Ejercicios – Tema 4

1. Suponga un posible escenario para la entrega telemática de la Declaración del Impuesto de la Renta de Personas Físicas (I.R.P.F.) que contempla su pago inmediato a través de Internet. Los agentes implicados serán la persona que presenta la declaración (P), la Agencia Estatal de Administración Tributaria (AT) y el banco donde la persona tiene una cuenta (BP).

   En este escenario hipotético se intercambian los mensajes indicados debajo, donde certificado_digitalX se refiere al certificado digital de X, KprivX() al cifrado mediante la clave privada de X, KpúbX() al cifrado mediante la clave pública de X, datos_fiscalesX a los datos de la declaración de I.R.P.F. de X, importe a la cantidad a pagar como resultado de la declaración de I.R.P.F. de X, código_para_pagar_IRPF es un código indicado por la AEAT para que la persona realice el pago en su banco y código_IRPF_pagado es un código indicado por el banco a la persona como comprobante de su pago.

P → AT: $certificado\_digital_P$
AT → P: $certificado\_digital_{AT}$
P → AT: $Kpriv_P$ ($Kpúb_{AT}$ ($datos\_fiscales_P$, $importe$))
AT → P: $Kpriv_{AT}$ ($Kpúb_P$ ($código\_para\_pagar\_IRPF$))
P → BP: $certificado\_digital_P$
BP → P: $certificado\_digital_{BP}$
P → BP: $Kpriv_P$ ($Kpúb_{BP}$ ($importe$, $código\_para\_pagar\_IRPF$))
BP → P: $Kpriv_{BP}$ (Kpúb$_P$ ($código\_IRPF\_pagado$))
P → AT: $Kpriv_P$ ($Kpúb_{AT}$ ($certificado\_digital_{BP}$, $código\_IRPF\_pagado$))
AT → BP: $Kpriv_{AT}$ ($Kpúb_{BP}$ ($identidad_P$, $código\_para\_pagar\_IRPF$))
BP → AT: $Kpriv_{BP}$ ($Kpúb_{AT}$ ($identidad_P$, $código\_IRPF\_pagado$))
AT → P: $Kpriv_{AT}$ ($Kpúb_P$ ($mensaje\_declaración\_correcta$))

   Todos los certificados digitales han sido expedidos por una Autoridad de Certificación fiable (e.g. la Fábrica Nacional de Moneda y Timbre). Además, la AEAT conoce la identidad de los bancos a través de los cuales se puede realizar el pago telemático de la declaración de I.R.P.F. Responda razonadamente las siguientes cuestiones:

   a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?
   b) ¿Qué debilidades/vulnerabilidades presenta el esquema y, en su caso, cómo podrían solucionarse?

2. Explique el objetivo que se persigue al utilizar firmas digitales. Exponga detalladamente los mecanismos de firma digital que conozca.

3. ¿Es posible autenticar mutuamente con garantías dos entidades A y B, tal que A dispone de certificado digital y B no? Explique la respuesta adoptando las suposiciones que estime necesarias.

4. Describa el funcionamiento del protocolo de aplicación PGP (Pretty Good Privacy). Describa los pasos para el envío y la recepción de un mensaje, incluyendo qué aspectos de seguridad se garantizan y cómo.

5. ¿Qué tres objetivos fundamentales tiene la firma digital? Describa tres procedimientos para realizar una firma digital.

6. ¿Son DES o IDEA algoritmos de sustitución o trasposición? Explique un esquema para evitarlo.

7. Explique cómo establecer una clave secreta a través de un canal no seguro. ¿qué debilidades tienes? Ponga un ejemplo de protocolo estandarizado en el que se use ese procedimiento.

8. Suponga un protocolo que por cada mensaje en texto plano M, envía (M, H(M) $\oplus$ KS), donde
   H(x) es un compendio o Hash de x
   (a $\oplus$ b) es la X-OR de a y b
   K_s es una clave secreta compartida entre los dos extremos.
   ¿Qué aspectos de seguridad y cuáles no garantiza? Justifique la respuesta y proponga en su caso una alternativa –con las mismas herramientas– que sea más segura.

