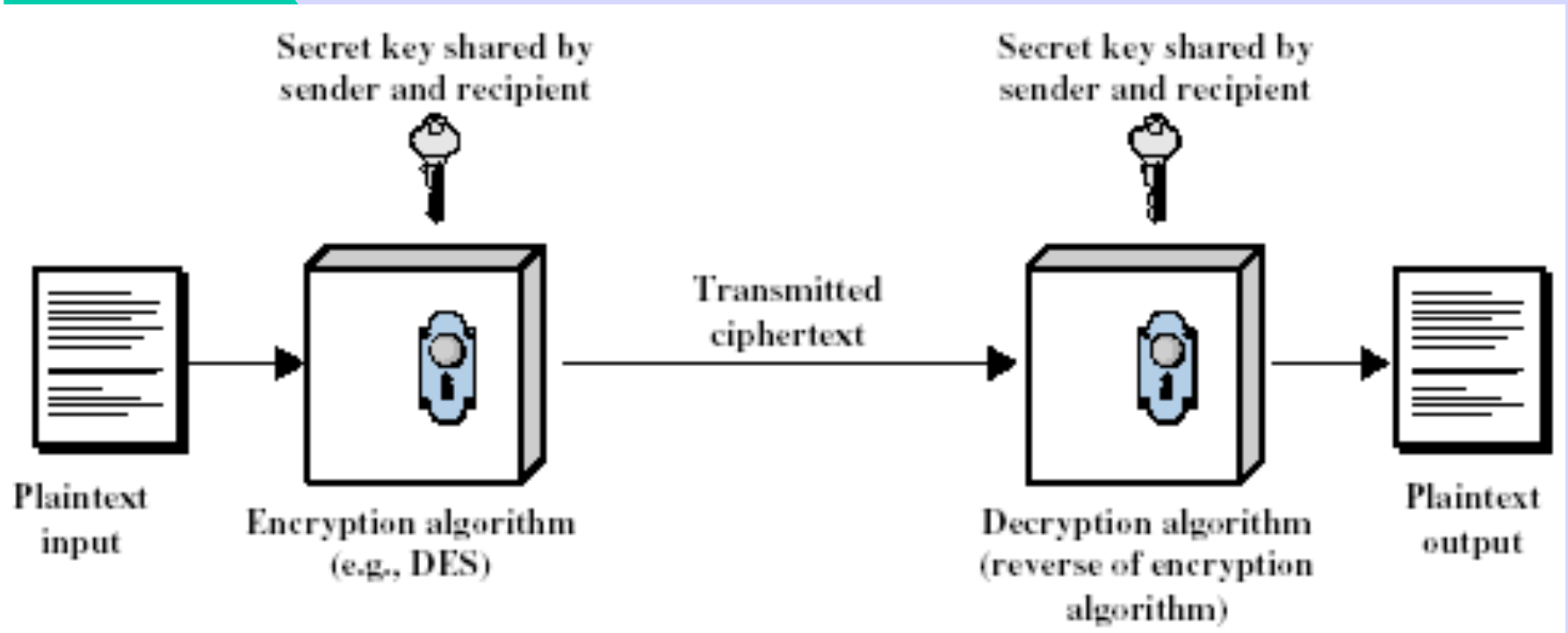
Introducción a la Seguridad en Sistemas Informáticos

Francisco Rodríguez-Henríquez
CINVESTAV-IPN
Depto. de Ingeniería Eléctrica
Sección de Computación

Motivación y Antecedentes

Modelo simplificado de Cifrado



Fundamentos de Seguridad Informática

Cryptografía

- Mecanismos y algoritmos básicos para la
- Protección de la información.

Protocolos Seguros

- Servicios de Autenticación
- Comunicaciones seguras y transacciones

PKI – Infraestructura de Llave Pública

- Generación, distribución y administración de certificados de llave pública.

Políticas de Administración de Servicios

- Servicios de autorización y control de acceso
- Políticas y normas de seguridad
- ...

