Seguridad en Sistemas de Información

Dr. Luis Gerardo de la Fraga

Departamento de Computación
Cinvestav
E-mail: fraga@cs.cinvestav.mx

25-26 Octubre, 2011

Seguridad en Sistemas de Información

Modelo de capas para sistemas de seguridad

Aplicaciones:
Correo electrónico seguro, monedero digital, redes virtuales, elecciones electrónicas

Protocolos de comunicación:
SSL/TLS/WTLS, IPSEC para IPv4, IEEE 802.11, etc.

Serviciones de seguridad: Confidencialidad, integridad de datos, autenticación, no-repudio.

Funciones criptográficas:
cifrar/decifrar, firmar/verificar

Algoritmos de llave pública: RSA, ECC
Algoritmos de llave simétrica: AES, DES, RC4, etc.

Aritmética computacional:
suma, elevar al cuadrado, multiplicación, inversión y exponenciación.

http://cs.cinvestav.mx/~francisco/ssi/ssi11.html

Dilema fundamental de la seguridad

- Usuarios sin conciencia de la seguridad tienen demandas específicas pero sin tener ningún conocimiento técnico
- Solución: Niveles de seguridad predefinidos y clasificados con algún grupo de criterios.

Tres leyes de la seguridad

- No existen sistemas totalmente seguros
- Para reducir su vulnerabilidad a la mitad se tiene que doblar el gasto de seguridad
- Típicamente, los intrusos brincan la criptografía, no la rompen.

Recursos y métodos de ataque

Recurso	Adolescente	Académico	Crimen Org.	Gobiernos
Tiempo	limitado	moderado	mucho	mucho
Presupuesto	<$1000	$10K–$100K	$100K+	¿?
Creatividad	varía	alta	varía	varía
Detectabilidad	alta	alta	baja	baja
Objetivo	reto	publicidad	dinero	varía
Número	muchos	moderado	pocos	¿?
Organizado	no	no	sí	sí
Dist. info?	sí	sí	varía	no

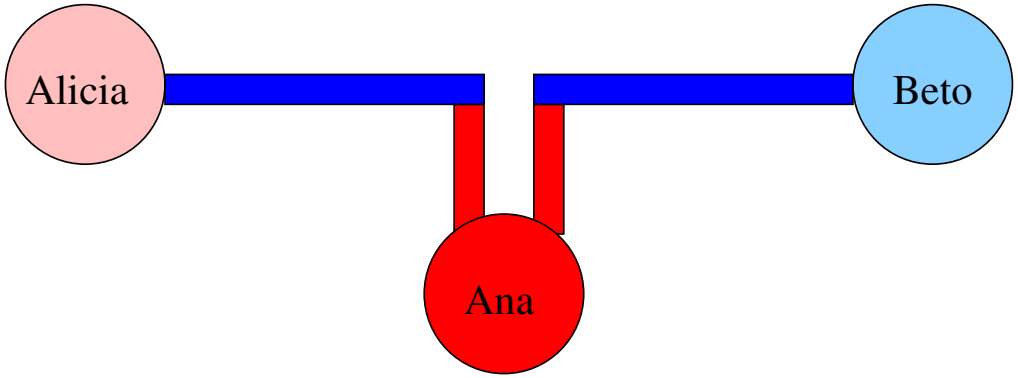
Source: Cryptography Research, Inc. 1999, "Crypto Due Diligence"

Ataques a la seguridad: activos y pasivos

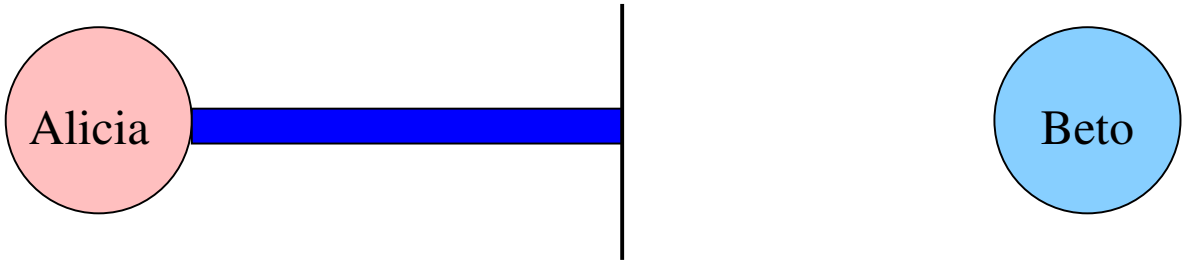
- Activos
  - Suplantación de identidad
  - Retransmitir (replay)
  - Modificación de mensaje
  - Denegación de servicio
- Pasivos
  - Análisis de tráfico
  - Distribución no autorizada de la información

