CRIPTOGRAFIA

Qué es, usos y beneficios de su utilización

Introducción

- Antes, computadoras relativamente aisladas
- Hoy, computadoras en redes corporativas conectadas además a Internet
- Transmisión de información a través de la Red
- Medios de comunicación inseguros implican amenazas latentes
- Se usa la Criptografía para:
  - Proveer privacidad y seguridad
  - Proteger documentos en disco duro o en cualquier medio de almacenamiento digital

Criptografía: Definición

- La RAE (Real Academia Española) define criptografía (del griego: oculto + escritura) como:

"*el arte de escribir con clave secreta o de modo enigmático*".

- Esta definición resulta muy poco ajustada a lo que es realmente la criptografía en los tiempos actuales.

Imprecisiones de esta definición

- Arte: la criptografía ha dejado de ser un arte. Es una ciencia.
- Escritura de documentos: no sólo se escriben mensajes; se envían o se guardan en una computadora diversos tipos de documentos y formatos.
- Se supone una clave: los sistemas actuales usan una o dos. En varias aplicaciones de Internet entran en juego 4 claves.
- Clave secreta: existirán sistemas que usan una sola clave y otros sistemas (muy importantes) que usan dos: una clave privada (secreta) y la otra pública.
- Representación enigmática: la representación binaria de la información puede ser enigmática para nosotros, pero es el lenguaje natural de las computadoras.

Criptografía: Una definición mas precisa

Rama inicial de las Matemáticas y en la actualidad también de la Informática, que hace uso de métodos y técnicas con el objeto principal de hacer ilegible (es decir, **cifrar**), y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

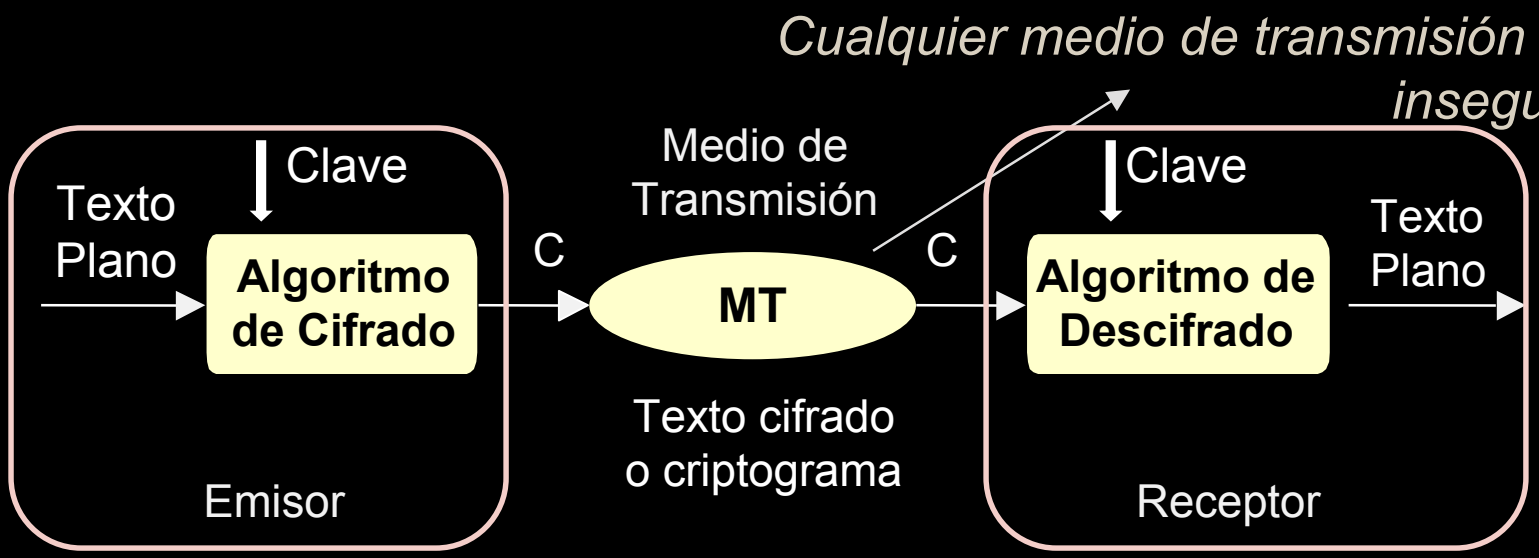
Definición (Cont)

- La Criptografía es una herramienta que permite ocultar la información con el objetivo de protegerla y preservarla.
- Transforma el texto original (“texto plano”) en un texto modificado (“texto cifrado”), que usualmente parece un texto ilegible.

Problemas resueltos por la Criptografía

- Confidencialidad
- Integridad
- Autenticidad
- No Repudio

Criptosistema



Sea cual sea el medio de transmisión o almacenamiento (enlace, red telefónica, red de datos, disco magnético, disco óptico, etc.), éste será siempre y por definición un medio inseguro. Por lo tanto, habrá que adaptarse a este medio usando el cifrado.

Tipos de Criptosistemas

- Según el tipo de Claves:
  - Cifradores Simétricos o de Clave Privada.
  - Cifradores Asimétricos o de Clave Pública.
- Existe otra clasificación:
  - Según el tratamiento del texto plano:
    - Cifradores de Bloque: cifrado por conjunto (bloque) de bits.
    - Cifradores de Flujo: cifrado bit a bit.

