**RELACIÓN DE EJERCICIOS**

**EJERCICIO 1:**

Dado el siguiente protocolo:

1. **A 🡪 B: EKs1{data1} + EKs2{data2} + EKpub\_B{Ks1} + EKpub\_C{Ks2} + H(data1) + H(data 2) + EKpriv\_A{H(H(data1)+H(data2))}**
2. **B 🡪 C: EKs2{data2} + EKpub\_C{Ks2} + H(data1) + EKpriv\_A{H(H(data1)+H(data2))}**

**Analizar el protocolo, contestando a las siguientes preguntas:**

1. **¿Qué tipo de protocolo se está aplicando aquí?**

Un set con firma dual

1. **¿Qué tipo de servicios se están ofreciendo con este protocolo?**

Confidencialidad, Autenticacion, No repudio e integridad.

1. **¿Podría existir un ataque de DoS? Razonar la respuesta. En caso afirmativo, indicar cómo se podría evitar la amenaza.**

Probablemente debido a que no usa nonces o marcas de tiempo para que no se repliquen sin problemas.

**EJERCICIO 2:**

**¿Cómo se podría adaptar el protocolo de firma dual a un sistema sanitario?**

Se usaria para mandarle al doctor unicamente la informacion que requiere y a la administracion sanitaria el resto, pudiendo asi unirlas con la firma dual, que las enlaza a la vez que nos da no repudio

**El sistema cuenta con tres actores importantes:**

* **Un paciente.**
* **El doctor.**
* **Administracin.﷽﷽﷽﷽﷽﷽﷽﷽cicuenta con tres actores importantes:ema sanitario?ón.**

**¿Qué utilidad tendría aquí la firma dual en este escenario? Razonar la respuesta.**

Daria confidencialidad al paciente evitando que el doctor vea datos sensibles que no requiere mientras que permite identificarlo desde la administracion

**EJERCICIO 3:**

Dado el siguiente protocolo:

1. **Alice 🡪 Bob: Bob, L, C, NO**
2. **Bob 🡪 Alice: Alice, L, NR**
3. **Alice 🡪 TTP: Bob, L, K, proc\_K**
4. **TTP 🡪 Bob: Alice, Bob, L, K, pub\_K**
5. **TTP 🡪 Alice: Alice, Bob, L, K, pub\_K**

Donde:

* L: representa la secuencia del protocolo y se basa de un entero.
* S: indica la firma digital.
* C: el cifrado de un mensaje, es decir: EK{M}.
* K: La clave simétrica aplicada en el cifrado de M.
* NO = *SAlice(Bob, L, H(C)).*
* NR = *SBob(Alice, L, H(C)).*

Contestar a las siguientes preguntas:

1. **¿Qué tipo de protocolo se está aplicando aquí?**

Una distribucion de clave de claves simetricas(renovacion de claves)

1. **¿Qué tipo de servicios se están ofreciendo con este protocolo?**

Autentificacion, No repudio e Integridad.

1. **¿Qué contenido debería tener proc\_K y pub\_K?**

Proc\_k: A,B – Peticion de clave de sesion nueva

Pub\_K: EkAT(K2) || EkBT(K2)

1. **¿Podría existir un ataque de DoS? Razonar la respuesta. En caso afirmativo, indicar cómo se podría evitar la amenaza.**

No, porque se usa el entero L que es unico.

**EJERCICIO 4:**

Adaptar el siguiente protocolo del ejercicio 3 al protocolo de firma dual (basado en una comunicación estrella – no en línea).

Dicho de otro modo, combinar ambos protocolos y contestar a la siguiente pregunta:

1. ¿Qué tipo de servicios se están ofreciendo con este protocolo combinado?

Ahora tendra ademas de Autenticacion, No repudio e Integridad   
Confidencialidad.