Ataques activos

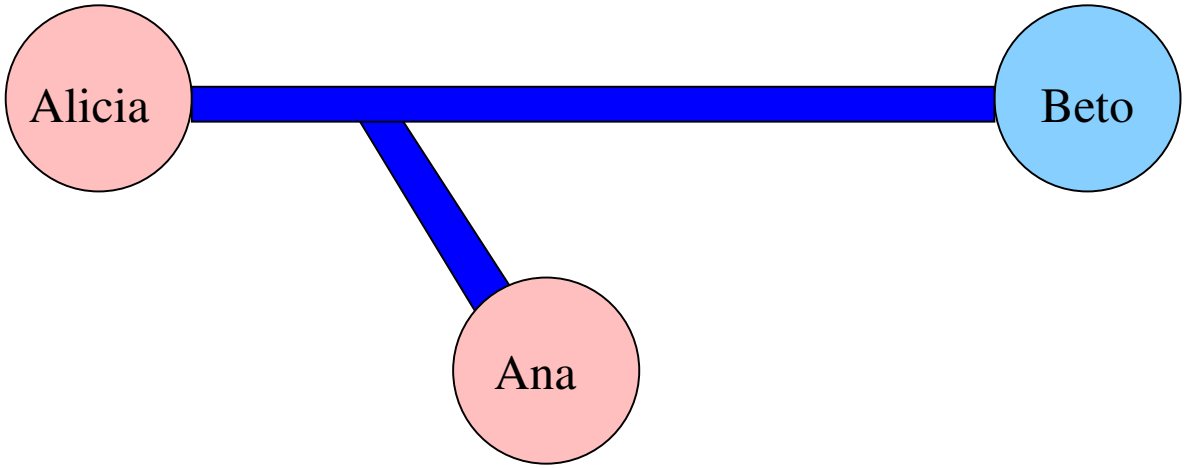
- Interrupción
- Intercepción
- Modificación
- Fabricación



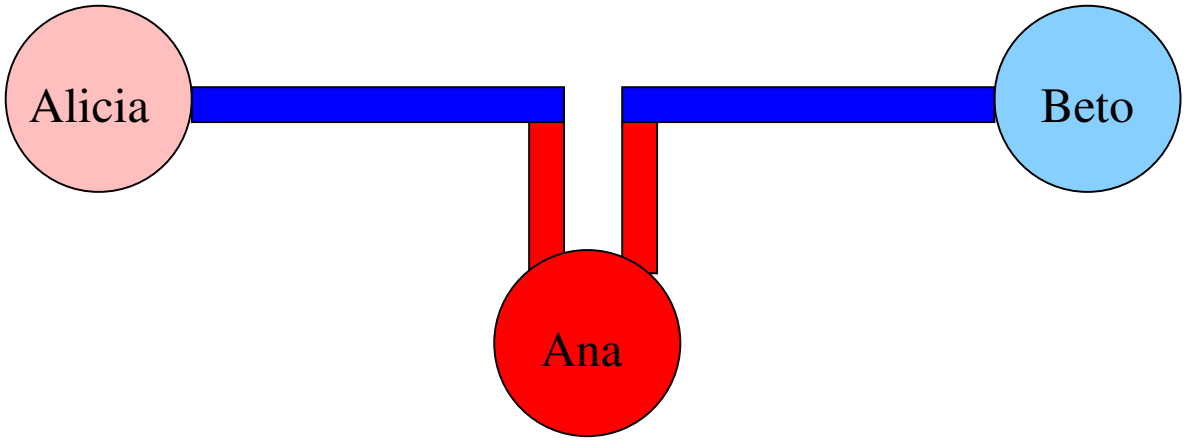
Ataques activos: Interrupción (Disponibilidad)



