Criptografía y Cifrado de Información 2021

Lab 04

12.agosto.2021

En este laboratorio implementaremos tet estadísticos para evaluar la calidad de los genereadores pseudo-aleatorios (PRGs).

1. Implementar una batería de 10 tests estadísticos para cadenas de bits, incluidos en el estándar 800-22 de NIST.
   Para simplificar el trabajo, se puede usar alguna de las implementaciones en Python ya existentes (disponibles en Github):

   - `https://github.com/GINARTeam/NIST-statistical-test`
   - `https://github.com/dj-on-github/sp800_22_tests`

   Aquí la idea es que cada uno de los 10 tests reciba como argumento una cadena de bits, y devuelva los siguientes: p el p-valor de probabilidad, y un resultado booleano que indique si la cadena pasó o no pasó el test ($1 =$ success, $0 =$ fail).

2. Elabore una función que, dada una cadena de bits, elabore una tabla resumen de los 10 tests estadísticos (similar a la que se mostró en el aula).

   Aplicar esta función a sus tres ejemplos buenos y sus tres ejemplos malos del Lab 03, para tener una métrica de evaluación de sus ejemplos. Para cada uno, elaborar una tabla que resuma sus métricas.
   A partir de los resultados de los tests, indique si sus cadenas se pueden considerar aleatorias o no.

3. Con los generadores pseudo-aleatorios implementados en el Lab 03, genere 1000 cadenas pseudo-aleatorias diversas (1000 de cada uno). Ejecute la batería de test para estas cadenas y elabore un histograma de frecuencias del número de tests fallados por sus cadenas aleatorias.
   En función de la gráfica obtenida, discuta si su generador pseudo-aleatorio hace un buen trabajo o no.