Recursos y Métodos de Ataques

Recurso	Adolescente	Académico	Org. Crimen	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

Seguridad: Amenazas y Ataques

Las amenazas pueden provenir de varias fuentes, pudiendo ser clasificadas como:

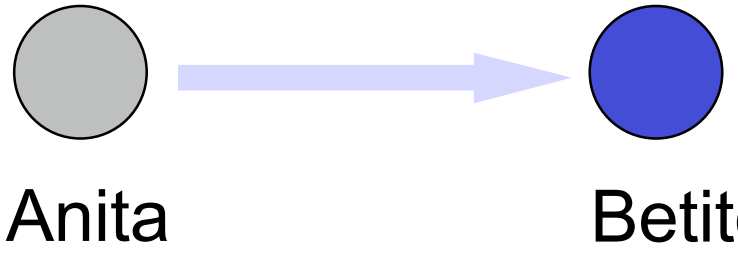
- 55% errores humanos
- 10% empleados insatisfechos
- 10% empleados corruptos
- 10% acceso exterior
- accidentes/incidentes (fuego, terremoto, etc)

Ataques a la Seguridad: Activos y Pasivos

- Activo
  - Mascarada (impersonar)
  - Replay
  - Modificación del mensaje
  - Denegación de servicio (DoS)
- Pasivo
  - Análisis de tráfico
  - distribución no autorizada de la información

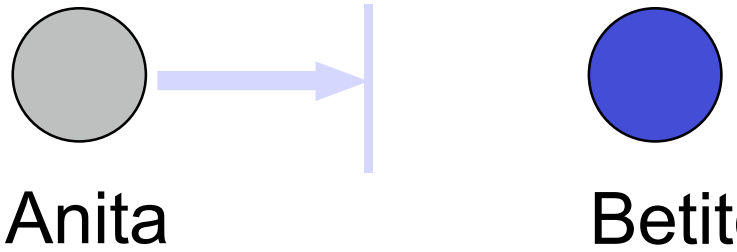
Clases de Ataques a la Seguridad

- Interruption
- Interception
- Modification
- Fabrication



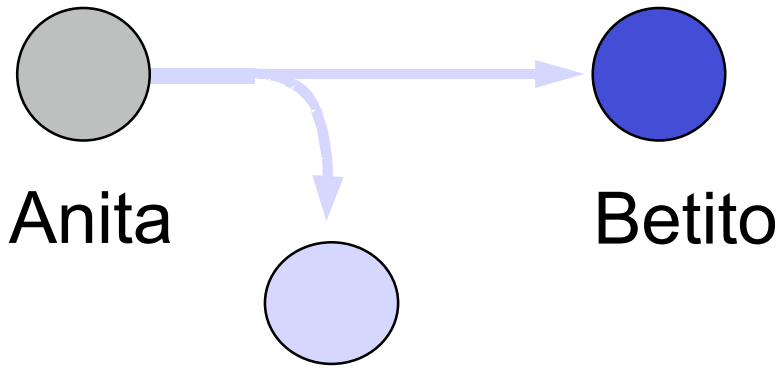
Clases de Ataques a la Seguridad: Interrupción

- Interrupción
  - Disponibilidad
- Intercepción
- Modificación
- Fabricación



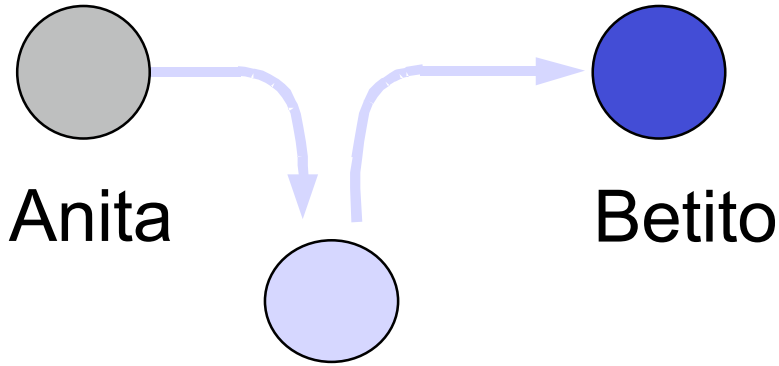
Clases de Ataques a la Seguridad: Intercepción

- Interrupción
- Intercepción
  - Confidencialidad
- Modificación
- Fabricación



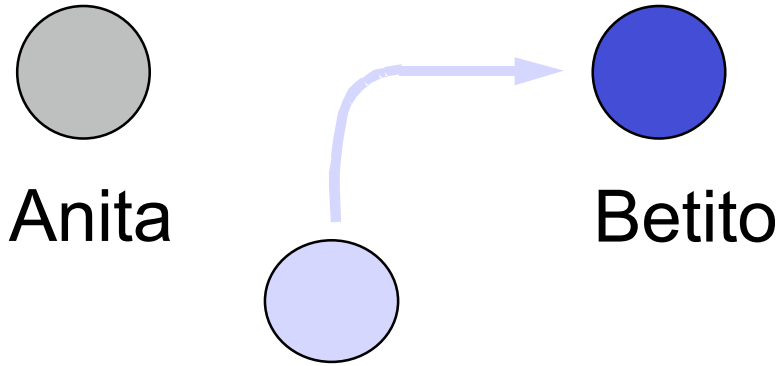
Clases de Ataques a la Seguridad: Modificación