Criptosistemas Simétricos y Asimétricos

- Vamos a ver cómo se obtienen en cada uno de estos sistemas de cifrado los dos aspectos más relevantes de la seguridad Informática:

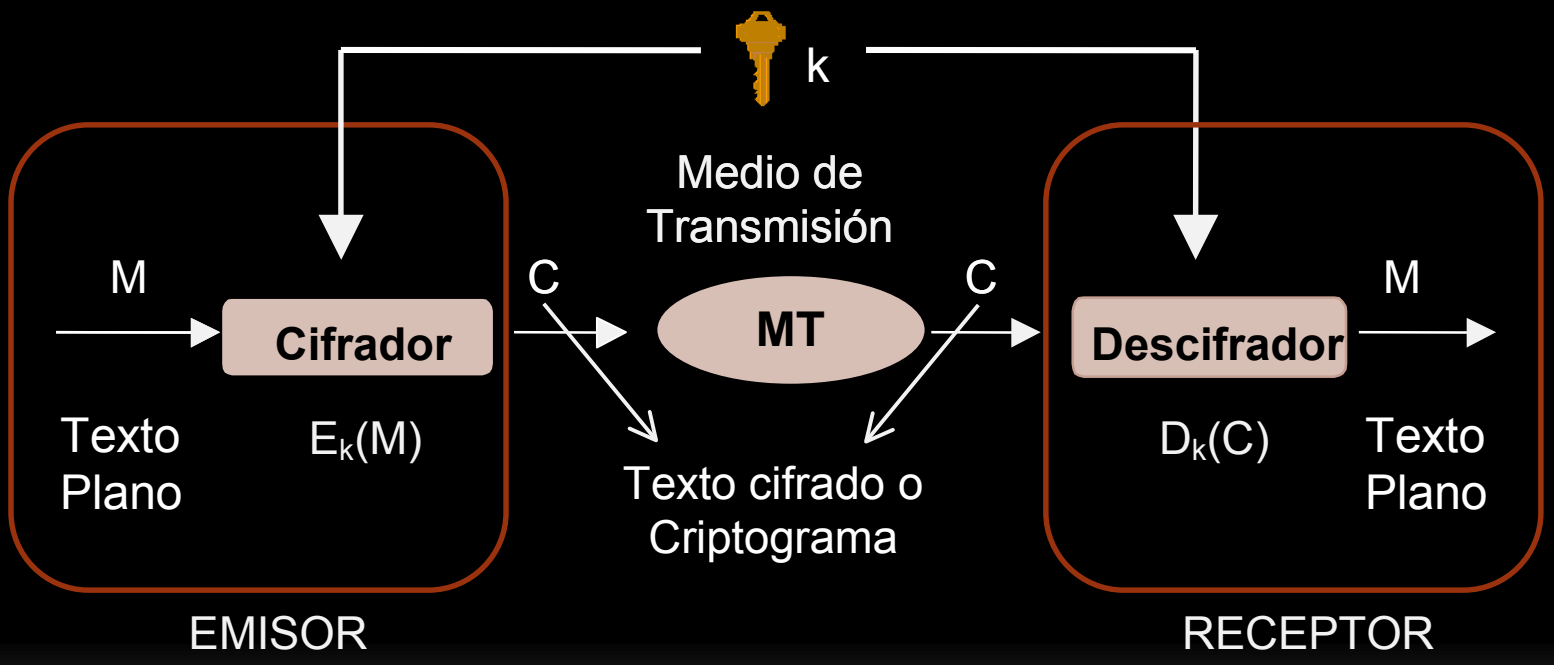
La Confidencialidad y la Integridad de la Información

- Al analizar el sistema asimétrico, veremos un concepto de mucha utilidad en criptografía .

