

Responder a preguntas como:

¿Cuánto tiempo tardaría descifrar el mensaje usando un computador?

El tiempo que tardaría una computadora en descifrar un mensaje depende de varios factores, la complejidad del cifrado, el método utilizado y la potencia de la computadora, una computadora podría descifrarlo en cuestión de segundos.

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

El tiempo que un grupo de personas se tarde en descifrar un mensaje cifrado va a depender de que tan robusto o complicado sea el mensaje que se envíe y que método de cifrado utilicé, podría tomar mucho tiempo, incluso años, descifrarlo

¿Es un método seguro para comunicar datos?

El cifrado de cesar en la actualidad no es seguro, es una técnica de cifrado simple y es vulnerable a ataques de fuerza bruta.

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

Puedo utilizar un desplazamiento en diferentes partes del mensajeo extender el rango de caracteres que podamos cifrar.

Formas de mejorar el cifrado César:

1. **Cifrado de Vigenère:**

En lugar de un desplazamiento fijo, se utiliza una palabra clave para determinar el desplazamiento en cada posición del mensaje. Esto hace que el cifrado sea más complejo y más difícil de descifrar.

2. **Extender el rango de caracteres:**

En lugar de usar solo letras del alfabeto, se pueden incluir números, símbolos y otros caracteres, lo que aumenta el espacio de claves posibles.

3. **Generación aleatoria de claves:**

Se puede generar una clave aleatoria para cada mensaje, lo que dificulta la predicción de la clave utilizada.

4. **Uso de múltiples claves:**

Se pueden utilizar diferentes claves para diferentes partes del mensaje, lo que dificulta el análisis de frecuencia y otros métodos de ataque.

5. **Cifrado en capas:**

Combinar el cifrado César con otros algoritmos de cifrado para aumentar la complejidad y seguridad.