Criptografía y sus aplicaciones

Indice de temas

- Conceptos básicos de criptografía
- Firma digital
- PKI
- PGP
- Esteganografía

Criptografía y sus aplicaciones

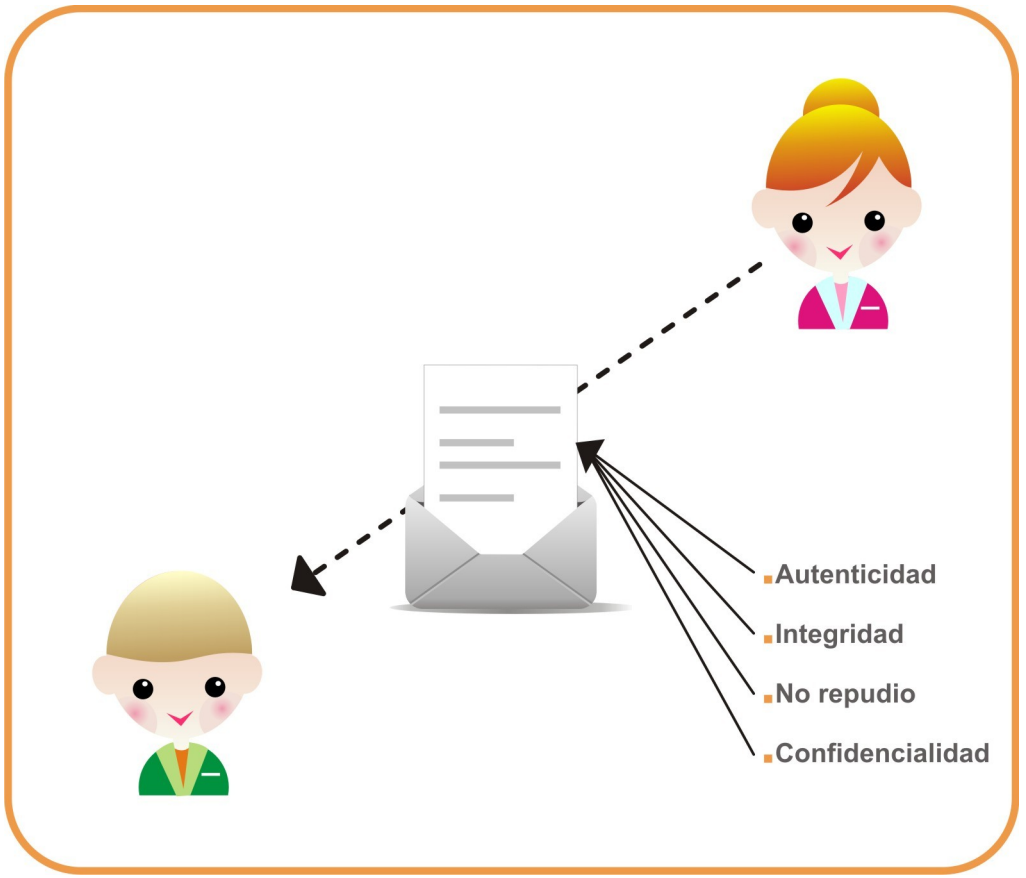
Queremos garantizar

- Autenticidad del emisor
- Integridad del mensaje
- Actualidad del mensaje
- No repudio del emisor
- No repudio del receptor

Criptografía y sus aplicaciones

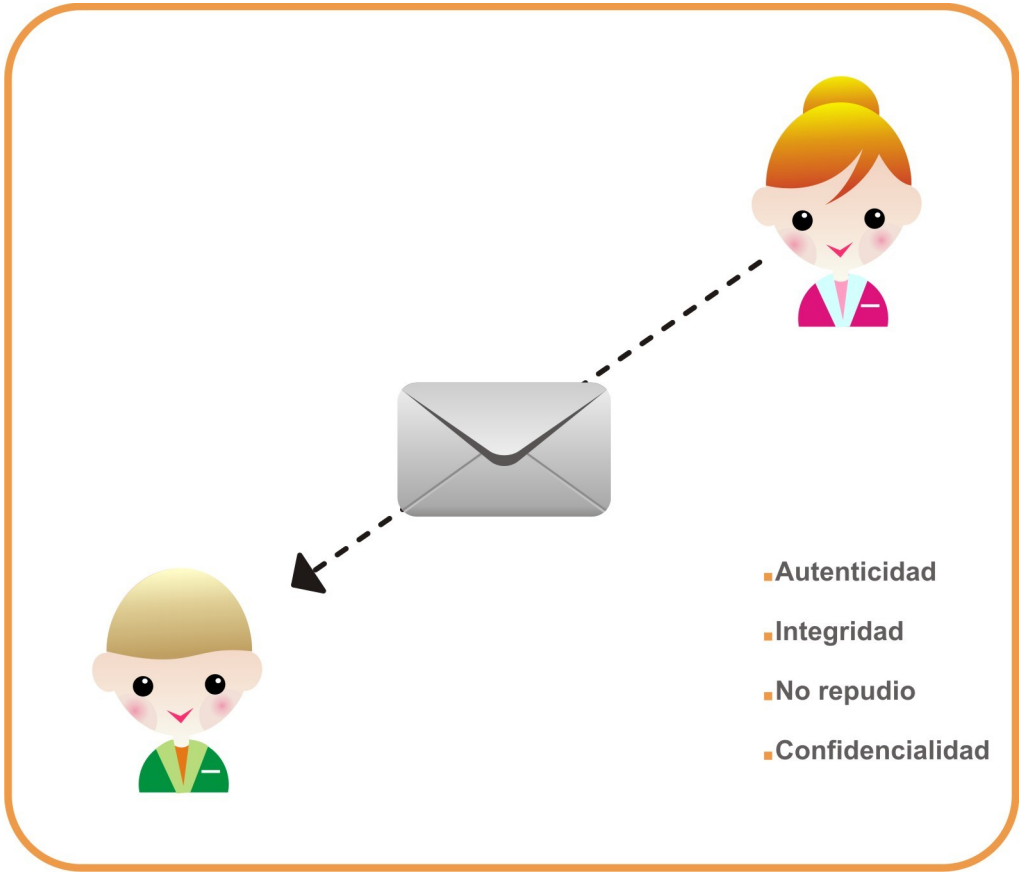
Seguridad en el mundo basado en papel

El término “Seguridad” a menudo se confunde con “Privacidad”.Para entender los requerimientos existentes en el mundo digital y las soluciones que para ello existen, es importante comprender previamente cómo se garantizan los atributos de seguridad en las transacciones basadas en papel.



Criptografía y sus aplicaciones

Seguridad en el mundo basado en papel



Criptografía y sus aplicaciones

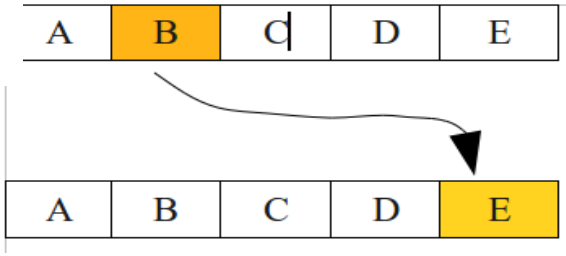
¿Qué es la criptografía?

La criptografía (del griego “ocultar” y “escribir” literalmente “escritura oculta” es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura de forma tal que sólo puedan ser leídos por las personas a quienes van dirigidos.

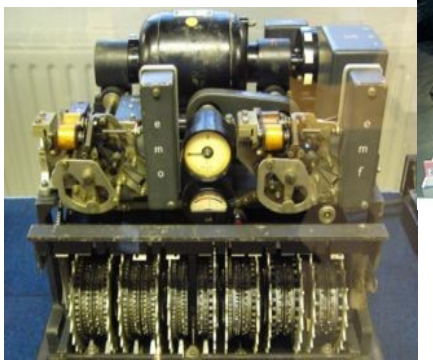
Criptografía y sus aplicaciones

Un poco de historia

Escítala



Método de César



La máquina alemana de cifrado de Lorenz, usada en la Segunda Guerra Mundial para el cifrado de mensajes para los generales de muy alto rango

La máquina Enigma utilizada por los alemanes durante la II Guerra Mundial

Criptografía y sus aplicaciones

Algunos principios básicos

Grupos de métodos de cifrado:

- Trasposición
- Sustitución
  - Cifrado monoalfabético
  - Cifrado polialfabético

Criptografía y sus aplicaciones

La criptología (del griego krypto: lo oculto, lo escondido y logos: estudio) es el estudio de los criptosistemas. Sus áreas principales de estudio son:

- la criptografía
- el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.
- Y también incluye la esteganografía.

Criptografía y sus aplicaciones

Sistemas de criptografía

Existen dos tipos básicos de criptosistemas:

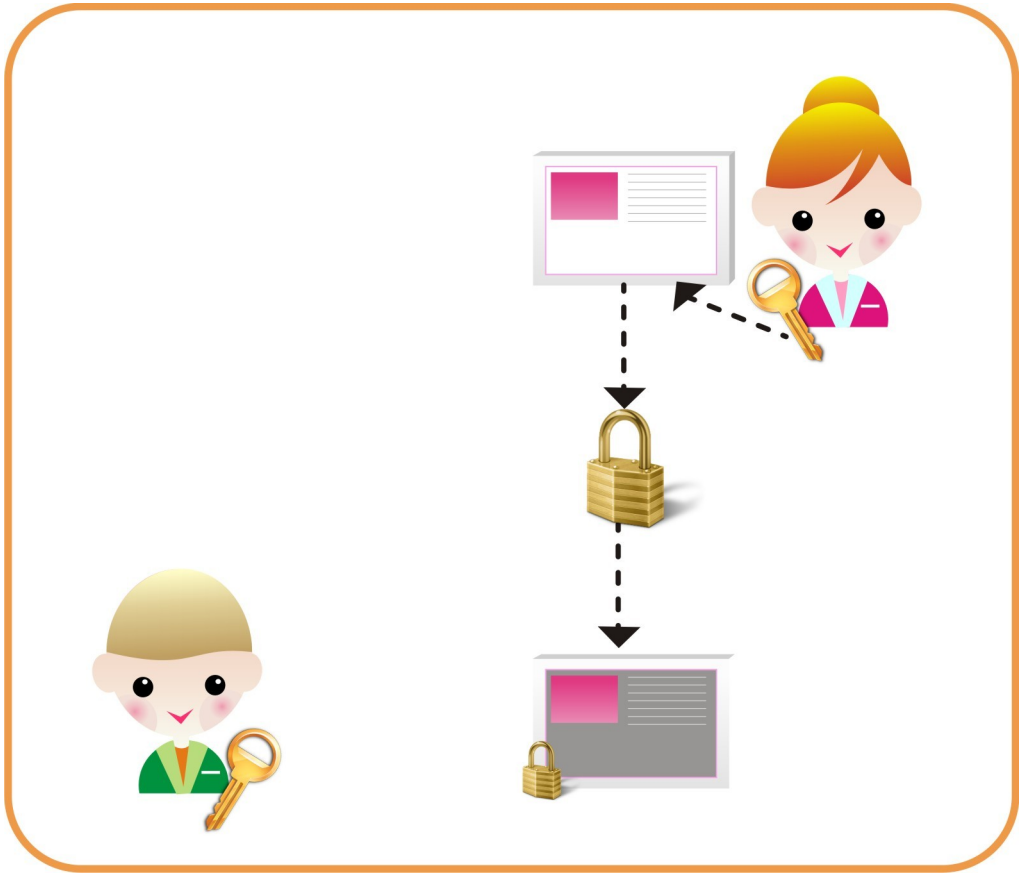
- Sistemas de cifrado simétrico (también conocidos como sistemas de clave secreta o clave privada)
- Sistemas de cifrado asimétrico (también conocidos como sistemas de clave pública)