Criptosistemas Simétricos

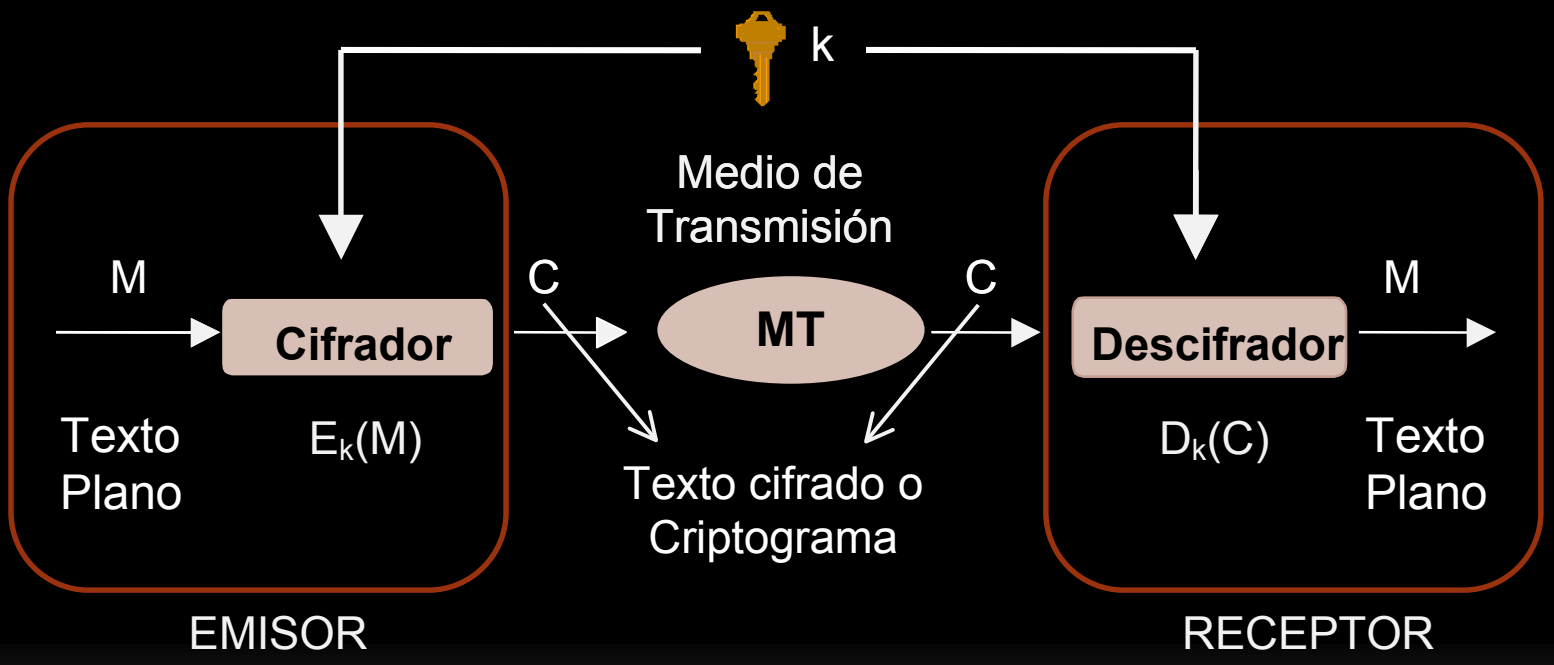
- Existe una única clave (secreta) que deben compartir emisor y receptor.
- Con la misma clave se cifra y se descifra por lo que la seguridad reside en mantener dicha clave en secreto.

Criptosistemas Simétricos



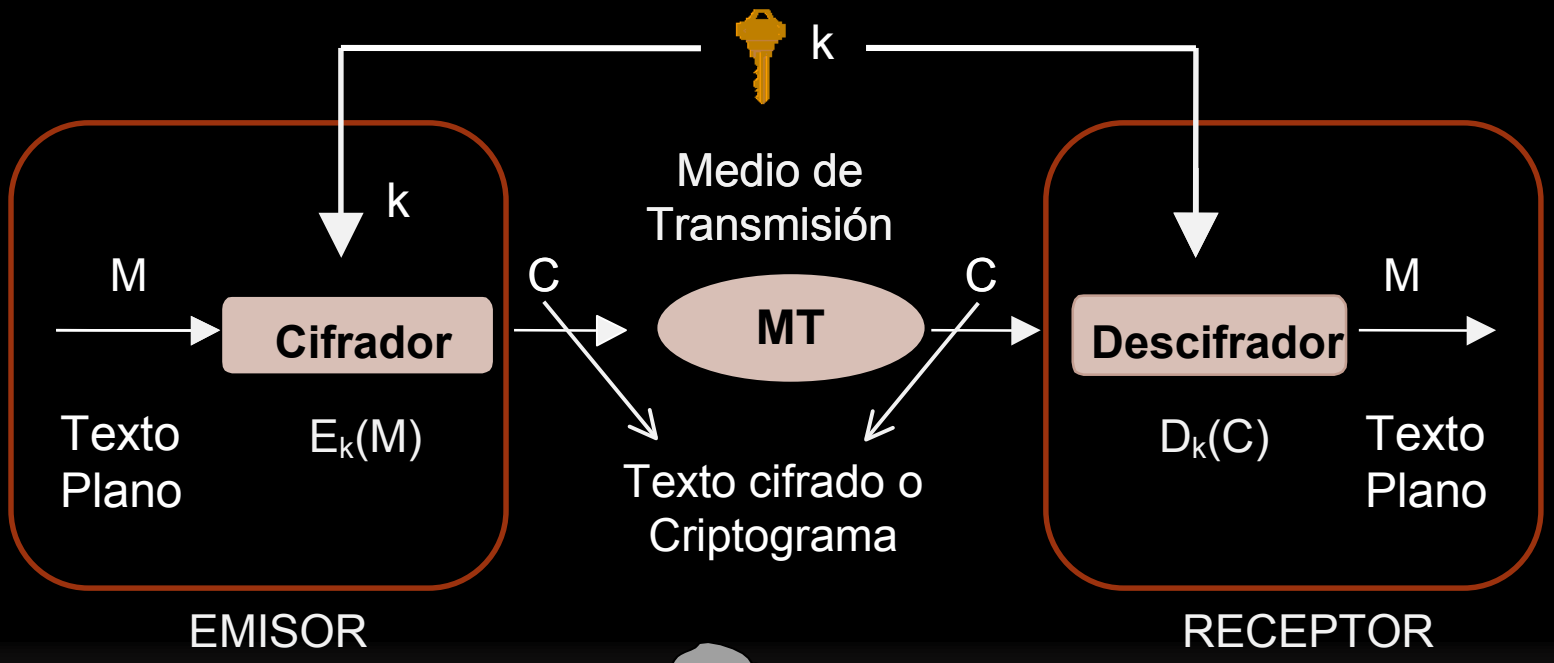
La confidencialidad y la integridad se logra si se PROTEGE LA CLAVE SECRETA.