9. La figura y mensajes siguientes describen un hipotético protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.

PC → NAS: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: desafio
PC → NAS: $Kpub_{NAS}$(MD5(usuario:K_{PC-AS}:desafio))
NAS → AS: peticion_autenticacion + usuario + desafio + MD5(usuario:K_{AS-PC}:desafio))
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(ó peticion_rechazada)
NAS → PC: $Kpriv_{NAS}$ (peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$))
(ó $Kpriv_{NAS}$ (peticion_rechazada))
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta)

Siendo:

- $Kpub_X$ cifrado con la clave pública de X
- $Kpriv_X$ cifrado con la clave privada de X
- K_{X-Y} la clave secreta entre X e Y
- MD5 es una función *hash*

Aceptadas la disponibilidad y validez de las claves públicas involucradas en base a la existencia de una entidad superior confiable, responda razonadamente:

a) ¿Qué servicios de seguridad se proporcionan en el protocolo descrito?
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

10. Suponga una transacción comercial en Internet con cuatro entidades involucradas: C (cliente), P (proveedor), Bc (entidad bancaria del cliente) y Bp (entidad bancaria del proveedor). Entre ellas se intercambian los mensajes indicados abajo a la derecha; donde

KpbX se refiere al cifrado con la clave pública de X, KX-Y al cifrado con la clave privada entre X e Y, producto a la identificación del producto adquirido/vendido, importe a su valor económico, R a un reto, C, P, Bc y Bp a la identidad de las entidades correspondientes y datos_X a la información bancaria correspondiente a X-Bx.

Aceptadas la disponibilidad y validez de las claves públicas involucradas gracias a la existencia de una entidad superior confiable (es decir, al uso de certificados digitales), responda justificadamente a las siguientes cuestiones:

¿Qué servicios de seguridad se proporcionan en la transacción indicada?

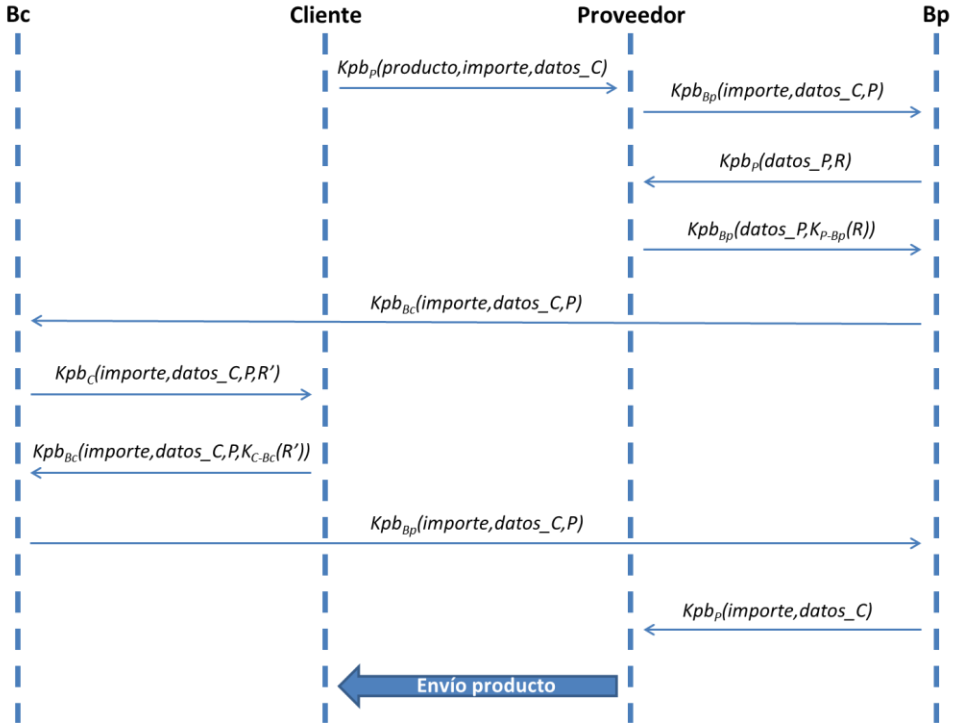
¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?