- Interrupción
- Intercepción
- Modificación
  - Integridad
- Fabricación



Clases de Ataques a la Seguridad: Fabricación

- Interrupción
- Intercepción
- Modificación
- Fabricación
  - Autenticidad

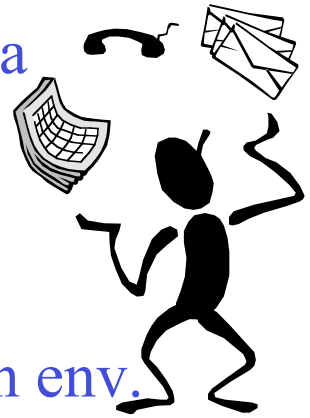


Aplicaciones y Servicios

Francisco Rodríguez Henríquez

Servicios de Seguridad

- Confidencialidad - protege el valor de la información
- Autenticación - protege el origen de la información
- Identificación - asegura la identidad de los usuarios
- Integridad - protege la validez de la copia
- No-repudio - impide repudiar un envío
- Cont. de acceso - acceso a recursos/datos
- Disponibilidad - asegura que los datos puedan env.

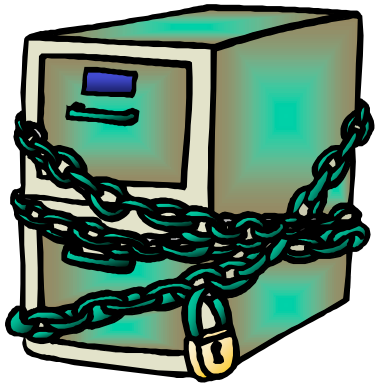


Algunas Aplicaciones Prácticas

"Any sufficiently advanced technology is indistinguishable from magic."

Arthur C. Clarke.

- e-mail seguro
- comunicaciones seguras
- autenticación de red
- elecciones electrónicas
- notario electrónico
- monedero digital
- distribución de datos



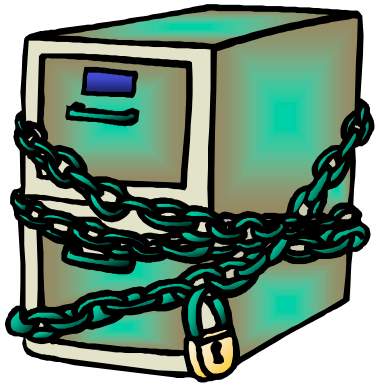
Secure Mail: PGP (Pretty Good Privacy)

- Pretty Good Privacy (PGP) fue creado por Philip R. Zimmermann. El gobierno estadounidense le entabló juicio por más de tres años debido a que Zimmermann se empeñó en que PGP fuera freeware.
- A pesar de la persecución PPG se convirtió pronto en el programa de email seguro más usado en todo el mundo.
- PGP sigue siendo freeware.

PGP puede ser obtenido en:http://web.mit.edu/network/pgp.html

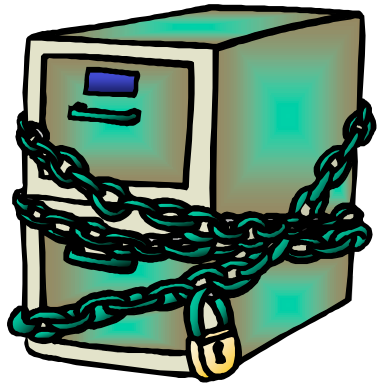
Comunicaciones Seguras

- Escenarios
  - Securidad para enlaces electrónicos en tiempo real
  - Redes de área local
  - Enlaces seguros
  - Comunicación en celulares, faxes, teléfonos, etc.
- Objetivos
  - privacidad
  - autenticación
  - no-repudio
- Herramientas
  - Protocolos de intercambio de llaves
  - Criptosistemas de llave secreta
  - Criptosistemas de llave pública
  - Firmas digitales
  - certificados



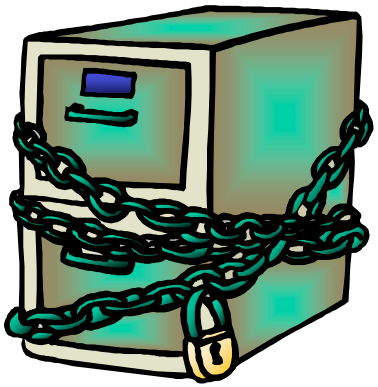
Distribución de Datos

- Escenarios
  - Acceso condicional a TV
  - distribución software vía CD-ROM
  - Boletines de información
- Goals
  - operación de transmisión (TV, CD-ROM)
  - privacidad de mensajes
  - Recepción selectiva
- Tools
  - criptografía de llave secreta
  - Criptografía de llave pública
  - Hardware seguro