Cripto. Simétricos: Confidencialidad



Aunque un espía vea el criptograma C, si no tiene la clave secreta k, no puede descifrarlo.

Cripto. Simétricos: Integridad

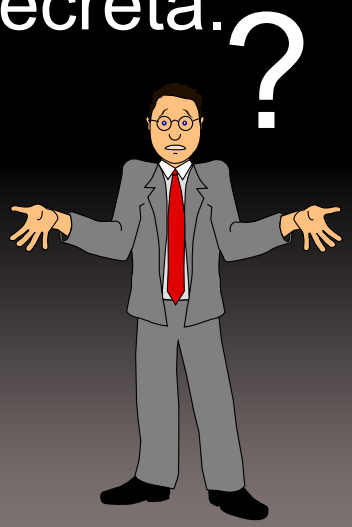


Espía

Un espía no puede cifrar un texto plano M' y enviarlo al receptor como C' = E_k(M'), si no tiene la clave secreta .

Cripto. Simétricos: Problemas

- Si se deduce la clave:
  - Se descifra la información.
  - Se crean otros textos cifrados.
- Ambas partes deben conocer la clave secreta.



Si las partes están alejadas:

¿Cómo transmitir la clave en forma segura?

Criptosistemas Asimétricos

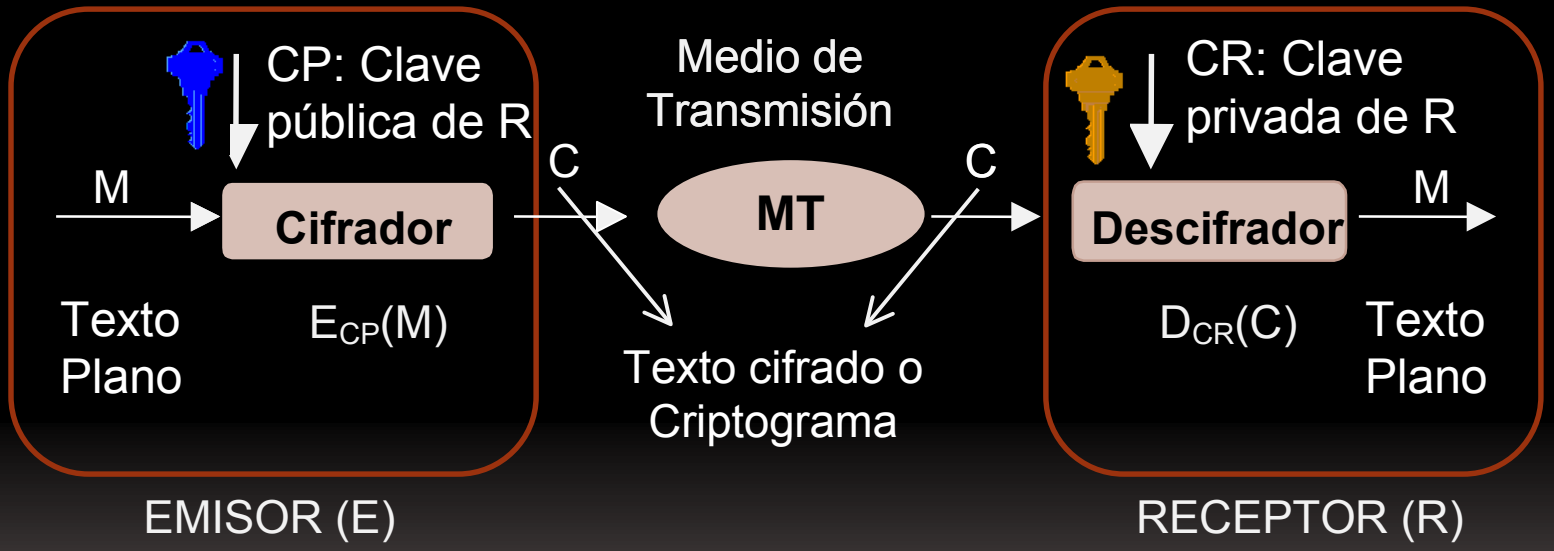
- Cada usuario tiene un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito.
- Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa.
- La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública.
- Para ello, se usan funciones matemáticas de un solo sentido.

Criptosistemas Asimétricos

- Este nuevo concepto permite lograr:
  - Confidencialidad.
  - Autenticación.
  - Firma Digital.
- Esto se logra según cómo se realice el cifrado.

Cripto. Asimétricos: Confidencialidad

- Cifrado con Clave Pública del receptor



- Se usa para el Intercambio de claves.

Autenticación y Firma Digital

- Aunque es importante mantener la confidencialidad de un mensaje, en muchos casos es más relevante poder certificar la autenticidad del emisor y el receptor.

- Se presentan algunos problemas.

