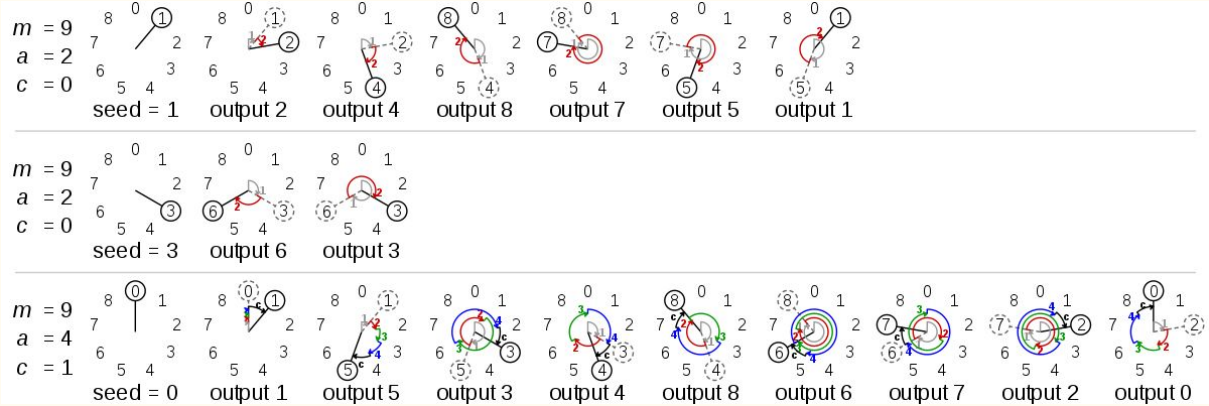
Lehmer random number generator

—

Grupo #6 Cifrado de información

¿Cuál es la historia del PRG? (Brevemente)

Es un tipo de generador de congruencia lineal (LCG) que opera en grupo multiplicativo de enteros módulo n . Fue primeramente implementado en 1951, sin embargo, fue propuesto por Stephen K. Park y Keith W. Miller en 1988



¿Cómo funciona? (Pseudocódigo)

```
Begin
   Declare variables n, a, b, c and seed
   Read variables n, a, b, c and seed
   Uniform()
   Declare variable hi, lo, t
   hi=seed divided by b
   lo = seed - b * hi
   t = a * lo - c * hi
   if (t > 0)
      seed = t;
   else
      seed = t + n;
      return seed;
   Done
   For i =0 to n
      Call the function random
   Done
End
```

¿Se sigue usando en la actualidad? ¿Por qué?

Como tal, no se sigue utilizando el formato original que se estableció en 1951. Aun así, el diseño de este ha sido de muy gran influencia para generadores creados en la actualidad.

¿Recomendarían que el PRG se use en la vida real? ¿Por qué?

Consideramos que no sería muy eficaz su implementación actualmente, ya que es un generador un poco antiguo y extenso. A pesar que su diseño es muy limpio, es mejor tomarlo solamente como base para crear otros.

Referencias

Wikipedia (2020), Lehmer random number generator Extraido de: https://en.wikipedia.org/wiki/Lehmer_random_number_generator