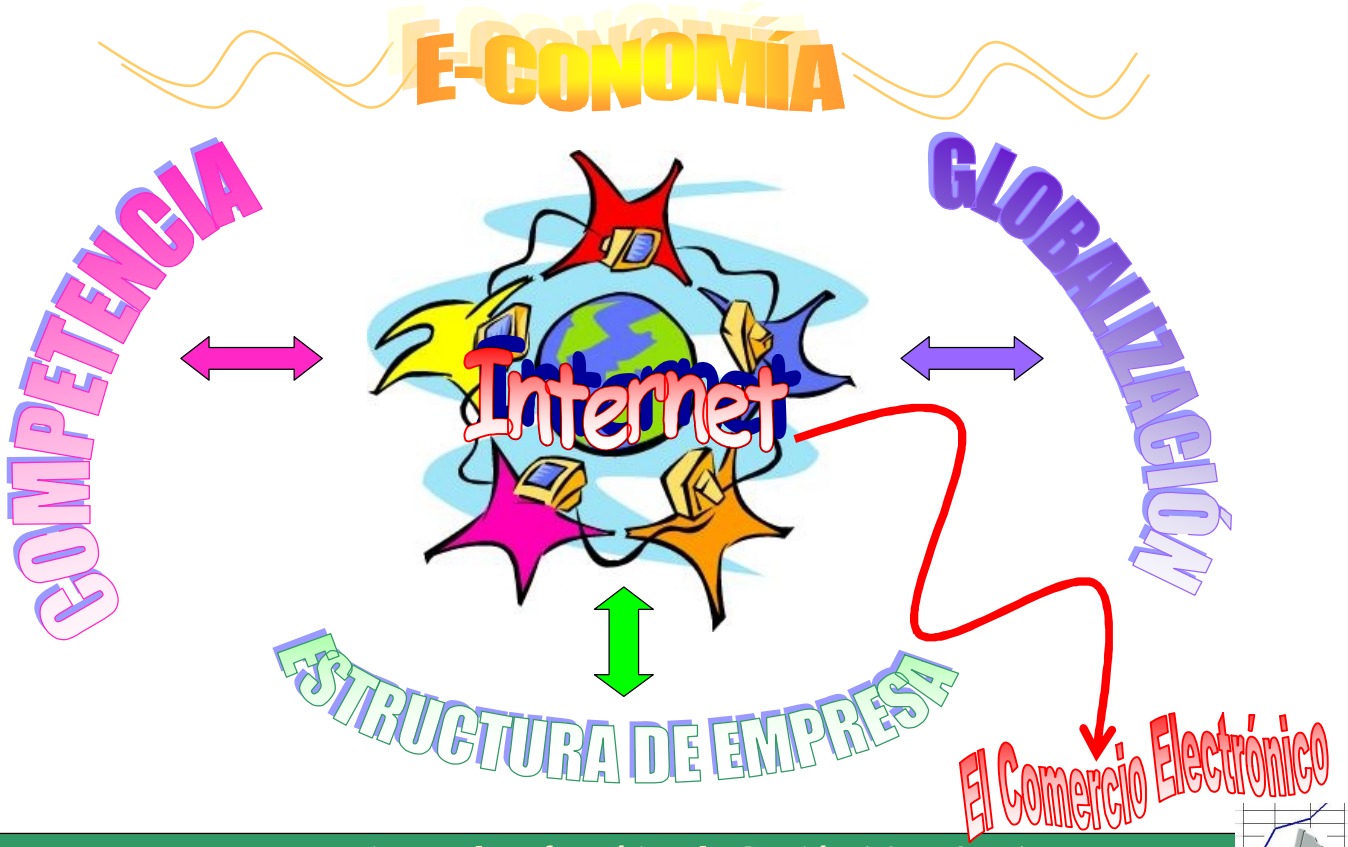
Tema 5

Internet en la empresa:
e-business y e-commerce

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT



Herramientas de Informática de Gestión (2ºB LADE)