Problemas de Integridad

- Autenticidad del emisor

  ¿Cómo comprueba el receptor que el mensaje recibido del emisor que dice ser X es efectivamente de esa persona?

- Integridad del mensaje

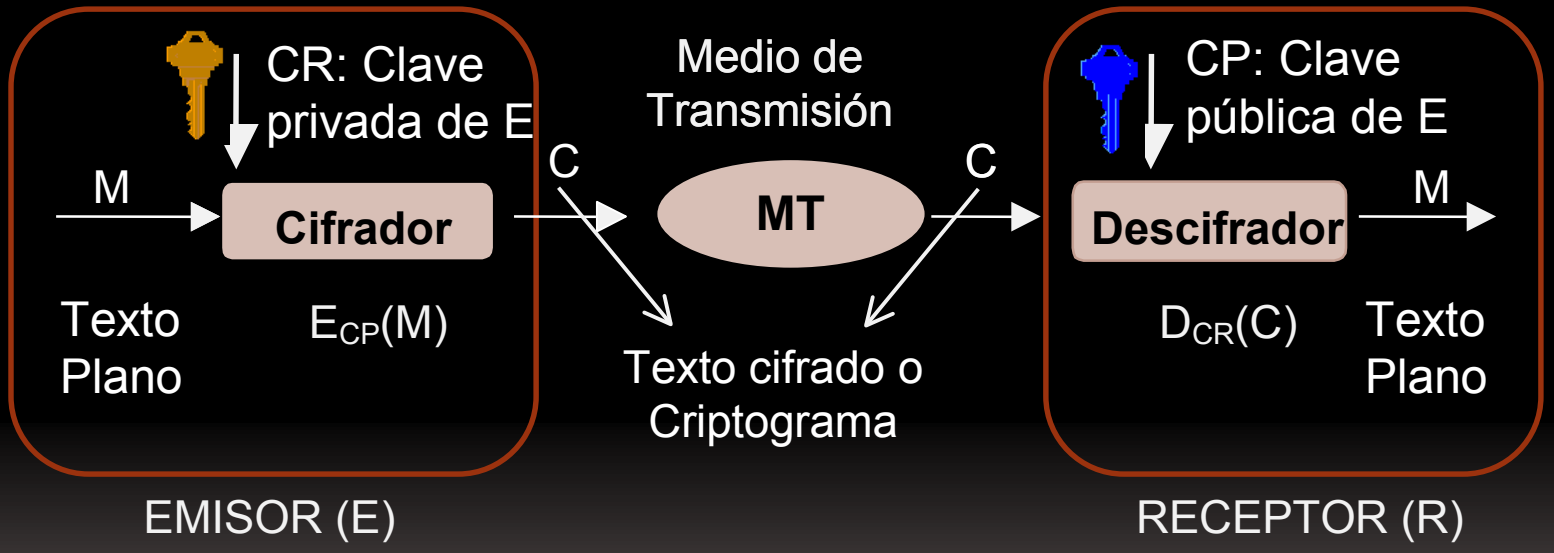
  ¿Cómo comprueba el receptor que el mensaje recibido del emisor X es el auténtico y no un mensaje falso?

- No repudio del emisor

  ¿Cómo comprueba el receptor que el mensaje enviado por el emisor –quien niega haberlo enviado- efectivamente ha llegado?

