Firma electrónica

2017

José Felix Muñoz Soro, Javier Casado Cadarso, Julián Lucea Saenz

Diputación Provincial de Huesca

CRIPTOGRAFÍA

¿Qué es?

Wikipedia: la ciencia que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados

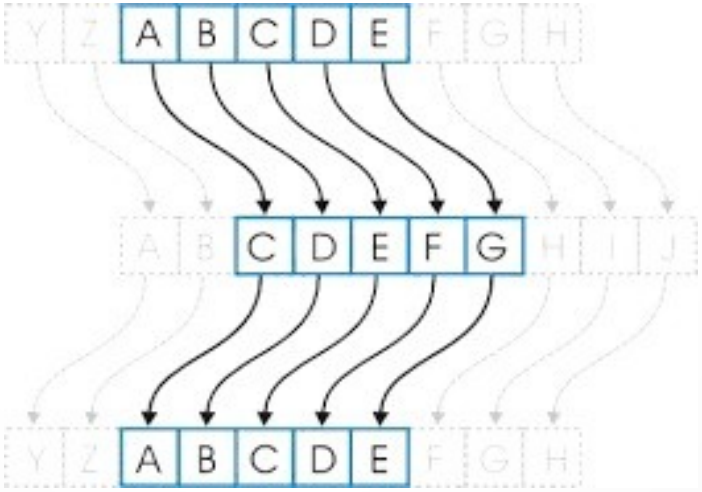
CRIPTOGRAFÍA

Tiene sus comienzos en la edad antígüa, Se basaba en métodos de trasposición y sustitución.

Se cree que uno de los primeros métodos de trasposición conocidos fue la Escítala. Utilizada en la Grecia antígua.

CRIPTOGRAFÍA

Julio César empleó un método de sustitución, basado en sustituir caracteres por otros posicionados más adelante en el alfabeto:



Técnicas de criptografía: algoritmos

1.- Algoritmo criptográfico: un ejemplo de trasposición y sustitución:

el perro de roque no tiene rabo

Técnicas de criptografía: algoritmos

Paso 1: cambiamos el orden de los caracteres: el primero por el segundo, el tercero por el cuarto, etc. (incluyendo los espacios):

lep reord eoruq eon teien arob

Técnicas de criptografía: algoritmos

Paso 2: desplazamos las vocales hacia la derecha (cambiamos a por e, e por i, etc.):

lip riurd iuraq iun tioi erub

Técnicas de criptografía: algoritmos

Paso 3: desplazamos las consonantes hacia la derecha, saltando las bocales (b por c, c por d, etc):

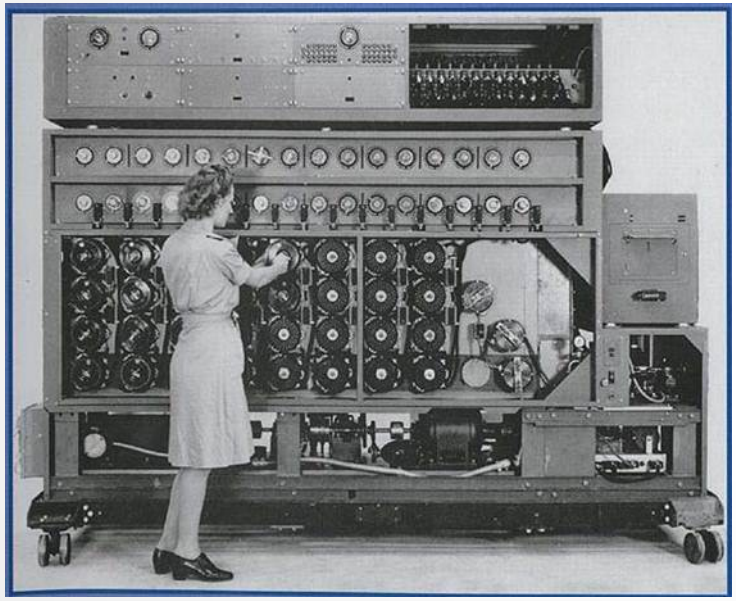
miq siusf iusar iup vioi esuc

Técnicas de criptografía: algoritmos

El avance significativo se produce durante la 2ª guerra mundial. Aparece enigma: los rodillos funcionaban como clave

Técnicas de criptografía: algoritmos

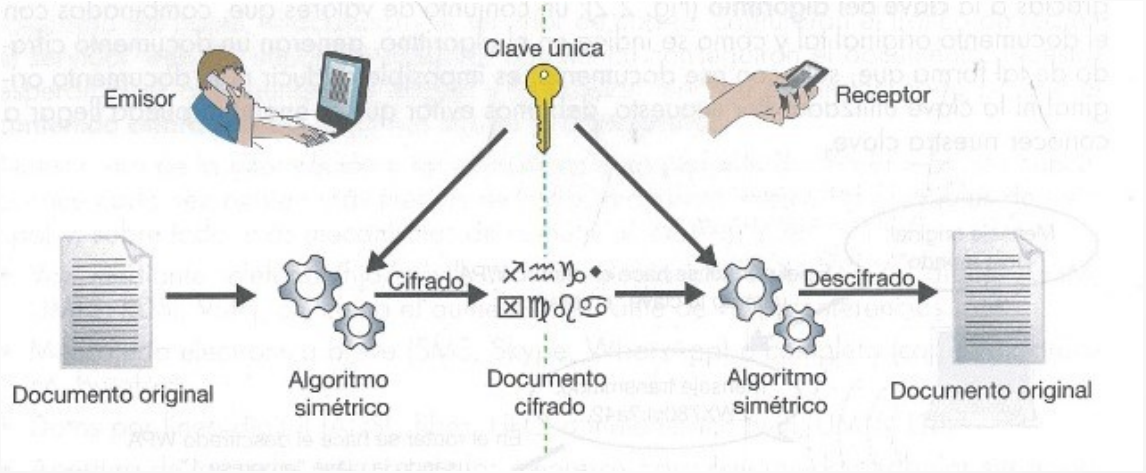
Los esfuerzos por descifrar enigma provocan enormes avances en las técnicas de criptoanálisis: Escuela Gubernamental de Códigos y Cifras de Bletchey Park.



Maquina Bombe basada en los trabajos de Alan Turing

Técnicas de criptografía: algoritmos basados en clave simétrica

A partir de los 70 aparecen los procedimientos públicos que utilizan una clave personal para cifrar y la misma clave para descifrar, hay muchos: AES, DES, 3DES, IDEA, etc.



