Cifrado Escítala

**Resumen**:

Una escítala ([griego](https://es.wikipedia.org/wiki/Idioma_griego): skytálē) es un sistema de [criptografía](https://es.wikipedia.org/wiki/Criptograf%C3%ADa) utilizado por los [éforos](https://es.wikipedia.org/wiki/%C3%89foro) [espartanos](https://es.wikipedia.org/wiki/Esparta) para el envío de mensajes secretos. Está formada por dos varas de grosor variable (pero ambas de grosor similar) y una tira de cuero o papiro, a las que ambas se pueden denominar escítala.

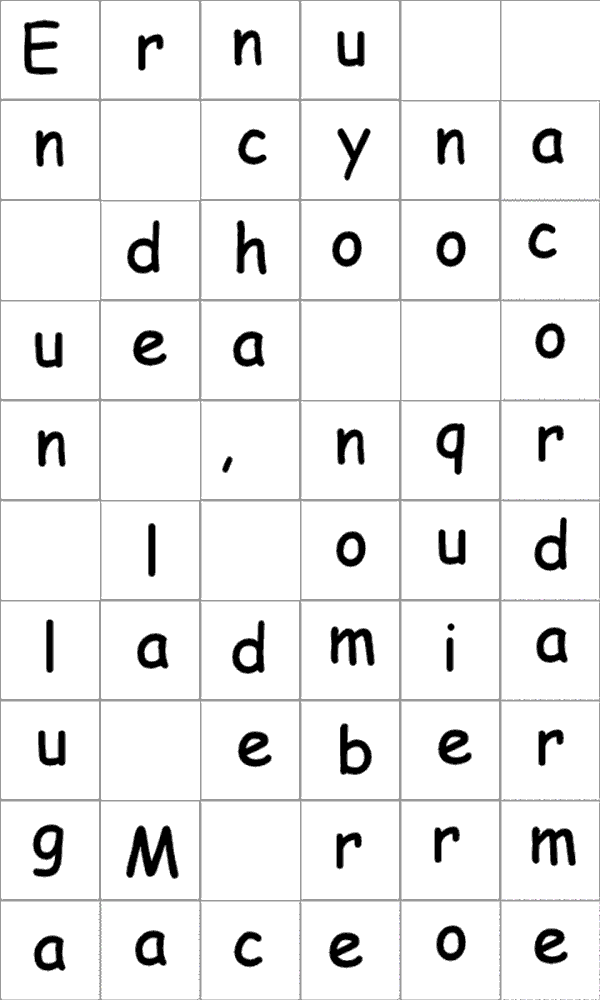
**Creacion de la matriz:**

Para cifrar el mensaje tenemos que colocar el mensaje en una matriz de ancho y altura determinada, asegurar llenar con estacios si todavía el mensaje no tiene el tamaño de la matriz.

**Ejemplo:**



Sea el mensaje a cifrar: *"En un lugar de la Mancha, de cuyo nombre no quiero acordarme"* y sea la escítala de 10 caras, se construye una tabla entonces de 10 medidas de ancho y *largo(mensaje) / 10* medidas de alto (6). A continuación, vamos disponiendo el texto en filas tal como aparece en la imagen de la izquierda.

El texto cifrado resulta al tomar linealmente sin saltos la misma tabla, pero ahora recorriéndola en columnas. Siendo por tanto el mensaje cifrado resultante: *"Ernu n cyna dhoocuea on ,nqr l oudladmiau ebergM rrmaaceoe"*

Descifrar el texto con la escítala es volver a meter la tira de cuero enrollada sobre el palo con el mismo número de caras. De modo similar el mensaje obtenido queda descifrado volviendo a aplicar el mismo método sobre la tabla, sin más que intercambiar las medidas del ancho por el alto. En la segunda imagen (la de la derecha) puede apreciarse el caso.

**Referencias**:

<https://infow.wordpress.com/2008/11/12/criptografia-clasica-i-la-escitala/>

https://es.wikipedia.org/wiki/Escítala