Codificando y decodificando

El envío de mensajes cifrados para evitar miradas indiscretas se lleva estudiando desde la antigüedad. El método más simple consiste en manejar tablas de traducción que contienen, para cada letra, por qué otra letra se sustituirá en el mensaje cifrado. El descifrado maneja las tablas inversas que permiten recomponer el mensaje original. Además, para dificultar el trabajo a los posibles espías, muchos de estos mecanismos primitivos *no* consideran el espacio separador de palabras como parte del mensaje por lo que el receptor al decodificar ve todas las letras seguidas y tiene que ser él, a la vista de las mismas, el que separe las palabras.

Existe otro mecanismo simple que consiste en, sencillamente, *cambiar de orden* las letras, siguiendo unas determinadas reglas. Si esas reglas están bien elegidas, el proceso de codificación y el de decodificación es el mismo, por lo que no se necesita implementar algoritmos distintos en cada lado de la comunicación.

Los alumnos del Grado de Ciberseguridad, tras conocer y entender el funcionamiento de las estructuras de datos tipo árbol, han ingeniado un método para poder codificar/decodificar palabras mediante el uso de esta estructura.

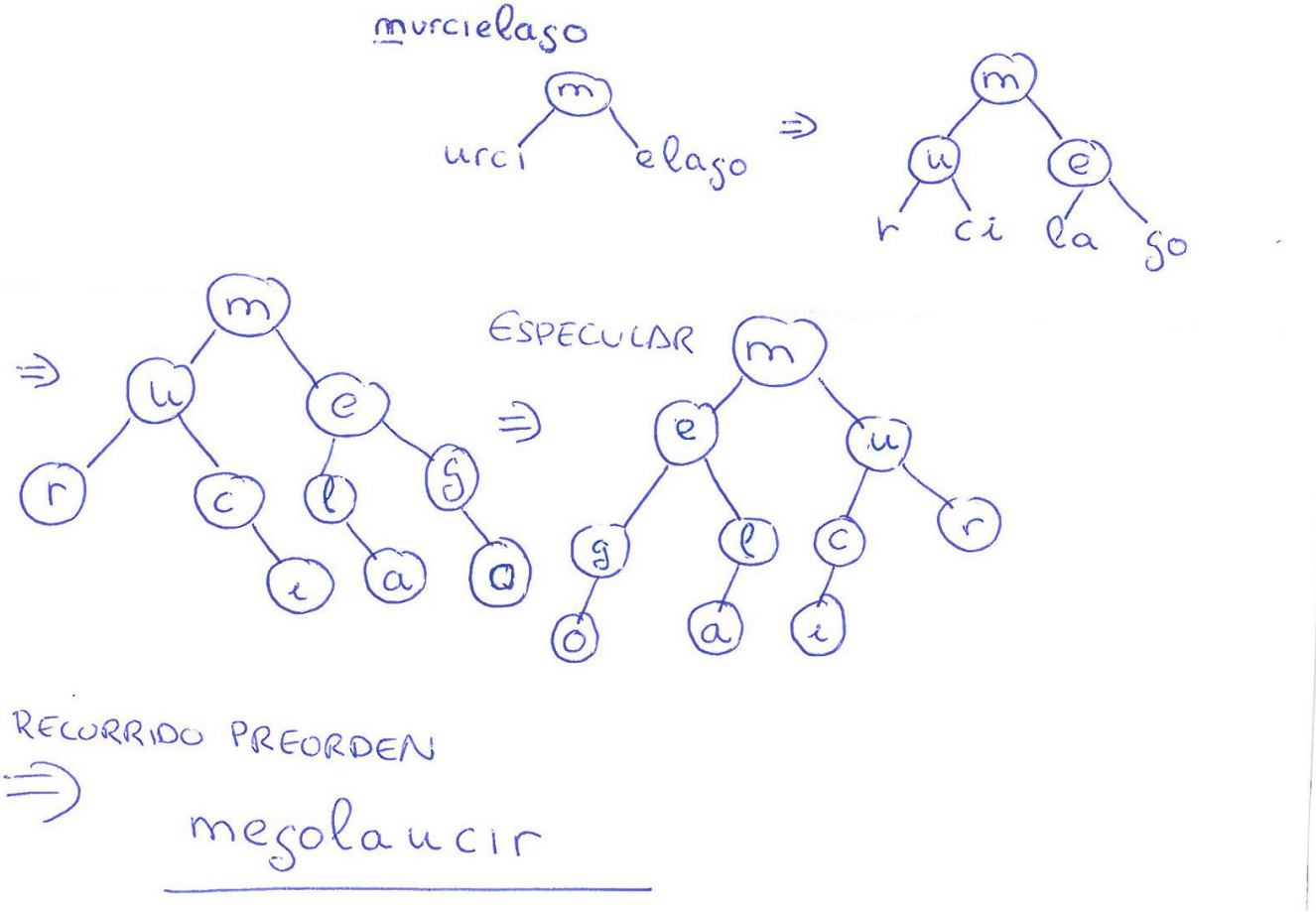
Dicho mecanismo de codificación/decodificación se basa en representar el mensaje como un árbol binario tal que su recorrido en *preorden* es la palabra a codificar/decodificar, además de incluir una "simetrización" del árbol.