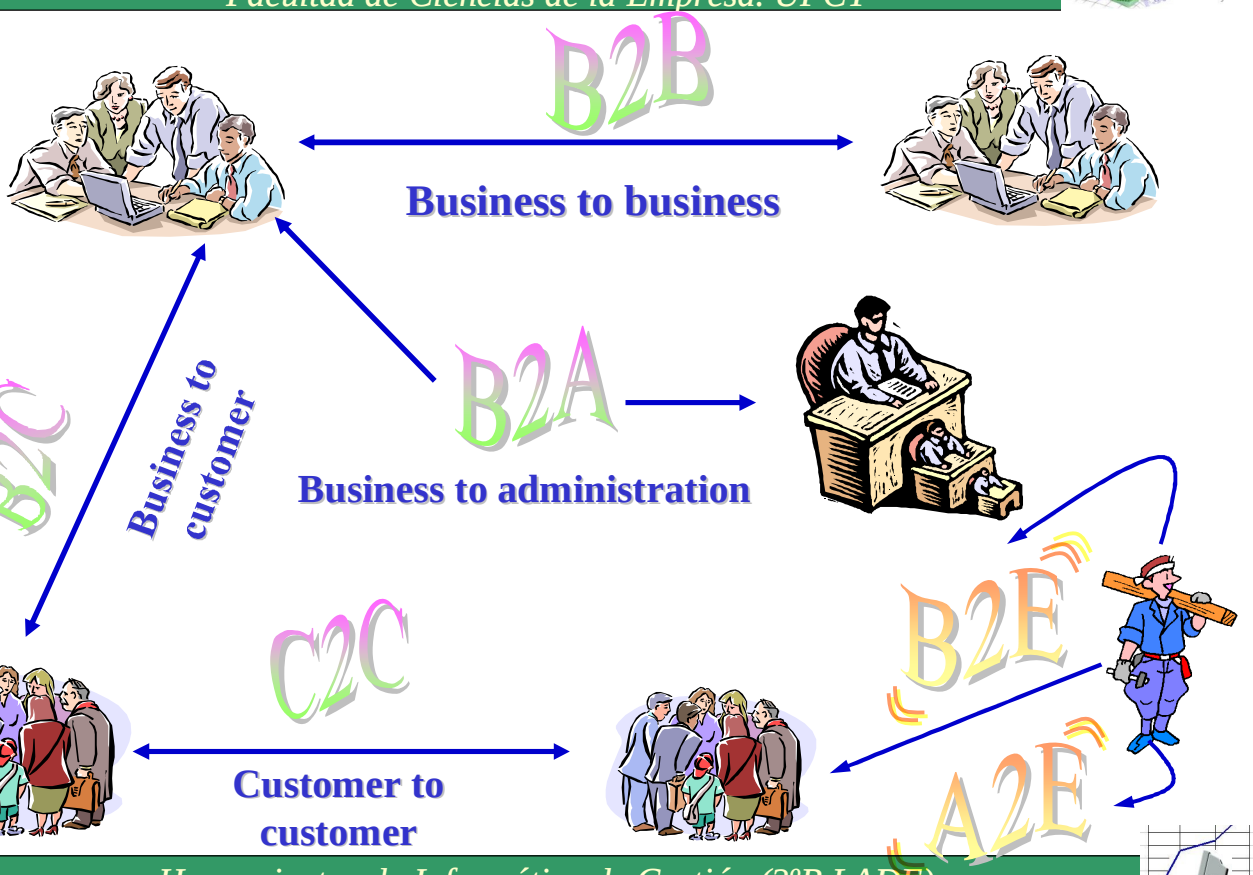
El Comercio Electrónico

Cualquier forma de transacción o intercambio de información comercial basado en la transmisión electrónica de datos, antes, durante o posteriores a dicha transacción

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

EDI (Intercambio electrónico de datos): es el intercambio de información de negocios mediante redes de ordenadores: propuestas de precios, contratos, facturas, documentos de envío, pagos y otra información que sólo se comunica en papel o vía telefónica.

- Antiguamente contratar software y terceras empresas
- **Actualmente** a través de la web. El XML permite ahorros y lenguaje estándar
- **Desventaja**: no hay control sobre la velocidad de la comunicación. Mucho tráfico implica que alguna transacción no se pueda ejecutar correctamente. Además problemas en la seguridad (encriptación)



Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Oportunidades

Oferentes

- Globalización de su presencia y su actividad comercial de forma simultánea y sin realizar grandes cambios en la estructura de la empresa.
- Se acortan las cadenas de distribución ya que desaparece la utilidad de algunos intermediarios aunque aparecen otros diferentes, así como servicios adicionales.
- Ahorro de costes.
- Adaptación a la demanda, mejor segmentación y ofertas personalizadas.
- Mejora en la competencia, fortaleza frente a los competidores.
- Se abren nuevas oportunidades de negocio.

Demandantes

- La elección se convierte en global (más proveedores, mejor proceso de búsqueda).
- La respuesta a necesidades concretas es más rápida (acortamiento en las cadenas de distribución y a la automatización del comercio que permite obtener los suministros "just in time").
- El ahorro en los costes, así como el incremento en la competencia implica la reducción en los precios de los productos.
- La personalización de los servicios y productos.
- El incremento en la competencia deriva en una mejor oferta, mayor calidad en el servicio y mejora en los servicios complementarios.
- Acceso a nuevos productos y/o servicios

Economía y e-business

Ä *Capa Logística* o de intercambio físico de los productos, basada en la integración de las cadenas logísticas de aprovisionamiento y distribución.

Ä *Capa Transaccional* o de intercambio de información mediante mensajes y documentos electrónicos.

Ä *Capa Financiera* o de medios de pago, asociada a los intercambios de información, bienes y servicios.

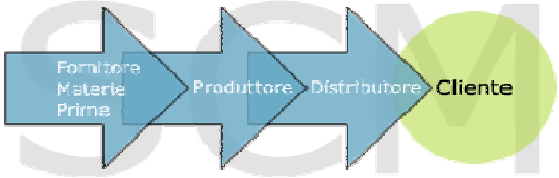
Ä Estas tres capas son soportadas por una infraestructura (capa que falta para completar los cuatro indicadores en la economía de Internet).

Barreras

- ü *culturales* y *lingüísticas*
- ü *psicológicas* y *sociales*
- ü *económicas y financieras*
- ü *políticas* y *legales*

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Soluciones e-business
El e-business engloba a toda una serie de modelos de negocio basados en tecnología internet encaminados a mejorar las relaciones comerciales entre empresas, cadenas de aprovisionamiento, mercados verticales y un largo etcétera de posibilidades. En última instancia un sistema de e-business puede tomar múltiples formas y es la empresa quien debe decidir la mejor o más adecuada según sus necesidades.