Criptografía y sus aplicaciones

Criptografía simétrica

El mensaje original es encriptado usando la **clave compartida.** 

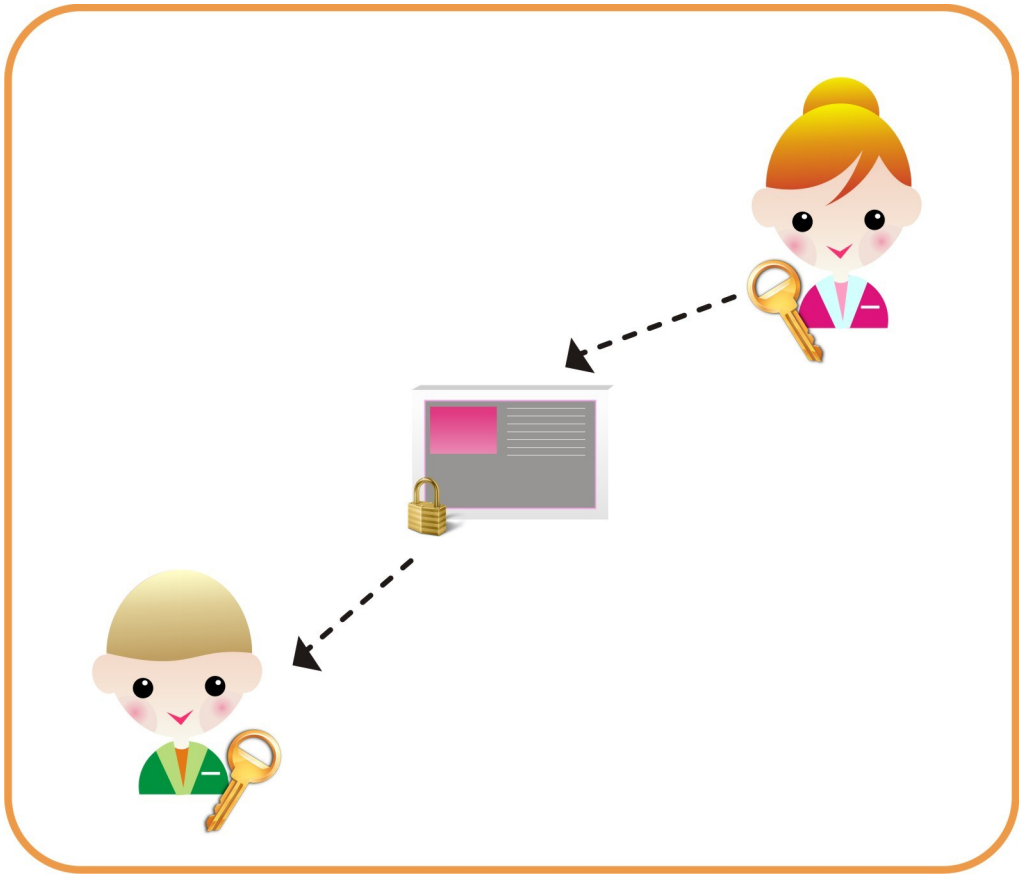
Se obtiene como resultado un mensaje encriptado.



Criptografía y sus aplicaciones

Criptografía simétrica

El mensaje es enviado al destinatario

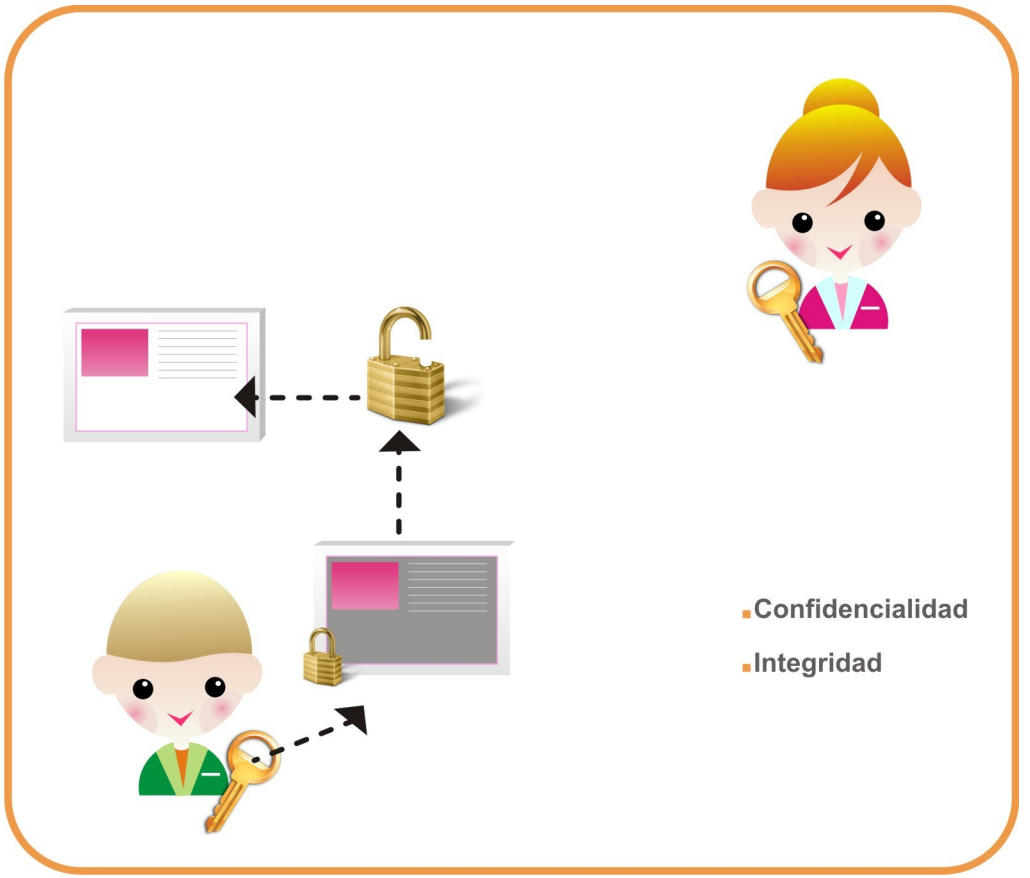


Criptografía y sus aplicaciones

Criptografía simétrica

El mensaje recibido se **desencripta** usando también la **clave compartida.**

Se obtiene como resultado el mensaje original.



- Confidencialidad
- Integridad

Criptografía y sus aplicaciones

Criptografía simétrica

Los sistemas simétricos o de clave privada utilizan la misma clave para encriptar y desencriptar

Existen dos modos de operación básicos:

- Cifrado en bloques
- Cifrado de flujo

Criptografía y sus aplicaciones

Criptografía simétrica – Cifrado en bloques y cifrado de flujo

- ### Cifrado en bloque

  El mensaje en texto claro se divide en bloques de longitud fija (8,16, … bytes) y luego se aplica el algoritmo de cifrado a cada bloque utilizando una clave secreta. Ejemplos: DES, AES.

  Existen distintos modos de operación dependiendo de cómo se mezcla la clave con el texto claro: ECB: Electronic Codebook, CBC: Cipher Block Chaining, CFB: Cipher FeedBack y OFB: Output FeedBack

- ### Cifrado de flujo

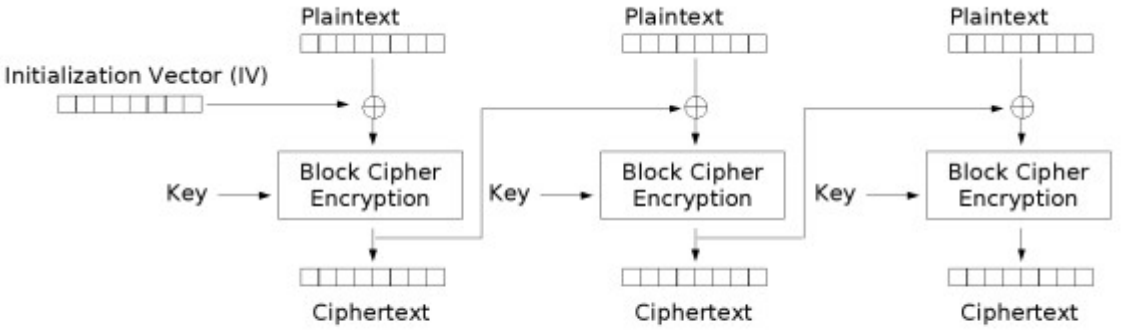
  Para algunas aplicaciones, como el cifrado de conversaciones telefónicas, el cifrado en bloques es inapropiada porque los datos se producen en tiempo real en pequeños fragmentos. Las muestras de datos pueden ser tan pequeñas como 8 bits o incluso de 1 bit. El algoritmo genera una secuencia pseudoaleatoria (secuencia cifrante o keystream en inglés) de bits que se emplea como clave. El cifrado se realiza combinando la secuencia cifrante con el texto claro. Ejemplo: RC4.

Criptografía y sus aplicaciones

Criptografía simétrica – Cifrado en bloques

Modo ECB
El texto se divide en bloques y cada bloque es cifrado en forma independiente utilizando la clave.

Modo CBC
El texto se divide en bloques y cada bloque es mezclado con la cifra del bloque previo, luego es cifrado utilizando la clave.