Técnicas de criptografía: algoritmos basados en clave simétrica

Práctica, encriptar fichero con 7z

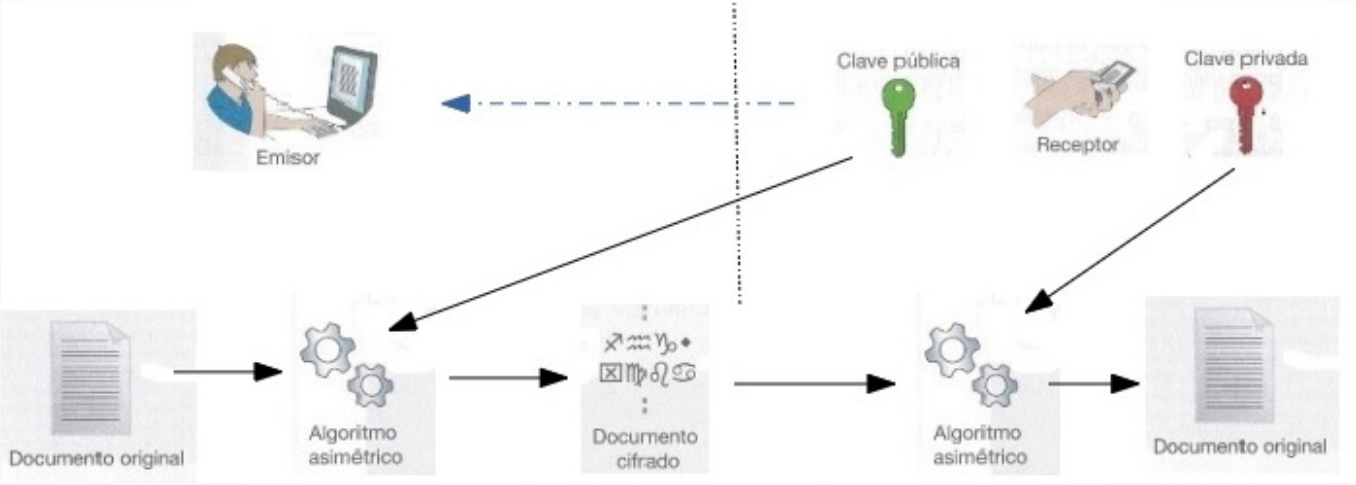
Técnicas de criptografía: algoritmos basados en clave asimétrica

En 1977 Ronald Rivest, Adi Shamir y Leonard Adleman describen el primer algoritmo de clave asimétrica (o clave pública): RSA
Cada persona tiene dos claves: pública y privada.
El texto cifrado con la clave privada se descifra con la clave pública.
El texto cifrado con la clave pública se descifra con la clave privada.

Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo: un emisor cifra un mensaje para que solo lo lea un receptor:

1.- El emisor toma la clave pública del receptor.
2.- El emisor cifra con esa clave.
3.- El receptor descifra con su clave privada.



Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren establecer unas comunicaciones seguras.

Hacker

ALMACEN DE CLAVES

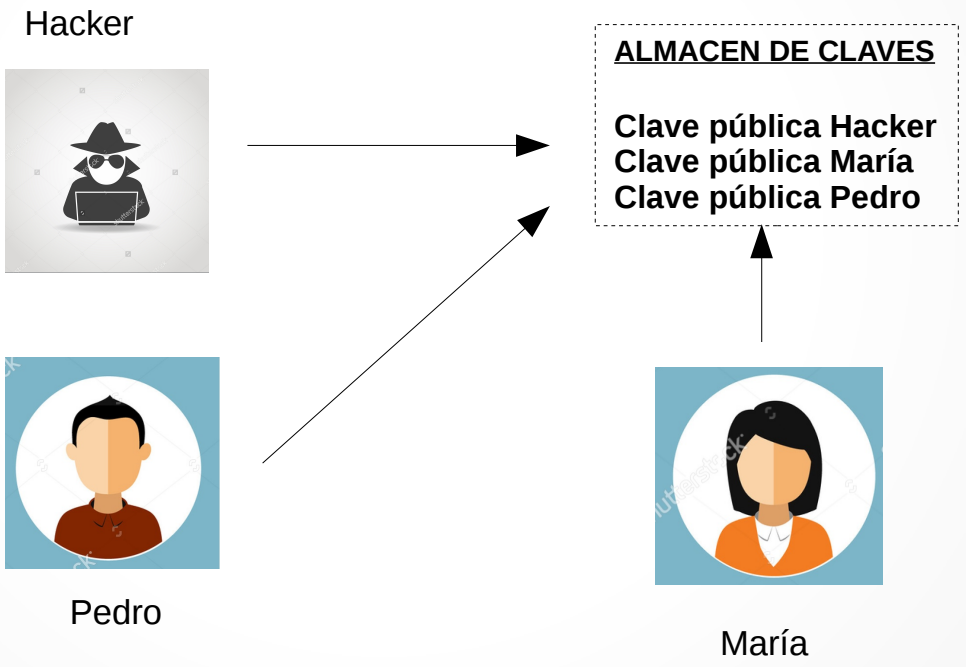
Clave pública Hacker
Clave pública María
Clave pública Pedro

Pedro

María

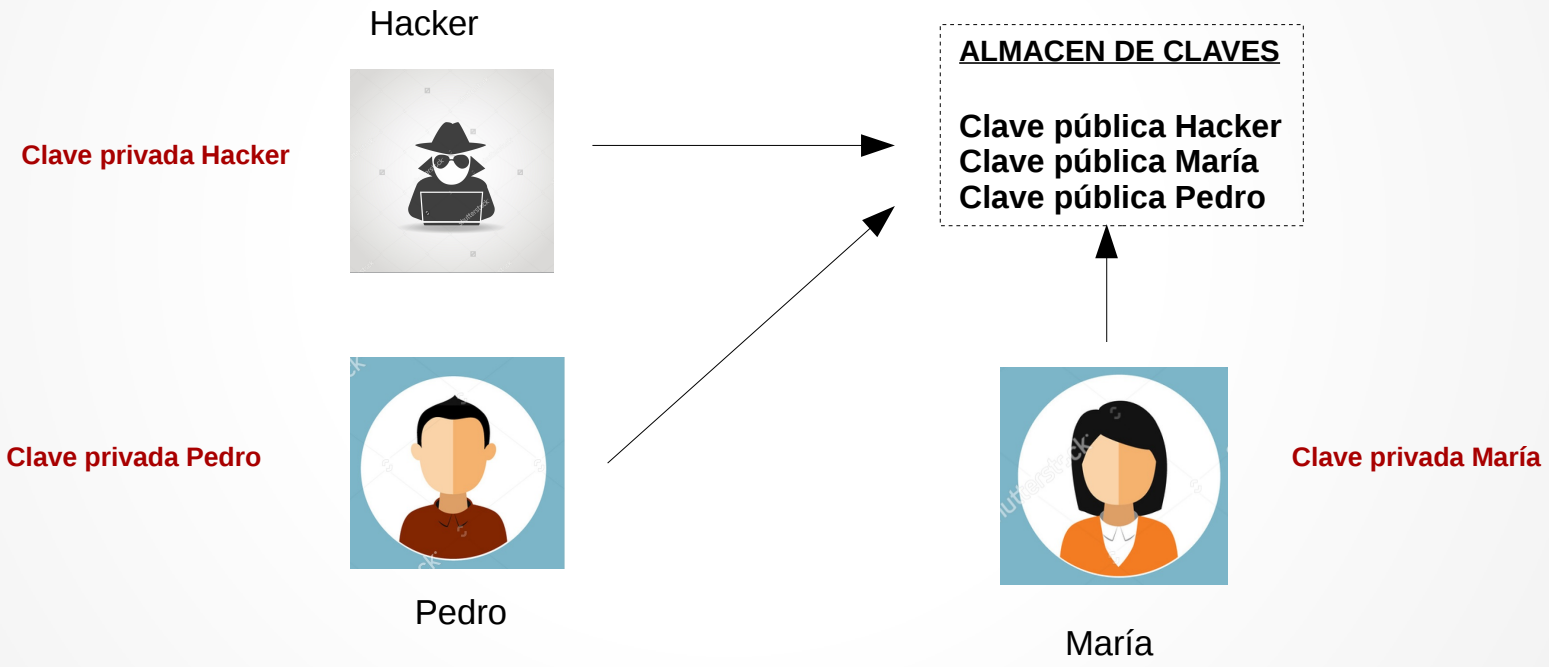
Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren establecer unas comunicaciones seguras: todos acceden al almacen de claves públicas.