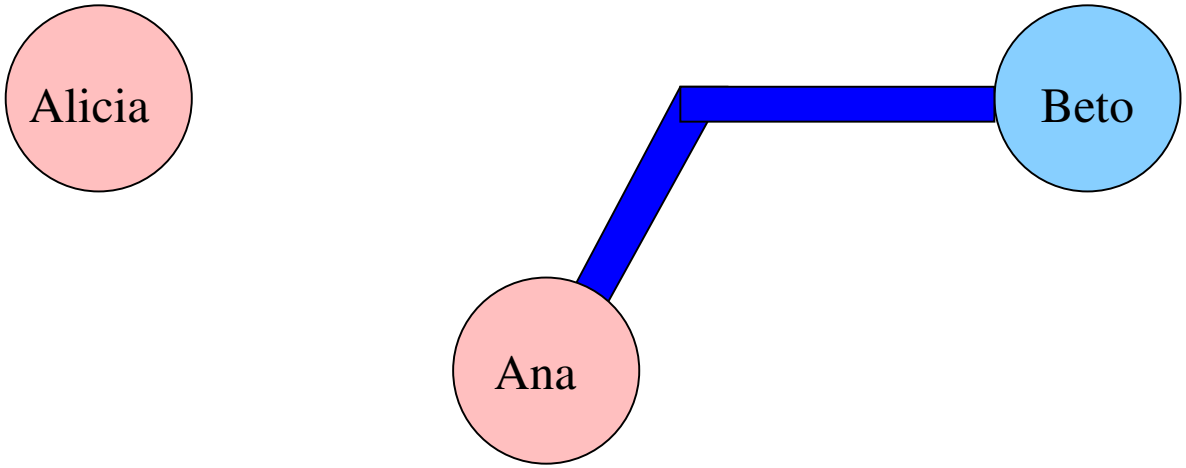
Ataques activos: Intercepción (Confidencialidad)



Ataques activos: Modificación (Integridad)



Ataques activos: Fabricación (Autenticidad)



Ataques: accidental, intencional

- Accidental
  - Errores de software
  - Errores de hardware
  - Administración mala
- Intencional
  - Pasivos
  - Activos

Servicios de seguridad (1/3)

- Confidencialidad
- Autenticación
- Integridad
- No-repudio
- Control de acceso
- Disponibilidad

Servicios de seguridad (2/3)

- **Confidencialidad** – La confidencialidad asegura que la información sensible solo podrá ser consultada o manipulada por usuarios, entidades o procesos autorizados.
- **Integridad** – La integridad da la certeza de que la información no ha sido modificada por entidades no autorizadas para hacerlo. Dentro de la posibles modificaciones están la escritura, modificación o borrado de segmentos de datos.

Servicios de seguridad (3/3)

- **Autenticación –** La autenticación asegura que la identidad de los participantes es verdadera. Se pueden evaluar tres aspectos para autenticar usuarios: verificar algo que el usuario *tiene*; poner a prueba al usuario sobre algo que *sabe*, esto es, pedirle una contraseña y, finalmente, el tercer aspecto es verificar algo que el usuario *es*, por ejemplo, analizar sus huellas dactilares o su retina.
- **No repudio –** El no repudio ofrece protección a un usuario o entidad frente a que otro usuario niegue posteriormente que en realidad se realizó cierta transacción.

Tipos de autenticación (1/3)

- Del mensaje
- De la entidad
- De la llave
- De la transacción

Tipos de autenticación (2/3)

- **Del mensaje** – Consiste en la verificación de que una de las partes es la fuente original del mensaje, es decir, autentica la procedencia de un mensaje. Este tipo de autenticación asegura la integridad del mensaje.
- **De la entidad** – Consiste en el proceso donde una parte se asegura de la identidad de la segunda parte involucrada en el protocolo de comunicación.