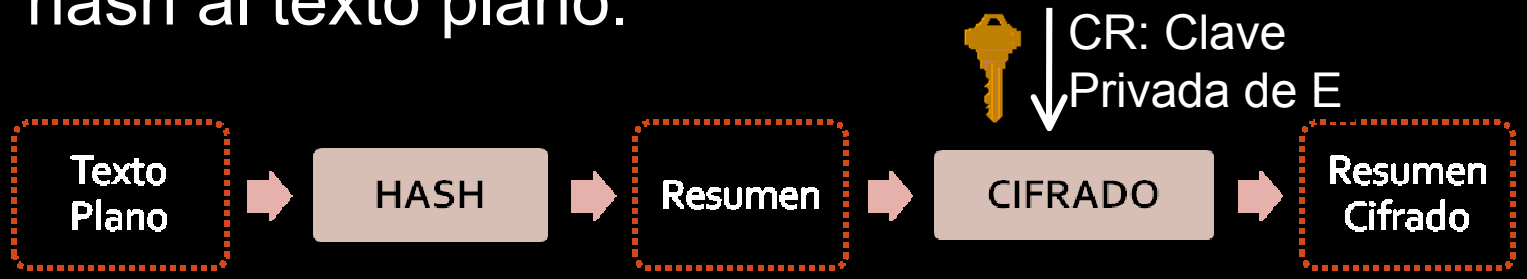
Cripto. Asimétricos: Autenticación

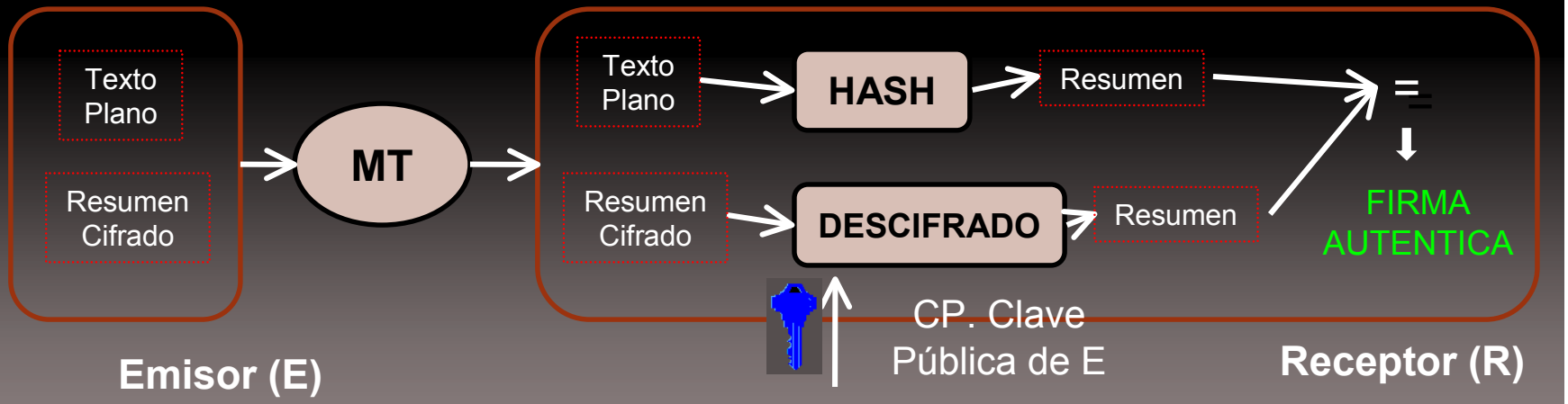
- Cifrado con Clave Privada del Emisor



Cripto. Asimétricos: Firma Digital

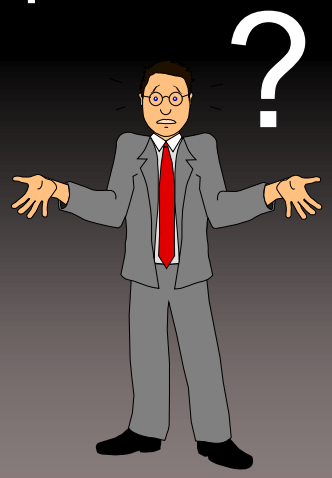
- Es similar a la Autenticación, solo que se cifra un resumen que se obtiene al aplicar una función hash al texto plano.





Simétricos vs. Asimétricos

- Los sistemas asimétricos son muy lentos pero permiten un fácil intercambio de clave y dan soporte a la firma digital.
- Los sistemas simétricos son muy rápidos pero carecen de lo anterior.



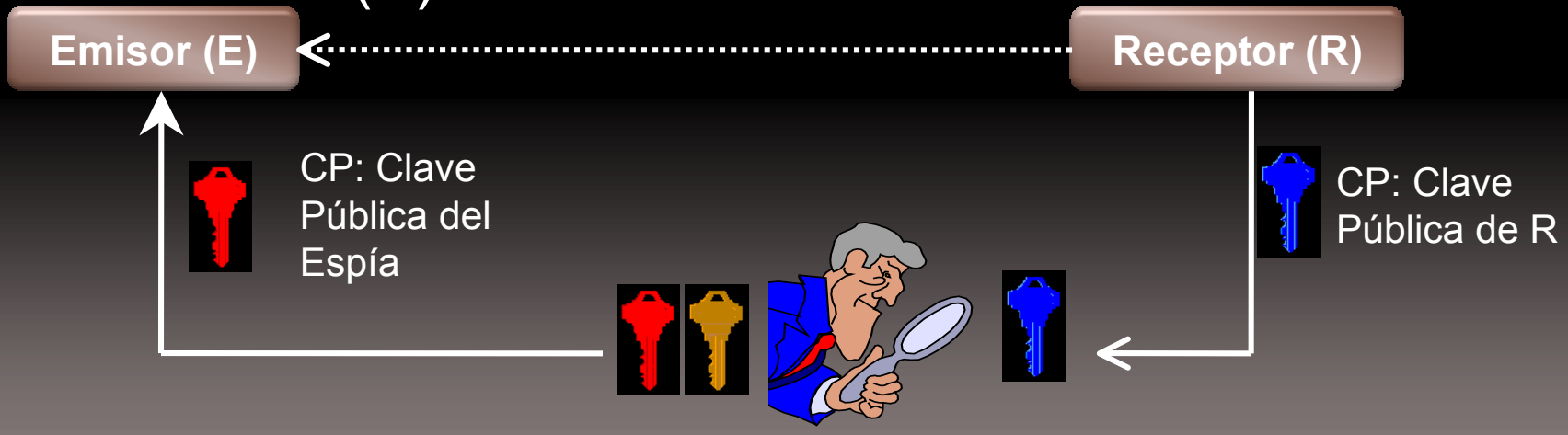
Cifrado de la información:
- Usaremos sistemas simétricos

Firma e intercambio de clave de sesión:
- Usaremos sistemas asimétricos

Certificados Digitales

- Usurpación de identidad del emisor o del receptor

¿Cómo comprueba un usuario (X) que otros usuarios están enviando mensajes firmados como él (X)?



Certificados Digitales (Cont)

Escenario de desconfianza

Solución. Uso de una tercera parte de confianza no siempre activa. Esta parte sólo actúa cuando se produce un conflicto entre los partes que se comunican.

