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

1 Ejercicios

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 transmitor 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 de AC correspondiente para 1000 células, 4000 generaciones, determinando distancia de Hamming media, entropía espacial media y entropía temporal. Filtrará aquellas reglas que se puedan considerar lo suficientemente caóticos para actuar en el cifrado.
- Escogerá una de las reglas resultantes del filtrado, justificando por qué, para desarrollar el cifrado.
- Desarrollará el cifrado de forma que se puedan cifrar textos cortos e incluso ficheros de texto. Para la primera opción, la aplicación tendrá una ventana donde se mostrará el texto llano y otra donde se mostrará el texto cifrado. Para la segunda, se escogerá el fichero de texto navegando en la estructura de carpetas de la forma habitual.
- La clave se introducirá mediante texto estándar, y la aplicación las transformará en la secuencia de bits de la configuración incial del autómata celular.

2 Procedimiento y Plazo de Entrega

Se ha habilitado una tarea de subida en *Moodle* que le permite subir cada fichero que forma parte de los productos de la práctica de forma individual en el formato original. Para ello, suba el primer fichero de la forma habitual, y luego siga la secuencia de etapas que el propio *Moodle* le irá marcando. Recuerde además que:

- Los documentos escritos que no sean ficheros de código deben generarse **obligatoriamente** utilizando Latex, a través del editor OverLeaf o con la aplicación que usted quiera.
- No debe hacer intentos de subida de borradores, versiones de prueba o esquemas de las soluciones. *Moodle* únicamente le permitirá la subida de los ficheros por **una sola vez**.
- La detección de plagio o copia en los ficheros de las prácticas, o la subida de ficheros vacíos de contenido o cuyo contenido no responda a lo pedido con una extensión mínima razonable, invalidará plenamente la asignación, sin perjuicio de otras acciones disciplinarias que pudieran corresponder.
- El plazo de entrega de la práctica se encuentra fijado en la tarea de subida del Campus Virtual.
- Entregas fuera de este plazo adicional no serán admitidas, salvo causa de fuerza mayor debidamente justificadas mediante documento escrito.
- Se recuerda que la entrega de todas las asignaciones de prácticas es recomendable, tanto un para un correcto seguimiento de la asignatura, como para la evaluación final de prácticas, donde puede ayudar a superar esta según lo establecido en la ficha de la asignatura.