Nociones de Criptografía.

La criptografía es la ciencia que se ocupa, mediante ciertos algoritmos, de ocultar la información que va a transmitirse a terceras personas.

El proceso de modificación para ocultar un mensaje se llama **cifrado,** el proceso inverso, es decir poner en claro un mensaje cifrado se llama **descifrado.**

En criptografia se utilizan algoritmos y claves para el cifrado de información, hay dos tipos principales de claves de cifrado;

1. Simétricas, la misma clave se usa para cifrar y descifrar los mensajes, ejemplo AES(El cifrado AES, o advanced encryption standard, es un cifrado simétrico en bloques que se utiliza para cifrar datos confidenciales.)
2. Asimetricas, se usan distintas claves para cifrar y descifrar, el par de claves publica/privada de PKI es la mas conocida, los algoritmos usados para cifrado/descifrado con claves asimetricas son mucho mas costosos desde el punto de vista de potencia de cálculo que los que usan claves simetricas por lo que es habitual usar ambos conjuntamente, por ejemplo se usa cifrado asimetrico para cifrar la clave simetrica con la que se ha cifrado un mensaje.

Algoritmos de hash, el hashing es una importante herramienta criptográfica para transformar los datos en los llamados valores hash. Para ello se utiliza una función hash especial, normalmente en forma de algoritmo. La tarea central del hashing se puede adivinar por la traducción del término al español, esta es, “picar o mezclar”. Y en el hashing no ocurre nada más que eso: conjuntos de datos como contraseñas, datos de empresas y usuarios u otras formas de datos se descomponen y se transforman en una nueva **forma abreviada, el valor hash.**

Cerificados digitales introducción y conceptos generales

Certificados digitales.

Un certificado digital es un archivo o fichero que contiene información en forma digital que identifica de manera inequivoca, garantizada por una autoridad de certificación, a una persona física, una entidad juridica o un servidor web.

El sistema de seguridad de certificados digitales se llama PKI(siglas en inglés de Infraestructura de Clave Pública) y consta de;

un par de claves privada+pública asignadas a una persona/entidad y

de una infraestructura formada por autoridades (CAs) que emiten, validan y revocan esas claves.

___ooo___

El par de claves privada/pública los genera la autoridad de certificación, mediante un algoritmo matematico (el más habitual, RSA, está basado en los números primos), y los asigna y entrega a la persona o entidad certificada, bien en un soporte fisico(tarjeta parecida a un DNI electrónico) o en un fichero que se descargará de internet.

ACR

¿Para qué sirven el par de claves privada / pública?

La respuesta breve es para cifrar y descifrar información, pero con unas propiedades muy interesantes;

La **clave privada** tiene dos finalidades;

- Firmar digitalmente un mensaje, **no repudio** y
- **Descrifrar** los mensaajes cifrados con la clave pública asociada.

La **clave publica** se usa para **cifrar información**, el mensaje cifrado solo puede descifrarse con la clave privada asociada, la clave pública permite mantener la **confidencialidad** de la información.

La alteración de un mensaje cifrado hará imposible su descifrado.

La clave privada debe ser secreta y debe mantenerla siempre en su poder el propietario del certificado digital sin comunicarla a nadie más, la clave pública, como su nombre indica, se comunica a cualquier entidad con la que se intercambie información.

El propietario del certificado digital cuando envía un mensaje lo cifra con la clave pública del destinatario, el receptor del mensaje lo descifrará con su clave privada asociada a esa clave publica concreta, si el proceso de descifrado funciona, es decir devuelve el mensaje en claro, significa que no ha habido manipulación del mensaje en transito. Para responder, usará la clave pública del remitente para cifrar la respuesta, el remitente descifrará la respuesta usando su clave privada. En este ejemplo la **confidencialidad** está asegurada en los dos sentidos, es decir, envio de mensaje y respuesta a él.

La clave privada se usa, además de para descifrar mensajes cifrados con la clave publica asociada, para **firmar** información, sean documentos o mensajes, la forma de hacerlo es aplicar un algoritmo de **hash** al mensaje y luego usando la clave privada generar una firma de ese **hash,** la **firma digital** creada solo puede descifrarse con la clave pública asociada a la clave privada con que fue creada, el propietario de la clave privada no puede alegar que él no creo el mensaje porque si no hubiese sido cifrado con su clave privada no hubiese podido ser descifrado con la pública correspondiente, esto se conoce como **no repudio** , es decir el propietario de la clave privada que envía un mensaje con su firma digital no puede alegar no haberlo hecho. El robo y utilización fraudulenta de una clave privada da lugar al delito de **impersonación,** es decir alguien que se hace pasar por el legitimo propietario de la clave privada.