E-procurement. Abastecimiento electrónico de productos y servicios vía internet. Bajo estas plataformas se gestionan los procesos de compra a proveedores bien sean compras de productos directos (implicados en el proceso de producción del producto final): materias primas, o indirectas (no implicadas en el producto final): papelería, informática, servicios varios. La principal ventaja del uso de estas plataformas radica en el ahorro de tiempo en la gestión de compras, la comodidad y la reducción de los precios de adquisición de productos y la posibilidad de acceder a nuevos proveedores.

Breogan.com es principalmente una plataforma de e-procurement que aúna bajo un mismo interface web las funcionalidades más inmediatas que una empresa puede necesitar en internet.

Herramientas de Informática de Gestión (2ºB LADE)

Modelos de Negocio

Venta

Margen comercial

- Ø Cybertrades o exclusiva online
- Ø Venta tradicional y en red o Clicks&Bricks
- Ø Venta por catálogo

Intermediación

Comisión

- Ø Programas de Afiliación. Control de ventas de la web inicial hacia otras de destino; comisión sobre compra final.
- Ø Venta de Bits. Productos puramente digitales.
- Ø Venta desde Fábrica.

Publicidad

Tráfico/Audiencia

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

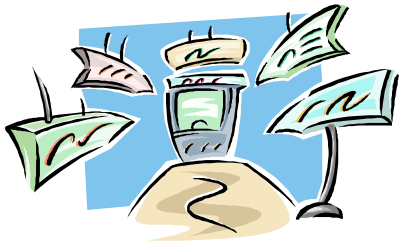
Intermediación

- Ø Infomediarios o Metamediarios. Gestión imparcial de información. Reducción de costes. Direccionamiento.
- Ø Lonjas Digitales. Especializados en el mercado empresarial. Máx. información sobre ofertas.

- Ø Distribuidor especializado. Recoge catálogos de fabricantes de un sector y acumula pedidos para posterior entrega.
- Ø Ciber-Malls o Galerías comerciales online. Caso especial son los Virtual Resellers es decir malls que proporcionan infraestructura y tienen también inventarios (venta directa al consumidor).
- Ø Grupos de Compra. Se unen compradores que desean un producto determinado. Mejoran condiciones de negociación y de compra.
- Ø Subastas. Beneficio consiste en cobrar comisión sobre el precio final de venta.
- Ø Mercados invertidos. El cliente fija el precio máximo final y la oferta es la que se moviliza (para stocks excedentarios) .
- Ø Anuncios Clasificados.

Herramientas de Informática de Gestión (2ºB LADE)

Publicidad



- Ø Portal Horizontal o Genérico. Cubre las áreas de contenido, comunicación, comunidad y comercio. Variante: Portal Multimedia.
- Ø Portal Vertical o Temático. Variante: Portal de Negocio y Portal Intranet.
- Ø Comunidad Virtual.
- Ø Programas de Incentivos.
- Ø Servicios Gratuitos.

Otros modelos

- Ø Gestión de la Información.
- Ø Modelos de Suscripción.
- Ø Sindicación de contenidos. Venta o cesión a otras páginas. Ingresos por cuota fija o variable y/o publicidad.
- Ø Franquicias.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Los problemas de **seguridad** en el comercio electrónico tienen tres aspectos:

- ðTecnológicos: protección física.
  - øDestrucción: Antivirus y copias de seguridad
  - øIntrusos: Firewalls, cifrado de ficheros, identificadores biométricos...
- ð Legales: protección jurídica
- ð Psicológicos: Confianza

Herramientas de Informática de Gestión (2ºB LADE)

Protocolos de Seguridad en las Trasmisiones de Pago

Transparentes para el usuario:

SSL: Secure Socket Layer

***Privaticidad sobre Internet (Nestcape*)**
Autentifica as Servidor al que se conecta.
(Clave hasta 128 Bits)
Canal seguro. Clave asimétrica.

SHTTP: *Secure HiperText Transfer Protocol*

- **Encriptación simétrica**
- **Objetivo: confidencialidad, integridad y autenticidad del comercio, no del comprador**
- **Sin claves ni certificados. En el navegador.**

No transparentes:

SET: Secure Electronic Transaction

- **Encriptación asimétrica y firma. (clave pública y privada)**
- **Software específico: Wallet o cartera electrónica.**
- **Certificación electrónica.**
- **Objetivo: confidencialidad, autentificación, integridad, interoperabilidad.**

PGP: *Pretty Good Privacy*

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Cookies : es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. En ocasiones también se le llama "huella". Al ser el protocolo HTTP incapaz de mantener información por sí mismo, para que se pueda conservar información entre una página vista y otra (como ***login*** de usuario, preferencias de colores, etc), ésta debe ser almacenada, ya sea en la URL de la página, en el propio servidor, o en una ***cookie*** en el ordenador del visitante.

Usos más frecuentes:

1. Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una ***cookie*** para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo una cookie no identifica a una persona, sino a una combinación de computador y navegador.

2. Conseguir información sobre los hábitos de navegación del usuario, e intentos de spyware, por parte de agencias de publicidad y otros. Esto puede causar problemas de privacidad y es una de las razones por la que las ***cookies*** tienen sus detractores.

Las cookies pueden ser borradas, aceptadas o bloqueadas según desee, para esto sólo debe configurar convenientemente el navegador web.

