EJERCICIO C2/3

1. Descifrar un texto mediante un cifrado de transposición.

La transposición constituye uno de los métodos básicos de cifrado. Su principio se basa en cambiar la posición de un carácter en el texto. Un ejemplo de sistema de cifrado de transposición es el conocido como parrilla de Fleissner, cuyo funcionamiento puede verse en la imagen siguiente. Este sistema de cifrado, inventado en el siglo 16, fue descrito por Julio Verne en su novela Mathias Sandorf.

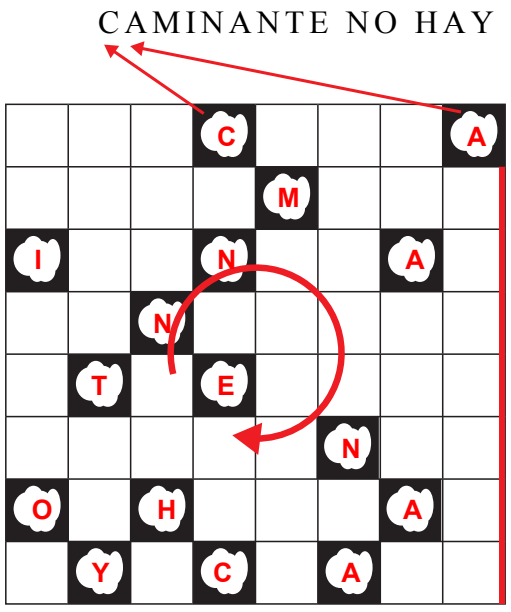
El siguiente mensaje ha sido cifrado mediante un cifrado de transposición simple. Para descifrar lo que debemos hacer es preparar una parrilla de descifrado. El descifrado se realiza a partir de desplazamientos correctos de la parrilla y la lectura gradual de los caracteres que se pueden ver a través de sus ventanas.

Escribe el texto cifrado en la parrilla vacía (abajo) - de izquierda a derecha y de arriba a abajo. Ajusta la parrilla de descifrado. Lee y ten en cuenta los caracteres visibles, a continuación, gira la rejilla de 90 ° y repita el procedimiento (tres veces). Sólo se pueden conseguir los resultados correctos si la colocación inicial de la rejilla es la correcta y la dirección de su rotación también.

¡Atención! Tenga en cuenta que la rejilla se puede girar hacia en sentido de las agujas del reloj o en dirección contraria, y no se sabe su posición inicial.

CMACL IAANN HOMDA AISRN EDAOH XNAAC NEXTX EXTCX AOMXN NXIOI HOXNA XMYXC AAXO
CAMINANTE NO HAY CAMINO, SE HACE CAMINO AL ANDAR ANTONIO MACHADO

En este ejemplo, la posición inicial es cuando el borde marcado en negrita (se considera que es el borde superior de la parrilla) está en la derecha. Durante el cifrado se va girando la parrilla hacia la derecha (en sentido horario). La división del texto cifrado en bloques tiene razones históricas; la transmisión se basaba en el número de palabras (no caracteres) y la longitud media de las palabras en inglés es de 5 caracteres. El texto no contiene caracteres especiales (nacionales).



Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.