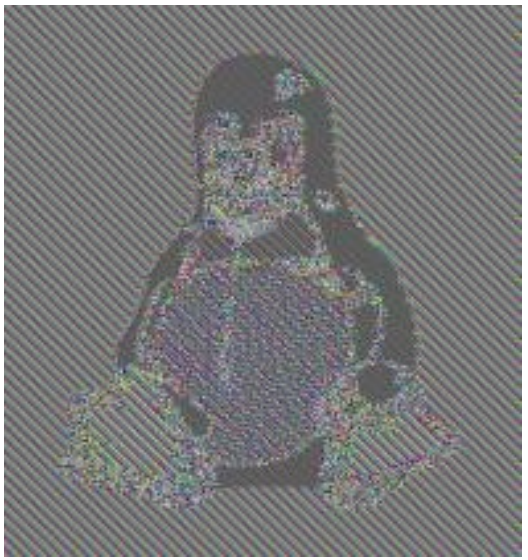


Cipher Block Chaining (CBC) mode encryption

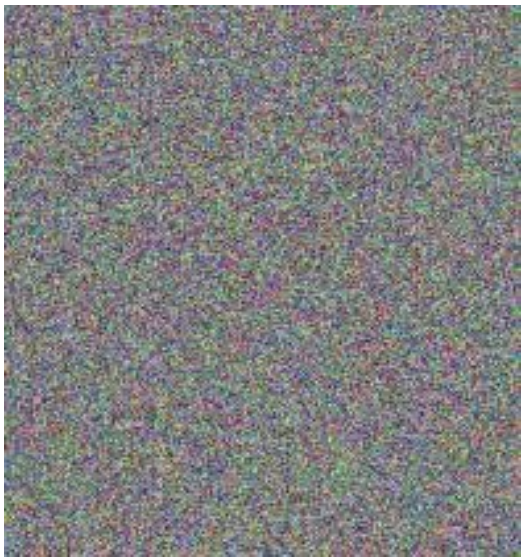
Criptografía y sus aplicaciones

Cifrado en bloques – EBC – Ejemplo

EBC puede revelar patrones en los datos cifrados



MODO ECB



MODO CBC

Fuente: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Criptografía y sus aplicaciones

Criptografía simétrica

Ventajas:

- Gran velocidad de cifrado
- No aumenta el tamaño del mensaje
- Tecnología muy conocida y difundida

Desventajas:

- La seguridad depende de un secreto compartido entre el emisor y el receptor
- La administración de claves no es “escalable”
- La distribución de claves debe hacerse a través de algún medio seguro

Ejemplos de algoritmos:

3DES, IDEA, AES, Blowfish

Criptografía y sus aplicaciones

Criptografía asimétrica

- Los sistemas asimétricos utilizan dos claves, una privada y una pública (siendo una la inversa de la otra). Ambas pueden ser usadas para encriptar y desencriptar, dependiendo del modo de operación utilizdo.

  Dichas claves están matemáticamente relacionadas entre sí y además:

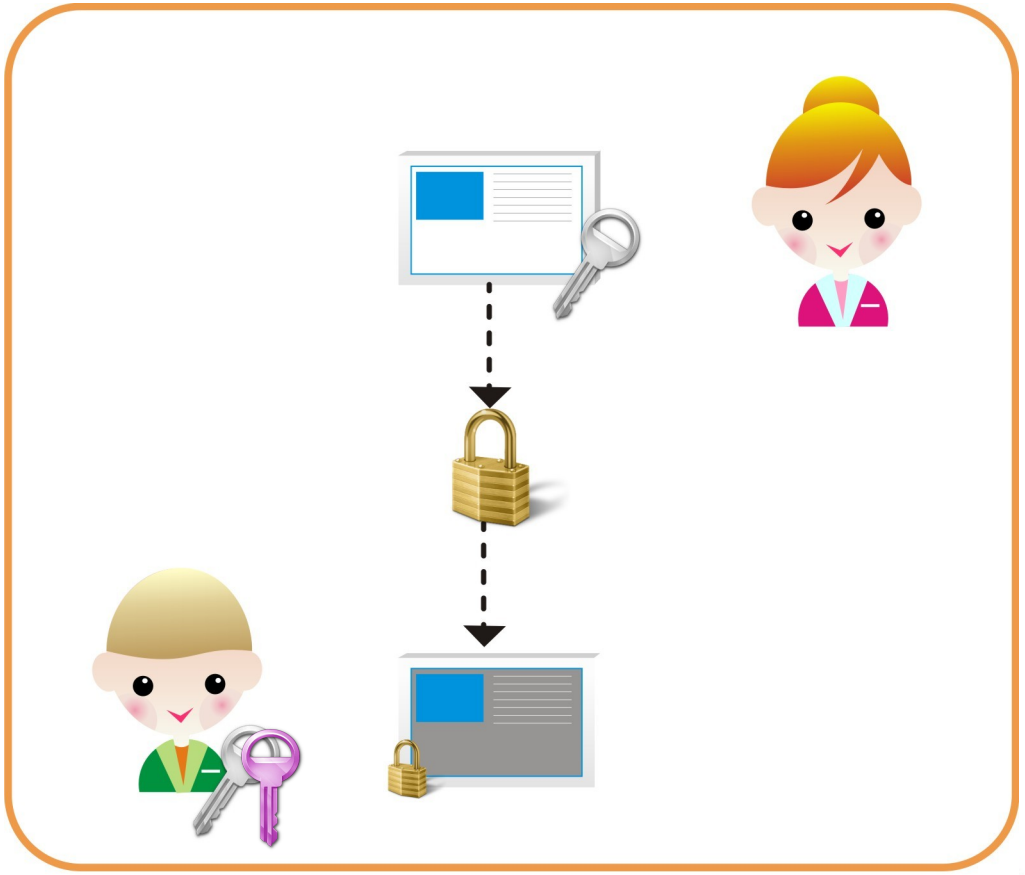
  - La clave pública está disponible para todos.
  - La clave privada es conocida sólo por el individuo dueño del par de claves.

Criptografía y sus aplicaciones

Criptografía asimétrica – Modo encripción

El mensaje **original** es encriptado usando la **clave pública del receptor.**

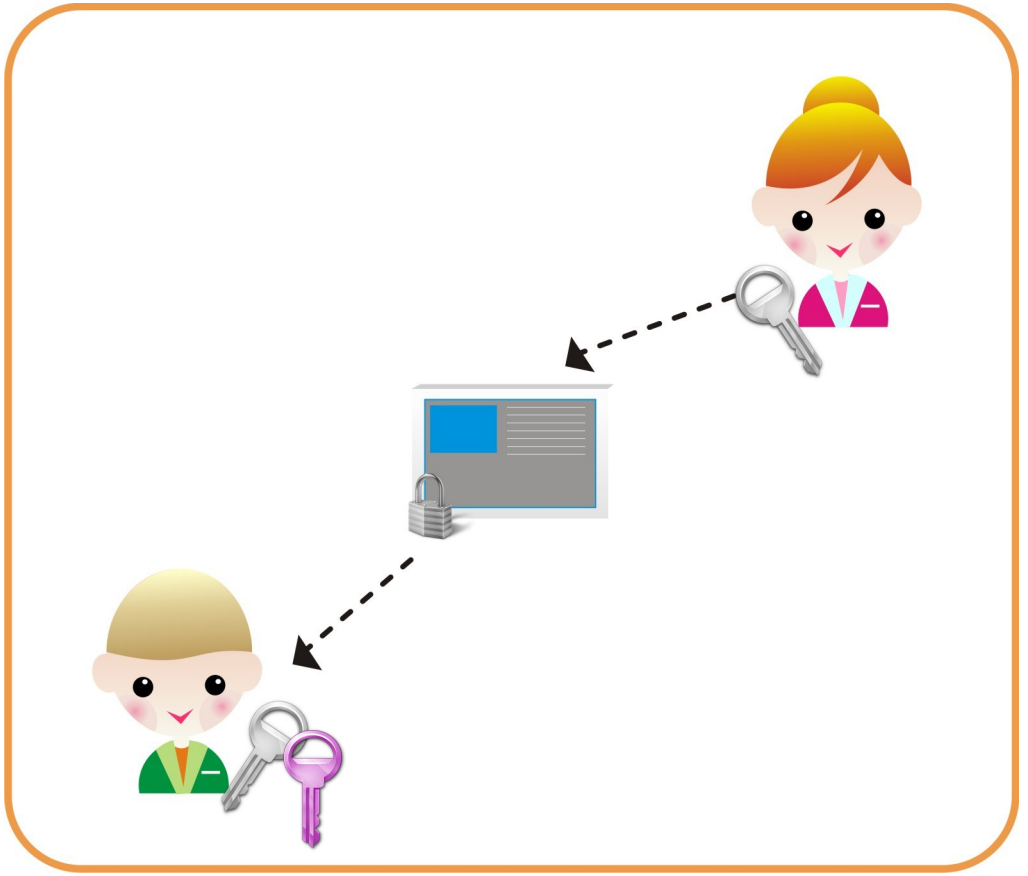
Se obtiene como resultado un mensaje encriptado.



Criptografía y sus aplicaciones

Criptografía asimétrica – Modo encripción

El mensaje **encriptado** es enviado al destinatario.

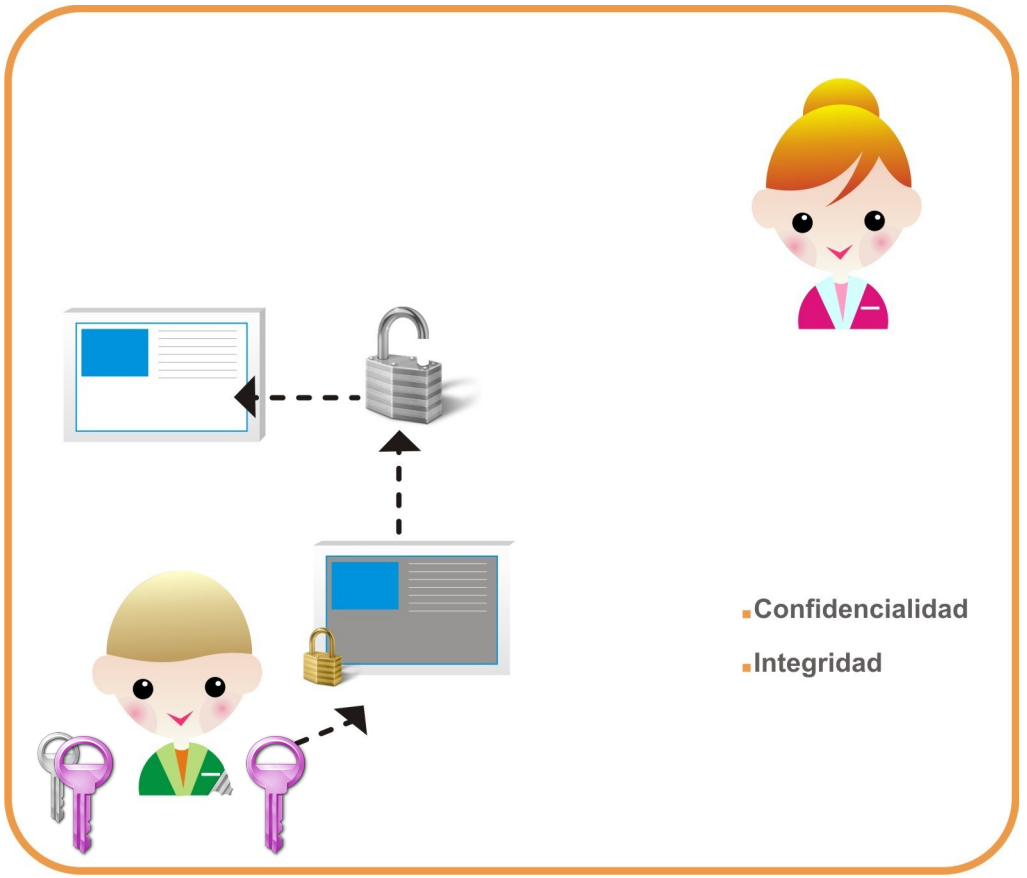


Criptografía y sus aplicaciones

Criptografía asimétrica – Modo encripción

El mensaje se **desencripta** usando la **clave privada del receptor.**

Se obtiene como resultado el mensaje original.

