Modelos de Computación
Grado en Ingeniería Informática
Asignación de Prácticas Número 5

1. Descripción

Los cifrado de flujo son útiles en aquellas situaciones donde el volumen de datos a transmitir cifrados no es constante en el tiempo, como por ejemplo una conversación telefónica. Se construyen cifrando los bits de mensaje mediante la función XOR, aplicada bit a bit entre un bit de mensaje y un bit cifrante. El cifrado es tan robusto como lo sea la secuencia de bits cifrantes, que deberá tener una clave privada compartida entre transmisor y receptor. Generalmente, la secuencia de bits de cifrado se provee a través de alguna técnica de generación de bits aleatorios. En nuestro caso, utilizaremos como secuencia de bits de cifrado la evolución temporal de la célula central de un autómata celular 1-D. Para ello deberá:

- Investigar el espacio de reglas aditivas con $k = 2$ y $r = 1$. Para cada una de ellas desarrollará un análisis del AC correspondiente para 1024 células, 1000 generaciones, configuración inicial aleatoria, determinando distancia de Hamming media, entropía espacial media y entropía temporal para una célula dada (por ejemplo, la central). Filtrará aquellas reglas que se puedan considerar lo suficientemente caóticas para actuar en el cifrado.
- Escogerá una de las reglas resultantes del filtrado, justificando por qué, para desarrollar el cifrado. La reglas válidas, la regla escogida y la justificación se incluirán en un documento `analisis.pdf`.
- Desarrollará el cifrado de forma que se puedan cifrar textos cortos con la regla escogida.
- Hay ayudas para la implementación, **junto con especificaciones adicionales a cumplir obligatoriamente en el documento de Notas Auxiliares** disponible en la carpeta de la prácticas.

2. Procedimiento de Entrega

Tarea Moodle, donde entregará única y exclusivamente los ficheros que se indican a continuación. Los fuentes .java deben compilar directamente con cualquier distribución razonablemente reciente del kit de desarrollo de Java sin necesidad de recurrir a entornos auxiliares.

- `analisis.pdf`
- `cipherVernam.java`