Herramientas de Informática de Gestión (2ºB LADE)

SPAM ð Se llama también ***correo basura o sms basura*** a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso de forma masiva) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. Aunque se puede hacer por distintas vías, la más utilizada es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de correo basura incluyen grupos de ***noticias, usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups y todo tipo de imágenes y textos en la web***. El correo basura también puede tener como objetivo los ***teléfonos móviles*** a través de mensajes de texto y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, etc.
También se llama spam a los virus sueltos en la red y páginas filtradas (***casino, sorteos, premios, viajes y pornografía***); se activa mediante el ingreso a páginas de comunidades o grupos o al acceder a links en diversas páginas.

Las listas de correo basura con las direcciones de correo electrónico de los clientes potenciales (o víctimas seguras) se crean frecuentemente cribando los mensajes de Usenet, robando direcciones en las listas de distribución o comprándolas en las bases de datos de los servicios en línea de Internet o bien buscando direcciones por la red. Irónicamente, los propios spammers usan el spam para anunciarse.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

La forma más fácil de transmitir un timo por la red es a través del spam y entonces se le denomina *SCAM*. Fraudes más frecuentes: en subastas, abuso de tarjetas de crédito, marketing de nivel o timos piramidales, "trabaje desde casa" y "hágase rico inmediatamente", fraudes en viajes, teléfonos, sanitarios, etc…

SPIM son mensajes instantáneos no solicitados (20% de usuarios lo sufren frente a un 60% del Spam).

PHISHING o timo de los bancos: Variedad de ataque de ingeniería social consistente en envío de páginas que falsifican otras reales (*fake*), normalmente de bancos o lugares dónde se solicita introducir tarjetas de crédito y que piden introducir paswords y login que se reenvían a un hacker.

HOAX o bulos, falsos anuncios de virus que se expanden en progresión geométrica al ser reenviados. Caso del virus sulfnbk.exe que finalmente era un archivo del sistema Windows.

Ingeniería social o práctica para obtener información confidencial a través de la manipulación del usuario, ya que éste es el eslabón más débil del sistema. Por ejemplo, el envío de solicitudes para renovar permisos de acceso a páginas web o las famosas "cadenas". Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

LA CRIPTOLOGÍA

que ofrecen medios seguros de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo. Sus áreas principales de estudio son la criptografía y el criptoanálisis, pero también se incluye la esteganografía

Criptografía: es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que a su vez engloba tanto las técnicas de cifrado, es decir la criptografía propiamente dicha, como sus técnicas complementarias, entre las cuales se incluye el criptoanálisis, que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código.
Encriptar o Cifrar consiste en substituir los elementos (letras o palabras) de un texto legible por un conjunto de caracteres (letras, números o símbolos) que resultarán incomprensibles para cualquier persona que no sepa (no tenga la clave necesaria) reconvertirlos en el texto original. Los algoritmos no deben ser secretos, así la seguridad del criptograma depende fundamentalmente de las claves empleadas.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

La información original que debe protegerse se denomina *texto en claro*. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*) se basa en la existencia de una *clave*: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto.

Las dos técnicas más sencillas de cifrado son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la trasposición (que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

Ejemplos de Criptografía Clásica Sencilla

Sustitución: si usamos la "clave **murcielago**" para escribir mensajes secretos, donde a las letras de la palabra "murcielago" se les asignaban los números 0,1,2,3,4,5,6,7,8 y 9 respectivamente. Así la palabra "**hola**" se transforma en "**h967**", etc.

Trasposición: consiste en dezplazar las letras en "n" lugares, por ejemplo con un desplazamiento de 1 la palabra "**hola**" se convierte en "**ipmb**" (cada letra se desplaza un lugar hacia la siguiente).

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, en conjunto es lo que constituyen un criptosistema, que es con lo que el usuario final trabaja e interactúa.

Pero, ¿que es lo que se protege?:

- **Autenticación**, que asegura que el usuario y la información son los auténticos.
- **Confidencialidad**, que oculta los datos a observaciones no deseadas.
- **Integridad**, para garantizar que la información no ha sido alterada.
- **No repudio**, para evitar que se rechace el acceso a un usuario autorizado.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Existen dos grandes grupos de cifras: los algoritmos que utilizan una única clave tanto en el proceso de cifrado como en el de descifrado, y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas, de clave simétrica o de clave privada y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y forman el núcleo de las técnicas de cifrado modernas

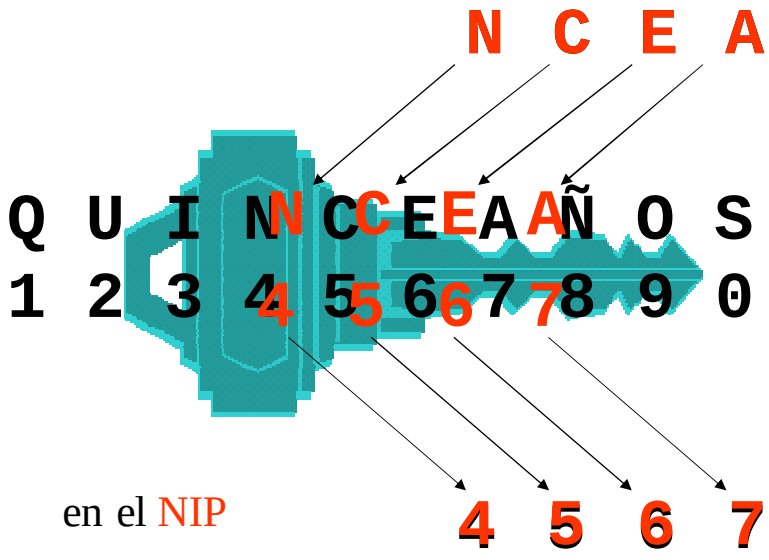
En la **criptografía simétrica** las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Éste método pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, *no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando*. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo.

