



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_digital_X se refiere al certificado digital de X, Kpriv_{X()} al cifrado mediante la clave privada de X, Kpúb_{X()} al cifrado mediante la clave pública de X, datos_fiscales_X 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_digitalP
AT → P: certificado_digitalAT
P → AT: KprivP(KpúbAT(datos_fiscalesP, importe))
AT → P: KprivAT(KpúbP(código_para_pagar_IRPF))
P → BP: certificado_digitalP
BP → P: certificado_digitalBP
P → BP: KprivP(KpúbBP(importe, código_para_pagar_IRPF))
BP → P: KprivBP(KpúbP(código_IRPF_pagado))
P → AT: KprivP(KpúbAT(certificado_digitalBP, código_IRPF_pagado))
AT → BP: KprivAT(KpúbBP(identidadP, código_para_pagar_IRPF))
BP → AT: KprivBP(KpúbAT(identidadP, código_IRPF_pagado))
AT → P: KprivAT(KpúbP(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. 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 Kpb_X se refiere al cifrado con la clave pública de X, K_{X-Y} al cifrado con la clave secreta 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 en base a la existencia de una entidad superior confiable, responda justificadamente a las siguientes cuestiones:

Este ejercicio es el 14, que ya está resuelto.



- a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?
- b) ¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?
- C→P: $Kpb_P(producto, importe, datos_C)$
P→Bp: $Kpb_{Bp}(importe, datos_C, P)$
Bp→P: $Kpb_P(datos_P, R)$
P→Bp: $Kpb_{Bp}(datos_P, K_{P-Bp}(R))$
Bp→Bc: $Kpb_{Bc}(importe, datos_C, P, R')$
Bc→C: $Kpb_C(importe, datos_C, P, R')$
C→Bc: $Kpb_{Bc}(importe, datos_C, P, K_{C-Bc}(R'))$
Bc→Bp: $Kpb_{Bp}(importe, datos_C, P)$
Bp→P: $Kpb_P(importe, datos_C)$
P→C: ...entrega del producto...
4. ¿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.
5. 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.
6. ¿Qué tres objetivos fundamentales tiene la firma digital? Describa tres procedimientos para realizar una firma digital.
7. ¿Son DES o IDEA algoritmos de sustitución o trasposición? Explique un esquema para evitarlo.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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: $K_{pub\text{NAS}}$ (peticion_acceso + usuario)
NAS → PC: desafío
PC → NAS: $K_{pub\text{NAS}}(\text{MD5}(\text{usuario}:K_{PC-AS}\text{:desafío}))$
NAS → AS: peticion_autenticacion + usuario + desafío + $\text{MD5}(\text{usuario}:K_{AS-PC}\text{:desafío})$
AS → NAS: peticion_aceptada + $K_{sesion\text{PC-NAS}}$ + $K_{PC-AS}(K_{sesion\text{PC-NAS}})$
 (ó peticion_rechazada)
NAS → PC: $K_{priv\text{NAS}}$ (peticion_aceptada + $K_{PC-AS}(K_{sesion\text{PC-NAS}})$)
 (ó $K_{priv\text{NAS}}$ (peticion_rechazada))
PC → NAS: $K_{sesion\text{PC-NAS}}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $K_{sesion\text{PC-NAS}}$ (datos_de_respuesta)

Siendo:

- K_{pubX} cifrado con la clave pública de X
- K_{privX} 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?
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?
14. 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 K_{pbX} se refiere al cifrado con la clave pública de X, K_{X-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?