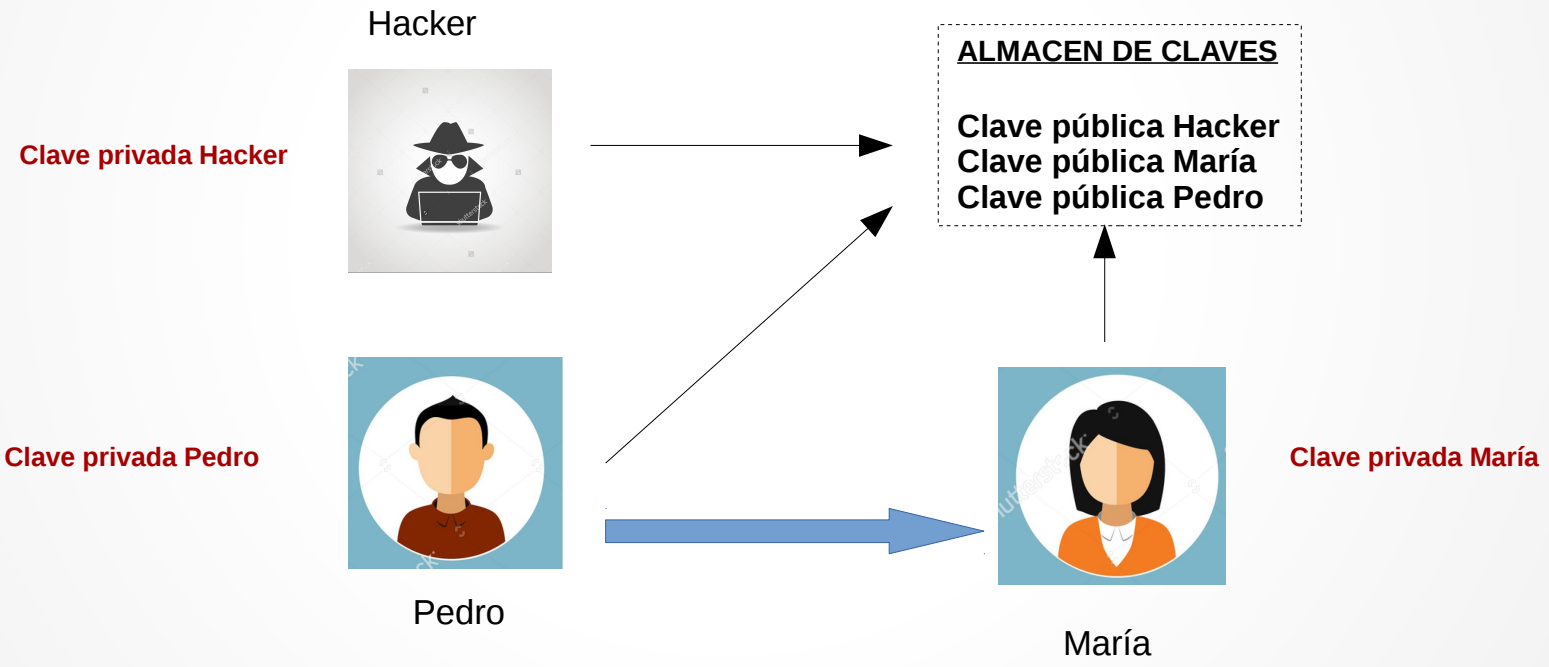
Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren establecer unas comunicaciones seguras: cada uno tiene su clave privada.



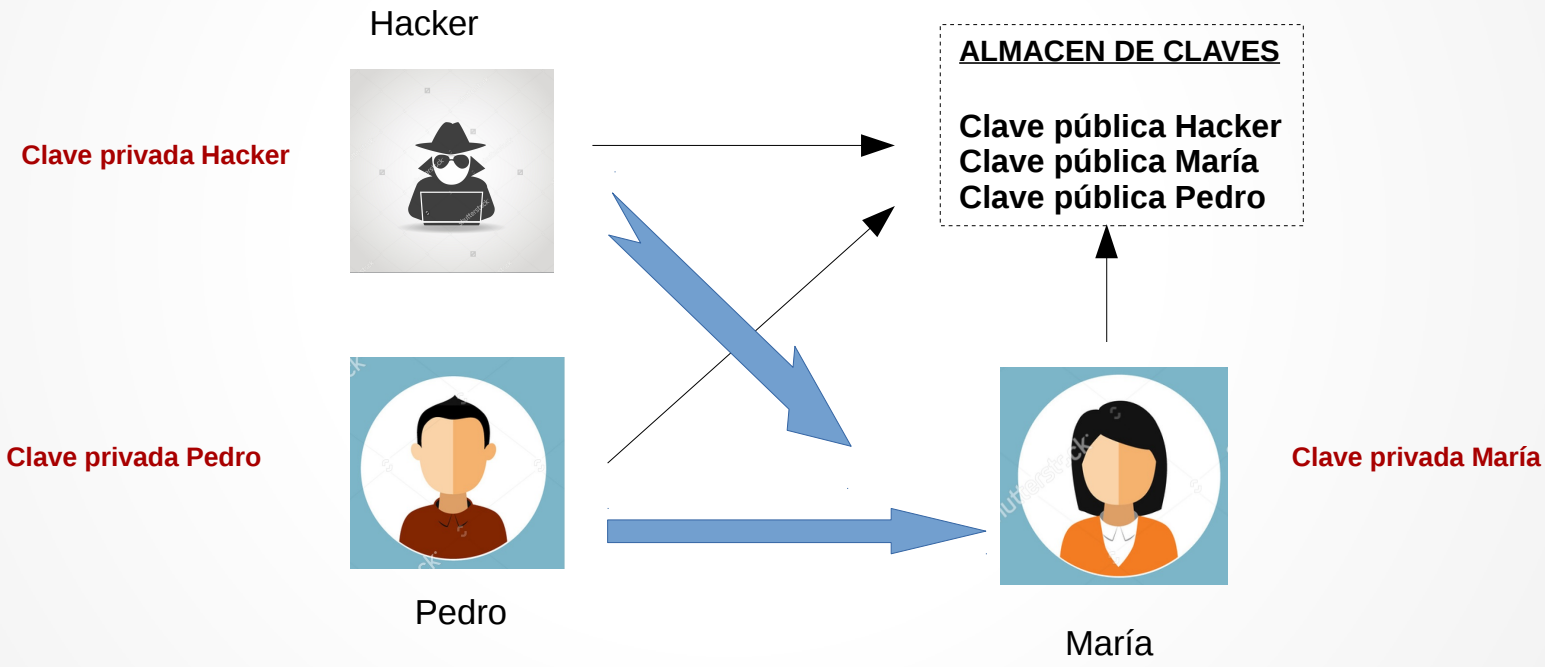
Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren establecer unas comunicaciones seguras: Pedro lee la clave pública de María, cifra el mensaje con esa clave y se lo envía a María, María lo descifra con su clave privada.