Se usará criptografía asimétrica

En este caso la figura del juez se conoce como una Autoridad de Certificación (AC).

- Su función es certificar que una clave pública es válida y pertenece a una determinada persona.
- Se guarda la clave pública junto con información adicional en un Certificado Digital.
- El Certificado tiene la firma digital de la Autoridad de Certificación.

Certificados Digitales (Cont)

- Como emisor y receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública esté firmada por dicha autoridad.
- Una de las certificaciones más usadas y un estándar en la actualidad en infraestructuras de clave pública (PKIs) es el X.509.

Certificado Digital X.509.

- Se basa en criptografía asimétrica y usa firma digital.
- Se suministra el servicio de autenticación mediante el uso de certificados.

  - Un certificado contiene: el nombre de la AC, el nombre del usuario, la clave pública del usuario y cualquier otra información como puede ser un indicador de tiempo o *timestamp*.
  - El certificado se cifra con la clave privada de la AC.
  - Todos los usuarios poseen la clave pública de la AC.

Certificados Digitales (Cont)

- Evitan problemas de usurpación de identidad en Internet.
- Dos técnicas para conseguir nombre de usuario y clave de acceso:
  - KeyLoggers
  - Phishing.

Comercio Electrónico

- Aumento en la cantidad de operaciones comerciales a través de Internet.
- Se generan incertidumbres en las dos partes intervinientes.
- Protocolos de Comunicación que usan criptografía.

Protocolos Criptográficos

- Protocolo: es el conjunto de acciones coordinadas que realizan dos o más partes o entidades con el objeto de llevar a cabo un intercambio de datos o información.
- Protocolos criptográficos son protocolos que usan algoritmos y métodos criptográficos a los efectos de satisfacer algún objetivo específico de seguridad.
- Permiten dar una solución a distintos problemas de la vida real, especialmente en aquellos en donde puede existir un grado de desconfianza entre las partes.