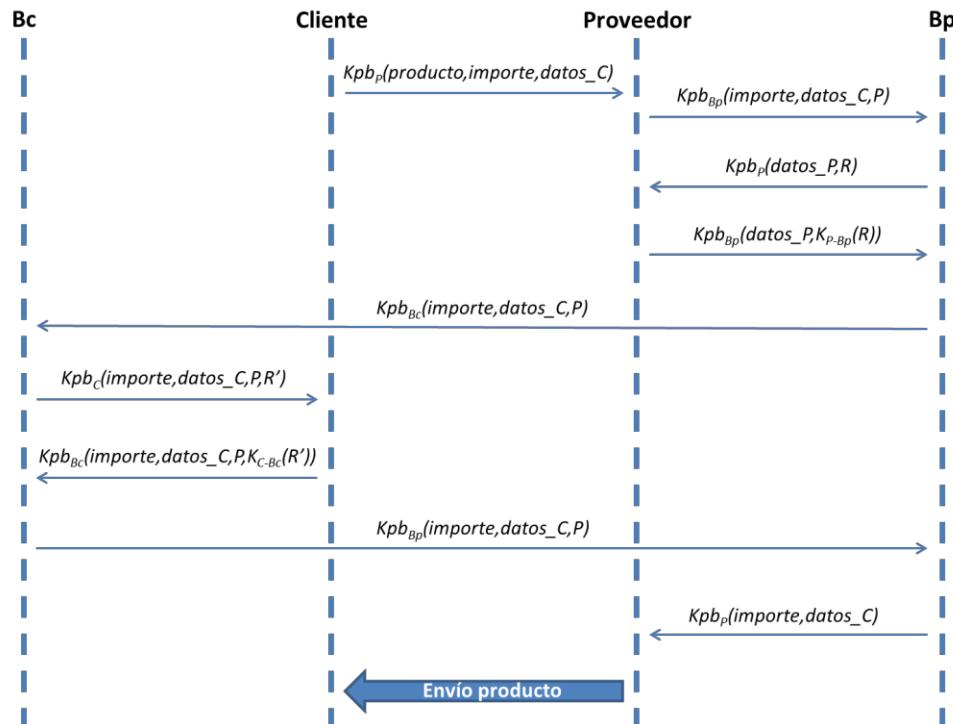
¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?

C→P:
 $KpbP(\text{producto}, \text{importe}, \text{datos}_C)$
 P→Bp: $KpbBp(\text{importe}, \text{datos}_C, P)$
 Bp→P: $KpbP(\text{datos}_P, R)$
 P→Bp: $KpbBp(\text{datos}_P, Kp-Bp(R))$
 Bp→Bc: $KpbBc(\text{importe}, \text{datos}_C, P)$
 Bc→C: $KpbC(\text{importe}, \text{datos}_C, P, R')$
 C→Bc:
 $KpbBc(\text{importe}, \text{datos}_C, P, KC-Bc(R'))$
 Bc→Bp: $KpbBp(\text{importe}, \text{datos}_C, P)$
 Bp→P: $KpbP(\text{importe}, \text{datos}_C)$
 P→C: ...entrega del producto...

MENSAJES:

- **$KpbX$** → 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 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 B_C y por P a B_P . 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 privada) y el receptor del mensaje lo desencriptaría con la clave pública correspondiente. Igualmente, el banco podría mandar una confirmación de la operación realizada firmada digitalmente con su clave privada.
- **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).

$P \rightarrow AT: certificado_{digital}_P$
 $AT \rightarrow P: certificado_{digital}_{AT}$
 $P \rightarrow AT: Kpriv_P(Kpúb_{AT}(datos_fiscales_P, importe))$
 $AT \rightarrow P: Kpriv_{AT}(Kpúb_P(código_{para_pagar_IRPF}))$
 $P \rightarrow BP: certificado_{digital}_P$
 $BP \rightarrow P: certificado_{digital}_{BP}$
 $P \rightarrow BP: Kpriv_P(Kpúb_{BP}(importe, código_{para_pagar_IRPF}))$
 $BP \rightarrow P: Kpriv_{BP}(Kpúb_P(código_{IRPF_pagado}))$
 $P \rightarrow AT: Kpriv_P(Kpúb_{AT}(certificado_{digital}_{BP}, código_{IRPF_pagado}))$
 $AT \rightarrow BP: Kpriv_{AT}(Kpúb_{BP}(identidad_P, código_{para_pagar_IRPF}))$
 $BP \rightarrow AT: Kpriv_{BP}(Kpúb_{AT}(identidad_P, código_{IRPF_pagado}))$
 $AT \rightarrow P: Kpriv_{AT}(Kpúb_P(mensaje_declaración_correcta))$

- 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?

Confidencialidad: Se cumple porque todos los mensajes van cifrados con la clave pública del receptor (la cual sabemos gracias al certificado digital), de forma que solo el receptor podrá descifrar la información usando su clave privada.