Técnicas de criptografía: algoritmos basados en clave asimétrica

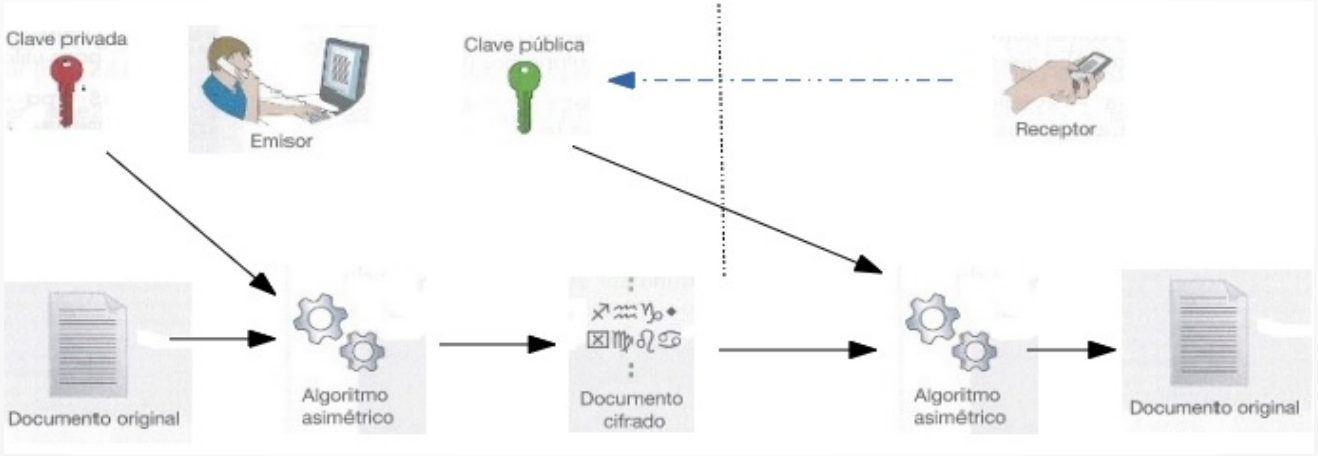
Ejemplo de cifrado con clave pública: María y Pedro quieren establecer unas comunicaciones seguras: Hacker captura el mensaje, intenta descifrarlo con la clave pública de María, pero no lo consigue.



Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo: un emisor cifra un mensaje para que lo lea cualquier receptor.

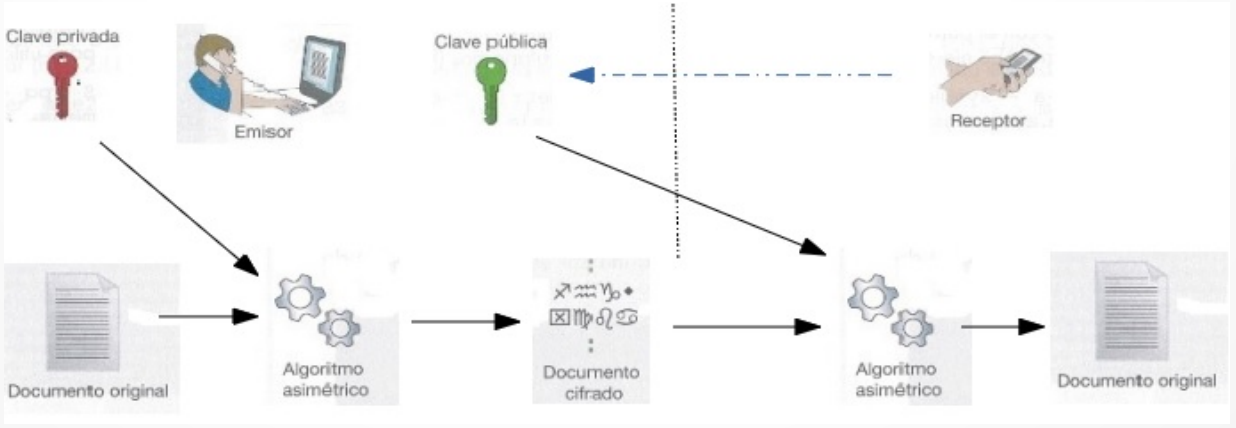
1.- El emisor cifra con su clave privada.
2.- El receptor toma la clave pública del emisor.
3.- El receptor descifra con la clave pública del emisor.



Técnicas de criptografía: algoritmos basados en clave asimétrica

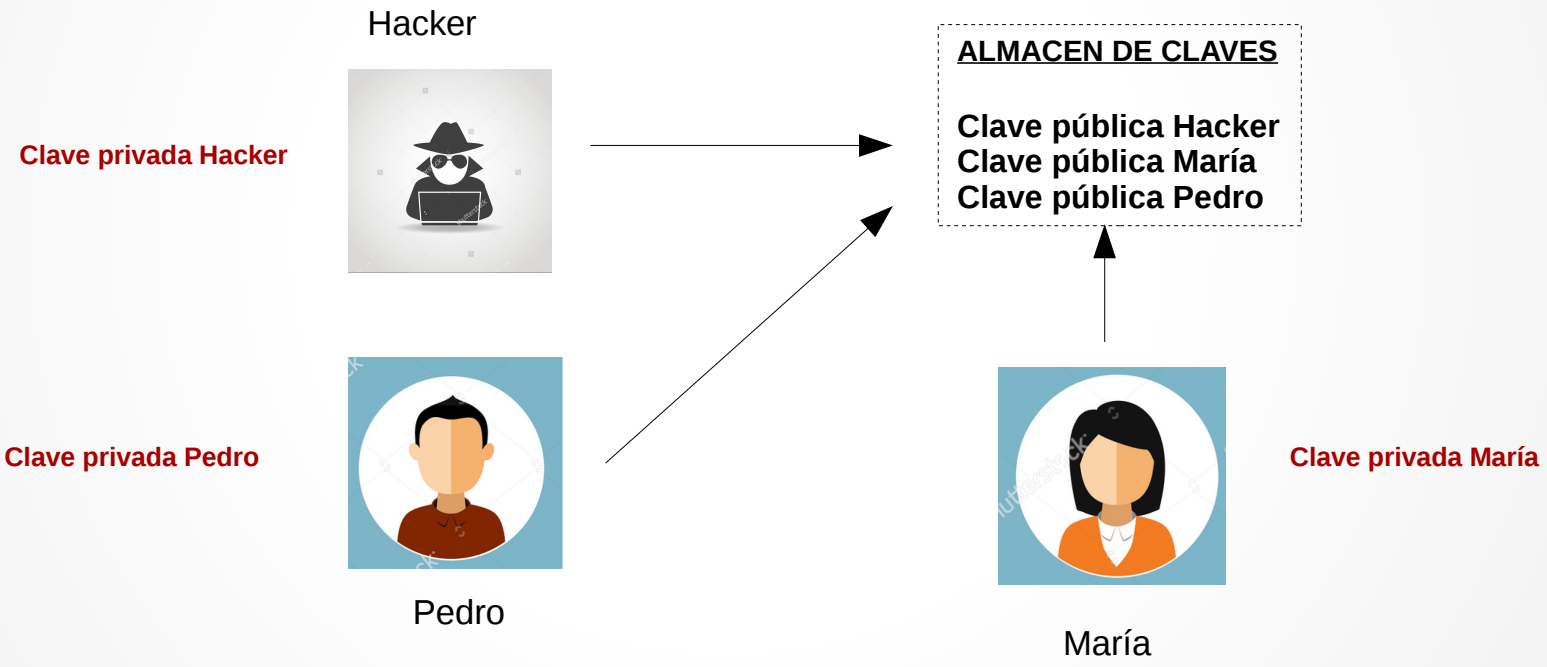
Ejemplo: un emisor cifra un mensaje para que lo lea cualquier receptor.

