CRIPTOGRAFIA

Práctica 2

FSR Y CIFRADO EN FLUJO

Juan José Segura González - Valentín Pérez Carrasco 11/05/2011 Para ejecutar los programas bastará con usar la opción java –jar nombr_jar.jar y se abrirá en un modo terminal debido a las limitaciones a la hora de realizar la práctica no se ha podido entregar una interfaz. Las instrucciones de los parámetros de cada ejecutable están claramente expuestas una vez que se ejecutan.

- Para la ejecución del cálculo del periodo se ejecutara postulados_y_periodo.jar, ya que en el mismo se han incluido el cálculo del periodo de una semilla y el cumplimiento de los tres periodos.
- Para el nlfsr se usará el ejecutable nlfsr.jar.
- Para el a51 se usará el ejecutable a51.jar
- Para el Ifsr se usará el ejecutable Ifsr.jar.
- Para cifrar y descifrar, cadenas de números, se usará cifrado.jar.

Los resultados obtenidos del periodo y el cumplimiento de los postulados son los siguientes:

- Encontrarperiodo1.txt → 8191.
- Encontrarperiodo2.txt → No tiene.
- Encontrarperiodo3.txt → 31.
- Encontrarperiodo4.txt → No tiene.

Postulados:

- Postulados1.txt → Cumple el 1 y el 2, el 3 tarda mucho en calcularlo.
- Postulados2.txt → Cumple el 1, 2 y 3 postulado.
- Postulados3.txt → Cumple el 1 postulado. El 2 y el 3 no.
- Postulados4.txt → Cumple el 1 y el 2 postulado. El 3 no.
- Postulados5.txt → Cumple el 3 postulado. El 1 y el 2 no.