Por otra parte cualquiera que tenga nuestra clave pública podrá enviarnos un mensaje con la **confidencialidad** de ese mensaje asegurada ya que solo quien tenga la clave privada podrá descifrarlo.

Ejemplo muy simplificado

Para que se entienda bien todo lo anterior voy a poner un ejemplo. Cel ejemplo de accedeso a una cuenta bancaria mediante internet usando usuario y contraseña, recordemos que el uso de cualquier web en internet es un dialogo entre dos programas, nuestro navegador y el servidor con el que se comunica, cada vez que enviamos un pantallazo es un mensaje en la dirección navegador->servidor, cada vez que recibimos un pantallazo es un mensaje en la dirección servidor-> navegador, en este caso el dialogo con la web del banco funciona así;

ACR

Enviamos un pantallazo con la URL del banco, este nos responde enviándonos la pantalla de logon, pero también envía al navegador su clave pública y nosotros veremos si clicamos en el candado que aparece en el navegador que autoridad concedió el certificado digital, cuando enviamos el pantallazo al banco con nuestro usuario y contraseña, esa información va cifrada con la clave pública del banco, solo él puede descifrarla, **confidencialidad asegurada,** cuando el banco nos envía un mensaje con nuestros datos los cifra con nuestra clave publica y al descifralas con nuestra clave privada tenemos la **certeza** de que provienen del banco y solo de él, es decir no ha habido un hacker en medio que alteró el contenido.

Otro ejemplo sería cuando presentamos en Hacienda la Declaración de la Renta, en este caso hacienda nos obliga a que usemos nuestro certificado digital, porque así cuando le enviemos información irá **firmada** con nuestra clave privada y por tanto no podremos **repudiarla,** es decir si los datos son erróneos no podremos alegar que no hemos sido nosotros los autores.

¿Qué es una Huella Digital?

. La huella digital o resumen (**hash**) de un mensaje se obtiene aplicando una función, denominada hash, a ese mensaje, esto da como resultado un conjunto de datos único de longitud fija.

Una función hash tiene entre otras las siguientes propiedades:

Dos mensajes iguales producen huellas digitales iguales.

Dos huellas digitales idénticas pueden ser el resultado de dos mensajes iguales o de dos mensajes completamente diferentes.

Dos mensajes parecidos producen huellas digitales completamente diferentes.

Una función hash es irreversible, no se puede deshacer, por tanto, su comprobación se realizará aplicando de nuevo la misma función hash al mensaje y comparando el resultado con la huella.

