Ejercicio 1: Simulación de API REST segura en Java (sin frameworks)

Objetivo: Simular una API REST básica con autenticación mediante un token para proteger los endpoints.

Instrucciones:

- Crea un servidor HTTP simple utilizando `ServerSocket` que escuche en el puerto 8080.
- Implementa la verificación de un token en el encabezado `Authorization`.
- Si el token es válido, concede acceso; si no, responde con un error de autenticación.

Ejercicio 2: Validación de entradas en una API

Objetivo: Validar correctamente los parámetros de entrada en una API para evitar inyecciones como SQL Injection.

Instrucciones:

- Implementa un método que valide nombres de usuario usando expresiones regulares.
- Asegúrate de que el nombre solo contenga caracteres alfanuméricos y tenga una longitud entre 3 y 15 caracteres.
- Rechaza nombres con caracteres peligrosos como `<`, `>`, `'`, etc.

Ejercicio 3: Encriptación de respuestas sensibles

Objetivo: Cifrar respuestas sensibles antes de enviarlas al cliente.

Instrucciones:

- Usa codificación Base64 para simular el cifrado de un mensaje.
- Implementa un método para cifrar la respuesta antes de enviarla.
- Simula en el cliente la decodificación de esa respuesta cifrada.

Ejercicio 4: Control de acceso por rol en API

Objetivo: Implementar control de acceso basado en roles (por ejemplo, sólo los administradores pueden acceder a ciertos recursos).

Instrucciones:

- Simula una base de datos de usuarios con roles asignados (admin, user, guest).
- Verifica que solo los usuarios con rol `admin` puedan acceder a un recurso sensible.
- Rechaza el acceso a usuarios con otros roles.