C→P:
KpbP(producto,importe,datos_C)
P→Bp: KpbBp(importe,datos_C,P)
Bp→P: KpbP(datos_P,R)
P→Bp: KpbBp(datos_P,KP-Bp(R))
Bp→Bc: KpbBc(importe,datos_C,P)
Bc→C: KpbC(importe,datos_C,P,R')
C→Bc:
KpbBc(importe,datos_C,P,KC-Bc(R'))
Bc→Bp: KpbBp(importe,datos_C,P)
Bp→P: KpbP(importe,datos_C)
P→C: …entrega del producto…

MENSAJES:

- ***Kpb$_X$*** → cifrado con la clave pública de *X*
- ***K$_{X-Y}$*** → cifrado con la clave privada entre *X* e *Y*
- ***producto*** → identificación del producto adquirido/vendido
- ***importe*** → valor económico de un producto
- ***R*** → reto
- ***datos_X*** → información bancaria correspondiente a X-Bx

EL PROTOCOLO SERÍA:



a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?

- **Confidencialidad** → sí, ya que todos los mensajes están cifrados con clave pública, por tanto, sólo el dueño de la clave privada puede obtener su contenido.
- **Integridad** → no, ya que no se usan funciones hash.
- **Autenticación** → sólo el cliente/proveedor con sus bancos respectivos, mediante el envío cifrado del reto propuesto (R y R'). Sin embargo, los bancos no se autentican entre ellos ni con sus clientes.
- **No repudio** → no, ya que ninguna transacción se firma. Además, el cliente no tiene ninguna prueba de que el proveedor haya aceptado la transacción que implica cierto producto y su importe. Ni siquiera de que haya realizado el pago, ya que su banco no le envía la confirmación de la operación con algún campo que sólo hubiese podido incluir él.
- **Disponibilidad** → no, ya que la red podría dejar de funcionar en cualquier momento, por ataques en capas inferiores o por fallos de la misma.

b) ¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?

- **Integridad** → se podría usar una función compendio (hash) para comprobar la integridad de los datos.
- **Autenticación** → podría haber autenticación entre los bancos el cliente/proveedor mediante un reto propuesto por C a Bc y por P a Bp. También podría haber autenticación entre los bancos proponiéndose un reto cada uno.
- **No repudio** → tanto cliente como proveedor podrían firmar digitalmente sus mensajes antes de transmitirlos (con su clave de certificado digital) y el receptor del mensaje lo desencriptaría con la clave pública correspondiente. Igualmente, el banco podría mandar una confirmación de la operación realizada firmada con su certificado digital.
- **Disponibilidad** → el enunciado no da información que permita indicar si hay problemas de disponibilidad (Ej: redundancia de conexiones, posibles problemas ante ataques en capas inferiores, etcétera).

11. Explique detalladamente qué es un certificado digital y **qué información contiene**. Describa cómo se podría, **UTILIZANDO CERTIFICADOS DIGITALES**, garantizar la autenticación, la integridad y el no repudio en las comunicaciones entre dos entidades con certificados digitales emitidos por entidades de certificación fiables.

12. Explique detalladamente cómo se puede utilizar certificados digitales para realizar firmas digitales (únicamente firmas digitales **USANDO CERTIFICADOS DIGITALES**). Para ese procedimiento concreto, explique qué aspectos de seguridad se garantizan.

13. Un protocolo de reto-respuesta…
    3.1. ¿Qué es y para qué sirve?
    3.2. Suponiendo la existencia de una clave secreta compartida ponga un ejemplo de mensajes intercambiados.
    3.3. Identifique sus posibles debilidades.
    3.4. ¿Sería posible realizarlo si dispusiera de certificados digitales? En su caso ¿cómo?