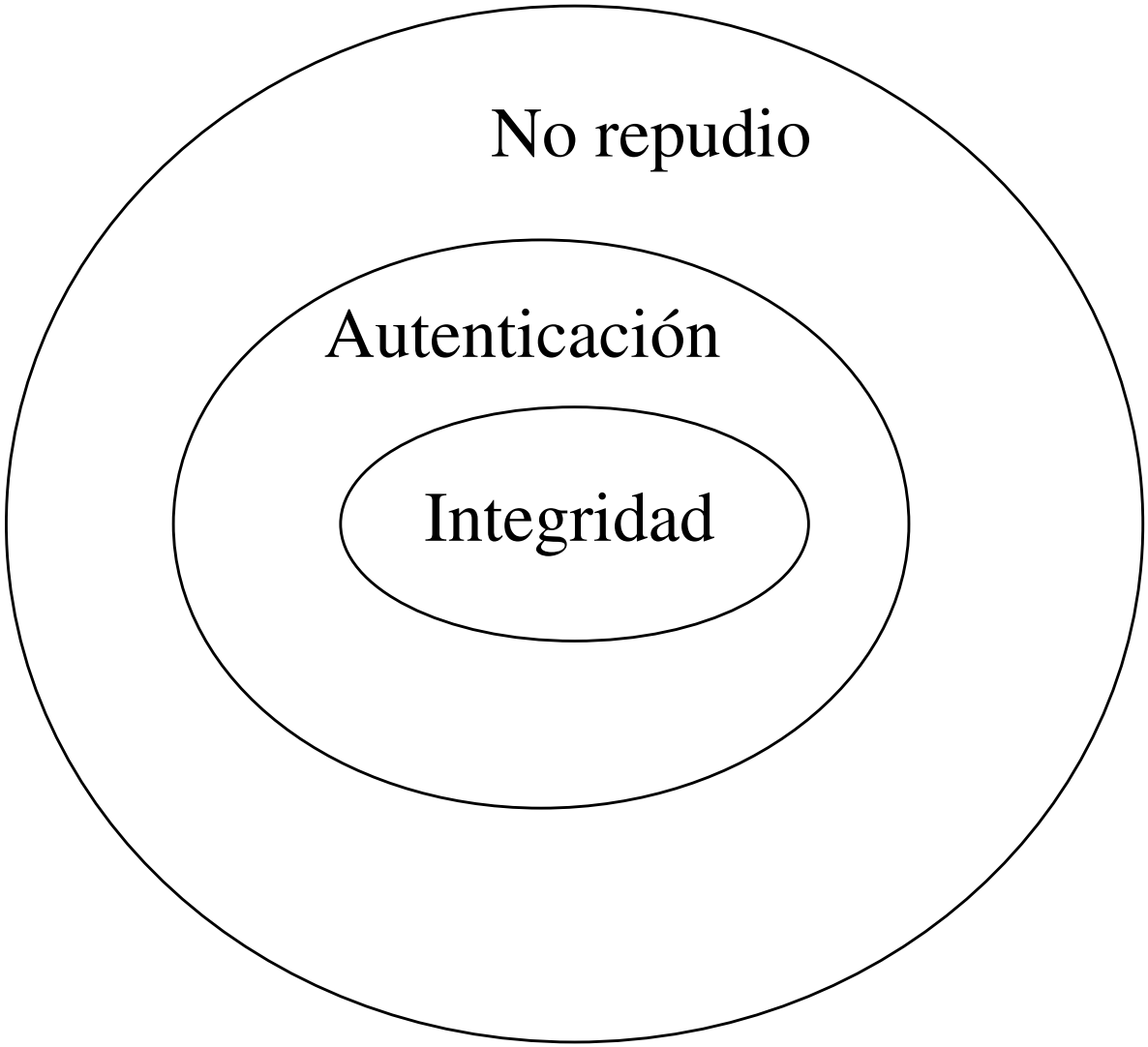
Tipos de autenticación (3/3)

- **De la llave –** Este tipo de autenticación permite que una parte se asegure que ninguna otra entidad no confiable pueda tener acceso a la llave privada correspondiente.
- **De la transacción –** Este tipo de autenticación provee autenticación de mensaje y además garantiza la existencia única y temporal de los datos.

Propiedades de los tipos de autenticación

Propiedades Autenticación	Identificación de origen	Identificación de datos	Tiempo o unicidad
Aut. mensaje	Ok	Ok	–
Aut. de transacción	Ok	Ok	Ok
Aut. de entidad	Ok	–	Ok
Aut. llave	Ok	Ok	deseable

