(4) Génération de nombres aléatoires.

(RNG : Random Number Generator).

(4.1). 3 types de RNG :

- **True RNG :** TRNG. Caractérisé par le fait que la suite ne peut être reproduite. Par exemple : flipper une pièce 100 fois : 2^{100} possibilités. TRNG utilisé pour engendrer des clés de session

- **Pseudo-Random :** PRNG. génère une suite (s_i) à partir d'une "base", comme :

$$\begin{cases} s_0 = \text{base} \\ s_{i+1} = f(s_i) \quad i = 0, 1, 2, \dots \end{cases}$$

ou. $s_0 = \text{base}$. et $s_{i+1} = f(s_i, s_{i-1}, \dots, s_{i-t})$, t entier fixé.

Exemple. $\begin{cases} s_0 = \text{"base"} \\ s_{i+1} = a \cdot s_i + b \mod m \end{cases}$; $a, b \in \mathbb{N}$. $i = 0, 1, 2, \dots$

Sortie de PRNG. approxime statistiquement. T-RNG.

- **Cryptography Secure PRNG :** CSPRNG.

C'est un PRNG avec la propriété :

Etant donné n bits de (s_i). consécutifs, $s_{i+1}, \dots, s_{i+n}$, il est difficile de trouver un algorithme polynomial calculant s_{i+n+1} avec une probabilité de succès $> \frac{1}{2}$.