En este caso se tiene la garantía de que el mensaje ha sido cifrado por la persona que tiene la clave privada del emisor; es decir el emisor ha firmado el mensaje.



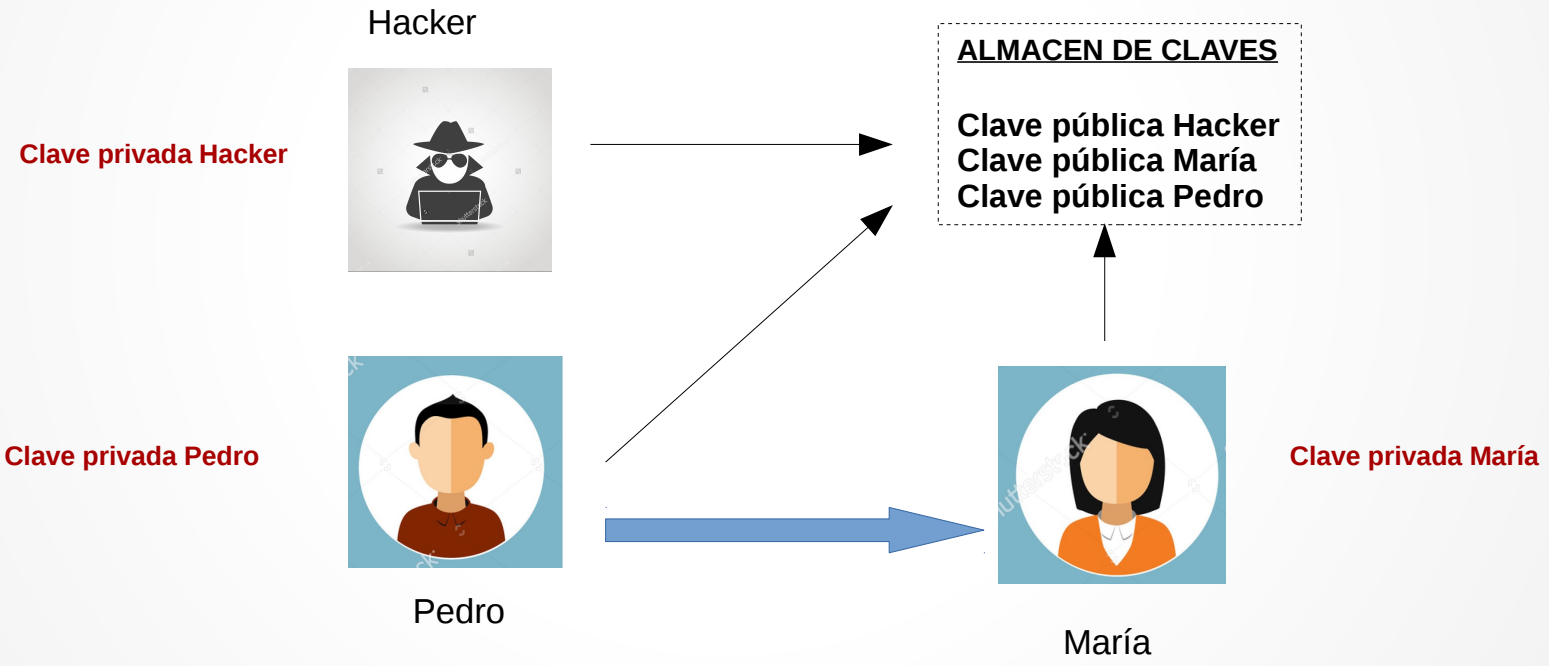
Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren intercambiar mensajes.



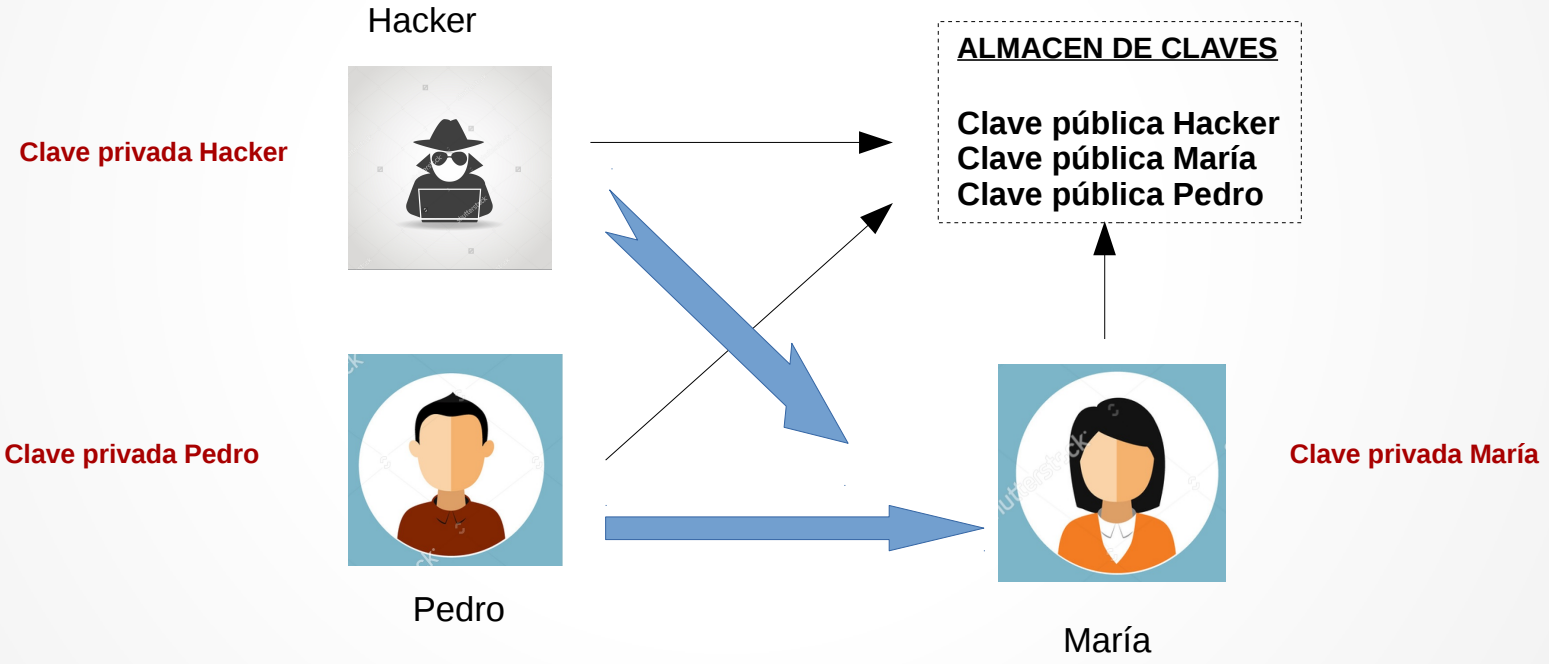
Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren intercambiar mensajes. Pedro cifra el mensaje con su clave privada y se lo manda a María. Como María lo puede descifrar con la clave privada de Pedro sabe que el mensaje es de él, es decir, Pedro ha firmado el mensaje.