Dado que existan muchos posibles árboles que cumplan lo anterior, han desarrollado un método para construir un árbol cuyo recorrido *preorden* coincide con el de la palabra. Para ello, de cada palabra cogen la primera letra, la cual es la raíz del árbol. El resto de los caracteres de la palabra son partidos en dos partes. Estas partes serán iguales si dicho número es par o bien una de las dos tendrá un carácter más que la otra. **En este punto se diferencian el procedimiento de codificar/decodificar. Si se está codificando la palabra, es la segunda mitad la que tendría un carácter más. Si, por el contra, se está decodificando, es la primera parte la que tendría el carácter adicional**. Este proceso se repetiría de manera recursiva con cada una de las partes en las que ha sido dividida la palabra original. Cuando la palabra sea vacía, se devolverá el árbol vacío. En el siguiente ejemplo se puede ver como se "arbolifica" la palabra *murciélago* y como se decodifica la palabra *megolaucir* (cuya descodificación da murciélago).

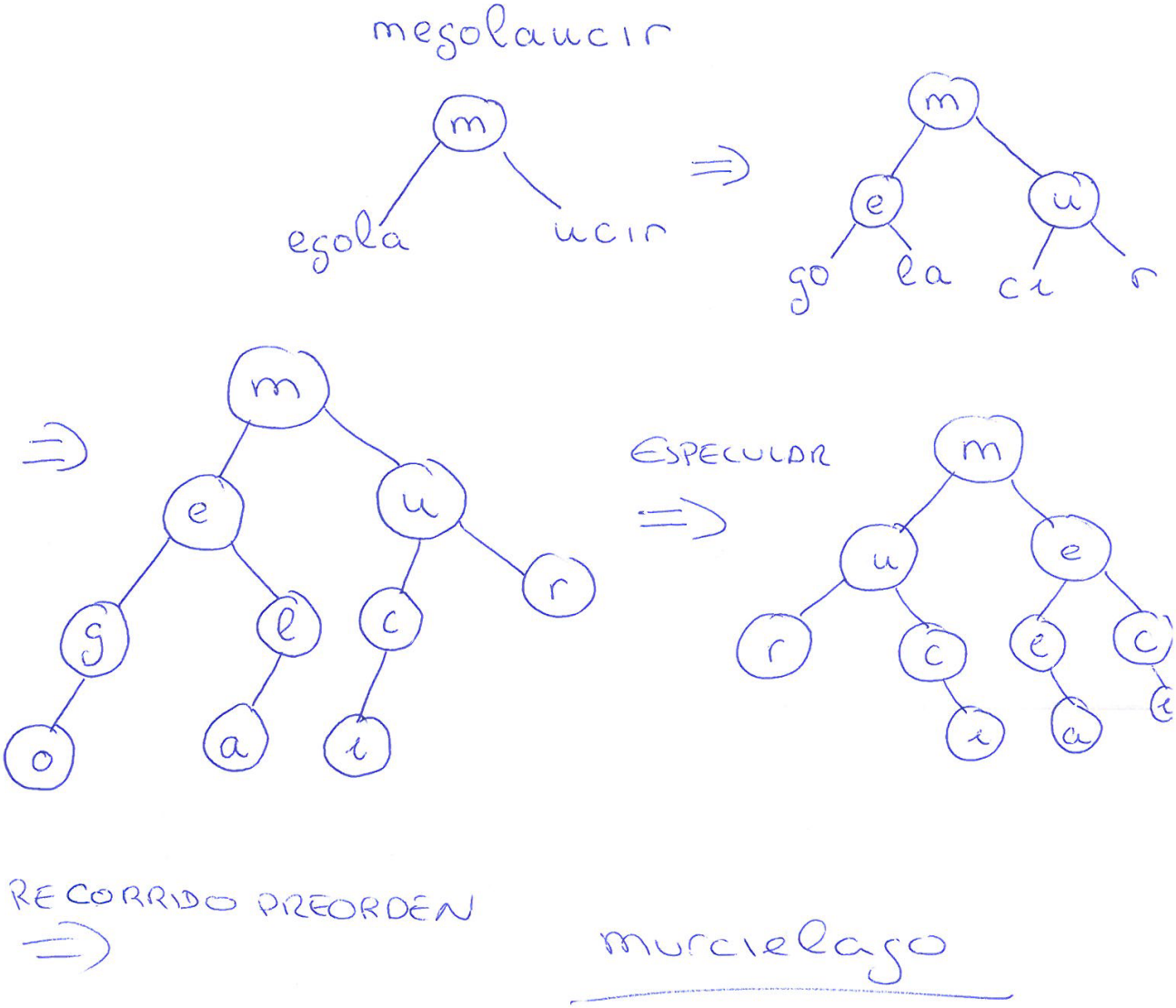
Una vez que se tiene el árbol binario de la palabra a codificar/decodificar, se creará la imagen especular del árbol. El resultado final de la codificación/decodificación será el recorrido preorden del árbol especular.

Nota**: Si tienes implementado en el TADArbol las operaciones espejo y preorden, no es necesario implementar nada más en dicha estructura.**

Codificación murciélago



Decodificación *megolaucir*



RECORRIDO PREORDEN

murcielago