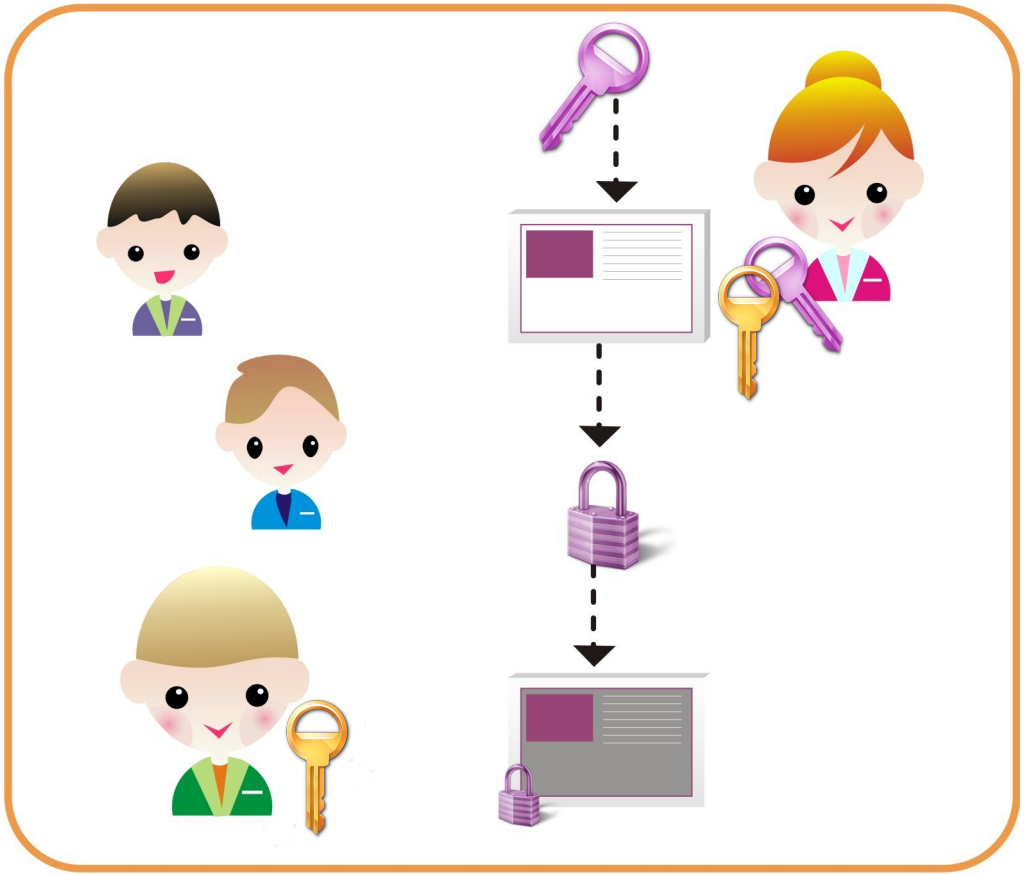


Criptografía y sus aplicaciones

Criptografía asimétrica – Modo autenticación

El mensaje **original** es encriptado usando la **clave privada del emisor.**

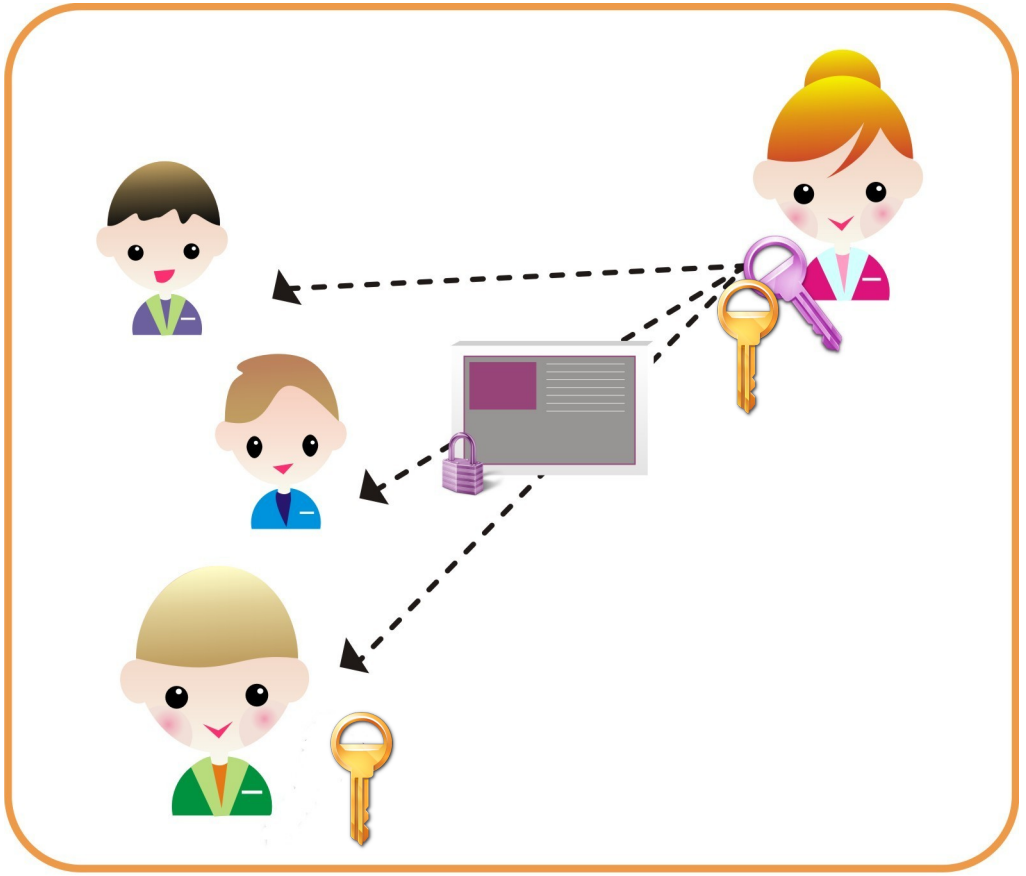
Se obtiene como resultado un mensaje encriptado.



Criptografía y sus aplicaciones

Criptografía asimétrica – Modo autenticación

El mensaje **encriptado** es enviado. El mismo puede ser enviado a **más de un destinatario**.

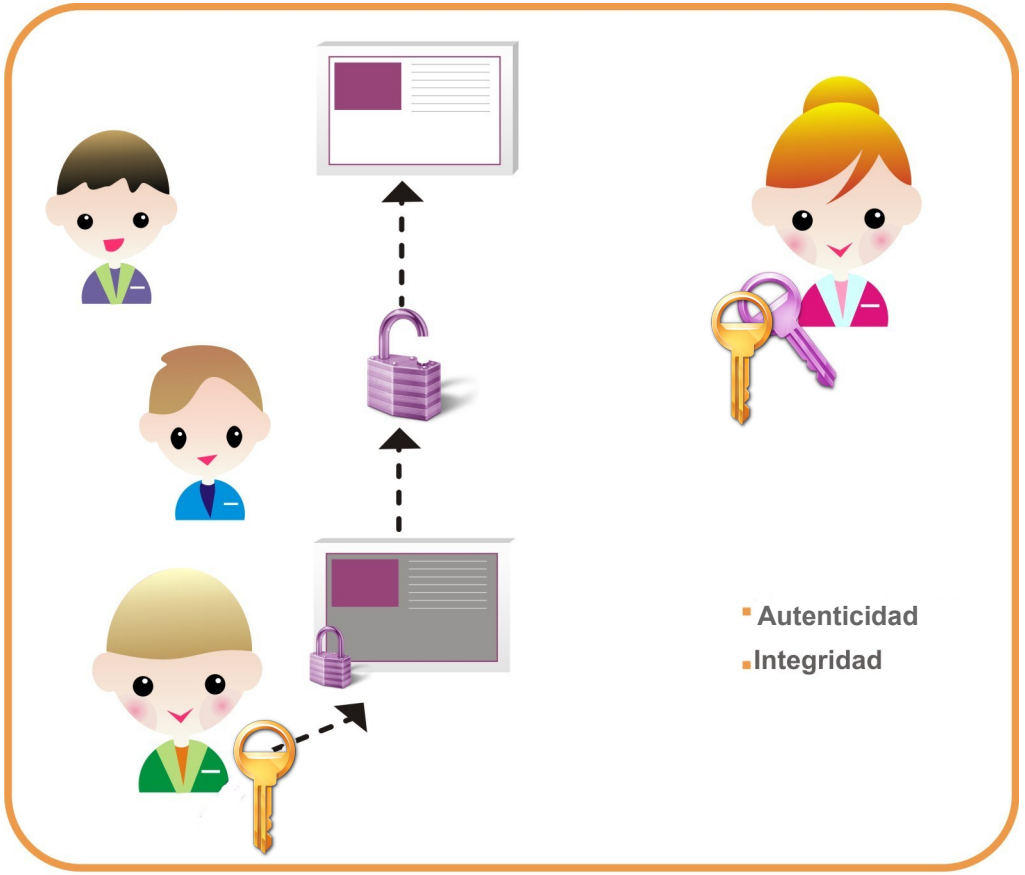


Criptografía y sus aplicaciones

Criptografía asimétrica – Modo autenticación

El mensaje se **desencripta** usando la **clave pública del emisor.**

Se obtiene como resultado el mensaje original.