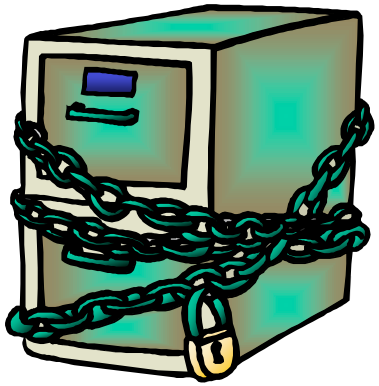
Elecciones Electrónicas

- Escenarios
  - Elecciones generales
  - Reuniones de accionistas
  - Computación distribuida segura
- Objetivos
  - anonimato
  - Sistema justo
  - Sistema auditable
- Herramientas
  - Algoritmo RSA
  - Firmas a ciegas
  - Protocolos seguros no rastreables



Monedero Digital

- Escenarios
  - Reemplazo del papel moneda
  - Mayor flexibilidad que las tarjetas de crédito
- Objetivos
  - anonimato
  - Protocolos no rastreables
  - Sistema justo
  - divisibilidad
  - Propiedad de transferencia
  - Operaciones off-line
  - universabilidad
- Tools
  - Protocolos de conocimiento cero
  - Hardware seguro
  - Algoritmo RSA



Seguridad: Bloques Básicos

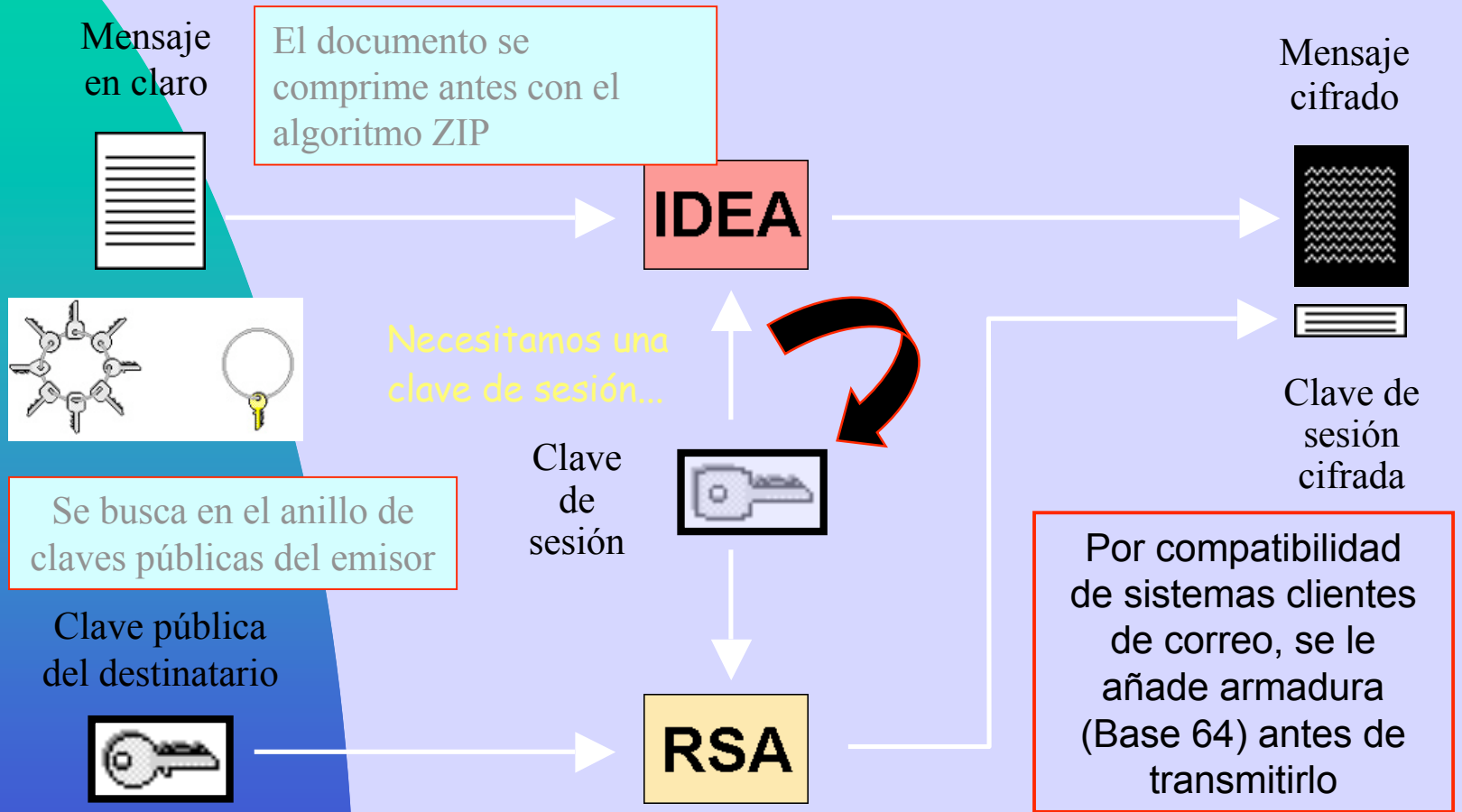
- Cifrado/descifrado provee:
  - confidencialidad, puede proveer autenticación e integridad de datos.
- Algoritmos Checksums/hash proveen:
  - Protección de integridad, puede proveer autenticación
- Firmas Digitales proveen:
  - autenticación, protección de integridad, y no-repudio.

