El resumen o yo que sé lol salu2.

# TEMA 5: APLICACIONES DE LA CRIPTOGRAFÍA.

1: Aplicaciones prácticas de la criptografía.

Su utilizad principal es que permite comprobar si un atacante no ha modificado una página web no contenga una versión falsa de la aplicación, garantizar identidades, etc.

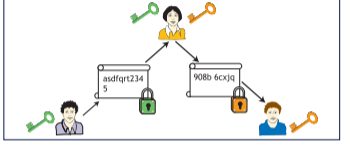
2: La firma digital.

Sirve para asegurarnos de que el mensaje recibido es exactamente igual al original, que viene de la persona quien dice venir, y que el emisor no pueda negar el haber sido quien generó el mensaje.

¿Qué es la firma digital? La firma digital es un conjunto de datos que se añaden a un mensaje original que permiten asegurar la identidad de la persona que firmó el mensaje, además de que el mensaje no haya sido modificado por terceros.

2.1: Firma digital con árbitro.

Se usan en sistemas de clave **simétrica**. Si dos personas (Jaime y Eduardo) no confían entre ellos, eligen a un tercero, en quien ambos confíen (Jorge). En este caso, Jorge será el intermediario. El árbitro (Jorge) **conoce las claves de ambos**. Eduardo le manda el mensaje a Jorge, y Jorge lo descifra con la clave de Eduardo. Luego, Jorge cifra el mensaje con la clave de Jaime, y Jaime recibirá el mensaje de parte de Jorge.



Dibujo mal recortado de la firma con árbitro

**2.2: Firma digital ordinaria.**

Se basan en el uso de funciones **hash** y de cifrado de clave **pública**. El emisor (Carlos) quiere mandar el mensaje al receptor (Víctor) de que ha pillado una gripe. Para ello, Carlos deberá aplicar la función hash al documento que contiene el mensaje. Tras ello, cifrará el hash con su clave privada (la de Carlos), convirtiendo ese hash en su **firma electrónica**. Lo adjuntará al documento firmado, y lo enviará a Víctor.

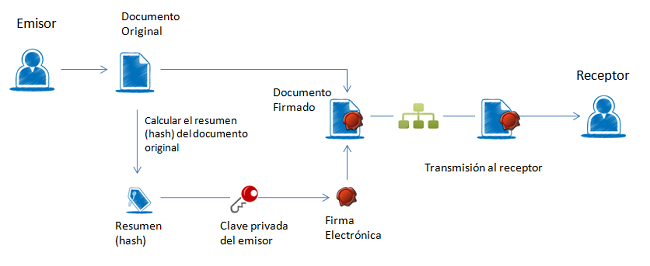


Imagen ilustrativa

Para comprobar que no ha sido editado ni modificado, Víctor debe aplicar una función hash sobre el archivo, y descifrar el hash del documento. Si coinciden, es que el archivo no ha sido modificado.

**2.3: Clases de firma digital.**

Hay 3 tipos:

**-Electrónica**. Un ejemplo de ello es cifrar un mensaje con nuestra clave privada. Sirven como medio de identificación del firmante.

**-Firma electrónica avanzada**. Permite identificar al firmante y cualquier modificación, utilizando los algoritmos hash y su cifrado.

**-Firma electrónica reconocida**: está basada en un **certificado reconocido** generada por un dispositivo seguro de creación de firma. Por ejemplo, firmar usando el DNIe.

Suele ser importante que la firma también tenga el momento exacto en el tiempo en el que se ha realizado. Por ello, se usa un mecanismo llamado **sellado de tiempo (timestamping)**, en el que una tercera persona certifica mediante su firma que la firma del primer usuario se produjo en un momento concreto.

**3: Certificados digitales**.

Había un problema con las firmas digitales: que no podías saber si la clave pública recibida era de la persona correcta y no un suplantador. Por ello, se implementó un documento de identidad electrónica. De ahí salieron los certificados digitales, que **son documentos electrónicos basados en la criptografía de clave pública y los sistemas de firma digitales.** Su misión principal es garantizar el vínculo entre una persona/entidad/servidor y una pareja de claves correspondientes.

**3.1: Concepto y característica**.

Me da mucha pereza seguir seguiré más adelante. Mientras, haré otro tema.

# Tema 6: Software malicioso.

El software malicioso **son aquellos programas (o software) que modifica el funcionamiento de un equipo, alterar la información que procesa, la modifica/borra o la envía sin nuestro conocimiento a terceras personas.** Es cualquier software que pueda representar una amenaza al sistema o ser molesto para el usuario.

El software se propaga a través de dos vulnerabilidades:

**-Vulnerabilidades del software**, que consiste en explotar debilidades del sistema operativo o algún programa. Algunos malware pueden copiarse a sí mismos y enviarse a través de la red para infectar más equipos.

Se recomienda tener actualizado el sistema y los programas utilizados.

**-Vulnerabilidades asociadas a las personas:** por desconocimiento, exceso de confianza, o por pura selección natural, **muchas veces son los usuarios quienes contribuyen a su propagación**. De nada sirve un sistema operativo seguro con el mejor antivirus, si el usuario es un irresponsable que acaba infectando su equipo (como las vacunas y la gente que no usa mascarilla).

Es necesario tener sentido común, prudencia y conocimiento.

También hay que tener en cuenta su difusión. La inmensa mayoría del malware está dirigido a sistemas Microsoft, aunque hay malware diseñado específicamente contra MacOS y Linux. También afectan a los dispositivos móviles.

**2: Clasificación del malware**.

Se pueden clasificar en función de:

**2.1: Impacto producido sobre la víctima**.

Según este criterio y el libro de los apuntes, hay tres niveles de peligrosidad: **bajo, medio o elevado**. Para evaluarlo, se estudia la gravedad de los efectos en un equipo infectado, su facilidad de propagación, y el número de infecciones producidas recientemente.

**2.2: Según su forma de propagación**.

Según su forma de propagación, pueden dividirse en **virus, gusanos y troyanos.**

**-Un virus informático es un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático sin el conocimiento o consentimiento de su usuario, corrompiendo o destruyendo archivos.** Al ejecutarse, **se propaga infectando otros ficheros**, pero **requiere de intervención humana** para que el programa malicioso se ejecute. El virus **se instala en la memoria RAM, desde donde infecta archivos**, y los graba en el disco duro.

Sus efectos pueden ser muy inofensivos, o muy peligrosos. Su forma de propagación puede ser variable también.

En resumen, **se propaga infectando otros ficheros, y requiere de intervención humana para ejecutarse.**

**-Gusanos**.

Es un malware **que se propaga automáticamente sin infectar otros archivos, sin la intervención del usuario**. Están pensados para consumir recursos de un sistema o red hasta saturarlo.

Suele ser difundido por canales de chat, redes peer to peer (en las que todos los equipos actúan como un cliente y un servidor), recursos compartidos en una red local, correo electrónico, entre otros. Igualmente, **su eliminación es más sencilla que la de un virus, ya que no modifican archivos.**

**-Troyanos.**

Es un malware **que aparenta ser un programa inofensivo, con la finalidad de que alguien tome el control de esa máquina. No infectan ni corrompen archivos, ni tienen la capacidad de propagarse automáticamente.**

Las infecciones suelen darse cuando el usuario ejecuta un programa infectado. Una vez se instale el troyano, pasará desapercibido. Continuaré con esto después de la merienda.