Técnicas de criptografía: algoritmos basados en clave asimétrica

Ejemplo de cifrado con clave pública: María y Pedro quieren intercambiar mensajes. Pedro cifra el mensaje con su clave privada y se lo manda a María. Como María lo puede descifrar con la clave privada de Pedro sabe que el mensaje es de él, es decir, Pedro ha firmado el mensaje. El Hacker también lo sabe pero da igual.



Técnicas de criptografía: funciones Hash

Problemas:

1.- Los algoritmos de clave pública son muy lentos: se consume mucho tiempo de proceso.
2.- El tamaño de los mensajes cifrados se duplica.

Solución: las funciones Hash, funciones que toman un fichero y obtienen una representación de él.

Una función Hash debe cumplir:

1.- Sea cual sea el tamaño del fichero de entrada, el tamaño de la representación es siempre el mismo.
2.- Es imposible obtener el fichero de entrada a partir de su representación.
3.- Cualquier cambio en el fichero de entrada, obtiene una representación totalmente diferente.
4.- Es improbable que dos ficheros de entrada diferentes obtengan la misma representación.

Técnicas de criptografía: funciones Hash

Algunas funciones hash:

MD5: produce un resultado de 128 bits

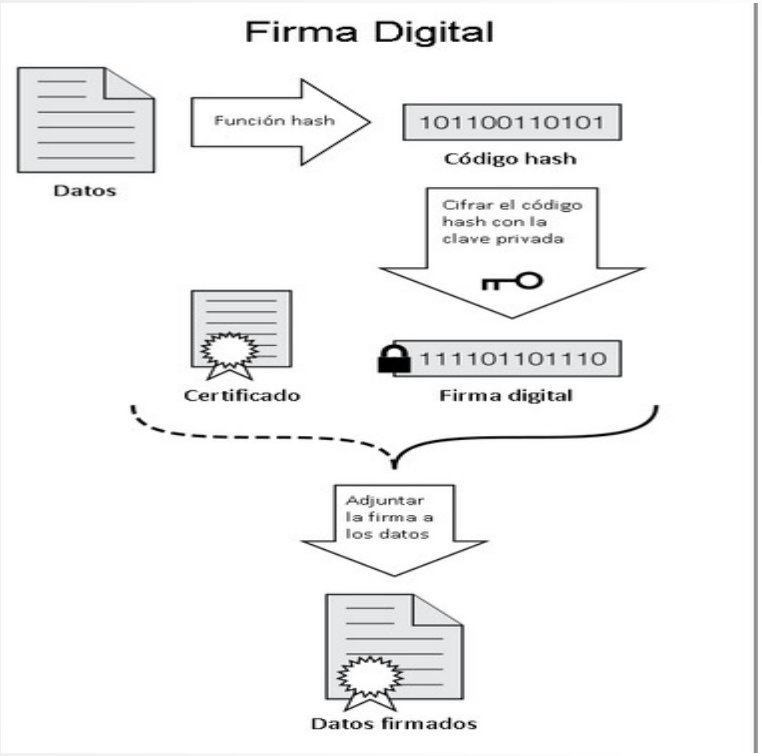
SHA-1: produce un resultado de 160 bits

SHA-2: funciones SHA-224, SHA-256, SHA-384, SHA-512

Muy utilizado en firma electrónica: SHA-256 y RSA.

Práctica funciones hash

Firma digital, ¿cómo se firma?

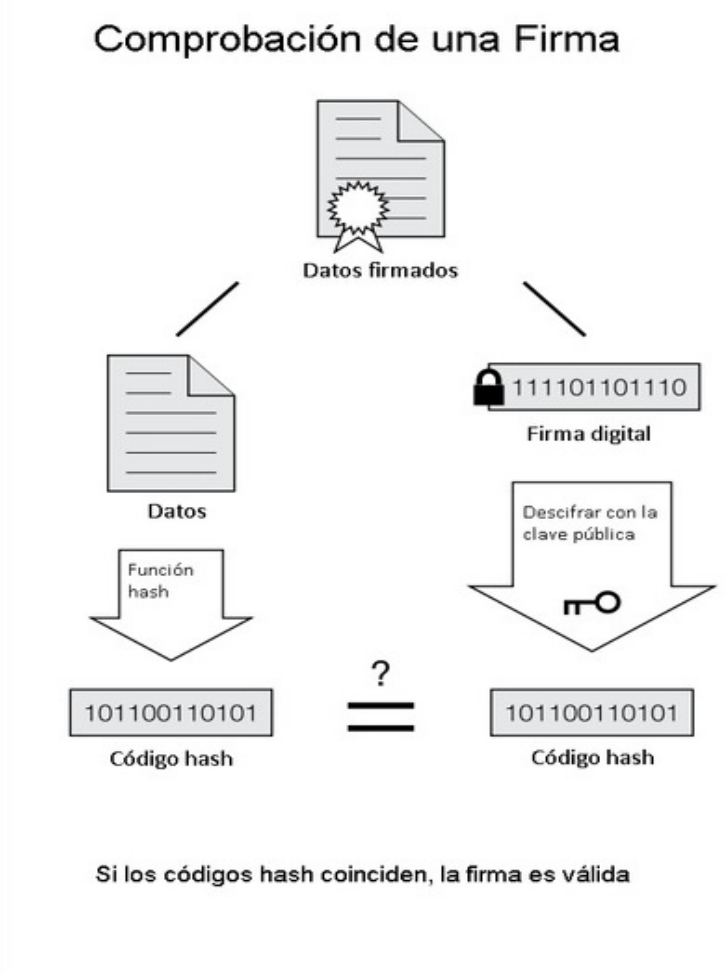


Paso 1: obtenemos código hash

Paso 2: ciframos código hash con nuestra clave privada

Paso 3: incorporamos nuestro certificado (clave pública) y el código hash cifrado al fichero original

Firma digital, ¿cómo se verifica?