Criptografía de llave secreta

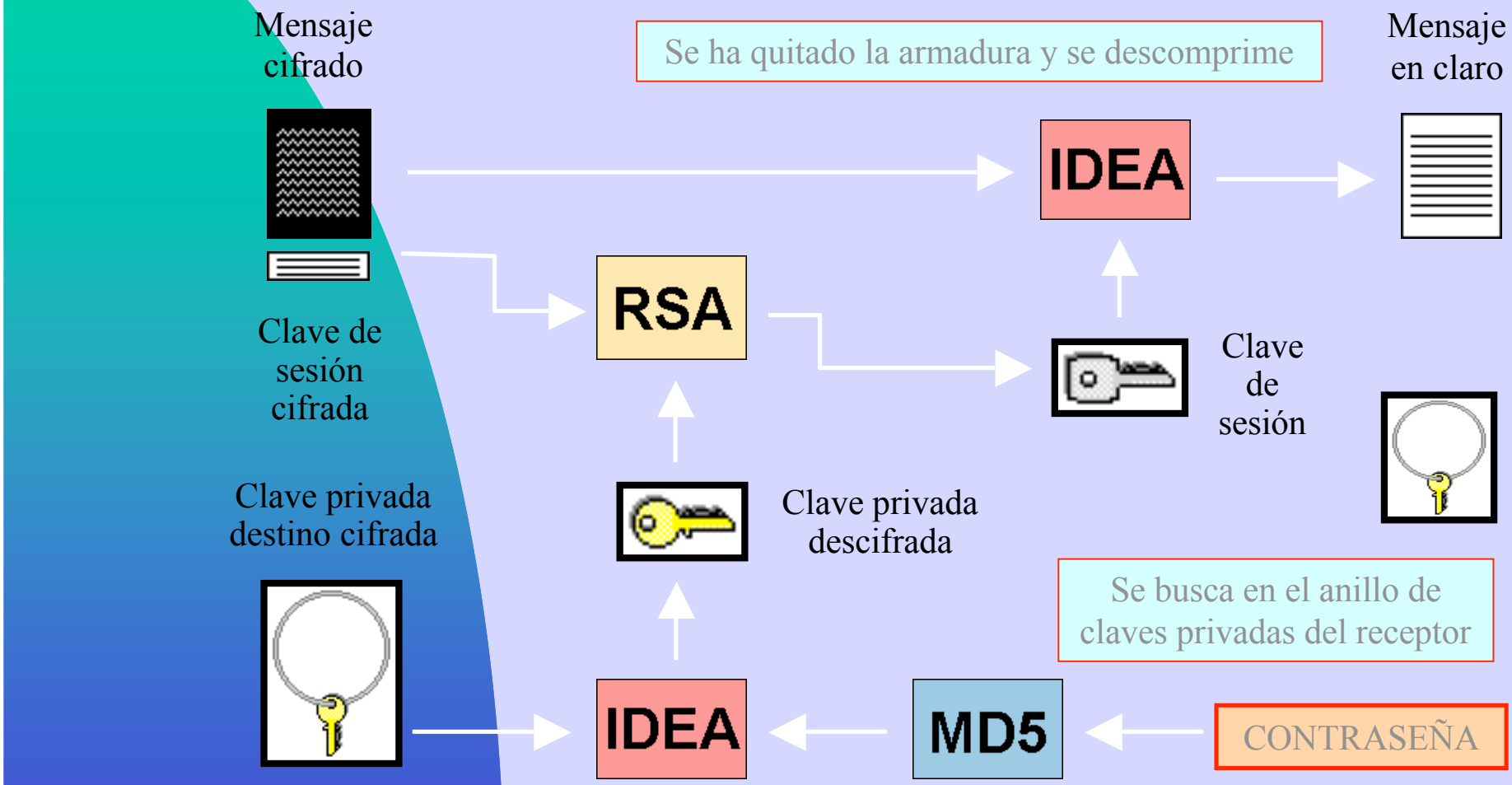
Llaves

- Llaves Simétricas
  - Ambas partes comparten el mismo secreto
  - Un problema importante es la distribución de las llaves.
  - DES - 56 bit key
  - 3DES usa tres llaves DES
  - IDEA 128 bits
  - AES fue escogido como el nuevo estándar de cifrado en el 2000.

Cifrado con clave pública de destino



Descifrado con la clave privada de destino



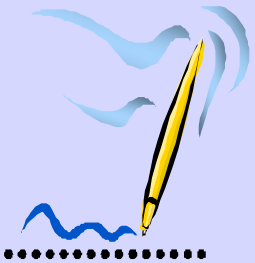
Criptografía de llave pública

Llaves

- Llave pública/privada
  - Una llave es el inverso matemático de la otra
  - Las llaves privadas son conocidas sólo por los legítimos dueños.
  - Las llaves públicas son almacenadas en certificados (estándar X.509).