Integridad: No se cumple, pues en ningún envío se hace uso de funciones hash. Por ello, el receptor no puede comparar con un resumen de los datos para detectar modificaciones.

Autenticación: Se cumple ya que todo va firmado con la clave privada del emisor.

No repudio: Se garantiza debido a que todas las entidades firman digitalmente los envíos usando su clave privada para encriptar.

Disponibilidad: No podemos comentar nada al respecto ya que no conocemos la infraestructura física ni las características del entorno.

Para lograr integridad, habría que adjuntar un resumen de lo que se envía en cada mensaje haciendo uso de funciones hash como MD5. En cuanto a la disponibilidad, habría que asegurar que hay redundancia de conexiones, entre otras cosas.

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

Las firmas digitales son un mecanismo de seguridad que se usa para lograr autenticación (una entidad es quien dice ser) y no repudio/irrenunciabilidad (no se puede negar algo que se ha hecho). En teoría se han visto 2 mecanismos de firma digital:

- **BIG BROTHER:** Existe una entidad central BB que se ocupa de la firma digital entre dos entidades A y B. El primer paso consiste en que A envía el mensaje P encriptado con una clave secreta que conocen A y BB (junto a P también se encripta el destino B y una marca de tiempo t). A continuación, BB desencripta lo que le ha enviado A usando Ka. Por último, BB envía a B un mensaje encriptado con una clave secreta Kb que solo conocen estas dos entidades. Lo que encripta incluye la marca de tiempo t, el mensaje P, el origen A y estas tres mismas cosas encriptadas con la clave privada de BB, siendo esto último lo que haría de firma digital.
- **DOBLE CIFRADO ASIMÉTRICO:** Una entidad A comienza cifrando lo que va a mandar (P) usando su clave privada para así conseguir la firma digital, y tras esto cifra lo obtenido del primer cifrado pero ahora con la clave pública de B (para conseguir confidencialidad), que es a quien lo va a mandar. Cuando B recibe el mensaje, descifra usando su clave privada y descifra una segunda vez usando la clave pública de A para asegurar que lo que le ha llegado es de A y no de otro emisor.

4. ¿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.

El certificado digital no se usa para autenticación, sino para garantizar el no repudio, por lo que este dato no es relevante. Por ello, para autenticar a las entidades A y B se pueden usar retos-respuesta o bien hacer uso de la firma digital (Big Brother o doble cifrado), que están explicados en el ejercicio 2.

5. 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.

El protocolo funciona de la siguiente manera:

1. Se genera un resumen R del texto P con la función hash MD5, y este resumen R se cifra con la clave privada del emisor A (es decir, se usa una firma digital).
2. Se genera una zip Z que incluye la firma digital FD y el texto P
3. A genera una clave aleatoria K con la que encripta el zip Z usando el algoritmo de cifrado IDEA.
4. A encripta la clave aleatoria usando la clave pública del emisor K'.
5. Por último, se envían al receptor B tanto la clave encriptada como el zip encriptado.

En el receptor B ocurre lo siguiente:

1. Usa su clave privada para poder desencriptar la clave aleatoria K, la cual le hace falta para poder desencriptar el zip Z.
2. Una vez tiene la clave aleatoria K, la usa para desencriptar el zip Z.
3. Extrae los elementos del zip Z, que son la firma digital FD y los datos P.
4. Usa la clave pública de A para obtener el resumen de P generado por A (R).
5. Genera el resumen de P con la función hash MD5, obteniendo R'.
6. Finalmente, comprueba que R y R' sean iguales para detectar si ha habido modificaciones.

Por último, nombramos qué aspectos de seguridad se garantizan y cómo:

Confidencialidad: Se garantiza gracias al uso de la clave pública de B, que es con la que se cifra la clave aleatoria K que luego nos permitirá obtener el resto de la información.

Integridad: Se garantiza gracias al uso de la función hash MD5 con la que se obtienen los resúmenes de lo enviado y lo recibido, los cuales se comparan para ver si coinciden.

Autenticación: Se garantiza debido al uso de la clave privada de A, la cual sólo la posee A y que se usa para la firma digital FD.

