PRÁCTICA 2

CIFRADOS CLÁSICOS O CIFRADO EN FLUJO

Para hacer esta práctica, hay que elegir una de las dos opciones que se plantean: Cifrados clásicos o cifrado en flujo.

2.1. Cifrados clásicos.

Si eliges esta opción, te serán entregados algunos textos que han sido cifrados siguiendo alguno de los sistemas que hemos visto (sustitución monoalfabética, Vigènere, Alberti, etc.).

El objetivo de la práctica es hacer un análisis de los textos para conseguir descifrarlos.

2.2. Cifrado en flujo.

Si eliges esta opción, deberás realizar un programa que:

- Dada una sucesión de bits, determine si es o no periódica, y en caso afirmativo, determine la longitud del periodo (para que sea periódica, el periodo debe aparecer en la sucesión al menos dos veces).

- Dado un polinomio $p(x) \in \mathbb{Z}_2[x]$ de grado n, y tal que $p(0) = 1$, y una sucesión de n bits, construya la sucesión pseudo-aleatoria que generaría un LFSR, con polinomio de conexión $p(x)$, y semilla la sucesión de n bits dada. La salida debe ser guardada en un fichero de texto, y debe contener, al menos, dos veces el periodo.

- Dada una sucesión de bits periódica, determine la complejidad lineal de dicha sucesión, y el polinomio de conexión que la genera. Para esto, se usará el algoritmo de Berlekamp-Massey.

- Dadas dos (o más) sucesiones periódicas, y una funcíón de mezcla, construya la nueva sucesión que resulta de aplicar la función de mezcla a las sucesiones dadas.

Las sucesiones que hay que introducir para los apartados primero, tercero y cuarto, deberán ser leídas de un fichero de texto, y opcionalmente, introducirlas por pantalla.

Aparte de esto, si se desea, el programa podrá realizar lo siguiente:

- Dada una sucesión periódica, determinar si se satisfacen los postulados de Golomb.

- Dada una función booleana de n variables, y una sucesión de n bits, construir la sucesión que generaría un NLFSR de n celdas, con función generadora la función dada, y semilla la sucesión de n bits.

La fecha límite para la entrega es el día 7 de mayo. Los ficheros hay que subirlos al SWAD, a la zona de "Mis trabajos". Si la práctica se hace en grupo, es suficiente con que la suba uno del grupo. Pero hay que indicar quienes son los componentes.

Para que la práctica se evalúe debe ser defendida por todos los miembros del grupo.