Actividad

Explicar a los estudiantes el cifrado césar y pedirles que formen 2 o más grupos (pares). Cada grupo definirá una clave (un número entero entre 1 y 27) que determina cuantos caracteres se rotará el alfabeto. Luego escribirán un mensaje.

Luego, los grupos intercambiarán mensajes para intentar descifrar el mensaje oculto.

Finalmente, cada grupo revelará la clave que tenía junto con el mensaje.

Al finalizar la actividad se debe discutir con los estudiantes qué tan seguro es el método de cifrado.

Responder a preguntas como:

¿Cuánto tiempo tardaría descifrar el mensaje usando un computador?

R: El tiempo que se tardaría en descifrar el mensaje con el algoritmo de cesar depende mucho de la velocidad del pc, si son menos de 100 caracteres serian milisegundos para mensajes cortos.

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

R: dependería mucho del factor porque si las personas trabajan en equipo más rápido pueden descifrar el mensaje, la experiencia también incluye, por lo general puede ser un proceso relativamente rápido, si se trabaja de manera eficiente.

¿Es un método seguro para comunicar datos?

R: El cifrado de cesar un es un método seguro porque es fácil de descifrar mediante fuerza bruta o un análisis de frecuencia y también no es resistente a ataques, lo que significa que un atacante puede descifrar el mensaje con relativa facilidad.

¿Cómo se puede mejorar el sistema para hacerlo más seguro?
R: para mejorar la seguridad del cifrado de cesar se pueden implementar varias modificaciones como, aumentar la complejidad del cifrado, utilizar un cifrado poli alfabético que es utilizar barios alfabetos, agregar una capa de cifrado adicional, utilizar claves mas seguras que tengan símbolos y que sean extensas, implementar autenticación y verificación estas serian algunas alternativas para poder mejorar el sistema, pero hay que tener en cuenta que el cifrado de cesar es un cifrado simple y no es adecuado para guardar información confidencial.