Question n°1 :

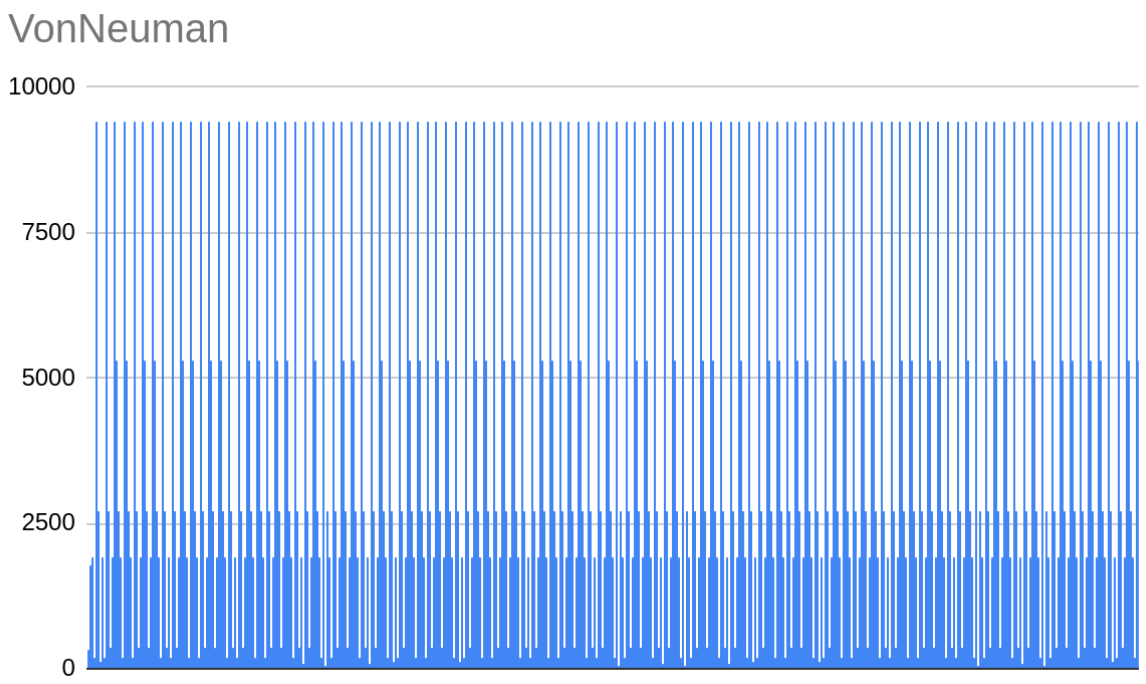
Python utilise la bibliothèque standard "random" pour générer des nombres aléatoires.
L'algorithme de génération de nombres aléatoires utilise une seed de départ. Généré à partir de la date système si non fourni.
Le langage utilise le générateur "Marsenne Twister".
Cependant, ce générateur est totalement déterministe, il ne convient pas à tous les usages, et est totalement inadapté à des fins cryptographiques.

Question n°2 :

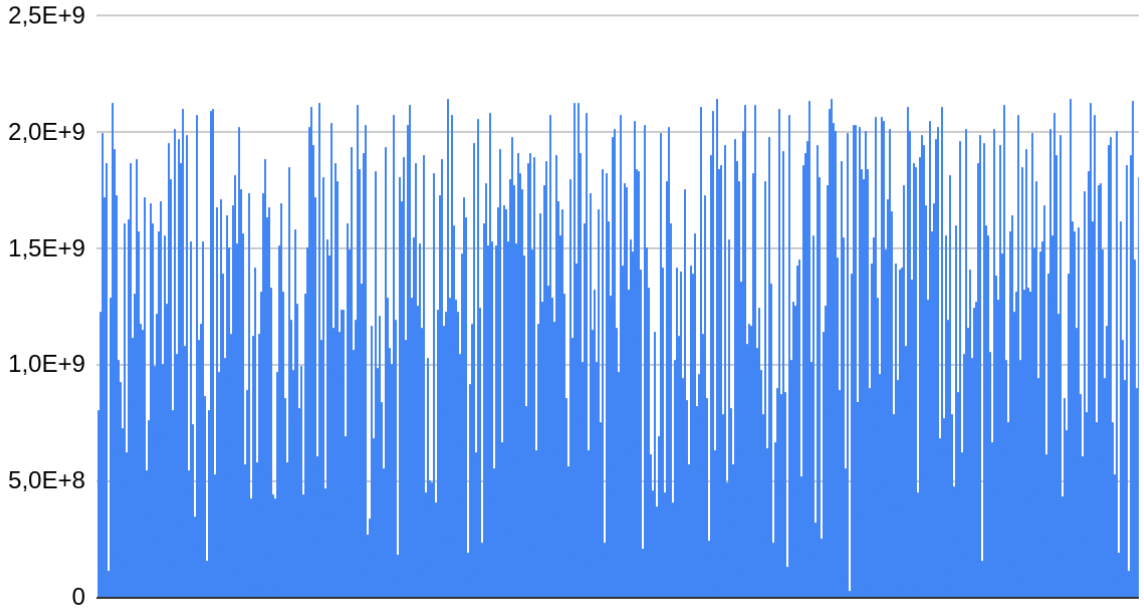
secrets est un module python permettant de générer des chaînes ou des nombres aléatoires cryptographique ment forts.
Pour fournir des nombres aléatoires cryptographique ment sécurisés, le système ne repose pas sur le calcul, mais sur des composants physiques qui répondent à des phénomènes microscopiques qui produisent de petits signaux de bruit aléatoires, tels que le bruit thermique ou l'effet photoélectrique.