La criptografía de clave secreta es la más antigua, utiliza una misma clave para encriptar y desencriptar, garantiza la **confidencialidad** pero no la autenticación. Los algoritmos más conocidos:

DES (*Data Encryption Standard*). El más utilizado desde hace 20 años. Usa una clave de 56 bits. Existe el **Triple DES** con claves de 128 bits.
IDEA (*Internacional Data Encryption Algorithm)*de 1990.
RC5, empleado por *Nestcape*.

Ejemplo de clave secreta o Clave simétrica

Es muy sencillo convertir las letras de la VISA

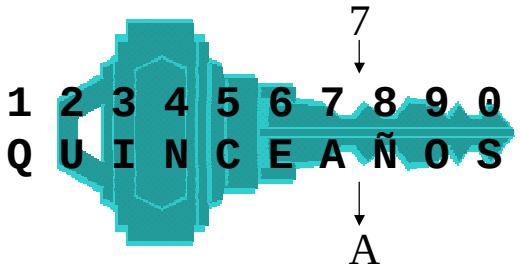


en el NIP

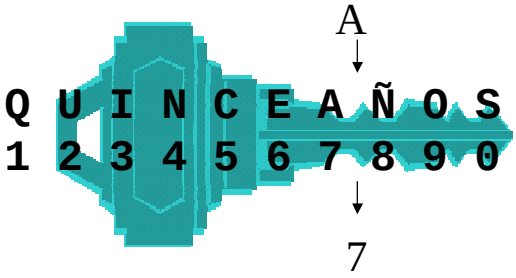
4 5 6 7

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

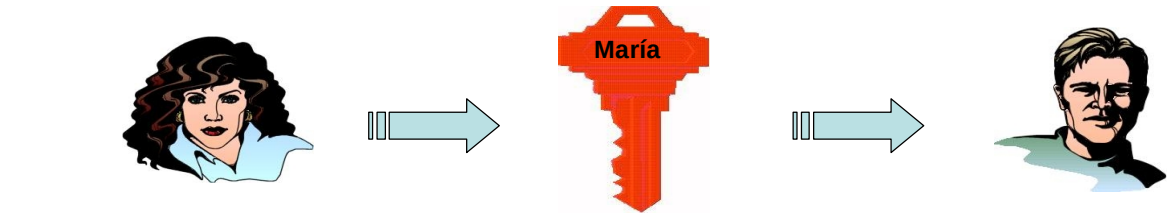
"Quinceaños" es una clave **simétrica** porque
la usamos para pasar del texto original al texto encriptado



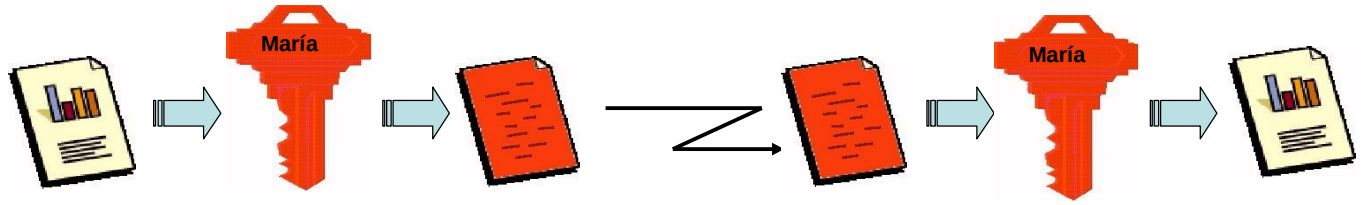
Y también para pasar del texto encriptado al texto original.



Clave única o Simétrica: Clave Privada



Emisor: *María* **Clave Privada** **Receptor: *Juan***



Existe un problema en la Confidencialidad: Los dos deben conocer la clave privada y sólo ellos.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

La **criptografía asimétrica** es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una **clave es *pública*** y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autenticación* del remitente, ya que se sabe que sólo pudo haber sido él quien utilizó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la **firma electrónica.**

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear.

En una operación criptográfica que use infraestructura PKI o lo que es lo mismo de clave pública, intervienen como mínimo las siguientes partes:

1. Un usuario iniciador de la operación
2. Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación:
   - ü **Autoridad de certificación** que es una entidad de confianza, responsable de emitir y revocar los *certificados digitales* o *certificados*, utilizados en la *firma electrónica*. Jurídicamente es un caso particular de *Prestador de Servicios de Certificación*.
   - ü **Autoridad de registro** que es una entidad de confianza que:
     a) Registra las peticiones que hagan los usuarios para obtener un certificado
     b) Comprueba la veracidad y corrección de los datos que aportan los usuarios en las peticiones
     c) Envía las peticiones a una CA (autoridad de certificación) para que sean procesadas
   - ü **Sistema de Sellado de tiempo** o *Timestamping* que es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.
3. Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Algunos algoritmos de técnicas de clave asimétrica son:

Diffie-Hellman: se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.