  - Algoritmos: RSA , Diffie-Hellman, DSA

Digestión de Mensajes

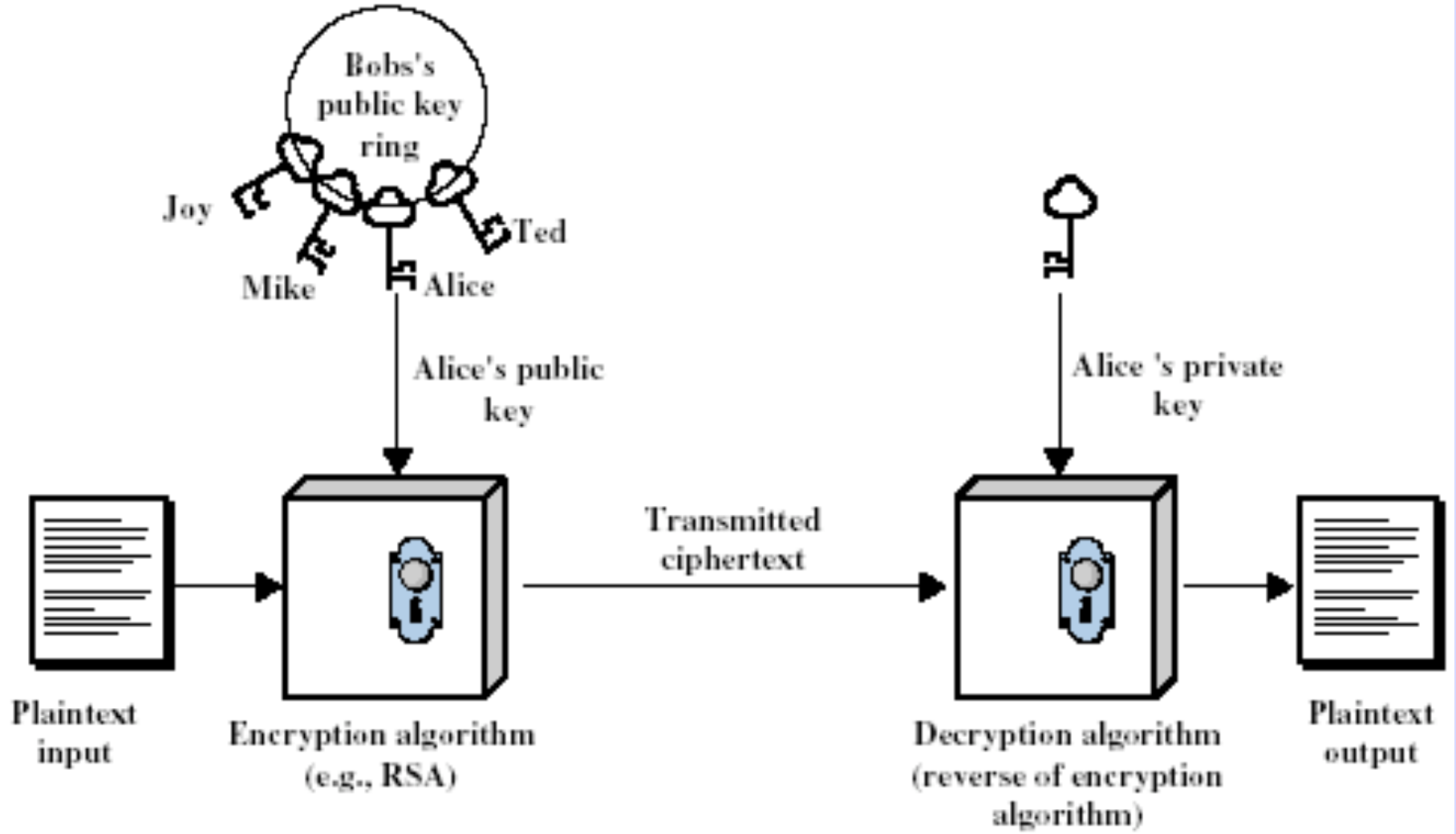
- También conocido como función hash de solo ida, es una huella digital única de longitud fija.
- Entrada de longitud arbitraria, salida de longitud fija (128 o 160 bits).
- Un buen algoritmo de digestión debe poseer las siguientes propiedades:
  - El algoritmo debe aceptar cualquier longitud de mensaje.
  - El algoritmo debe producir un digesto de longitud fija para cualquier mensaje de entrada.
  - El digesto no debe revelar nada acerca del mensaje de entrada que lo originó.
  - Es imposible producir un digesto pre-determinado.
  - Es imposible hallar dos mensajes que produzcan el mismo digesto.