Paso 1: extraemos el fichero original

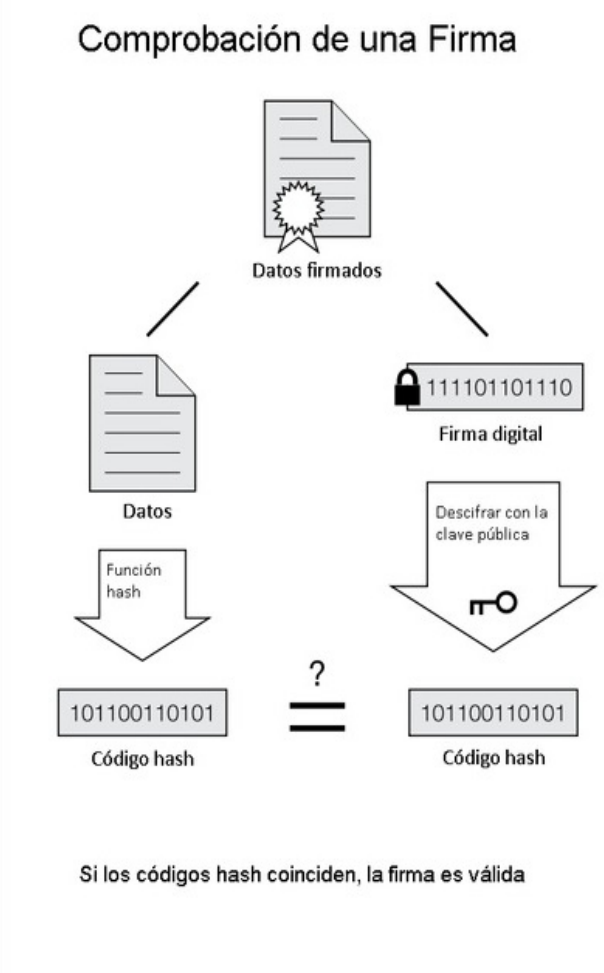
Paso 2: calculamos su hash

Paso 3: extraemos el hash cifrado con la clave privada del emisor

Paso 4: desciframos el hash con la clave pública del emisor

Paso 5: verificamos que los dos hash son iguales

Ley 59/2003 de firma electrónica



Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Documentos electrónicos

Artículo 3 Ley 59/2003. Firma electrónica, y documentos firmados electrónicamente.

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

Documentos electrónicos

Artículo 26 Ley 39/2015. Emisión de documentos por las Administraciones Públicas.

1. Se entiende por documentos públicos administrativos los válidamente emitidos por los órganos de las Administraciones Públicas. Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia.

2. Para ser considerados válidos, los documentos electrónicos administrativos deberán:

a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.

b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

c) Incorporar una referencia temporal del momento en que han sido emitidos.

d) Incorporar los metadatos mínimos exigidos.

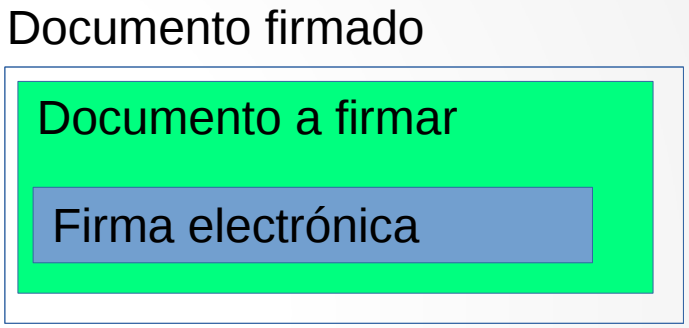
e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.

Se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos.

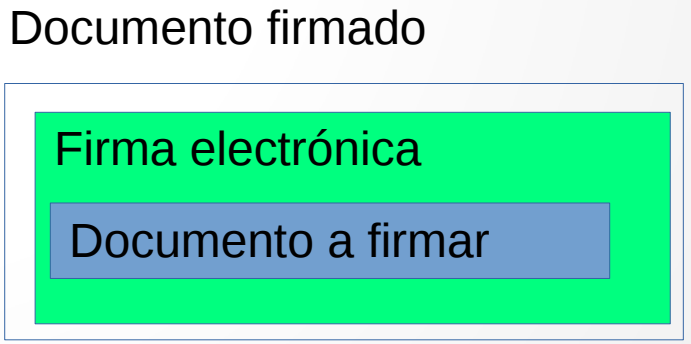
Documentos electrónicos. Tipos de firma.

1.- Firma incluida (attached): Los datos de firma residen en el documento firmado. El documento contiene todo lo necesario para validar e identificar al firmante. Hay dos tipos de firma attached:

1.1.- Incrustada (enveloped): el documento firmado está compuesto por el contenido mas la firma del contenido.

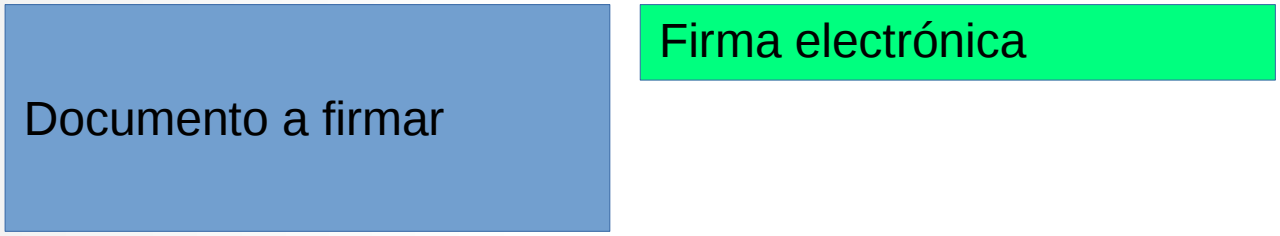


1.2.- Envolvente (enveloping): la firma del documento contiene también los datos firmados.



Documentos electrónicos. Tipos de firma.

2.- Firma excluida (detached): Los datos de firma residen fuera del documento a firmar pero asociados a este. Para validar la firma se crea un documento de evidencia electrónica que contenga de forma conunta el documento y los datos de firma.

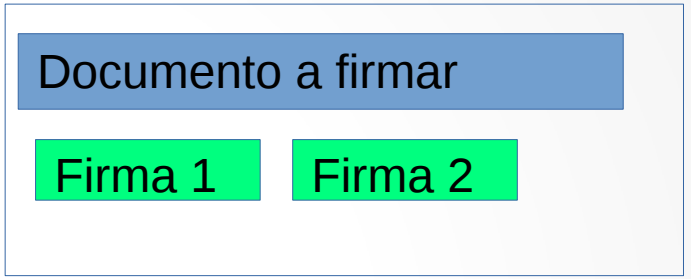


Documentos electrónicos. Multifirma

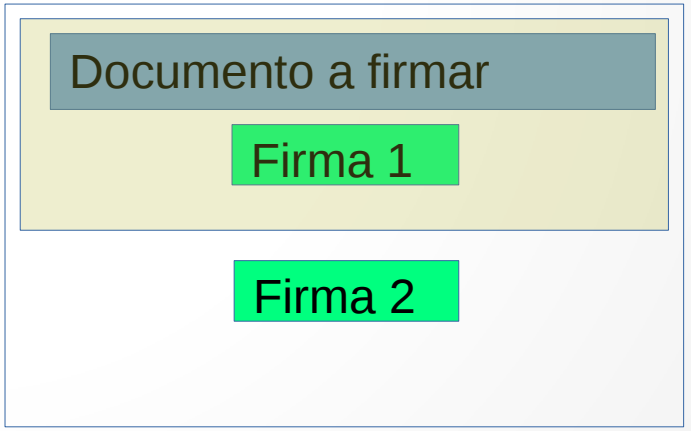
1.- Firma simple: el documento contiene una sola firma.

2.- Firma múltiple: el documento contiene dos o más firmas.

2.1.- En serie (co-firma): todas las firmas tienen el mismo valor.



2.2.- En paralelo (contra-firma): una firma avala a la otra.



Documentos electrónicos. Formatos.

Definen el contenido que ha de tener un documento electrónico y la distribución dentro del fichero: documento original, datos del firmante, fecha de la firma, algoritmos utilizados, caducidad, hash...

Existen muchos: PKCS#7, OOXML, ODF, XMLDsig, PDF Signature, XADES, CADES, PADES, …

Permiten que los ficheros electrónicos puedan ser intercambiables.

