



PASIÓN POR EDUCAR

**Nombre del alumno: Johanne Joaquín Arriaga Díaz**

**Nombre del profesor: Icel Bernardo Lepe Arriaga.**

**Nombre del trabajo: Mapa conceptual unidad II.**

**Materia: Simulación.**

**Grado: Octavo cuatrimestre.**

**Grupo: ISC13SDC0119-F**

PASIÓN POR EDUCAR

# NUMEROS PSEUDOALEATORIOS

Generación de números pseudoaleatorios.

Pruebas estadísticas de aleatoriedad.

Generación de variables aleatorias.

Un número pseudoaleatorio es el valor de una variable aleatoria  $x$  que tiene una distribución de probabilidad uniforme definida en el intervalo  $(0, 1)$ .

Aleatorio

La generación de cualquier variable aleatoria se va a basar en la generación previa de una distribución uniforme  $(0,1)$ . Y las transformaciones de dichos números generados en valores de otras distribuciones.

En experimentos de simulación es necesario generar valores para variables aleatorias representadas estas por medio de distribuciones de probabilidad.

Algo es aleatorio, cuando no se puede volver a reproducir con los medios actuales, en un tiempo más o menos corto, en exactamente las mismas condiciones.

Las técnicas se pueden agrupar en:

Para generar entradas estocásticas (probabilísticas) para un modelo de simulación, se necesita un generador de números pseudoaleatorios.

Seguridad en redes

- Ø Método de la transformada inversa
- Ø Método de aceptación-rechazo
- Ø Método de composición
- Ø Método de convolución

Métodos anteriores para generar números aleatorios.

Para la Informática, en la seguridad en redes tiene mucha importancia, ya sea en cifrados asimétricos como en los simétricos

Variables aleatorias discretas.

Seguridad-informática

Al realizar un experimento generalmente estamos interesados en alguna función del resultado más que en el resultado en sí mismo.

Ruedas giratorias, lanzamientos de dados, barajas, métodos aritméticos, pero la computadora permite crear generadores de números aleatorios de manera sucesiva.

En la seguridad-informática es muy importante la aleatoriedad. Anteriormente cuando se asignaban login la contraseña se formaba a partir de una política fija, con lo que cualquiera que supiera los datos de otro podía averiguar su contraseña. Es importante que aunque el usuario siga una política fija, la contraseña sea aleatoria.

Variables aleatorias continuas.

Para que los números sean aleatorios deben cumplir características:

Cifrado simétrico y asimétrico

Se dice que una variable aleatoria  $X$  es continua si su conjunto de posibles valores es todo un intervalo de números reales.

- Deben estar uniformemente distribuidos.
- Deben ser estadísticamente independientes.
- Su media debe ser estadísticamente igual a  $1/2$ .
- Su varianza debe ser estadísticamente igual a  $1/12$ .
- Deben ser reproducibles.

Primero se usó cifrado simétrico, ahora cifrado asimétrico con clave pública-privada, quizás el futuro la teoría del caos, al igual que en otras ciencias donde se ha pasado del determinismo a la estadística y de la estadística a la teoría del caos para poder explicar ciertos fenómenos.

Pruebas T.

La prueba t de 1 muestra se usa para estimar la media de procesos y compararla con un valor objetivo. Es sensible al supuesto de normalidad cuando la muestra es moderadamente grande y el intervalo de confianza  $t$  para la media son apropiados para cualquier muestra con un tamaño de 30 o más.