Criptografía y sus aplicaciones

Criptografía asimétrica

Ventajas:

- No es necesario efectuar ningún intercambio de claves.
- Es una tecnología muy conocida y comprendida.
- A través de sus distintos modos de uso cubre gran parte de los requisitos de seguridad de la información.

Desventajas:

- Requiere mayor potencia de cómputo para cifrar y descifrar que el método simétrico.
- El mensaje cifrado es de mayor tamaño que el original.

Ejemplos de algoritmos:

Diffie-Hellman, RSA, DSA, ElGamal, CCE

Criptografía y sus aplicaciones

Indice de temas

- Conceptos básicos de criptografía
- Firma digital
- PKI
- PGP
- Esteganografía

Criptografía y sus aplicaciones

Firma digital

Una firma digital certifica un documento y lo atribuye fehacientemente a su autor.

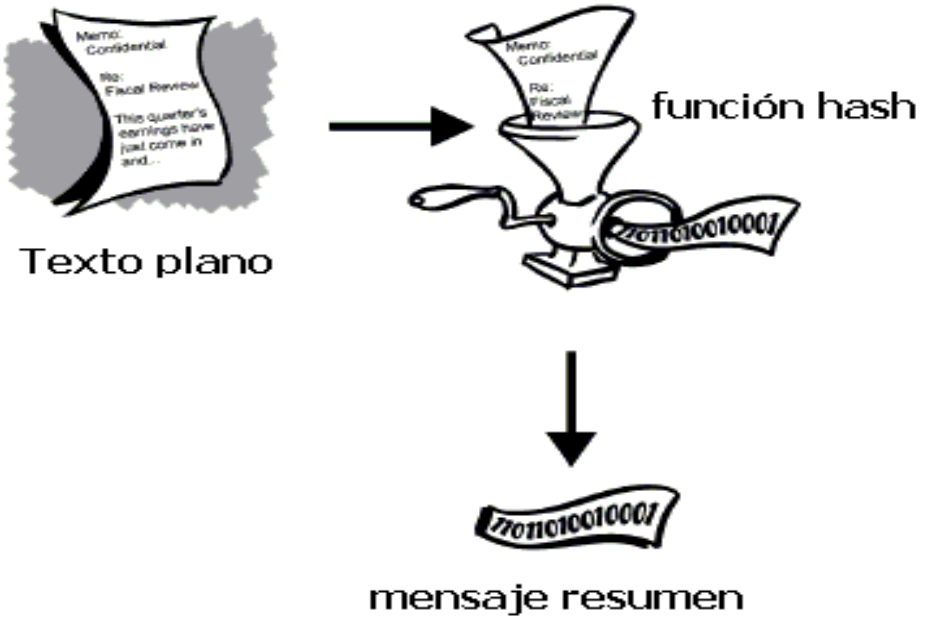
Usando el modo autenticación, el receptor del mensaje puede estar seguro que nosotros generamos dicha mensaje sin embargo, ésto puede resultar en un proceso ineficiente, lento y que produce gran volúmen de datos (al menos el doble que los datos originales)

Para mejorar el proceso, se utilizan funciones de hash (de una sola vía)

Criptografía y sus aplicaciones

Funciones de hash

Son funciones de transformación que toman una entrada y retornan un string de longitud fija, conocida como “message digest”.



Criptografía y sus aplicaciones

Funciones de hash

Propiedades

- El resultado es fácil de calcular.
- Es imposible obtener el mensaje original a partir del hash

Ejemplos:

- MD5 (128 bists, RFC 1321)
- SHA-1 (160 bits, NIST FIPS 180-2)
- SHA-256
- SHA-512

Criptografía y sus aplicaciones

¿Qué es la firma digital?

- Desde el punto de vista legal produce los mismos efectos que la firma hológrafa pero sobre un formato digital
- Desde el punto de vista técnico es una secuencia de bits de longitud fija, resultante de aplicar un conjunto de algoritmos criptográficos que permiten identificar al autor y verificar la integridad del contenido firmado.

  El proceso de firmar implica el cifrado, con la clave privada del firmante, del hash del mensaje a firmar.

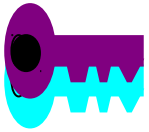
Criptografía y sus aplicaciones

Propósitos de la firma digital

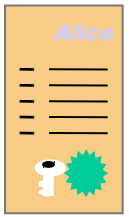
- Atribuir el documento a su autor de manera fehaciente (autenticidad del autor)
- Verificar que el contenido del documento no fue alterado (integridad del documento).
- Garantizar que el autor no pueda negar haber firmado el documento o mensaje (no repudio de la acción).

Criptografía y sus aplicaciones

¿Qué se necesita para firmar?



Un par de claves



Un certificado digital que identifica al firmante y contenga:

- La clave pública del firmante
- Datos del firmante
- Firma “confiable”

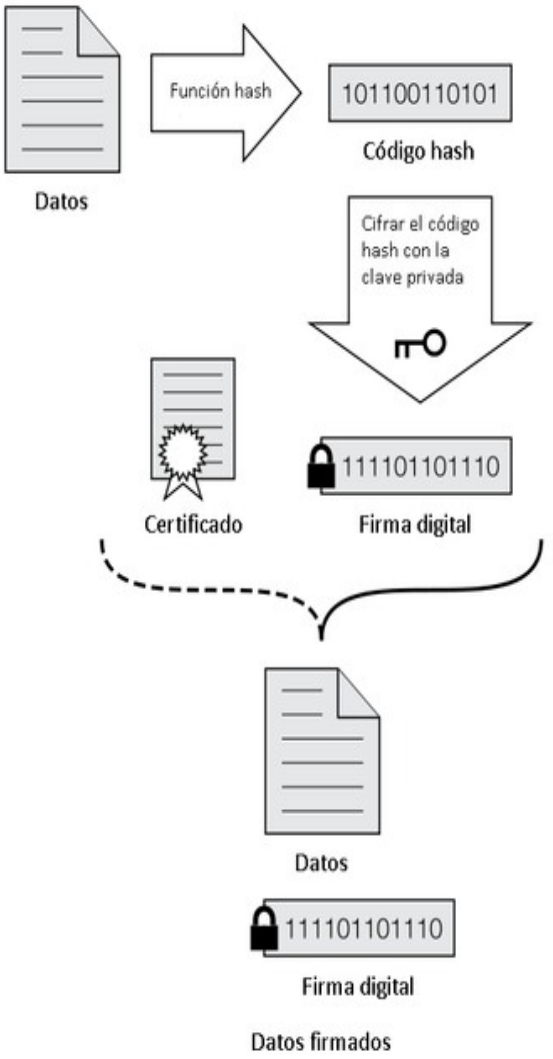
Criptografía y sus aplicaciones

Proceso de firma

Para crear una **firma digital** hay que crear un **resumen del mensaje original o "hash".** La función de resumen reduce el mensaje a una cadena de caracteres de tamaño fijo.

El emisor encripta el **resumen del mensaje** con su clave privada.

La función que genera el resumen y el proceso de encripción son llevados a cabo automáticamente por los módulos de hardware y/o software intervinientes.



Criptografía y sus aplicaciones

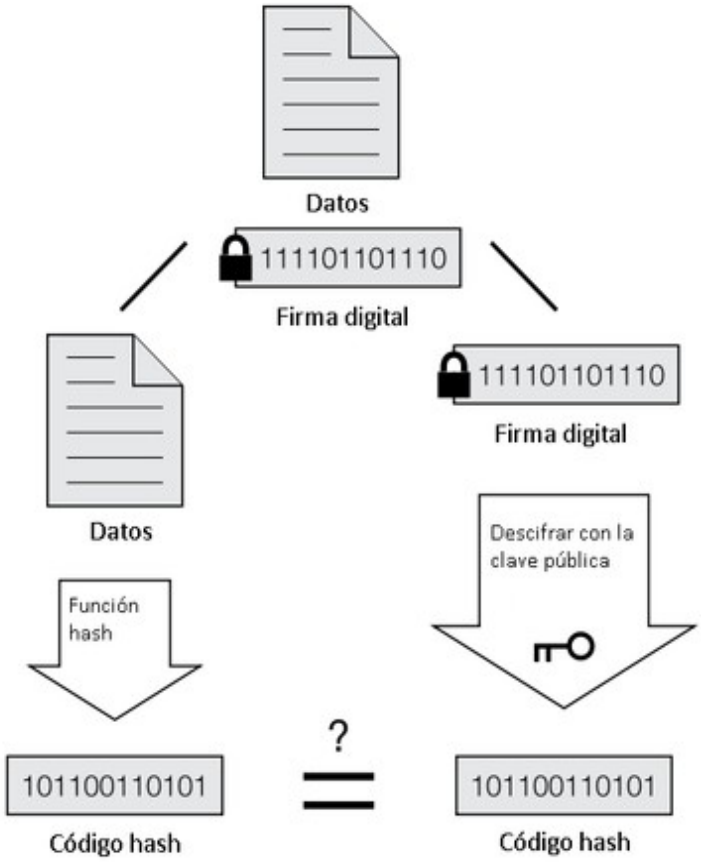
Proceso de verificación

La **clave pública del emisor** es utilizada para desencriptar la firma digital.

El sistema calcula un nuevo resumen a partir del mensaje recibido.

Se verifica si el resumen obtenido a partir del mensaje recibido coincide con el resultado de haber desencriptado la firma digital del mensaje.

