**RELACIÓN DE EJERCICIOS**

**EJERCICIO 1:**

Teniendo en cuenta el siguiente protocolo:

1. **A**  **B : A**
2. **B**  **A: Nb**
3. **A**  **B: KAT{Nb}**
4. **B** **T: KBT{A, KAT{Nb}}**
5. **T**  **B: KBT{Nb}**

Y que Trent tiene compartido una clase secreta KBT con B y una clave KAT con A. Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Qué significa cada parámetro del protocolo y para qué sirven?
2. ¿Qué principales problemas existen a la hora de trabajar con KBT y KAT?
3. ¿Hay algún problema de seguridad en el punto 4 del protocolo? Razonar la repuesta.
4. En caso afirmativo (punto 3), mencionar alguna forma de resolver el problema.

**EJERCICIO 2:**

Teniendo en cuenta el siguiente protocolo:

1. **A**  **B : A, Na**
2. **B**  **T : B, EKBT{A, Na, Nb}**
3. **T**  **A : EKAT{B, KAB, Na, Nb), EKBT{A, KAB}**
4. **A**  **B : EKBT{A, KAB}, EKAB{Nb}**

Y que Trent tiene compartido una clase secreta KBT con B y una clave KAT con A. Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Quién inicializa el proceso de negociación de la clave de sesión KAB?
2. ¿Quién inicializa el proceso de negociación de la clave KAB con T?
3. ¿Qué modelo sigue este protocolo (PULL o PUSH)?
4. ¿Existe posibilidad de ataques de repetición?
5. ¿Tiene B alguna forma de verificar que el mensaje viene de Alice y que está realmente hablando con ella?

**EJERCICIO 3:**

Teniendo en cuenta el siguiente protocolo:

1. **A** **B : A, EKAB{NA}**
2. **B** **A : EKAB{NA, NB}**
3. **A** **B : EKAB{NB}**
4. **B** **A : EKAB{KAB’, NB’}**

Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Se debe reordenar los mensajes para que tenga sentido el protocolo?

En caso afirmativo, reordenarlo.

1. ¿Qué se hace en los puntos 1-3 del protocolo?
2. ¿Qué significa la clave KAB’?
3. ¿Qué tipos de ataques podrían existir si asumimos previamente la existencia de M (Mallory)? Razonar la respuesta.
4. ¿Cómo se podría resolver dichos ataques? Razonar la respuesta.
5. ¿Qué sentido tendría usar un MAC en este protocolo.

**EJERCICIO 4:**

Supongamos ahora que en vez de aplicar criptografía simétrica para la gestión de claves KAB, aplicamos sólo y únicamente criptografía asimétrica para:

1. gestionar las claves públicas de cada entidad A y B, y desde T, y
2. para buscar la forma de compartir un nonce (Na y Nb) que les permitan a cada entidad (A y B) verificar el freshness de las transacciones.

Dado esto, y los mensajes siguientes:

1. **A, B**
2. **B, A**
3. **Kpub\_A{Na, Nb, B}**
4. **Kpriv\_T{Kpub\_B, B} 5. Kpub\_B{Nb}**
5. **Kpriv\_T{Kpub\_A, A}**
6. **Kpub\_b{NA, A}**

Se pide

1. reorganizar los mensajes teniendo en cuenta cuenta la existencia de Trent (T) - como mediador entre A y B-, y la existencia de sus claves Kpriv\_T y Kpub\_T.

Para realizar el ejercicio, es fundamental identificar y declarar el origen y el destino de cada mensaje (ej: A  B), y asumir que T conoce las claves públicas de A y B, y se encarga de enviarlos cuando ellos son necesitados.

* A🡪T: A, B
* T🡪A: **Kpriv\_T{Kpub\_B, B}**
* B🡪T: B, A
* T🡪B: Kpriv\_T{Kpub\_A, A}
* A🡪B: Kpub\_b{Na, A}
* B🡪A: Kpub\_A{Na, Nb, B}
* A🡪B: Kpub\_B{Nb}

1. ¿Qué hace realmente el protocolo? ¿Cuál es su objetivo final?

Hace un intercambio de nonces a partir de un intermediario T que los pone en conta

**EJERCICIO 5:**

Teniendo en cuenta el siguiente protocolo:

1. **A**  **B: Kpub\_A**
2. **B**  **A: Kpub\_B**
3. **A**  **B: Kpub\_B{KAB}**

Se pide:

1. Optimizar el protocolo para que Alice pueda verificar que la clave pública es genuina y pertenece a Bob.

* **A**  **B: Kpub\_A || CertB\_A**
* **B**  **A: Kpub\_B || CertA\_B**
* **A**  **B: Kpub\_B{KAB , NA}**

1. ¿Qué hace Alice y Bob cuando recibe la clave pública asumiendo la modificación del punto 1? Establecer la secuencia de acciones que toma cada parte para la verificación.

Extrae la clave Kpub\_b y con eso verifica si el certificado es correcto como si de una firma se tratase.

**EJERCICIO 6:**

Teniendo en cuenta el siguiente protocolo:

1. **CA1**  **A : CertA\_CA1**
2. **CA2**  **B : CertB\_CA2**
3. **A**  **B: CertA\_CA1**
4. **B**  **A: CertB\_CA2**

Asumiendo que A conoce **CA1** y tiene su clave pública **Kpub\_CA1** y B conoce **CA2** y tiene su clave pública **Kpub\_CA2,** se pide contestar a las siguientes preguntas:

1. ¿Puede A verificar el certificado **CertB\_CA2** si **CA1** =! **CA2**? Razonar la respuesta.

En principio no pero podria ser posible si puede conseguir CA2 a traves de un servidor publico o alguna otra forma

1. ¿Existe alguna forma de que A y B puedan compartir las claves de forma confiable?

Hay muchas opciones pero la major seria con certificados previamente aceptados por una CA