Cifrado César

Introducción

La cifra César es una de las más tempranamente conocidas y simple cifrado. Es una cifra de sustitución en la cual cada letra en el texto en claro es desplazado un cierto número de lugares en el alfabeto. Por ejemplo, con un desplazamiento de 1 la A sería reemplazada por la B, la B lo sería por la C, y siguiente. El método se llamó así en honor a Julio César, que aparentemente lo usaba para comunicarse con sus generales.

El muy conocido cifrado **ROT13** es simplemente un cifrado César con un desplazamiento de 13. Este cifrado no ofrece seguridad en las comunicaciones, y es fácil de romper, incluso a mano.

Ejemplo

Para enviar un mensaje cifrado de una persona a otra lo primero que se necesita es ponerse de acuerdo en la clave de la cifra. En este caso la clave es el número de desplazamiento.

Un ejemplo rápido de cifrado y descifrado con una clave (desplazamiento) de 1

```
texto en claro: defended el lado este del castillo
texto cifrado:  efgfoefe fm mbep ftuf efm dbtujmmp
```

Criptoanálisis

El cifrado César probablemente sea el más fácil de romper de todos ya que el desplazamiento tiene que ser un número entre 1 y 25. Basta con probar cada posibilidad y encontrar la que genera un texto coherente.

Un método más científico sería el análisis de frecuencias, como se comentó más arriba.