¿Cuánto tiempo tardaría descifrar el mensaje usando un computador?

Un computador puede probar las **25 posibles combinaciones** (de las letras del alfabeto, sin contar la original) en **menos de un segundo**.
Esto se debe a que el cifrado César tiene muy pocas claves posibles, por lo tanto, es vulnerable a un **ataque por fuerza bruta**.

¿Cuánto tiempo tardaría descifrar el mensaje a un grupo de personas?

Un grupo de personas, dependiendo de su experiencia, podría tardar entre **minutos o hasta una hora**. Al leer el mensaje cifrado, pueden hacer pruebas desplazando letras manualmente (por ejemplo, escribiendo el abecedario y buscando coincidencias).

Además, si el mensaje contiene palabras comunes, una persona con buena comprensión del idioma puede descifrarlo **rápidamente usando la lógica** y el contexto.

¿Es un método seguro para comunicar datos?

No.
El cifrado César **no es seguro** en la actualidad. Fue útil en la antigüedad (como en la época de Julio César), pero hoy se considera un sistema **muy débil**.
Cualquier persona con conocimientos básicos o una herramienta sencilla puede **romper la clave fácilmente**.

¿Cómo se puede mejorar el sistema para hacerlo más seguro?

1. **Usar cifrados más complejos** como:
    - **Cifrado de sustitución polialfabética (como el cifrado de Vigenère)**
    - **Cifrado simétrico moderno (como AES)**
    - **Cifrado asimétrico (como RSA)**
2. **Agregar autenticación y firmas digitales** para verificar la identidad del remitente.
3. **Evitar patrones simples**, usando claves más largas o que cambien dinámicamente.
4. **Cifrar usando software especializado** en lugar de métodos manuales o caseros.
5. **Combinar métodos**: usar múltiples capas de cifrado, VPNs o túneles seguros para transmitir datos sensibles.