

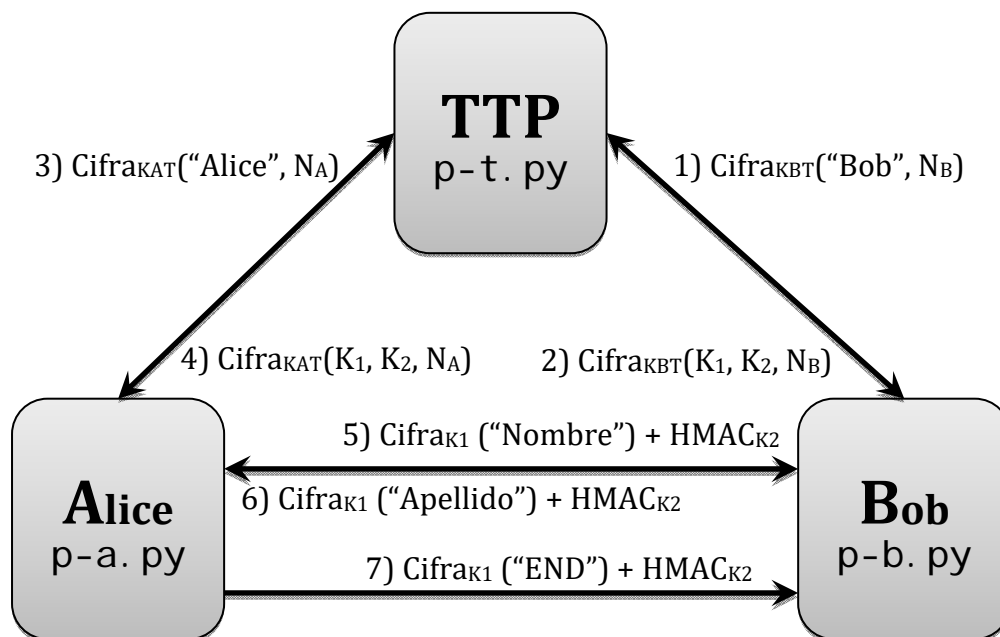
# PRÁCTICA: Protocolos II

Seguridad en la Información  
Curso 2022-2023

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

**RELACIÓN DE EJERCICIOS:**

1. Se pide implementar el siguiente protocolo entre Alice y Bob y la tercera **parte confiable TTP** indicado en la figura de abajo, donde tanto **B** como **A** contactan con el **TTP** y **reciben dos claves simétricas**; y posteriormente **A** envía a **B** el nombre del alumno/a, **B** responde a **A** con su apellido, y **A** le envía a **B** el comando END, tras lo cual tanto **A** como **B** cierran sus conexiones. El código fuente parcial del **TTP** (y las claves  $K_{AT}$  y  $K_{BT}$ , las cuales se generarán automáticamente al ejecutar TTP) y **B** ya se proporciona en el campus virtual.



El alumno/a deberá tener en cuenta los siguientes aspectos:

- a. En este ejercicio, se utilizará la clase `SOCKET_SIMPLE_TCP` del campus virtual
  - i. TTP actuará como servidor de las conexiones de **A** y **B**, mientras que **B** actuará como servidor de las conexiones de **A**.
- b. El mecanismo de cifrado a utilizar en los **pasos 1), 2), 3) y 4)** será **AES GCM**. Sin embargo, el mecanismo de cifrado en los **pasos 5), 6) y 7)** será **AES CTR**. Es por eso que para asegurar la integridad del mensaje será necesario el uso de **HMAC (SHA256) con la clave  $K_2$** . Para la implementación de las funciones criptográficas se utilizará la **librería funciones\_aes**, disponible en el campus virtual.
  - i. Cabe mencionar que la librería `funciones_aes` es distinta de la práctica anterior. Se aconseja revisar la API de la librería junto con los comentarios.
- c. Para construir los mensajes entre **A**, **B**, y **TTP**, se **utilizará el formato JSON**.
- d. Antes de ejecutar los pasos 5 y 6, **A** y **B** deben comprobar que los nonces recibidos de T son los que se enviaron anteriormente.