**Cifrado César**

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha. Con nuestro alfabeto el sistema quedaría así:

Alfabeto en claro: A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Alfabeto cifrado: D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

Por ejemplo, si se quiere enviar el mensaje ATACARALAMANECER, lo que se escribirá realmente es DWDFDUDÑDODPHFHU

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.