No repudio: También se garantiza gracias a la firma digital que se realiza con la clave privada de A.

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

Los tres objetivos fundamentales de la firma digital son:

1. Que el receptor pueda autenticar al emisor.
2. Que haya no repudio (el emisor no puede renunciar a una acción de su autoría).
3. Que el emisor tenga garantías de que su mensaje no ha sufrido ninguna falsificación (integridad).

En cuanto a los procedimientos para realizar una firma digital, hemos visto Big Brother (BB) y doble cifrado con clave asimétrica, que ya han sido explicados en el ejercicio 2. El tercer procedimiento es usando certificados digitales, lo cual está explicado en el ejercicio 11.

8. 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.

El algoritmo visto en teoría para ello es el intercambio de Diffie-Hellman. Consiste en lo siguiente:

La entidad A escoge tres números enteros (g , n , x). Después, calcula g elevado a x módulo n y lo envía a la entidad B. La entidad B escoge un número entero y . Al igual que A, calcula g elevado a y módulo n , y lo envía a A. Por último, ambas entidades elevan a su número secreto lo que les ha llegado de la otra (a^x en el caso de A y a^y en el caso de B). De esta forma, ambas entidades acaban obteniendo la misma clave secreta, que sería g elevado a xy módulo n .

La gran debilidad que tiene es que es vulnerable a ataques Man In The Middle, pues una entidad podría colocarse en medio de A y B, realizar el proceso descrito con cada una de las entidades (por lo tanto tendría una clave secreta con A y otra con B) y de esta forma, podría tanto interrumpir envíos como modificarlos.

Algunos protocolos en los que se usa este procedimiento son TLS (Transport Layer Security) y PGP (Pretty Good Security).

9. 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.

En el mensaje enviado se consigue integridad, pues se hace uso de una función hash que nos permite obtener un resumen del texto plano M y saber si se ha modificado algo de este (a pequeñas modificaciones, el resumen dado por H cambia mucho). También se consigue autenticación, ya que se está usando una clave secreta que solo los extremos conocen y por tanto, saben que con quien se comunican es quien dice ser. En cuanto a la disponibilidad no podemos decir nada y en cuanto al no repudio, no se garantiza ya que no se hace uso de firma digital (es decir, no se usa Big Brother ni doble cifrado con clave asimétrica). Tampoco se consigue confidencialidad, ya que el texto plano M puede ser leído por cualquier entidad no autorizada.

Usando lo que tenemos, podemos garantizar confidencialidad si lo que ciframos es tanto M como $H(M)$ con la clave secreta KS , es decir, $KS(M, H(M))$.

10. 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.

Un certificado digital sirve para garantizar la asociación entre identidad y claves. Por ello, funciona de la siguiente manera:

1. Una entidad obtiene sus claves pública y privada.
2. Ésta envía una solicitud firmada digitalmente a una autoridad de certificación (AC), indicando su identidad y clave pública.
3. La AC comprueba la firma y genera el certificado, en el que van incluidos la identidad del usuario, la identidad de la AC, la clave pública del usuario, el periodo de validez, etc.
4. Cuando la AC envía el certificado, lo firma con su clave privada, asegurando que no se pueda falsificar.

En cuanto a los contenidos del certificado tenemos:

Version: La versión del formato del certificado (se suele usar el formato X.509).

Serial number: Identificador único de la AC.

Issuer: El nombre de la AC definido por X.509.

Validity period: Período de validez del certificado. Cuando se cumple, la AC revoca el certificado.

Subject name: La entidad cuya clave pública se certifica.

Public key: La clave pública que se certifica, así como los algoritmos que la usan.

También está la firma privada de la AC y los algoritmos que la usan.

El no repudio se consigue gracias a que la AC encripta con su clave privada, y como el resto poseen su clave pública por ser una entidad autorizada, pueden obtener el certificado digital emitido, teniendo así la clave pública de la entidad que solicita el certificado, la cual sirve para garantizar que una acción ha sido realizada por A cuando esta encripta con su clave privada. Por esto, también se logra autenticación, pues al tener la clave pública de A, A puede firmar digitalmente usando el doble cifrado. Por último, la integridad se conseguiría haciendo uso de funciones hash.

