Моделирование информационных процессов и систем

Генерация случайных чисел в стандартной библиотеке C

Подготовили студенты:
Чигарев Дмитрий (381807-1)
Параничев Денис (381807-1)
Бржезинская Полина (381807-2)

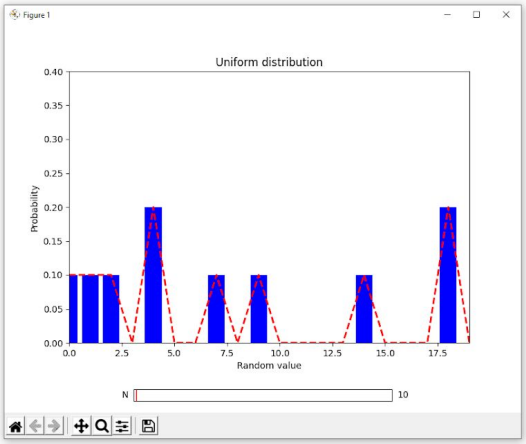
Генерация псевдослучайных чисел в C

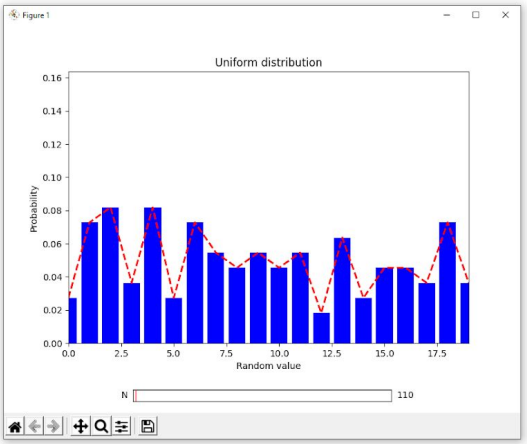
Стандартные функции генерации случайных чисел во многих языках программирования (в том числе и языке *C*) реализуются через [линейный конгруэнтный метод](). Суть метода заключается в обходе зацикленной числовой последовательности, начиная с заданного параметром seed места: $X_{n+1} = (aX_n + c) \% m \mid a, c, m \in Z$
Так, например при параметрах: $X_0 = a = c = 7,\ m = 10$ получим последовательность: $7,\ 6,\ 9,\ 0,\ 7,\ 6,\ 9,\ 0\ ...$

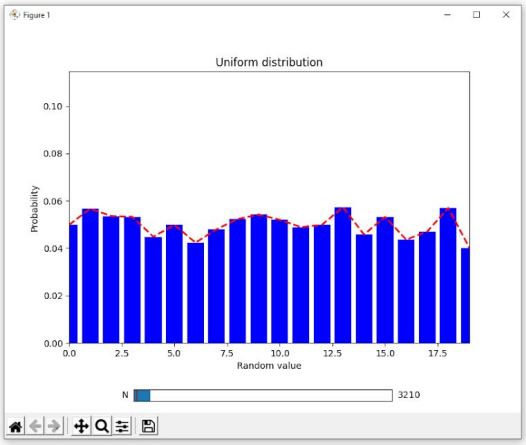
При реализации генератора псевдо-случайных чисел параметры последовательности подбираются [таким образом](), чтобы достичь наибольшей длинны цикла.

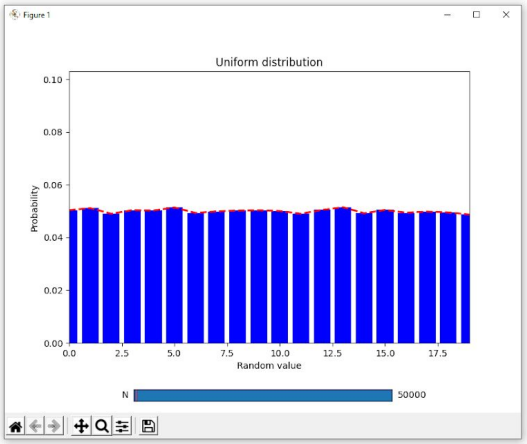
Псевдослучайные последовательности сгенерированные таким образом, обладают свойством равномерного распределения и имеют слабую криптографическую стойкость, т.к. линейным по параметру m перебором можно определить текущее положение в последовательности и затем с точностью предсказывать все последующие числа, которые будет выдавать генератор.

Провизуализируем работу функции $rand$ из стандартной библиотеки языка C. Будем N раз генерировать случайные целые числа в диапазоне $x \in [0,\ 20] \mid x \in Z$, получим последовательность на основе которой сможем построить ряд распределения случайной дискретной величины x. Отобразим ряд на графике:









Как видим, при достаточно большом N мы получили практически прямую линию вероятности.

Приложения

1. Линейный конгруэнтный метод: https://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D0%BD%D0%B5%D0%B9%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BD%D0%B3%D1%80%D1%83%D1%8D%D0%BD%D1%82%D0%BD%D1%8B%D0%B9_%D0%BC%D0%B5%D1%82%D0%BE%D0%B4
2. Код программы на github: https://github.com/proxodilka/random_visualization