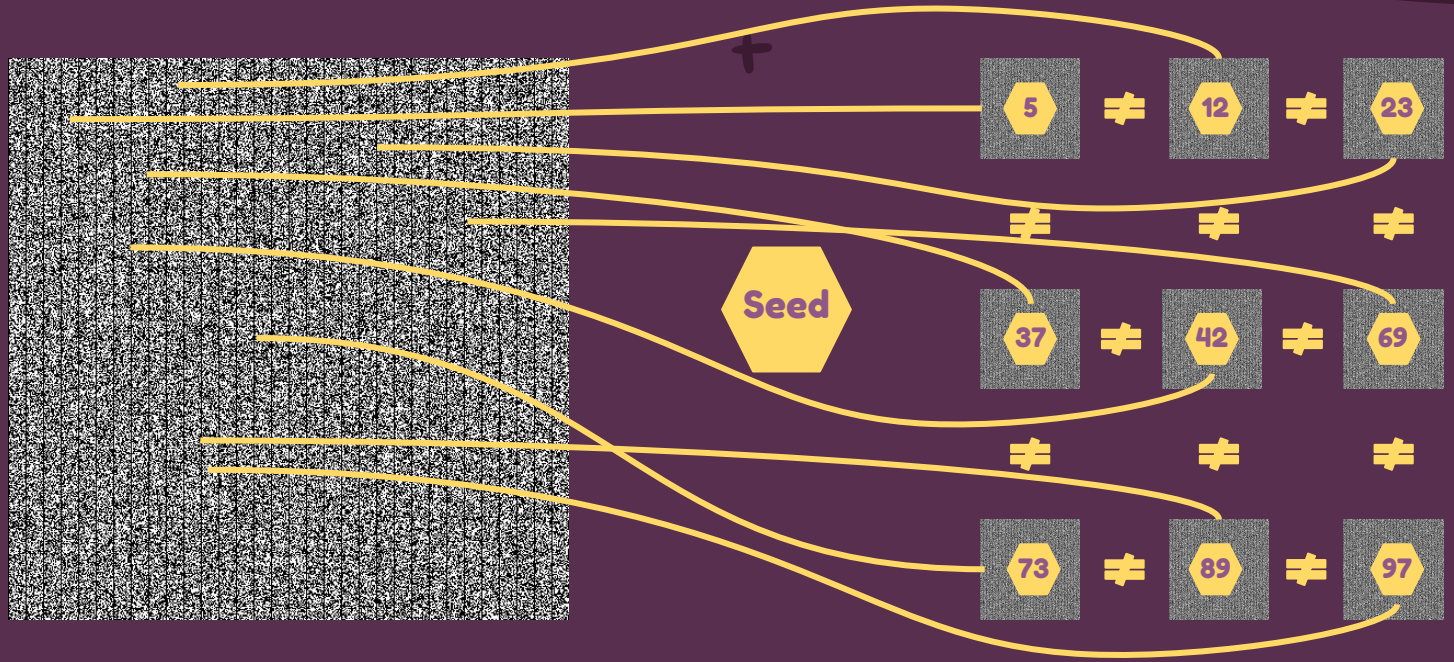
random.random()

+

random.seed()

Aléatoire, qui a dit aléatoire?

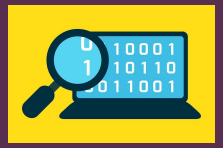
Représentation graphique de l'algorithme Random

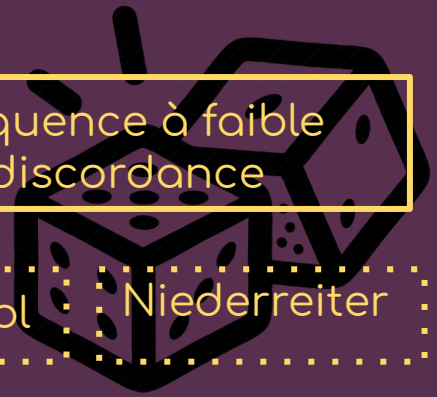


Importance de la graine “seed”

Utiliser la bonne graine tu dois!

Générateurs de nombre pseudo aléatoire





Séquence à faible discordance

Sobol

Niederreiter

Générateur congruentiel linéaire

Générateur d'automate cellulaire étendu

Extended CA

Générateur Intel MKL

Générateur congruentiel multiplicatif

WichmannHill

Générateur de registre à décalage de rétro-action généralisé

Générateur de registre à décalage

MCG31

MCG59

R250

Générateur Mersenne Twister

Les limites des nombres pseudo-aléatoires

- Prévisibles
- Facile à hacker
- pas du tout adapté à la cyber sécurité.

Qu’est que le vrai aléatoire ?

« Les événements amenés par la combinaison ou la rencontre de phénomènes qui appartiennent à des séries indépendantes, dans l'ordre de la causalité, sont ce qu'on nomme des événements *fortuits* ou des résultats du *hasard* »

***Exposition de la théorie des chances et des probabilités*, Augustin Cournot**

Générateur de nombres aléatoires

Wall of entropy

Nom de Zeus!!