Si los resultados coinciden significa que la firma es válida y que el mensaje no fue alterado



Si los códigos hash coinciden, la firma es válida

Criptografía y sus aplicaciones

Certificado digital

El certificado digital es una estructura de datos que contiene:

- La identidad del poseedor de la clave pública
- La clave pública
- Período de validez
- Identidad del emisor
- Información adicional (cargo, política de certificación, etc)
- Firma del emisor (entidad usualmente denominada autoridad de certificación, o tercero confiable)

Criptografía y sus aplicaciones

Certificado digital

Opcionalmente contiene:

- Identificador único del emisor.
- Identificador único del sujeto
- Extensiones

Criptografía y sus aplicaciones

PKI – Infraestructura de clave pública

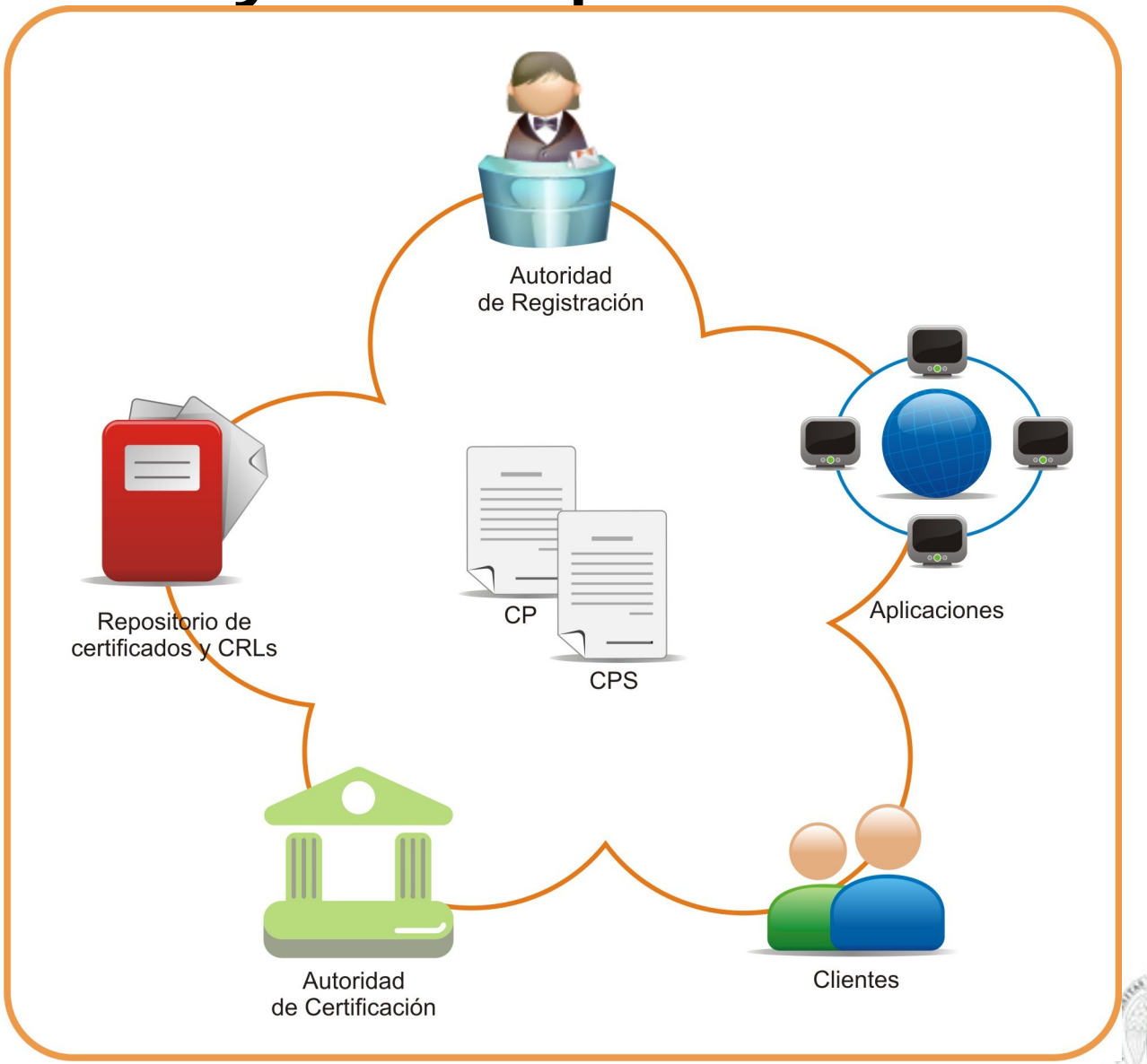
La PKI es la infraestructura encargada del manejo de certificados digitales. A través de los mismos, provee la seguridad requerida para la transmisión de información sensible en Internet.

Su objetivo consiste en asociar una clave a la identidad de su poseedor mediante la emisión de certificados digitales X509v3

Criptografía y sus aplicaciones

PKI

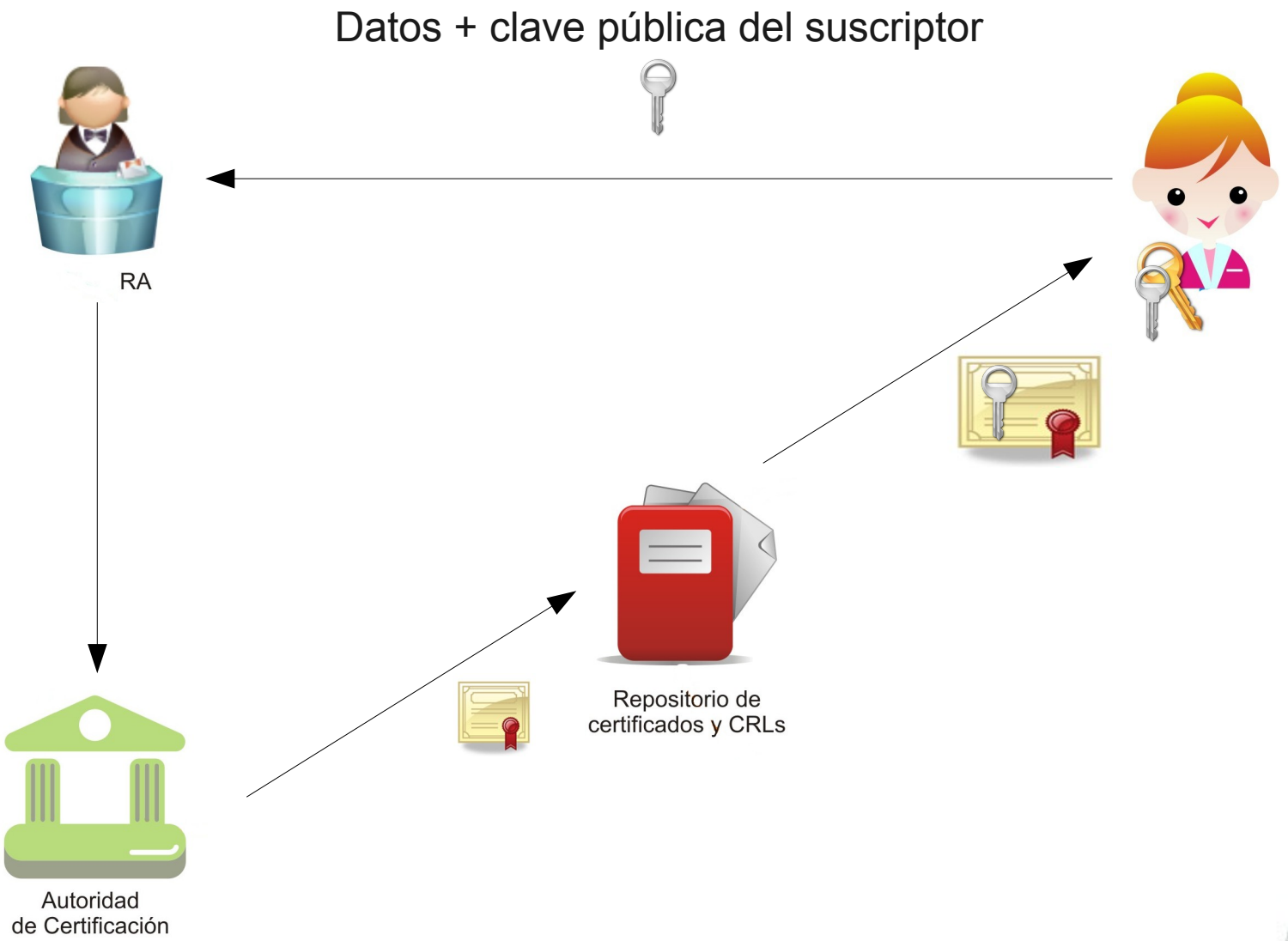
Componentes



Criptografía y sus aplicaciones

PKI

Proceso de Emisión



Criptografía y sus aplicaciones

PKIX, es un grupo de trabajo del IGTF

- RFC 3280 – Certificate and Crl profile
- RFC 3647 – Cert Policy and Certification Practices Framework
- RFC 3820 – Internet X.509 Public Key Infraestructure Proxy Certificate Profile
- RFC 3494 – LDAP
- RFC 2560 – OCSP

Criptografía y sus aplicaciones

PKCS

Conjunto de especificaciones técnicas desarrolladas por Netscape, RSA y otros, cuyo objeto es uniformizar las técnicas y protocolos de criptografía de clave pública.

Algunos ejemplos:

- PKCS#1: RSA Cryptography Standard
- PKCS#3: Diffie-Hellman Key Agreement Standard
- PKCS#12: Personal Information Exchange Sintax Standard
- PKCS#15: Criptographic Token Information Format Standard
- PKCS#7: Cryptographic Message Sintax Standard
- PKCS#10: Certification Request Sintax Standard

Criptografía y sus aplicaciones

Opciones de implementación

Una organización o empresa puede:

- Implementar/instalar su propia PKI
- Contratar los servicios de certificación de una PKI existente.

Criptografía y sus aplicaciones

Ejemplos de PKIs en la red

- Entrust http://www.entrust.net
- Globalsign http://www.globalsign.net
- Verisign http://www.verisign.com
- AC de la Administración Pública Nacional http://www.pki.gov.ar
- UNLP PKIGrid CA http://www.pkigrid.unlp.edu.ar

Criptografía y sus aplicaciones

OpenCA

Constituye una implementación opensource de una infraestructura PKI

Componentes:

- Autoridad de certificación
- Autoridades de registración
- Servidor web público que posibilita la interacción con los usuarios de la PKI
- Repositorio de certificados

