RELACIÓN DE EJERCICIOS

EJERCICIO 1:

Teniendo en cuenta el siguiente protocolo:

1. **A → B: A, B**
2. **B → A: B, A, N_b**
3. **A → B: $K_{AT}\{N_b\}$, ____**
4. **B → T: B, T, $K_{BT}\{A, \_\_\_ , K_{AT}\{N_b\}\}$**
5. **T → B: T, B, $K_{BT}\{K_{AB}, N_b\}$, $K_{AT}\{K_{AB}, \_\_\_ \}$**
6. **B → A: B, A, $K_{AT}\{K_{AB}, \_\_\_ \}$**

y que Trent tiene compartido una clase secreta K_{BT} con B y una clave K_{AT} con A.

Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Qué significa cada parámetro del protocolo y para qué sirve?
2. ¿Qué problemas existen a la hora de trabajar con las claves K_{BT} y K_{AT}?
3. Completar el protocolo anterior para evitar ataques de tipo *replay*.
4. ¿Crees que está completamente controlado todos los posibles ataques de reenvío en todo el protocolo? Es decir, ¿Bob controla el ataque? ¿Y Alice?
5. ¿Hay desafío y respuesta? Si es así, dónde.
6. ¿De qué tipo es el protocolo? ¿pull o push?

EJERCICIO 2:

Teniendo en cuenta el siguiente protocolo:

1. **A → B : A, N_a**
2. **B → T : B, $E_{KBT}\{A, N_a, N_b\}$**
3. **T → A : $E_{KAT}\{B, K_{AB}, N_a, N_b\}$, $E_{KBT}\{A, K_{AB}\}$**
4. **A → B : $E_{KBT}\{A, K_{AB}\}$, $E_{KAB}\{N_b\}$**

y que Trent tiene compartido una clase secreta K_{BT} con B y una clave K_{AT} con A.

Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Quién inicializa el proceso de negociación de la clave de sesión K_{AB}?
2. ¿Quién inicializa el proceso de negociación de la clave K_{AB} con T?
3. ¿Qué modelo sigue este protocolo (PULL o PUSH)?
4. ¿Existe posibilidad de ataques de repetición?
5. ¿Tiene Bob 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, $E_{KAB}\{N_a\}$**
2. **B → A: $E_{KAB}\{f_1(N_a), N_b\}$**
3. **A → B: $E_{KAB}\{f_2(N_b)\}$**
4. **A → B: $E_{KAB'}\{f_3(N_{b'})\}$**
5. **….**
6. **B → A: $E_{KAB}\{N_{b'}\}$**
7. **B → A: $E_{KAB}\{K_{AB'}, N_{b'}\}$**

Analizar el protocolo, contestando a las siguientes preguntas:

1. ¿Se debe reordenar los mensajes para que tenga sentido el protocolo? En caso afirmativo, reordenarlo.
2. ¿Por qué se aplica f1, f2 y f3?
3. ¿Qué significa la clave $K_{AB'}$?¿Por qué se envía en el paso 5 un $N_{b'}$?
4. ¿Qué sentido tendría usar un código MAC en este protocolo?

EJERCICIO 4:

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

(i) gestionar las claves públicas de cada entidad A y B, y desde T, y
(ii) para buscar la forma de compartir un nonce (N_a y N_b) 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. **$K_{pub\_A}\{N_a, N_b, B\}$**
3. **$K_{priv\_T}\{K_{pub\_B}, B\}$**
4. **$K_{pub\_B}\{N_b\}$**
5. **$K_{priv\_T}\{K_{pub\_A}, A\}$**
6. **$K_{pub\_b}\{N_A, A\}$**

se pide

1. Reorganizar los mensajes teniendo en 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 el origen y el destino de cada mensaje (ej: A → B) y asumir que T (i) conoce las claves públicas de A y B y (ii) se encarga de enviarlas cuando ellos las solicitan.

2. ¿Qué hace realmente el protocolo? ¿Cuál es su objetivo final?
3. ¿Para qué sirve el N_A?

EJERCICIO 5:

Teniendo en cuenta el siguiente protocolo:

1. **Alice → Bob: Bob, M, S_{Alice}(Bob, H(M))**
2. **Bob → Alice: Alice, S_{Bob}(Alice, H(M))**

se pide:

1. Analizar el protocolo y determinar su principal objetivo.
2. ¿Crees que hay suficiente evidencia para asegurar el no repudio tanto en el lado del origen como en el destino?

EJERCICIO 6:

Si suponemos que el canal es fiable y las entidades NO son honestas, entonces se introduce una tercera persona confiable para este nuevo protocolo, tal que:

1. **Alice → TTP: TTP, Bob, M, S_{Alice} (TTP, Bob, H(M))**
2. **TTP → Bob: Alice, Bob, M, S_{TTP} (Alice, Bob, H(M))**
3. **TTP → Alice: Alice, Bob, S_{TTP} (Alice, Bob, H(M))**

se pide:

1. Analizar el protocolo y determinar su principal objetivo.
2. ¿Crees que hay suficiente evidencia para asegurar el no repudio tanto en el lado del origen como en el destino? ¿Quién firma esas evidencias?

EJERCICIO 7:

Si suponemos que el canal NO es fiable y las entidades NO son honestas, pero no se introduce una tercera persona confiable para este nuevo protocolo, tal que:

1. **Alice → Bob: Bob, C, S_{Alice}(Bob, H(C))**
2. **Bob → Alice: Alice, S_{Bob}(Alice, H(C))**
3. **Alice → Bob: Bob, K, S_{Alice}(Bob, K)**
4. **Bob → Alice: Alice, S_{Bob}(Alice, K)**

se pide:

1. Analizar el protocolo, y determinar qué es C en el punto 1 del protocolo y K en el punto 3 de dicho protocolo.
2. Determinar el principal objetivo de este protocolo, razonando la respuesta.
3. En el punto 3 y 4 no se realiza el H(K) para la firma, es decir: S_{Alice}(Bob, H(K)) o S_{Bob}(Alice, H(K)). Explicar las razones.

EJERCICIO 8:

Teniendo en cuenta el siguiente protocolo:

1. **A → B: K_{pub_A}**
2. **B → A: K_{pub_B}**
3. **A → B: $K_{pub\_B}\{K_{AB}\}$**

se pide:

1. Optimizar el protocolo para que Alice pueda verificar que la clave pública es genuina y pertenece a Bob.
2. ¿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.

EJERCICIO 9:

Teniendo en cuenta el siguiente protocolo:

1. **CA_1 → A : $Cert_{A\_CA1}$**
2. **CA_2 → B : $Cert_{B\_CA2}$**
3. **A → B: $Cert_{A\_CA1}$**
4. **B → A: $Cert_{B\_CA2}$**

y asumiendo que A conoce **CA_1** y tiene su clave pública **K_{pub_CA1}** y B conoce **CA_2** y tiene su clave pública **K_{pub_CA2}**, se pide contestar a las siguientes preguntas:

1. ¿Puede A verificar el certificado **$Cert_{B\_CA2}$** si **CA_1** =! **CA_2**? Razonar la respuesta.
2. ¿Existe alguna forma de que A y B puedan compartir las claves de forma segura?