Relación de los servicios



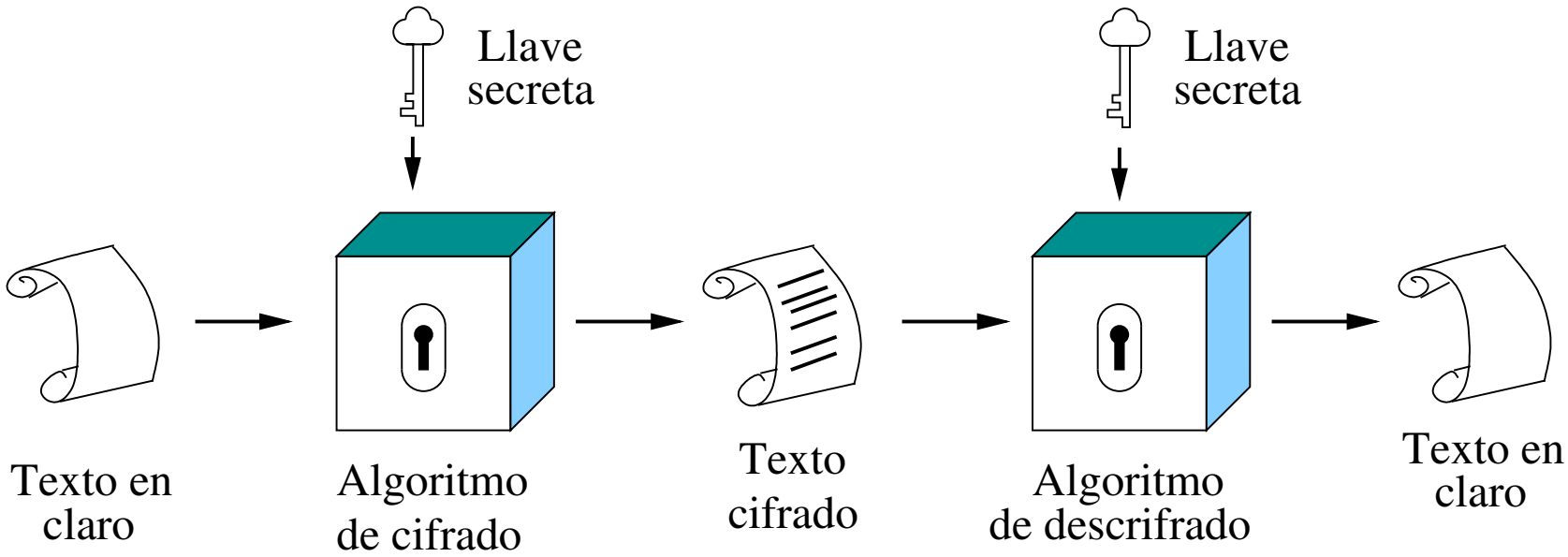
Bloques básicos

- **Cifrado/descifrado –**
  Proveen confidencialidad, puede proveer autenticación e integridad de datos.
- **Funciones hash –**
  Proveen protección de integridad, pueden proveer autenticación
- **Firmas digitales –**
  Proveen autenticación, protección de integridad y no-repudio.