RSA: el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando ordenador tradicional.

DSA o Algoritmo de Firma digital: Fue propuesto por el Instituto Nacional de Normas y Tecnología del gobierno de Estados Unidos para su uso en su Estándar de Firma Digital (DSS) Se hizo público en agosto de 1991 y sirve para firmar y no para cifrar información. Una desventaja es que requiere mucho más tiempo de cómputo que RSA.

ElGamal: puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar. Se basa en problemas matemáticos de algoritmos discretos y se usa en software de *GNU Privacy Guard*, versiones recientes de *PGP*, y otros sistemas criptográficos. No esta bajo ninguna patente, por lo que su uso es libre.

Criptografía de curva elíptica: puede ser más rápida y usar claves más cortas que los métodos antiguos

Doble Clave.Claves asimétricas:
Clave pública (PKI) y Clave privada

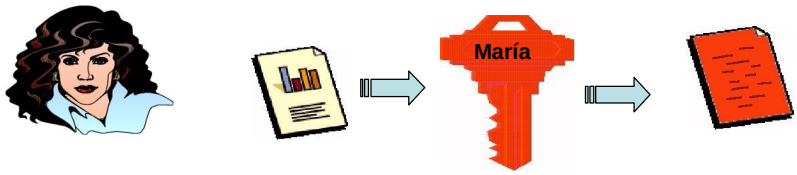
María

Lo que esté encriptado con la clave privada de *María*

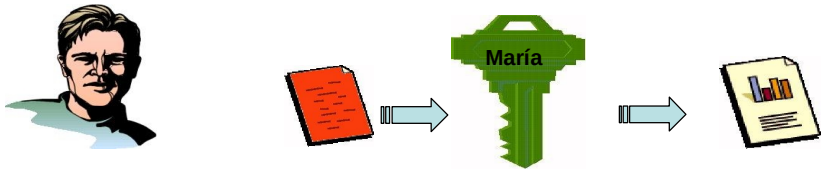
necesita la clave pública de *María* para desencriptarse

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Si *María* envía a *Juan* un mensaje encriptado con su clave privada (sólo la conoce ella)



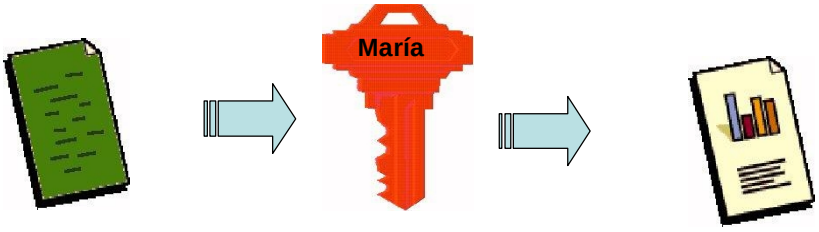
***Juan* necesitará la clave pública de *María* para desencriptarlo**
(en bases de datos públicas)



Y así *Juan* estará seguro de que ha sido *María*
y no otra persona la que envió el mensaje (Autenticación)

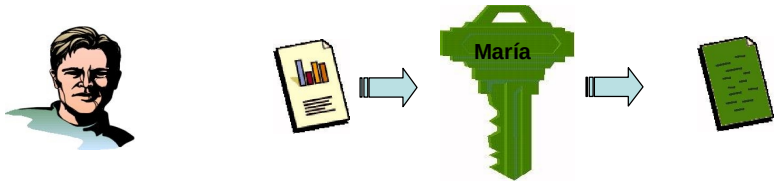
Y, al revés, lo que esté encriptado con la clave pública de *María*

necesita la clave privada de *María* para desencriptarse

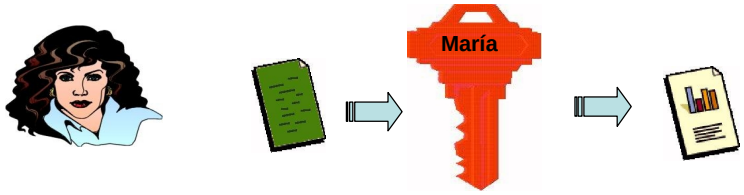


Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Si *Juan* quiere enviar un mensaje a *María*
lo encriptará con la clave pública de *María*



***María* necesitará usar su clave privada**
para desencriptar el mensaje de *Juan*



Sólo *María* puede entender los mensajes
encriptados con su clave pública

María **encripta el mensaje con su clave privada**

Las ventajas de las claves asimétricas se perciben plenamente cuando se combinan las claves de dos personas.

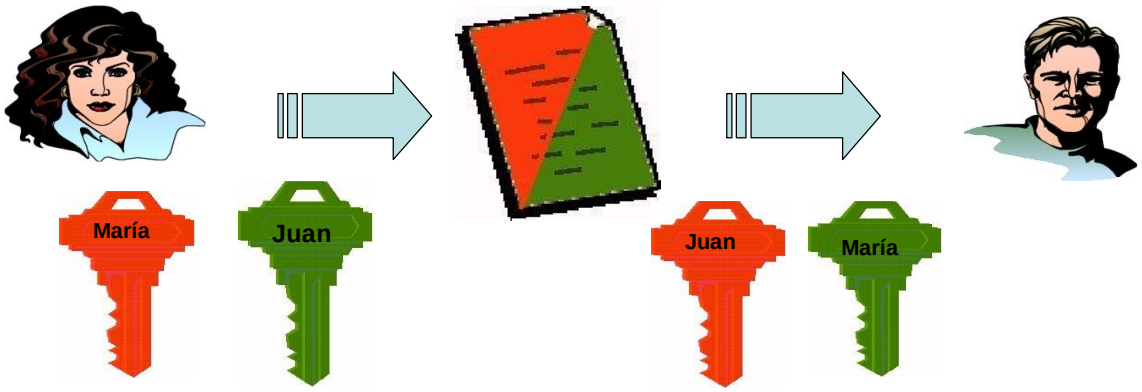
y con la clave pública de *Juan*

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Juan **desencripta el mensaje con su clave privada**

y con la clave pública de *María*

Herramientas de Informática de Gestión (2ºB LADE)



