Actividad 1: **Actividad cifrado césar** **UNIDAD 1**

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?

En un PC moderno: Aunque depende de su capacidad de procesamiento y RAM disponible, pensaría que al menos un 1 milisegundo, ya que solo requiere pasar 26 o 27 posiciones y es extremadamente rápido.

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

Depende del grupo de personas y del conocimiento que se tenga sobre los tipos de cifrado. Ejemplo: Sin conocimiento previo pero inteligente o meticulosos diría que minutos u horas (dependiendo del tamaño del mensaje). Un grupo podría probar manualmente los 27 desplazamientos en 10-30 minutos si son organizados y se reparten el trabajo, incluso podría ser más rápido si alguno descubre un patrón en las letras o una palabra en concreto.

Con conocimientos básicos de criptografía: Menos de 5 minutos usando Análisis de frecuencia de letras (como "e", "a", "o" son las más comunes en español). Patrones en palabras cortas ("y", "el", "la").

¿Es un método seguro para comunicar datos?

No es un método seguro, ya que su forma y escritura es sencilla de descifrar para alguien conocedor de criptografía. Sobre todo, porque no cambia sus espacios o cifra signos de puntuación lo que ayuda a intuir que es un texto plano. En pocas palabras el cifrado cesar es un algoritmo extremadamente vulnerable a ataques de fuerza bruta por su espacio de claves minúsculo.

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

Como tal el algoritmo cesar es considerado de los más básicos o fáciles de romper, de pronto aplicándole clave variable al texto. Es decir, cada palabra que tenga su propio código de desplazamiento, aunque intercepten una palabra el resto del texto seguirá cifrado si no tienen el código para leerla, sin embargo sería más trabajo para quien lo cifra y no es seguro ya que con tiempo puedes descifrar todas las letras, otra forma seria usar un doble cifrado, por ejemplo que el texto este escrito con símbolos y cifrado con cesar, la otra persona debe conocer el significado de los símbolos y desbloquearlos con el cifrado cesar para que tengan su orden original, aunque es un método aún mas ineficiente que el primero puede ayudar a despistar a más personas. Por último, Sustitución polialfabética que cambia el alfabeto de desplazamiento en cada carácter, pero esto es un tema diferente ya que entra en la categoría del cifrado Vigenère.