3 Algoritmos

¿Qué son los algoritmos?

Los **algoritmos** son los métodos que se utilizan para transformar el texto claro en el texto cifrado.

Vamos a analizar el cifrado por sustitución del César.

```
    El algoritmo consiste en:

    - Sustituir cada letra del texto sin cifrar por otra letra del mismo alfabeto
que se encuentra situada en el orden del diccionario N puestos por delante.
    - N es el valor de la clave, que como podemos ver, junto con el algoritmo,
determinará exactamente la letra que sustituirá a la original.
```

Algoritmos actuales

Como podemos imaginar, hoy en día se utilizan diferentes algoritmos, algunos válidos para criptografía de clave privada y otras para criptografía de clave pública.

- **Algoritmos de clave privada**: DES, 3DES, RC4, IDEA Y AES son nombres de algoritmos de clave privada.
- **Algoritmos de clave pública**: DH, EIGamal, RSA.

El algoritmo es público

“Suele ser un error muy frecuente pensar que los algoritmos de cifrado deben ser secretos para resultar seguros. Los algoritmos de cifrados utilizados son de dominio público y el código fuente asociado también. Sin embargo, siguen siendo seguros porque requieren que el usuario proporcione la clave secreta”