Question n°3/4/5 : (Cf. DM.py)

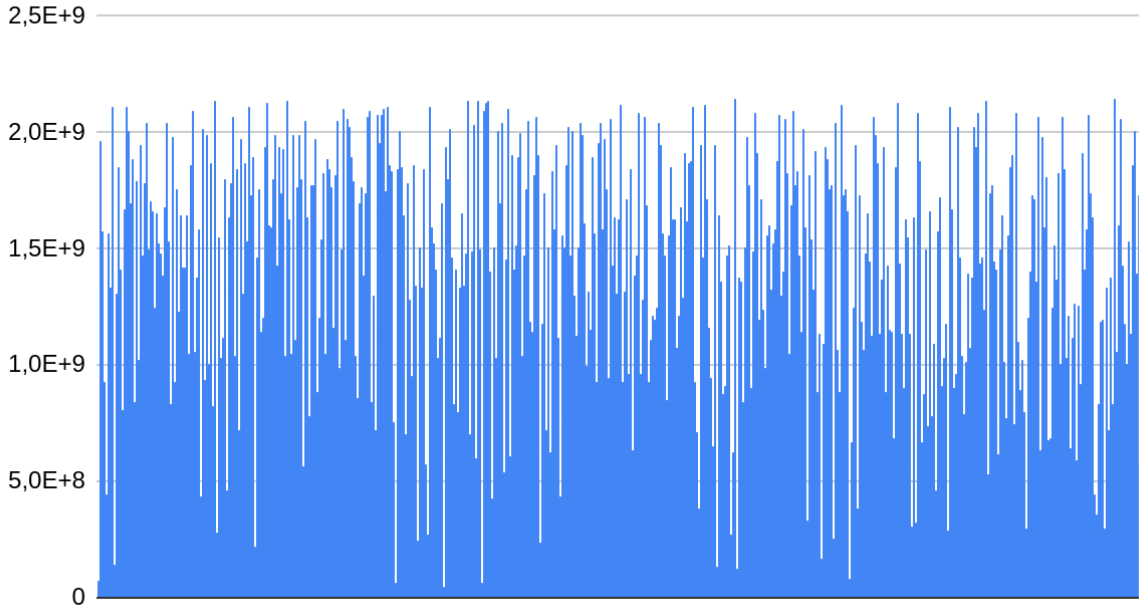
Question n°6 :

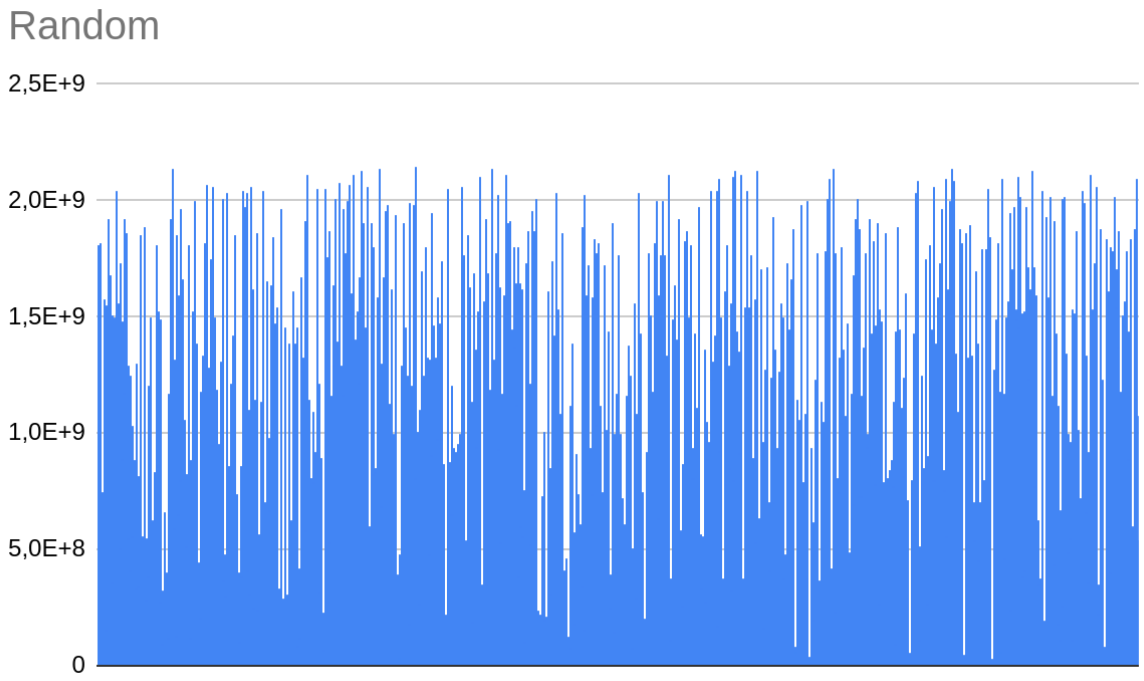


STM



RANDU





VonNeumann, créé un cycle de répétitions, ce sont toujours les mêmes valeurs.
Pour les 3 autres, les valeurs semblent être réparties assez aléatoirement.

Question n°7 :

La fonction erfc de la bibliothèque math permet de calculer la P_{valeur}.

Question n°8 à 10 : (Cf. DM.py)