ELENA MARÍA DEL RÍO GALERA

Enero de 2021

**PRÁCTICA 6a: CLAVES**

Ejercicio 1

**Preguntas**

1. Explica si el nodo receptor del mensaje Z puede o no descifrar el mensaje para acceder a su contenido.

Podrá descifrar el mensaje con su clave privada de modo que m = K- (K + (m)) ya que es el destinatario final y necesita solamente su clave privada.

2. Explica si el nodo receptor del mensaje Z estar seguro de la confidencialidad del mensaje, es decir, de que ningún otro nodo ha podido descifrarlo.

El nodo receptor está seguro ya que, para descifrarlo necesita clave privada que solo tiene él.

3. Explica si el nodo receptor del mensaje Z puede autenticar al nodo emisor del mensaje X.

No lo puede autentificar, puesto que X no lo ha firmado y puede decir que no es suyo y Z pensar que pertenece a otro. Al no estar firmado aunque no diga que es o no suyo Z no lo puede confirmar. Además cualquier intermediario puede modificar el mensaje al no estar firmado digitalmente.

4. Explica si el nodo receptor del mensaje Z puede estar seguro de la integridad del mensaje, es decir, que ningún otro nodo ha podido alterar el contenido del mensaje.

No puede estar seguro de la integridad del mensaje ya que, cualquiera puede modificarlo. Ya que no está autentificado o firmado.

5. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el texto del *mensajeParaZ*.

Un nodo cualquiera no puede conocer el texto del mensajeParaz porque no conoce su clave privada pero si podría modificar ese mensaje.

6. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el destino final del mensaje.

Los nodos B,C,D aprenden el siguiente salto pero no conocen el destino final. El destino final solo lo sabe quien envía el mensaje.

7. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el nodo que creó el mensaje.

No podrá conocerlo nadie solo el que lo creó.

Ejercicio 2

**Preguntas**

1. Indica cómo crees que debería enviarle la clave Ks de Alicia a Roberto.



2. Alicia no tiene la clave pública de Roberto ni Roberto la de Alicia. Indica cómo podría conseguir Alicia la K + R , sin quedar físicamente para intercambiarse las claves, y como puede Alicia estar segura de que esta clave se corresponde con la de Roberto.

A través de CA1 y CA2 que ambos conocen se pueden intercambiar las claves.

3. Con este sistema, ¿puede estar Alicia segura de que los mensajes que envía a Roberto son confidenciales y de que en realidad se está comunicando con Roberto? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.

Si son confidenciales ya que usa la clave de sesión Ks enviada cifrada con la clave pública de Roberto que ha sido previamente obtenida mediante los CA.

4. Con este sistema, ¿puede estar Roberto seguro de que los mensajes son confidenciales y provienen de Alicia? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.

Son confidenciales pero no se puede saber si provienen de Alicia porque ella no está usando la firma digital.

5. El certificado de la clave pública de Roberto ha caducado y ya no es válido. Roberto decide cambiar de autoridad de certificación y consigue un certificado de su clave pública emitido por la autoridad de certificación CA3. Esta autoridad de certificación CA3 no ha incluido su certificado autofirmado en las aplicaciones de comunicaciones del sistema, pero CA3 tiene un certificado de la clave pública de CA3 firmado por CA2. Indica si ahora Alicia podría enviar a Roberto mensajes confidenciales y auténticos y explica cómo lo haría.

Sí, a través de la cadena de certificación.

3. Ejercicio 3

Abre el navegador Firefox y a través del menú selecciona la opción:

Editar ! Preferencias ! ¡Privacidad y Seguridad ! Seguridad ! Certificados ! Ver Certificados.

En la pestaña Autoridades verás los certificados de las autoridades de certificación de primer nivel. Cualquier certificado que venga firmado por las autoridades de certificación que se encuentran en esta pestaña podrá ser verificado ya que se poseen de forma fiable las claves públicas de estas autoridades de certificación que permiten comprobar las firmas.

1. Escribe en la URL del navegador la siguiente dirección: www.amazon.es, una vez que se haya cargado la página verás junto a la URL un candado verde, pulsa sobre él y luego sobre la flecha derecha al lado de “Conexión segura” (“Mostrar detalles de la conexión”). Indica cuál es la autoridad de certificación que ha verificado esta conexión segura.

DigiCert Inc

2. En esa ventana de detalles de la conexión, pulsa sobre el botón “Más información” y luego en “Ver Certificado” y en la pestaña "Detalles". Indica cuál es la jerarquía de certificados que se está utilizando para verificar a Amazon. Selecciona empezando por www.amazon.es el campo “Emisor” y ve comprobando quiénes han sido las entidades que han generado los certificados que aparecen en la jerarquía. Comprueba la cadena de todos los certificados. Señala qué certificados de la jerarquía están autofirmados.

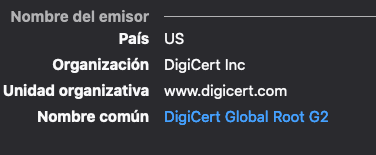
Emisor amazon



Jerarquía:



Emisor DigiCert Global CA G2 Emisor DigiCert Global Root G2



En estos dos últimos tenemos un sí en autoridad de certificación.

3. Vuelve a visitar la información de certificados de las Preferencias (Editar → Preferencias → Privacidad y Seguridad → . . . → Ver Certificados). Observarás que las dos entidades que aparecen en la jerarquía de certificados

de Amazon tienen instalado su certificado. Una de ellas muestra su certificado como Builtin object token, es decir, se trata de un certificado autofirmado de una autoridad de certificación raíz que venía instalado con la aplicación Firefox. El otro certificado se muestra como Disp. software de seguridad, por lo que no es un certificado autofirmado y la entidad que lo ha firmado es una autoridad de certificación raíz. Indica cuál de ellos es Builtin object token y cuál es Disp. software de seguridad.

