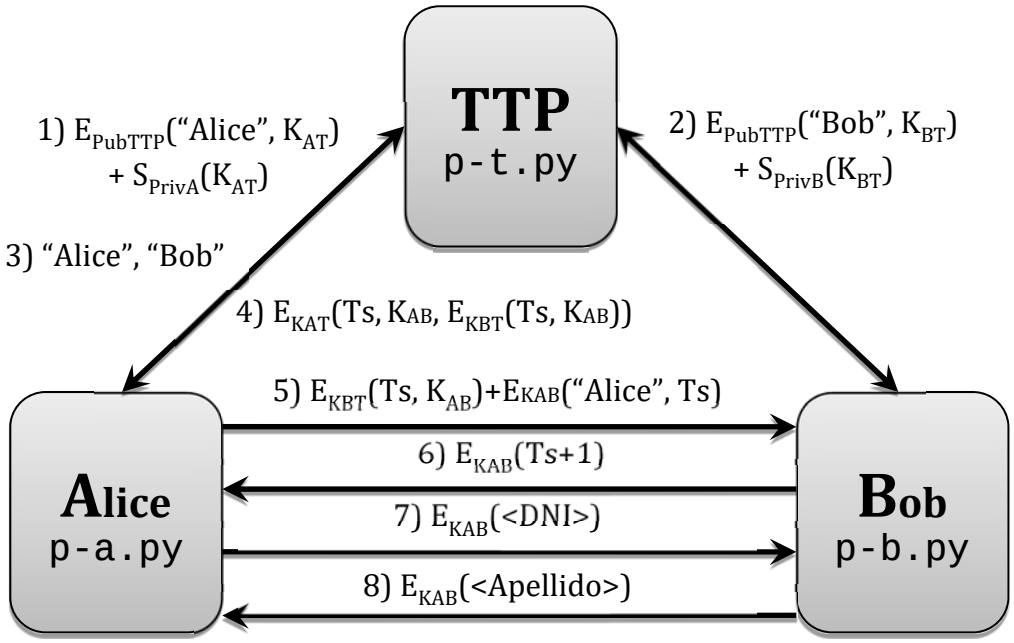
PRÁCTICA EVALUABLE: PROTOCOLOS

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. (**10 puntos**) Se pide implementar el siguiente protocolo entre **A**lice y **B**ob y la tercera parte confiable **TTP** indicado en la figura de abajo.



Al principio (pasos 1 y 2), tanto **A** como **B** contactan con la **TTP para enviarle una clave simétrica**, generada por ellos, que se utilizará para la comunicación posterior. Tras esto, cuando **A** quiera comunicarse con **B** mandará un mensaje a **TTP** informando de ello (paso 3) y la TTP responderá con un mensaje cifrado con la clave simétrica que comparte con **A** (paso 4). Este mensaje contiene, entre otras cosas, una **clave de sesión K_{AB}** que **A** y **B** usarán para comunicarse. A continuación (paso 5), **A** enviará a **B** un nuevo mensaje que consta de dos elementos, uno de ellos ya cifrado con la clave de sesión K_{AB} y otro obtenido del mensaje recibido en el paso anterior. **B** responde a **A** con un nuevo mensaje que contiene un valor de tiempo Ts, recibido de **A** y **TTP** al que **B** suma 1. Finalmente, si todo el proceso ha ido bien, A enviará a B un mensaje cifrado con la clave de sesión K_{AB} que contiene el DNI del alumno y **B** responderá con un mensaje igualmente cifrado que contiene el apellido del alumno.

Los pasos 1 y 2 contarán **3.5 puntos**, los pasos 3, 4, 5 y 6, **3.5 puntos**, y los pasos 7 y 8, **3 puntos**. En caso de que un paso sea incorrecto (p.ej. paso 3), no contarán puntuación los pasos posteriores (p.ej. pasos 4-8).

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 4-8 estará basado en AES.** Sin embargo, queda a elección del alumno el modo de cifrado a utilizar. En cualquier caso, será recomendable el uso de un modo de operación autenticado para los pasos 7 y 8. En caso de no utilizar un modo de cifrado autenticado, la puntuación máxima en esa parte será de 2 puntos.

c. Para construir los mensajes entre **A**, **B**, y **TTP**, se utilizará el formato JSON.
d. En todo momento se deberán comprobar que los mensajes y valores recibidos son correctos.

e. Suponemos que TTP genera una clave y la parte publica la pone en un fichero que tanto A como B disponen de ella para poder cifrar y comunicarse con TTP.