11. 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.

```

PC → NAS: KpubNAS (peticion_acceso + usuario)
NAS → PC: desafío
PC → NAS: KpubNAS(MD5(usuario:KPC-AS:desafío))
NAS → AS: peticion_autenticacion + usuario + desafío + MD5(usuario:KAS-PC:desafío))
AS → NAS: peticion_aceptada + KsesionPC-NAS + KPC-AS(KsesionPC-NAS)
(ó peticion_rechazada)
NAS → PC: KprivNAS (peticion_aceptada + KPC-AS(KsesionPC-NAS))
(ó KprivNAS (peticion_rechazada))
PC → NAS: KsesionPC-NAS (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: KsesionPC-NAS (datos_de_respuesta)

```

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

Salvo la disponibilidad, de la cual no podemos comentar nada porque no conocemos la estructura física ni elementos redundantes, comentaremos los otros 4 aspectos de seguridad:

Confidencialidad

El emisor cifra los mensajes de solicitud con la clave pública del receptor NAS, cumpliendo la confidencialidad. No se garantiza cuando el NAS envía los datos del usuario y el desafío en texto plano, pues podrían ser leídos por cualquier trabajador del ISP. Además, cuando el AS responde, en caso de aceptar la solicitud, envía la clave de sesión sin cifrar. Entre PC y NAS sí se envía cifrada, luego ahí sí se da confidencialidad. Una vez iniciada la sesión, los datos que envía el PC al NAS tampoco están cifrados ni los datos de respuesta del AS al NAS.

Autenticación

Solo se da cuando el PC se autentica al AS mediante el reto que le envía el NAS. Sin embargo, el NAS y el AS no se autentican entre sí, ni el NAS se autentica al PC.

Integridad

Salvo la respuesta al reto por parte de PC, que usa la función hash MD5, el resto de mensajes no usan funciones hash, por lo que son vulnerables a modificaciones que no pueden ser detectadas.

No repudio

Salvo la respuesta del NAS al PC con la clave de sesión, no se puede demostrar que el resto de mensajes y acciones han sido hechas por el PC, NAS y AS (por ejemplo no hay prueba de que el PC ha sido el que ha respondido al reto, ni que el rechazo de la petición o su aceptación ha sido realizada por el AS, etc).

Para solucionar estos problemas, cifraría con la clave pública del receptor aquellos envíos mencionados en los que no hay confidencialidad, para la autenticación añadiría los retos que faltan para que se identifiquen todas las entidades, para la integridad usaría funciones hash (MD5, SHA-1, SHA-512) en todos aquellos mensajes donde no se usen y, por último, para conseguir no repudio, haría uso de firmas digitales cifrando los envíos con la clave privada del emisor.

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?

3.1. Un protocolo de reto-respuesta es un procedimiento que se sigue para autenticar a un usuario.

3.2. El esquema de reto-respuesta de las transparencias es un ejemplo de secuencia de mensajes. Primero, la entidad B le manda un reto a la entidad A. Si A es quien dice ser, tendrá una clave secreta compartida con B, que es la que usará para encriptar el reto de B y enviarlo a B. Si A es quien dice ser, cuando le llegue la respuesta a B, podrá desencriptar el mensaje con la clave compartida con A y de esta forma autenticar a A. A también puede plantearle un reto a B para autenticarlo.

3.3. En este caso se cumple la autenticación, aunque no la confidencialidad, ni la integridad ni el no repudio. Veamos cómo conseguir cada una:

Confidencialidad: Habría que cifrar con la clave pública del receptor cada mensaje que se envíe. Así nos aseguramos de que no haya sniffing y solo pueda desencriptar el receptor correcto.

Integridad: Se soluciona haciendo uso de funciones hash, como MD5 o SHA.

No repudio: Se logra usando firmas digitales, es decir, cifrando con la clave privada del emisor.

Por ello, la secuencia de mensajes quedaría así:

1. $K_{pubB}(K_{privA}(S, MD5(S)))$ (Solicitud de A a B para autenticarse)
2. $K_{pubA}(K_{privB}(R, MD5(R)))$
3. $K_{pubB}(K_{privA}(K_{ab}(R), MD5(R)))$