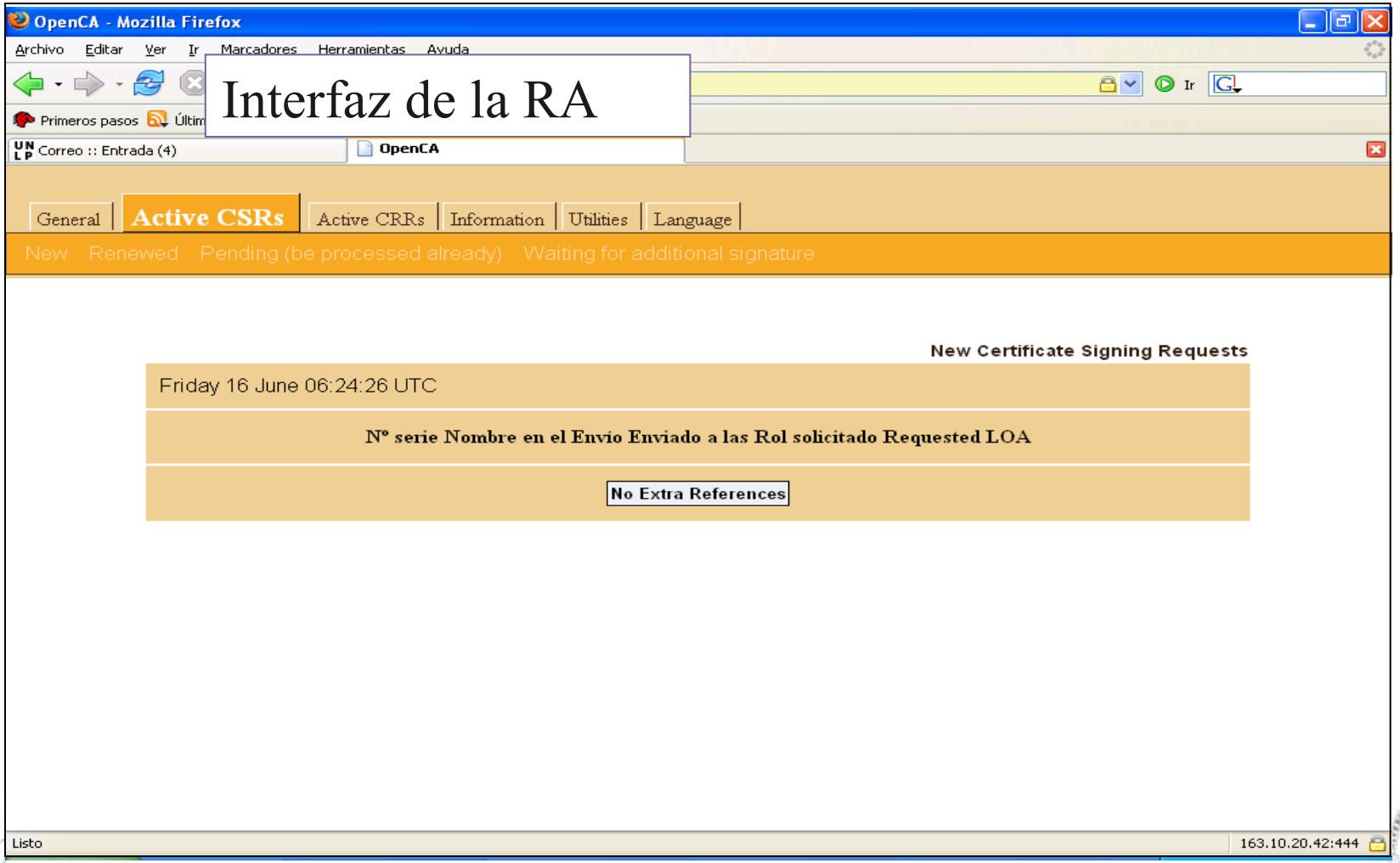
Criptografía y sus aplicaciones - OpenCA

Server Information for OpenCA Server Version 0.9.2

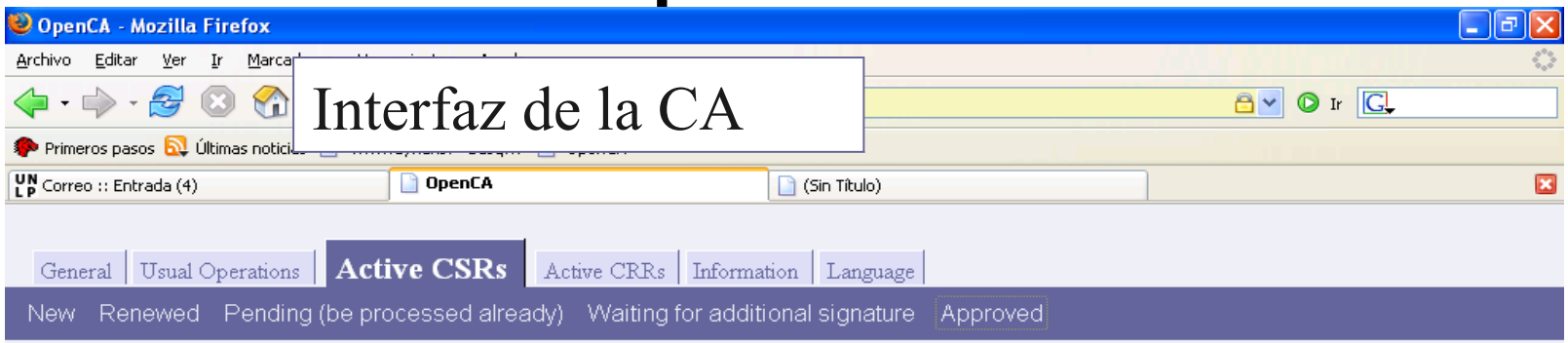
Friday 16 June 06:23:22 UTC

Módulo	Versión
OpenSSL	0.9.135.2.11
Tools	0.4.3
DB	2.0.5
Configuration	1.5.3
TRIStateCGI	1.5.5
REQ	0.9.61.2.1
X509	0.9.57
CRL	0.9.24.2.1
PKCS7	0.9.19.2.5

Criptografía y sus aplicaciones – OpenCA



Criptografía y sus aplicaciones – OpenCA



Approved Certificate Signing Requests

Friday 16 June 04:51:16 UTC

Operador	Nº serie	Nombre en el Envio	Aprobado a las	Rol solicitado	Requested LOA
n/d	5152	emailAddress=omega2000ar@yahoo.com.ar, CN=Berretti Fernando, L=CeSPI, OU=UNLP, O=e-Ciencia, C=AR	n/d	User	n/d
n/d	5408	emailAddress=d_zecchin04@yahoo.com.ar,CN=Danilo Zecchin,L=CeSPI,OU=UNLP,O=e-Ciencia,C=AR	n/d	User	n/d
n/d	5664	emailAddress=sserrano@iwinds.com.ar, CN=Serrano Sebastian, L=CeSPI, OU=UNLP, O=e-Ciencia, C=AR	n/d	User	n/d

No Extra References

Criptografía y sus aplicaciones

Firma digital – Situación legal en Argentina

- Ley 25.506 (promulgada el 11 de diciembre de 2001) reglamentada por el Decreto 2628/02 (20 de Diciembre de 2002) y por el Decreto 724/06 modificatorio del anterior (13 de junio de 2006)
- También existen un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

Criptografía y sus aplicaciones

Firma digital – Situación legal en Argentina

El conjunto de normas descriptas conforma una Infraestructura de Firma Digital de alcance federal integrada por:

- Autoridad de Aplicación: Jefatura de Gabinete de Ministros, establece las normas y procedimientos técnicos
- Comisión Asesora para la Infraestructura de Firma Digital: emite recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital.
- Ente Administrador de Firma Digital: encargado de otorgar las licencias a los certificadores y de supervisar su actividad

Criptografía y sus aplicaciones

Firma digital – Situación legal en Argentina

- Certificadores licenciados: organismos públicos que obtengan una licencia para actuar como proveedores de servicios de certificación
- Autoridades de Registro: son entidades con las funciones de validación de la identidad y otros datos de los suscriptores de certificados.
- Sistema de Auditoría: será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Criptografía y sus aplicaciones

PKI

Uso

de

Certificados

Autenticación
del usuario

Frima de
Documentos

Emisión de
Certificados x509

Comunicaciones
seguras

Correo
Electronico seguro

Criptografía y sus aplicaciones

SSL (Secure Sockets Layer)→ TSL

Protocolo originalmente desarrollado por Netscape

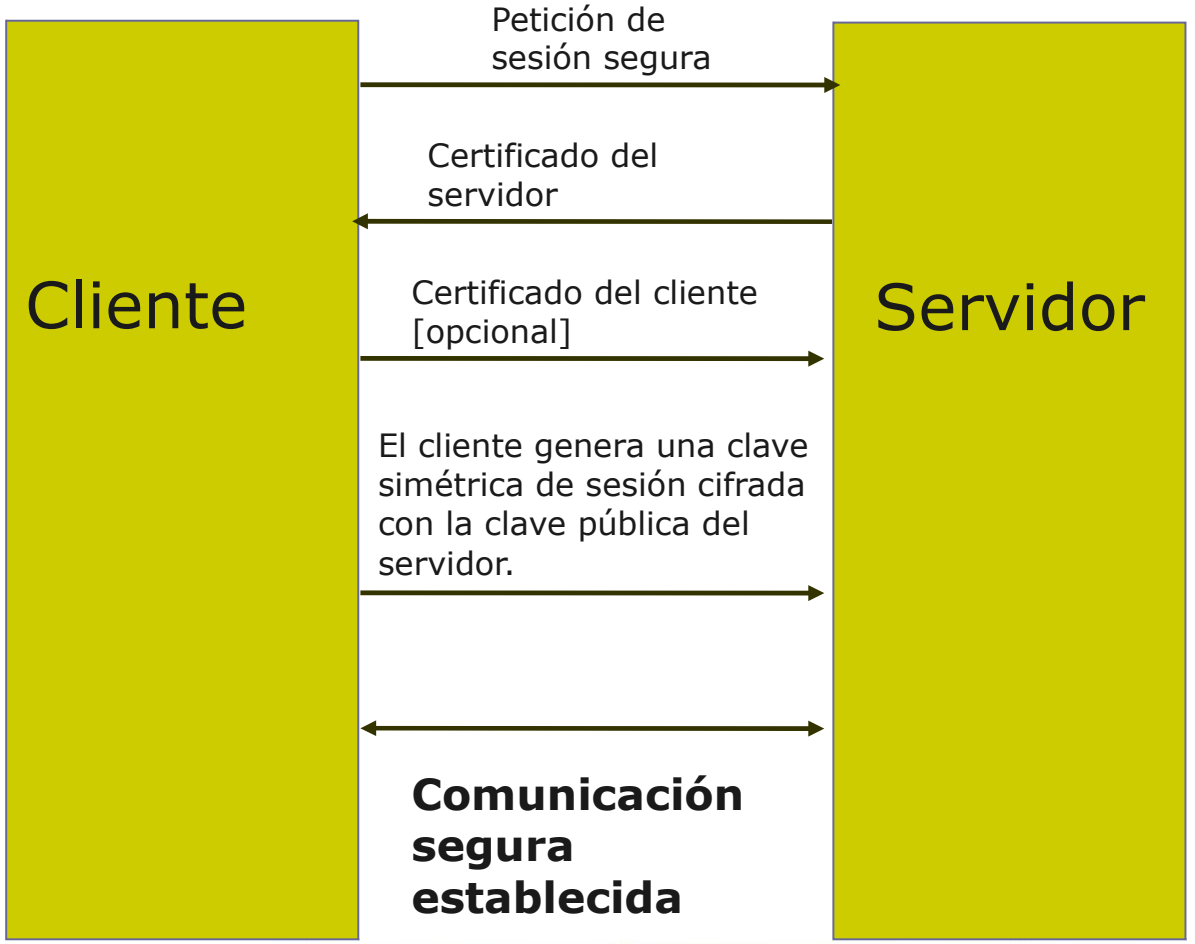
Se convirtió luego en el estándar de la web para:

- Autenticar Sitios WEB (servidores) frente a navegadores WEB (Clientes)
- Encriptar las comunicaciones entre clientes y servidores WEB.