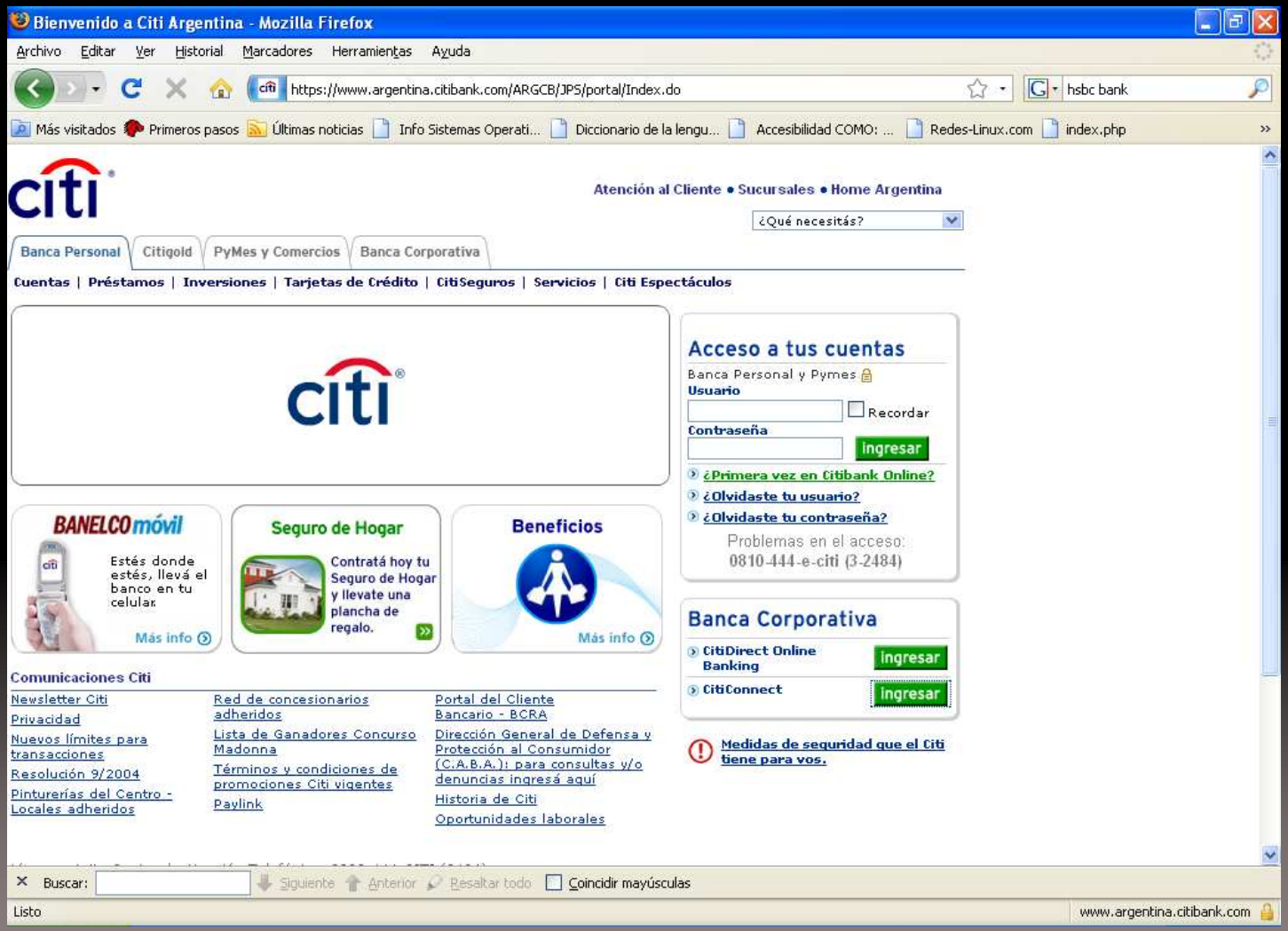
Ejemplos de Protocolos Criptográficos

- SSL
- SET
- PGP
- IPSec

SSL: Breve Introducción

- Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, y cifrando la clave de sesión de mediante un algoritmo de cifrado asimétrico.
- La clave de sesión es la que se utiliza para cifrar los datos que vienen y van al servidor seguro.
- Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea obtenida por un atacante en una transacción dada, no sirva para descifrar futuras transacciones.
- MD5 se usa como algoritmo de hash.
- SSL se inicia al seguir un enlace o abrir una página cuya dirección empieza por https://.

Ejemplo SSL


Bienvenido a Citi Argentina - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
https://www.argentina.citibank.com/ARGCB/JPS/portal/Index.do
hsbc bank
Más visitados Primeros pasos Últimas noticias Info Sistemas Operati... Diccionario de la lengu... Accesibilidad COMO: ... Redes-Linux.com index.php
citi
Atención al Cliente • Sucursales • Home Argentina
¿Qué necesitás?
Banca Personal Citigold PyMes y Comercios Banca Corporativa
Cuentas | Préstamos | Inversiones | Tarjetas de Crédito | CitiSeguros | Servicios | Citi Espectáculos
Acceso a tus cuentas
Banca Personal y Pymes
Usuario
Recordar
Contraseña
ingresar
¿Primera vez en Citibank Online?
¿Olvidaste tu usuario?
¿Olvidaste tu contraseña?
Problemas en el acceso:
0810-444-e-citi (3-2484)
BANELCO móvil
Estés donde estés, llevá el banco en tu celular.
Más info
Seguro de Hogar
Contratá hoy tu Seguro de Hogar y llevate una plancha de regalo.
Beneficios
Más info
Banca Corporativa
CitiDirect Online Banking
ingresar
CitiConnect
ingresar
Medidas de seguridad que el Citi tiene para vos.
Comunicaciones Citi
Newsletter Citi
Privacidad
Nuevos límites para transacciones
Resolución 9/2004
Pinturerías del Centro - Locales adheridos
Red de concesionarios adheridos
Lista de Ganadores Concurso Madonna
Términos y condiciones de promociones Citi vigentes
Paylink
Portal del Cliente Bancario - BCRA
Dirección General de Defensa y Protección al Consumidor (C.A.B.A.): para consultas y/o denuncias ingresá aquí
Historia de Citi
Oportunidades laborales
Buscar:
Siguiente Anterior Resaltar todo Coincidir mayúsculas
Listo
www.argentina.citibank.com

SSL y el pago electrónico

Aspectos Soportados

- Ofrece canal seguro para el envío del Nº de tarjeta de Crédito.
- Garantiza confidencialidad e integridad de los datos en tránsito.

Aspectos NO Soportados

- No Verifica validez del Nº de tarjeta y las transacciones entre los bancos.
- No asegura los datos en el servidor.
- No protege del phishing.

SET

- Asegura las transacciones por Internet que se pagan con tarjeta de crédito.
- **SET** cubre los huecos en la seguridad que deja **SSL.**
- **Requiere:**
  - **certificado digital en cada paso de autenticación**
  - **dos pares** de claves, una para el cifrado de la información de la compra que va en lo que se denomina sobre digital y otra para información de pago la firma, (**SSL solo usa** un par de claves).

SET : Servicios Ofrecidos

- **Autenticación**

  Todas las partes se autentican a través de Certificados Digitales.

- **Confidencialidad**

  El número de tarjeta de crédito es cifrado.

- **Integridad**

  La información intercambiada no puede ser alterada. Se usa Firma Digital.

PGP y el Correo Electrónico Seguro

- ¿Cómo podemos estar seguros que un mensaje enviado por correo electrónico ha sido abierto y su contenido conocido sólo por su destinatario autorizado?
- ¿Podemos enviar información confidencial por correo electrónico?

- La criptografía permite ocultar el mensaje de las miradas no autorizadas.
- Existen sistemas de Seguridad del Correo. Una opción es usar PGP (Pretty Good Privacy)

PGP y el correo electrónico seguro (Cont)

- PGP permite el cifrado del contenido del mensaje.
- Es un sistema que hace uso de la criptografía asimétrica y simétrica.
- Suministra los servicios de:
  - Integridad
  - Confidencialidad
  - Autenticación
  - No repudio

Conclusión

- Debemos estar conscientes de los riesgos a los que nos exponemos al usar e intercambiar información en formato digital.
- La Criptografía es una herramienta muy valiosa que nos permite proteger y preservar la información importante.
- Es una herramienta que está al alcance de todos.

¡MUCHAS GRACIAS!