Llaves

1. De llave privada (o llave secreta)
2. De llaves pública y privada

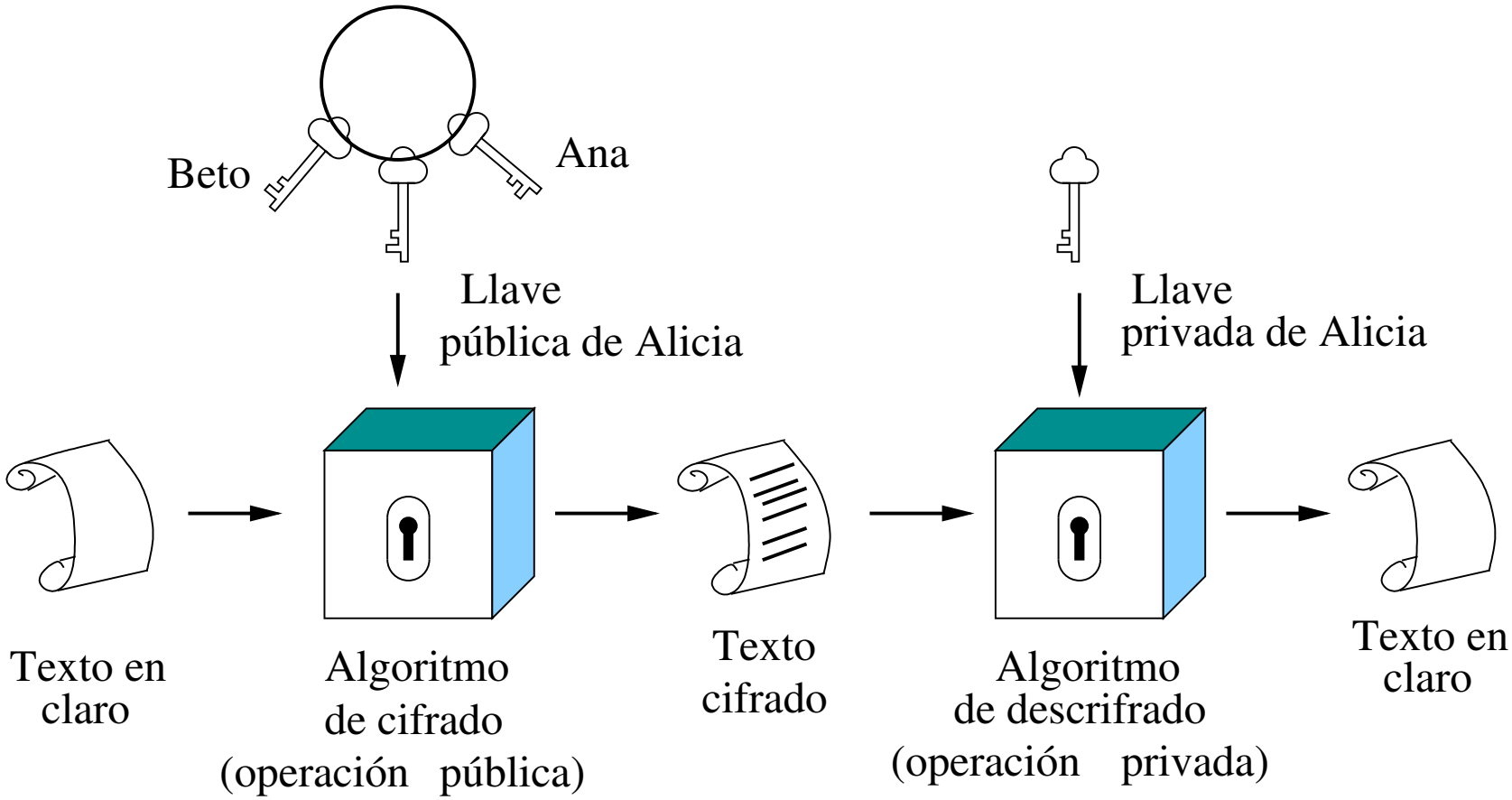
Criptografía de llave secreta (1/2)



Criptografía de llave secreta (2/2)

- Usa algoritmos altamente eficientes.
- Ambas partes convienen e compartir el mismo secreto
- Desventajas: un problema importante es la distribución de las llaves. En un sistema con n usuarios se necesitan generar $n(n-1)$ llaves.
- La administración de llaves tiende a ser un problema.
- Algoritmos utilizados:
  - DES - 56 bit key
  - 3DES usa tres llaves DES
  - IDEA 128 bits
  - AES fue escogido como el nuevo estándar de cifrado en el año 2000.

Criptografía de llave pública (1/2)



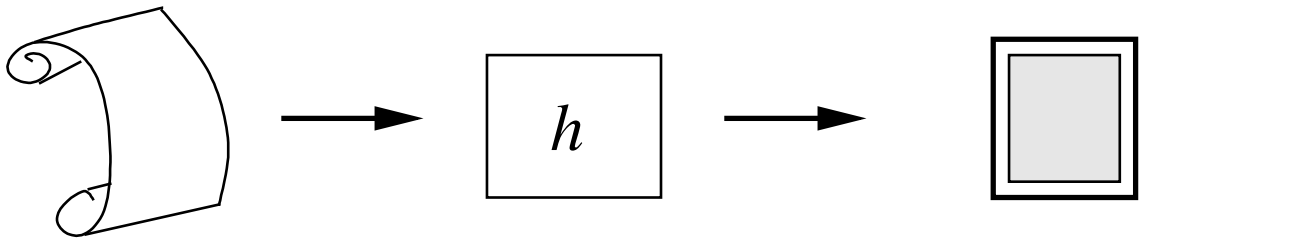
Criptografía de llave pública (2/2)

- Los algoritmos consumen alto tiempo de cómputo
- Las llaves privadas son conocidas sólo por los legítimos dueños.
- Las llaves públicas son almacenadas en certificados (estándar X.509).
- Algoritmos: RSA, ECC.