María **está segura de que sólo *Juan* ha podido leer el mensaje**

Autenticación

Juan **está seguro de que ha sido *María* la que lo ha enviado**

No repudio

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

LEYES

Ø Ley 15/99 de Protección de Datos Personales

ØLey 34/2002 (de 11 de julio) de Servicios de la Sociedad de la Información y Comercio Electrónico. (LSSICE). Directiva Europea 2000/31/CE. ***Requisitos:***

1. Prestado a distancia
2. Prestado por vía electrónica
3. Prestación a petición individual del destinatario
4. Que represente una actividad económica para el prestador

Ø La firma electrónica cuenta con legislación en España desde 1999 y también es reconocida por la directiva europea Eurofocus: *Directiva 41/99 13-20 de diciembre*. Actualmente se enmarca en la ***ley 59/2003 de 19 de diciembre de 2003***

Nace para dinamizar el mercado de prestación de servicios de certificación. Con respecto de la anterior, revisa la terminología, modifica la sistemática y simplifica el texto. Por ej: Se elimina el registro de prestadores de servicios de certificación dando un mayor protagonismo al sector privado en los sistemas de certificación, existe la posibilidad de certificación por parte de prestadores de servicios de certificación y los notarios podrán otorgar certificados digitales de firma electrónica.

Firma Digital y Firma Electrónica

La **firma digital** en la transmisión de mensajes y en la gestión de documentos electrónicos, es un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje. **Garantiza autenticación, integridad y no repudio.**

La **firma electrónica**, como la firma manuscrita, puede vincularse a un documento para identificar al autor, para señalar conformidad o no con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido. **Garantiza Autentificación.**

A veces estos términos se usan como sinónimo pero es incorrecto. **Firma digital** hace referencia a una serie de métodos criptográficos y **firma electrónica** es un término de naturaleza fundamentalmente legal y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Un ejemplo claro de la importancia de esta distinción es el uso por la Comisión europea. En el desarrollo de la Directiva europea 1999/93/CE que estable un marco europeo común para la firma electrónica empezó utilizando el término de firma digital en el primer borrador, pero finalmente acabó utilizando el término de firma electrónica para desacoplar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

En España, ***la Ley 59/2003 define tres tipos de firma:***

- **Simple**. Incluye un método de identificar al firmante (autenticidad)
- **Avanzada**. Además de identificar al firmante permite garantizar la integridad del documento, es decir cualquier cambio posterior en el mismo. Se emplean técnicas de PKI o criptografía de clave pública.

  Autenticación + No Repudio + Integridad
- **Reconocida**. Es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina Cualificada por traducción del término Qualified de la Directiva Europea de Firma Electrónica. Se equipara a la firma manuscrita.

Un ***certificado electrónico*** es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma y confirma su identidad.

Son ***certificados reconocidos*** los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley.

Un ***documento de identidad electrónico*** acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Herramientas de Informática de Gestión (2ºB LADE)

HASH

Función o método para generar claves o llaves que representen de manera casi unívoca a un documento. Una **función de hash** es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Un **hash** es el resultado de dicha función o algoritmo.

Una propiedad fundamental del *hashing* es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.

Se usan en múltiples aplicaciones, como en criptografía, procesamiento de datos y firmas digitales, entre otros. Por tanto, muchos sistemas relacionados con la seguridad informática usan funciones o tablas hash.

No encriptan pero sirven para garantizar la integridad de los textos. Convierten un texto en un bloque de longitud fija llamado compendio.

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Ejemplo: El código ASCII asigna un número a cada letra o signo de puntuación, sí cada tres caracteres, con sus códigos ASCII, se opera : (1º-2º)*3º. La suma de los resultados es una función HASH que identifica perfectamente el texto.

E	n		u	n		r	i	n	c	ó	n		d	e	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	
		-1312			224			990			-15840			-6868	-22806

	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
		-7372			-4365			1144			6500			6831	2738

u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
		-444			-8658			1254			7590			8927	8669
															-11399

Cualquier modificación en el texto provoca un cambio en el valor de la función HASH

E	n		u	n		r	i	n	c	o	n		d	e	
69	110	32	117	110	32	114	105	110	99	111	110	32	100	101	
	-1312			224			990			-1320			-6868		-8286

	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
	-7372			-4365			1144			6500			6831		2738

u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
	-444			-8658			1254			7590			8927		~~8669~~
															3121