Firma digital

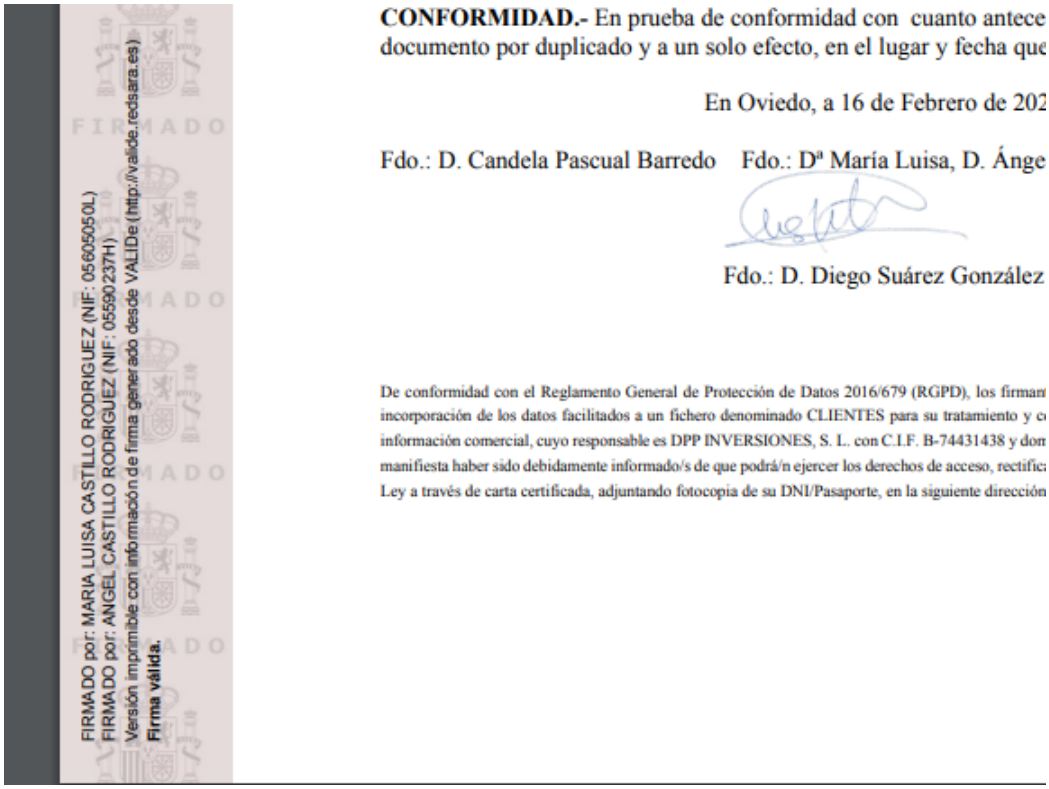
Firmar digitalmente un documento no es como muchos jovenes LOGSE dirían mojar un dedo en tinta y poner la huella en el documento, eso es firmar con el dedo. Firmar digitalmente un documento consiste en generar una huella digital, es decir un mensaje, y cifrarla con la clave privada del certificado digital y adjuntarla a dicho documento, si ese documento fuese alterado de alguna forma despues de su firma la huella digital no podría ser descifrada o bien las huellas generadas no coincidirian y por tanto se detectaría su falsedad, allá donde se envíe dicho documento firmado se podrá comprobar esa huella usando la clave pública correspondiente y el firmante al haber generado la huella con su clave privada **no puede repudiar** el documento.

Validacion e impresión de un documento firmado digitalmente.

Un documento firmado digitalmente no debe imprimirse sin seguir ciertas normas ya que la firma digital se perdería, ademas una vez firmado digitalmente no puede modificarse ya que eso le haría perder su validez.

ACR

Si queremos imprimirlo debemos ir a la página https://valide.redsara.es/valide/? Y allí seleccionar visualizar firma, seleccionaremos nuestro documento firmado, nos aparecerá entonces una versión del documento listo para imprimir si así lo deseamos.



Como puede observarse en la figura el docuemnto ha sido modificado por lo que ya solo podrá usarse como copia impresa.

ACR

Programa en Python para firmar un mensaje

```
from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256
# Pedir la contraseña de la clave privada y el mensaje a firmar
contrasena = input("Introduce la contraseña de la clave privada: ")
message = input("Introduce el mensaje: ")
# Cargar la clave privada
with open('private.pem', 'rb') as f:
    private_key = RSA.import_key(f.read(), passphrase=contrasena)
# Mensaje que queremos firmar
message = message.encode()
# Crear un objeto de resumen (hash) del mensaje
h = SHA256.new(message)
# Firmar el mensaje con la clave privada
firma = pkcs1_15.new(private_key).sign(h)
# Imprimir la firma
print("Firma digital generada:", firma)
```

Programa en Python para comprobar la firma de un mensaje

```
from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256
# Cargar la clave pública
with open('public.pem', 'rb') as f:
    public_key = RSA.import_key(f.read())
#Pedir mensaje y firma
message = input("Introduce el mensaje: ")
firma = input("Introduce la firma digital: ")from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256
# Pedir la contraseña de la clave privada y el mensaje a firmar
contrasena = input("Introduce la contraseña de la clave privada: ")
message = input("Introduce el mensaje: ")
```

ACR

```
# Cargar la clave privada
with open('private.pem', 'rb') as f:
    private_key = RSA.import_key(f.read(), passphrase=contrasena)
# Mensaje que queremos firmar
message = message.encode()
# Crear un objeto de resumen (hash) del mensaje
h = SHA256.new(message)
firma =eval(firma)
# Cargar el mensaje y la firma
message = message.encode()
# Crear un objeto de resumen(hash) del mensaje
h = SHA256.new(message)
# Verificar la firma
try:
    pkcs1_15.new(public_key).verify(h, firma)
    print("La firma es válida.")
except (ValueError, TypeError):
    print("La firma no es válida o la clave pública no es correcta.")
```

ACR