Protocolo de corrección de la práctica 2

Componentes del grupo

2.1 Estudio de secuencias pseudoaleatorias

Determinar el periodo de las secuencias contenidas en los archivos

encontrarperiodo1.txt sol:
encontrarperiodo2.txt sol:
encontrarperiodo3.txt sol:
encontrarperiodo4.txt sol:

2.2 Postulados de Golom

Determinar qué postulados verifican las secuencias (hay un sólo periodo) de los archivos siguientes:

postulados2.txt (longitud 41)
postulados3.txt
postulados4.txt
postulados5.txt (cumple el 3)

intentarlo también para

postulados1.txt (longitud 8191), aunque puede resultar largo

2.3 **LFSR**

Generar sendas secuencias de longitud 8191 con el polinomio

X^13+X^12+X^11+X^5+X^2+X+1

y las semillas

100 001 111 001 0
010 011 110 000 1

2.4 NLFSR

Generar secuencias de longitud 200 dígitos/bits con cada una de las combinaciones de los ficheros de mintérminos

minterminos1.txt
minterminos2.txt

con las semillas

(1) 0101011

(2) 0111111

llamarlos nlfsr_ab.txt siendo a el número del archivo de mintérminos y b el número de semilla.

2.5 A5/1

Generar una secuencia cifrante de 200 dígitos/bits obtenida con el archivo semilla1.txt y almacenarla en un archivo de nombre a5semilla1.txt

2.6 Cifrador en flujo

Cifrar, usando la semilla1.txt y A5/1, el archivo prueba

Intentar descifrar el archivo leeme_cifrado.txt usando A5/1 y semilla1.txt.

Realizar pruebas de cifrado y descifrado con los archivos en la carpeta CIFRAR.

Explicar las mejoras añadidas a la práctica.

SUBIR A SWAD JUNTO A LA PRÁCTICA:

- **los cuatro archivos nlfsr_ab.txt (a,b=1,2)**
- **el archivo generado con A5 a5semilla1.txt**
- **el cifrado del archivo prueba usando la semilla1.txt**