

# PRÁCTICA 3: Protocolos (Parte B)

Seguridad de la Información  
Curso 2019-2020

Lenguajes y Ciencias de la Computación.  
E.T.S.I. Informática, Universidad de Málaga

**RELACIÓN DE EJERCICIOS:**

---

1. Implementar el protocolo Needham-Schroeder básico (ver transparencias del tema 3, parte 1.2).

Tener en cuenta los siguientes aspectos:

- a. El cifrado entre todas las entidades (A, B y TTP) debe ser AES 128 GCM.
- b. Al igual que en la práctica 3 (Parte A), se utilizará la clase `SOCKET_SIMPLE_TCP` del campus virtual, que permite crear un cliente y un servidor TCP básicos.