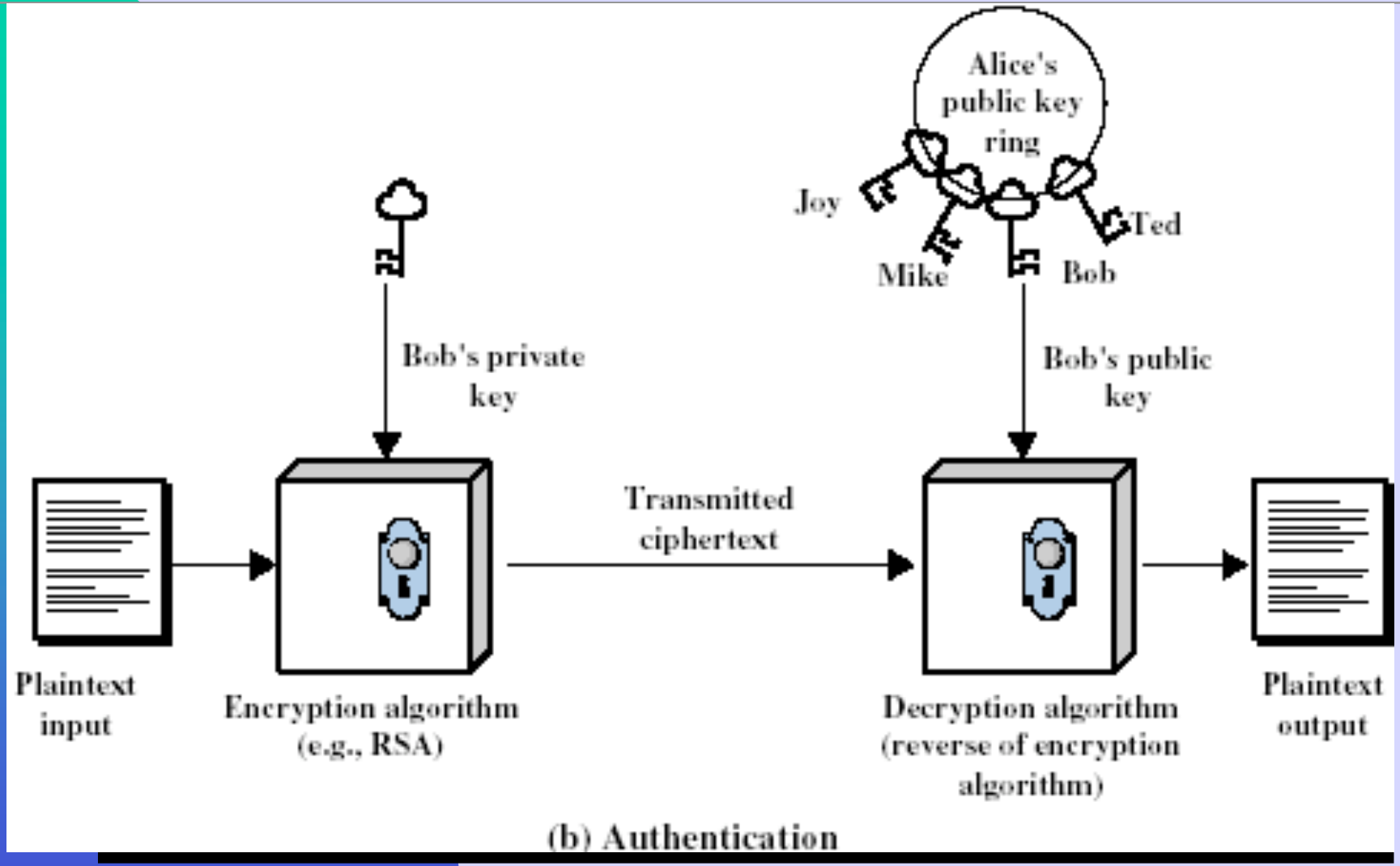
Algoritmos Hash

- 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.