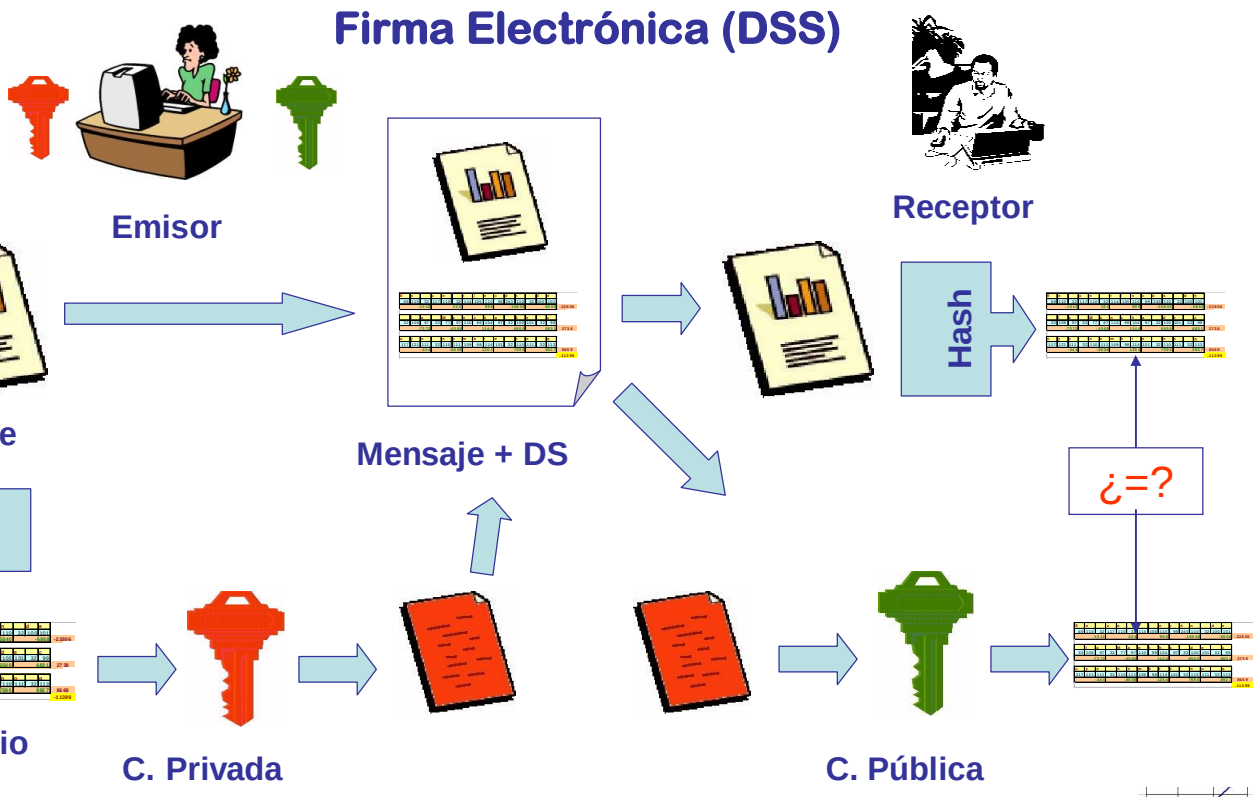
Por ejemplo, al substituir "**rincón**" por "**rincon**" sin acento, el valor HASH ha pasado de **-11.399** a **3.121**

Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Ejemplo de uso de la función HASH

María envía un mensaje a *Juan*.
Al final del mensaje le añade el valor HASH del texto según una función en la que se han puesto previamente de acuerdo.

Juan recibe el mensaje y calcula el valor HASH.
Si coincide con el que ha dicho *María* puede estar seguro de que el mensaje no ha sido modificado.



Dpto. de Métodos Cuantitativos e Informáticos
Facultad de Ciencias de la Empresa. UPCT

Aspectos Psicológicos: Confianza

Certificaciones independientes por terceras partes de confianza. Prestación de servicios de certificación.

- **Sello electrónico o *time stamping***, que acredita además fecha y hora.
- **Proveedor de servicios de certificación**: *Entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la Firma Electrónica.* En España los que son Públicos son el FNMT y Servicio de Correos y Telégrafos.
- **Registro de prestadores de Servicios de Certificación**: Obligaciones, responsabilidades, controles, reclamaciones, revocaciones, etc.

Elementos de un certificado:
Subjetivos: Prestador, titular y usuario.
Objetivos: Declaraciones de prácticas de certificación.

Qué es un Certificado de Usuario

Agencia Tributaria
OFICINA VIRTUAL

Es un **conjunto de datos** de:

- **Identificación** del titular del Certificado.
- Distintivos del Certificado:
  Número de Serie, Entidad que lo emitió, fecha de emisión, fecha de caducidad, etc.
- Una **pareja de claves**: pública y privada.
- La **firma electrónica** de la autoridad de certificación que lo emitió.

Estos datos se agrupan en:

- **Parte privada:**
  Clave privada.
- **Parte pública:**
  Resto de datos del certificado, incluida la firma electrónica de la autoridad de certificación que lo emitió.

La parte privada nunca es cedida por su propietario. Esta es la base de la seguridad.

- Características:
  - Con la pareja de claves se pueden realizar funciones de cifrado con la peculiaridad de que **lo que se cifra con la privada sólo se puede verificar con la pública y viceversa**.
  - Los certificados de usuario que se utilizan en los servicios que da la AEAT se ajustan a la versión 3 de la recomendación X.509 del ITU-T (International Telecommunications Union - Telecommunication).