Funciones hash

Usados para:

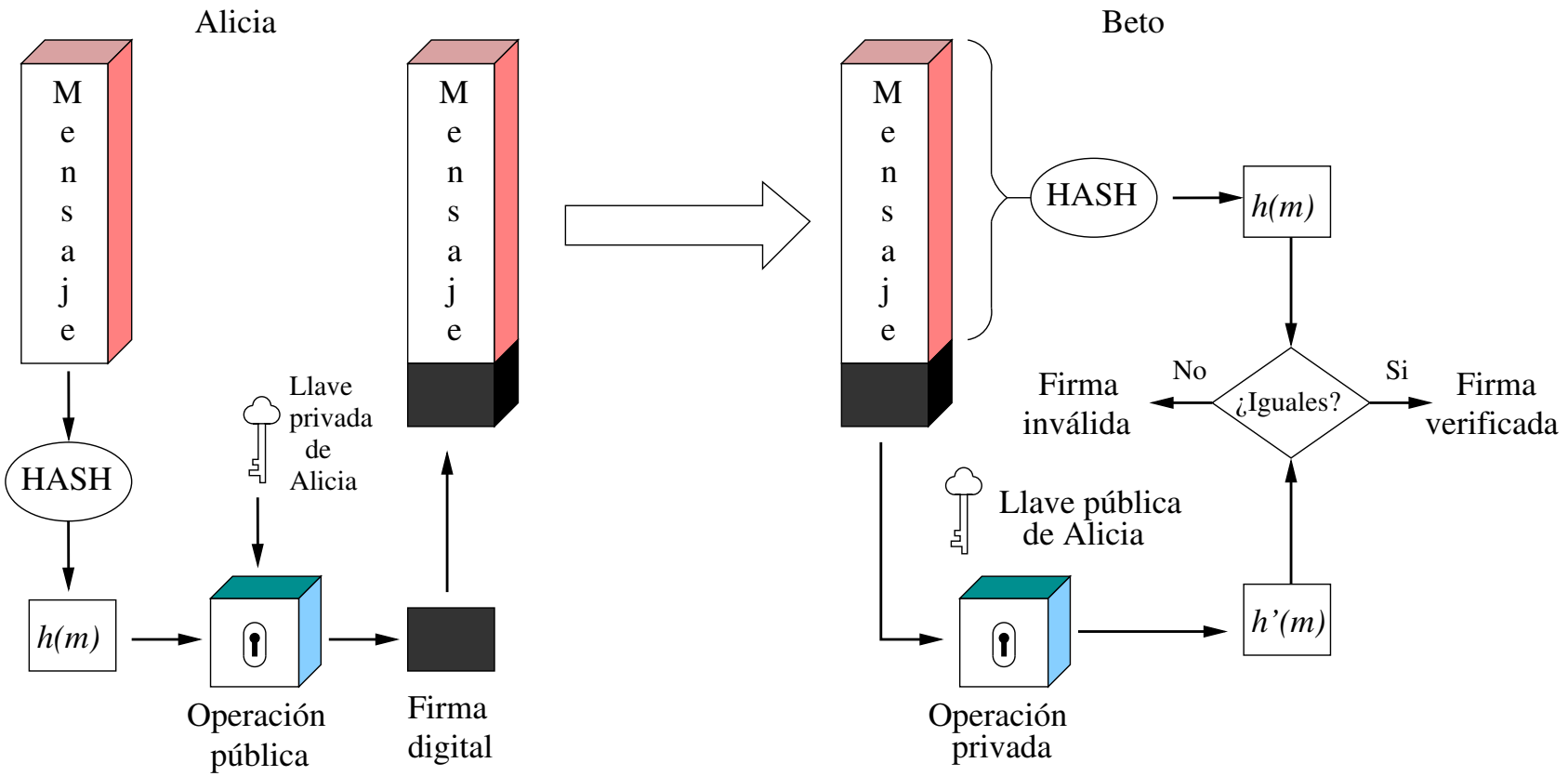
- Producir huellas digitales de longitud fija para documentos de longitud arbitraria
- Producir información útil para detectar modificaciones maliciosas
- Traducir contraseñas a salidas de longitud fija.



Texto en claro

Digesto o resumen (de longitud fija)

Firma digitales



Seguridad en un GIS

- Se debe analizar que servicios de seguridad se requieren
- No hay una solución fácil, rápida y barata.
- ¿Son los datos públicos? ¿Son privados? (confidencialidad)
- ¿Solo se permite usar al GIS a determinados usuarios? (autenticación)
- ¿Se tienen varios proveedores certificados? (autenticación)
- ¿Deben garantizarse las transacciones? (no repudio)
- ¿El almacenamiento de los datos no es confiable? (todos los servicios en una base de datos encriptada en un proveedor que no es confiable)