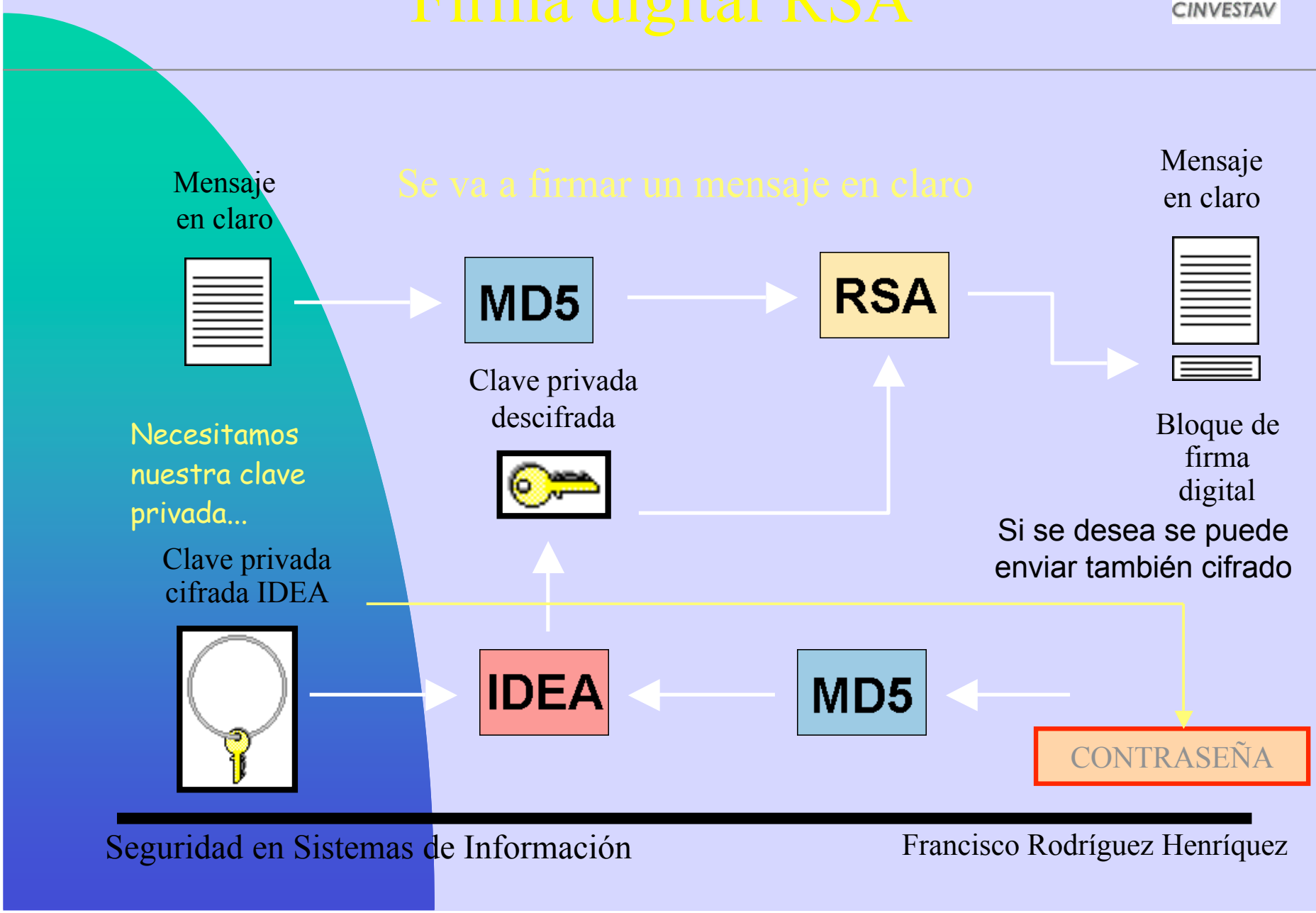
Criptografía de llave pública



Criptografía de llave pública



Firma digital RSA



Comprobación de la firma digital RSA