En la actualidad la funcionalidad de SSL está integrada en la mayor parte de clientes y servidores WEB

Criptografía y sus aplicaciones

SSL



Criptografía y sus aplicaciones

Indice de temas

- Conceptos básicos de criptografía
- Firma digital
- PKI
- PGP
- Esteganografía

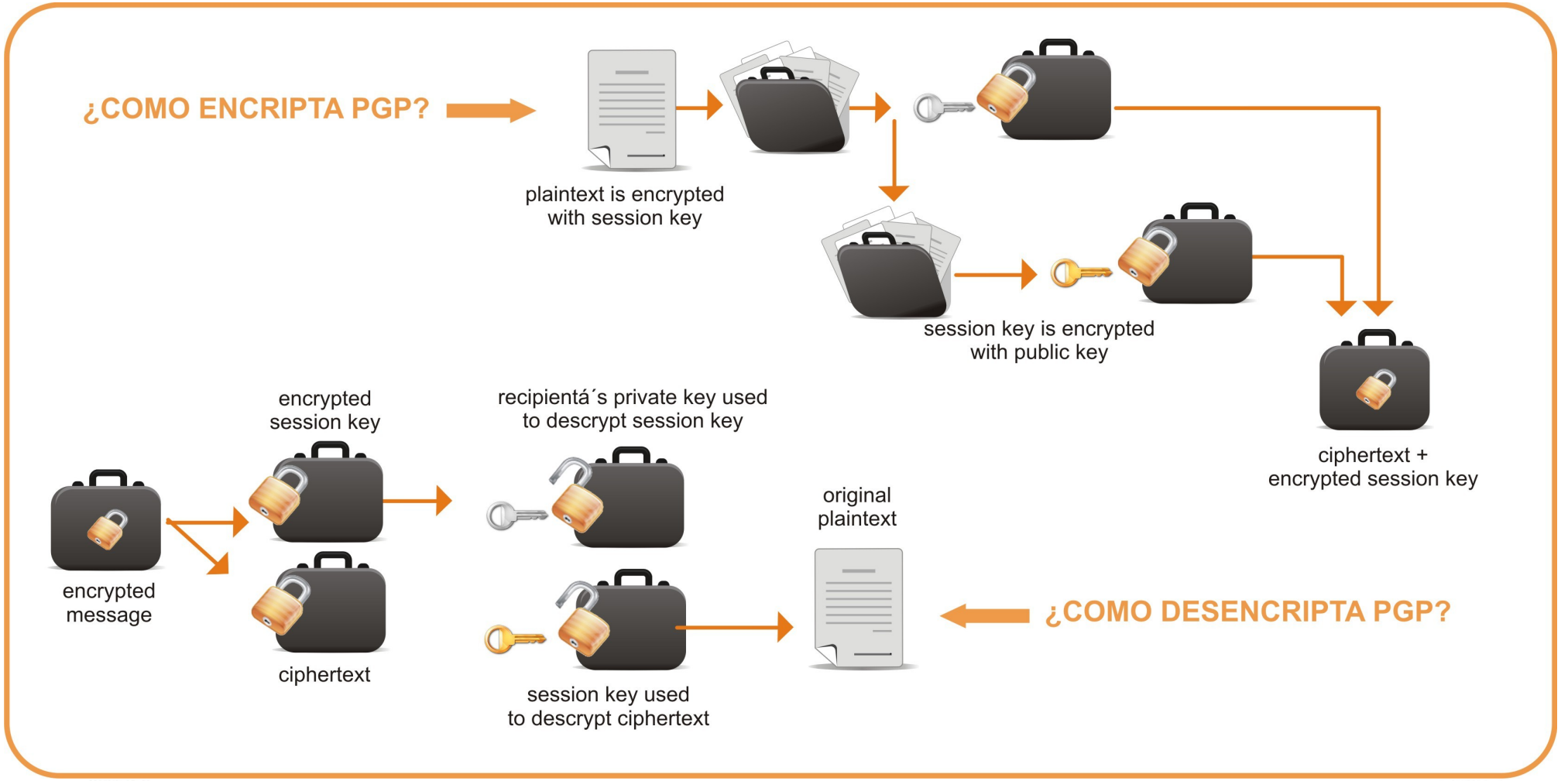
Criptografía y sus aplicaciones

PGP

PGP (Pretty Good Privacy) es un conjunto de programas creados por Phil Zimerman para proteger la información. En un criptosistema híbrido que utiliza criptografía de clave pública, criptografía simétrica y funciones de hash.

- Al convertirse en uno de los mecanismos más populares para utilizar criptografía, la IETF tomó como base su diseño para crear el estándar OpenPGP.
- Más fácil de utilizar que otros criptosistemas.
- Además de proteger los datos en tránsito también permite proteger los datos almacenados en discos, copias de seguridad, etc.

Criptografía y sus aplicaciones-PGP



Criptografía y sus aplicaciones

PGP – Anillos de claves

- Anillo de claves públicas: archivo en el que se guardan las claves públicas del usuario propietario y las claves públicas importadas.
- Anillo de claves privadas: archivo en el que se guarda la/s clave/s privada/s del usuario propietario.

Criptografía y sus aplicaciones

PGP – Anillos de claves

Si podemos confirmar la persona que utiliza una clave en particular, podemos firmar dicha clave con nuestra clave privada. Esto nos permitirá:

- Certificar que la clave efectivamente corresponde a esa persona
- Evitar la manipulación de nuestro anillo de claves por parte de un tercero.
- Las claves públicas se pueden subir a un servidor de claves. Las firmas realizadas a una clave también se puede subir a un servidor.
- Generalmente se conoce PGP partys a las reuniones en las que se validan, intercambian y se firman claves PGP.

Criptografía y sus aplicaciones

PGP – Esquema de confianza

- La confianza es algo subjetivo.
- Yo puedo confiar en la clave de una persona, pero no confiar en las claves en las que esa persona confía.
- Se pueden establecer relaciones de confianza indirecta.

Criptografía y sus aplicaciones

PGP – Niveles de confianza:

- Unknown: Desconocido. No se sabe nada sobre el dueño de la clave firmante. Las claves en nuestro anillo de claves que no nos pertenezcan tendrán al principio este nivel de confianza.
- None: Ninguno. Se sabe que el propietario firma otras claves de modo impropio.
- Marginal: Marginal. El propietario comprende las implicancias de firmar una clave y valida las claves de forma correcta antes de firmarlas.
- Full: Absoluto. El propietario comprende perfectamente las implicaciones de firmar una clave y su firma sobre una clave es tan buena como la nuestra.

Criptografía y sus aplicaciones

PGP – Esquema de confianza:

El nivel de confianza es asignado a una clave, es algo que sólo nosotros podemos establecer y se considera información privada.

Por otro lado, si firmamos una clave determinada, nuestra firma acompañará a la clave en cuestión y otras personas podrán ver dicha firma.

Criptografía y sus aplicaciones

PGP – Validez de una clave

Una clave K se considerará válida se cumplen dos condiciones:

- Si está firmada por suficientes claves válidas, lo que implica alguna de las siguientes condiciones:
  - Nosotros firmamos la clave
  - Alguien a quien le tenemos confianza FULL firmó la clave
  - La clave fué firmada por tres claves en las que confiamos MARGINALMENTE
- Si el camino de claves firmadas que nos lleva desde K hasta nuestra propia clave es de cinco pasos o menos.
- La longitud del camino, como el número de claves con confianza marginal requeridas se pueden cambiar.

Criptografía y sus aplicaciones

PGP Ventajas

- Su punto fuerte radica en la facilidad que ofrece a los usuarios para generar claves y gestionarlas, con un amplio campo de aplicación(permite, a individuos que quieren comunicarse entre sí de manera segura, encriptar archivos y mensajes)
- Existen versiones libres (GPG) y comerciales que implementan PGP, para manejo de claves y operaciones de criptografía, las cuales están disponibles para gran variedad de plataformas
- Basado en algoritmos extensamente revisados y considerados ampliamente seguros (RSA, DSS y Diffie-Hellman; CAST-128, IDEA y 3DES; SHA-1)

Criptografía y sus aplicaciones

PGP Ventajas

- El software y la documentación se encuentran disponibles en Internet.
- También existen versiones libres y comerciales que implementan Servidores de claves PGP.
- No fue desarrollado por ningún gobierno ni organización de creación de estándares, lo cual lo hace atractivo.

Criptografía y sus aplicaciones

PGP Desventajas

La gestión de claves en PGP se basa en la confianza mutua: ¡los amigos de tus amigos son mis amigos!

En un sistema abierto en Internet como puede ser el comercio electrónico, esta situación y otras más que pueden darse en este sistema de gestión de claves de confianza mutua, resulta inaceptable.

Criptografía y sus aplicaciones

Esteganografía

Es una disciplina que trata sobre técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

En la esteganografía digital tanto el mensaje como el portador es, en términos generales, un objeto software cualquiera. Aunque los medios portadores preferidos (por sus características) son archivos multimedia (imágenes, audio y vídeo).

Criptografía y sus aplicaciones

Esteganografía

Los mensajes ocultos muchas veces son cifrados previamente, lo cual le otorga un nivel de seguridad extra a la esteganografía: el sujeto receptor no sólo deberá conocer la existencia del mensaje, conocer el portador y la técnica (o clave) utilizada para esconderlo; sino que también deberá contar con el descifrador adecuado.

Existen diferentes técnicas para implementarla

Ejemplos de herramientas que la implementan:

- Camouflage
- Steganos
- MP3Stego
- Steghide

Criptografía y sus aplicaciones

Referencias

- Introducción a la criptografia (Criptografia Simetrica, Criptografia de clave pública, PGP, Firmas digitales, Funciones de Hash, Certificados digitales, Modelos de confianza y Revocaciones) http://www.pgpi.org/doc/pgpintro/
- PGP: GnuPG y administración de la confianza en el uso de claves: http://www.gnupg.org/gph/es/manual.html
- Sitio institucional con material adicional de PGP:

  http://privacidad.linti.unlp.edu.ar

Criptografía y sus aplicaciones

Referencias

- Página del grupo de trabajo PKIX http://www.ietf.org/hhml.charters/pkix-charter.html
- Requests For Comments:
  - Internet X.509 Public Key Infraestructure http://www.ietf.org/rfc/rfc4210.txt
  - Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc3647.txt
  - Sitio de Firma digital de la República Argentina http://www.pki.gov.ar
  - Informe de situación actual en firma digital en Argentina http://www.agn.gov.ar/informes/fichas/f_152_08_05_06.pdf
  - Herramienta opensource para la implementación de una infraestructura PKI http://www.openca.org