Los estándares son mantenidos por:

- W3C: World Wide Web Consortium
- IETF: Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet
- ETSI: European Telecommunications Standard Institute
- ISO: International Standard Organization

En España: el Consejo Superior de la Administración Electrónica es la entidad gestora encargada de publicar y actualizar la relación de las especificaciones de aplicación en las distintas políticas de firma.

Los formatos habituales en la Administración Pública: CADES, XADES, PADES.

Documentos electrónicos. Formato CADES.

Es apropiado para ficheros de gran tamaño porque optimiza el espacio de almacenamiento. Tras firmar la firma no puede verse porque queda almacenada en formato binario.

La firma puede ser attached o dettached.

PRÁCTICA FIRMA CADES

Documentos electrónicos. Formato XADES.

El fichero firmado queda almacenado en un fichero XML.

El fichero resultante es de mayor tamaño que en el formato CADES

La firma puede ser attached o dettached.

PRÁCTICA FIRMA XADES

Documentos electrónicos. Formato PADES.

El fichero a firmar debe ser un PDF.

La firma se incrusta en el documento PDF.

Es muy fácilmente verificable.

PRÁCTICA FIRMA PADES

Documentos electrónicos. Política de firma electrónica

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Artículo 18. Interoperabilidad en la política de firma electrónica y de certificados.

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

Documentos electrónicos. Política de firma electrónica

Alcance de la política de firma electrónica de la AGE v1.9

1.- Obliga a toda la Administración general del Estado.

2.- Detalla la identificación de la política.

3.- Establece criterios comunes de validación y generación de firma electrónica.

4.- Especifica los criterios de archivado y custodia.

Documentos electrónicos. Política de firma electrónica

Política de firma electrónica de la AGE v1.9

Las condiciones que se deberán dar para considerar una firma electrónica longeva son las siguientes:

1. En primer lugar, deberá verificarse la firma electrónica producida o verificad, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CadES o PAdES, y las referencias.

2. Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:
    a. Obtener las referencias a los certificados, así como almacenar los certificadosdel firmante.
    b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.

3. Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.

En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.

Documentos electrónicos. Política de firma electrónica

Política de firma electrónica de la AGE v1.9

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo de validez, se deberá seguir uno de los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas de tipo CAdES, XAdES o PadES:

- las plataformas de firma electrónica adoptadas en el ámbito de la AGE deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.
- la firma electrónica deberá almacenarse en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica (las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado criptográfico).

Es necesario que con posterioridad las firmas puedan renovarse (refirmado o countersignature) y permitan actualizar los elementos de confianza (sellos de tiempo), garantizando la fiabilidad de la firma electrónica.

Documentos electrónicos. Política de firma electrónica

Política de firma electrónica de la AGE v1.9

Actualmente se consideran formatos admitidos:

- **formato XAdES** (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. Asimismo, se admitirá la última versión 1.4.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma1.

- **formato CAdES** (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7. Asimismo, se admitirá la última versión 1.8.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- **formato PAdES** (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

Documentos electrónicos. Formatos, clases

La clase básica es ADES-BES.

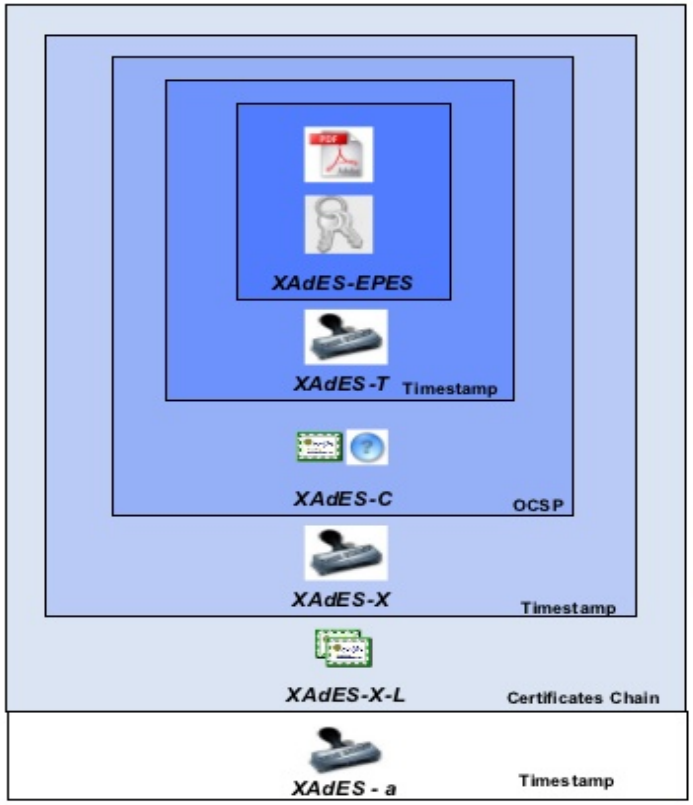
1.- ADES-EPES: añade la información sobre la política de firma.

2.- ADES-T: añade al anterior el sello de tiempo.

3.- Formatos longevos: previenen la caducidad de los certificados empleados en los documentos y la obsolescencia de los algoritmos de firma. Se utilizan para el archivado de larga duración: ADES-A y en el caso de PDF: PADES-LTV.

Documentos electrónicos. Formatos, clases

Xades, electronic signature composition



The *XAdES-T* envelope:
contains a trusted timestamp over the signature. The goal is to prove that the signer's certificate was valid at the time of signature.

The ***XAdES-X*** envelope:
"When an OCSP response is used, it is necessary to time-stamp in particular that response in the case the key from the responder would be compromised"

In other words, the goal is to prove that the OCSP responder's signing certificate was valid at the time of OCSP response.

"The SignatureTimeStamp encapsulates the time-stamp over the SignatureValue element."

XADES : XML Advanced Electronic Signatures
Specification from the ETSI that is built upon the Xmldsig specification.
It provides "signatures that remain valid over long periods.

TAA - Trusted Archive Authority , Fedisa | Juni 2011 | page 40 • Fedisa

Documentos electrónicos. Formatos, clases

Práctica formatos -EPES

Documentos electrónicos. Programas.

@firma: plataforma de la AGE utilizada para proporcionar servicios de verificación y firma con una gran cantidad de proveedores de servicios de certificación.
Es gratuito para las administraciones públicas.

Modos de funcionamiento:

- Programas de escritorio: cliente standalone @firma, autofirma.

- Applets Java: portafirmas DPH.

- Comunicación programa a programa: autofirma y clientes móviles.

- Servicios web.

Sistemas de firma para actuación automatizada

LEY 40/2015 de Régimen Jurídico del Sector Público.

Artículo 42. Sistemas de firma para la actuación administrativa automatizada.

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Sistemas de firma para actuación administrativa automatizada. Sellos.

Definición de certificado de sello electrónico

https://www.sede.fnmt.gob.es/certificados/administracion-publica/informacion-general/certificado-de-sello-electronico

Sistemas de firma para actuación administrativa automatizada. CSV.

Código seguro de verificación: una colección de caracteres creados según un algoritmo definido por cada entidad pública que:

- **Garantiza la no duplicidad de cada código.**

- **Asocia cada código a un único documento electrónico.**

En la DPH, se utiliza actualmente en los anuncios del Boletín Oficial de la Provincia y en todos los documentos firmados con el portafirmas.

Muchas gracias por su atención