TALENTO TECH
Bootcamp en Ciberseguridad
Estudiante: Marino Bastidas Rosero

Actividad cifrado César

¿Cuánto tiempo tardaría descifrar el mensaje usando un computador?

Sería cuestión de segundos si se cuenta con un script que evalúe los posibles desplazamientos y emplee diccionarios para detectar palabras válidas en el respectivo idioma.

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

En este caso se hablaría de minutos en función del número de personas y si el mensaje es muy largo se podría seleccionar una sección para intentar descifrarla por fuerza bruta e identificar el desplazamiento.

¿Es un método seguro para comunicar datos?

Absolutamente no, ya que tiene múltiples vulnerabilidades como por ejemplo la no codificación de los espacios en blanco, el número de caracteres de entrada es igual al de salida y requiere entre 26 y 27 desplazamientos posibles en un ataque de fuerza bruta.

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

Se debería codificar los espacios en blanco e implementar una llave dinámica para realizar operaciones adicionales con e texto a cifrar y logra mayor alinealidad entre la salida y la entrada.