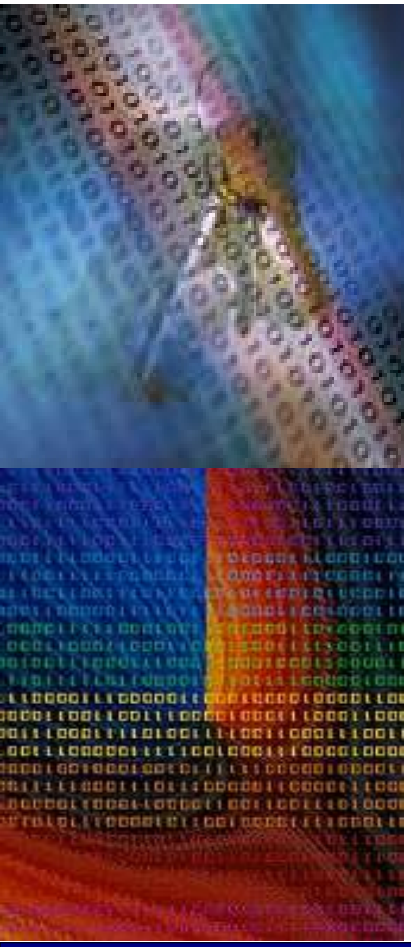
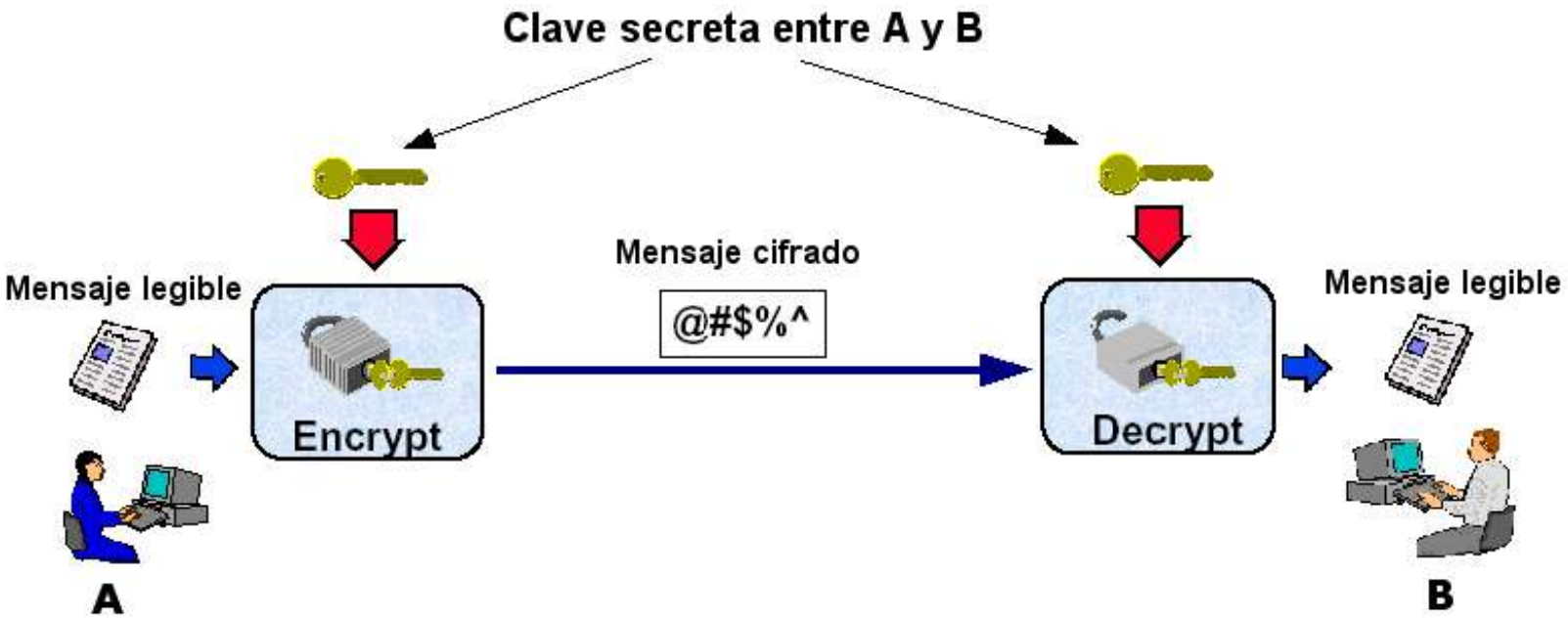


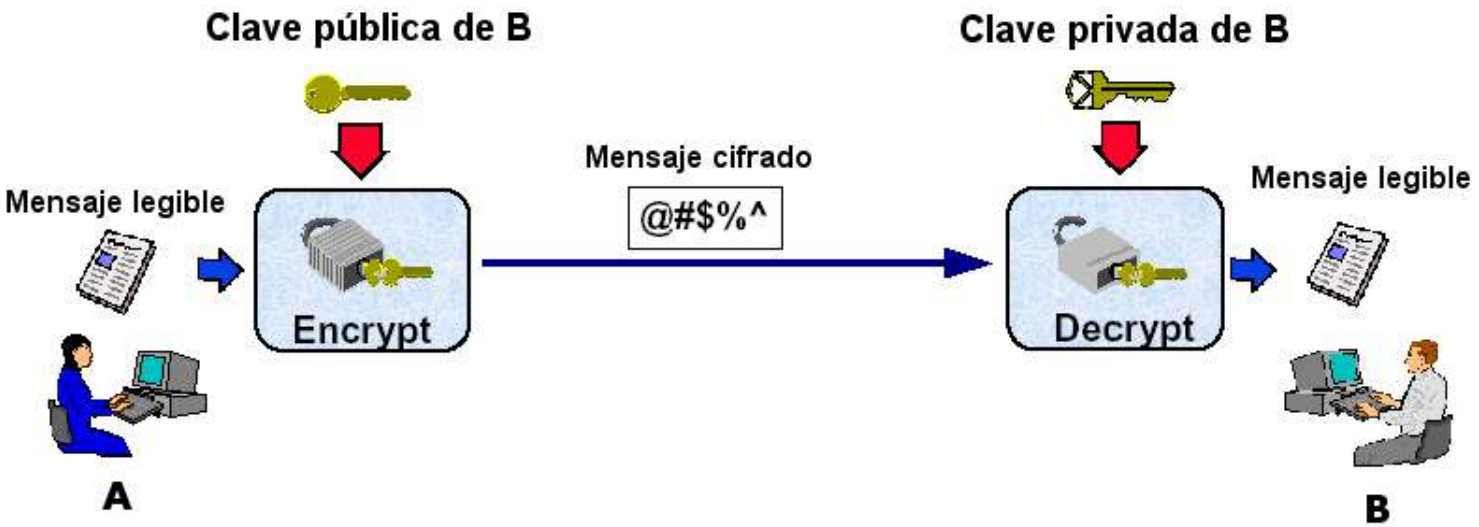
# Infraestructura para la Criptografía de Clave Pública

Juan Talavera
jtalavera@cnc.una.py

# Criptografía de Clave Simétrica



# Criptografía de Clave Pública



# Algunos algoritmos criptográficos

## Clave simétrica

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- RC5

## Clave Pública

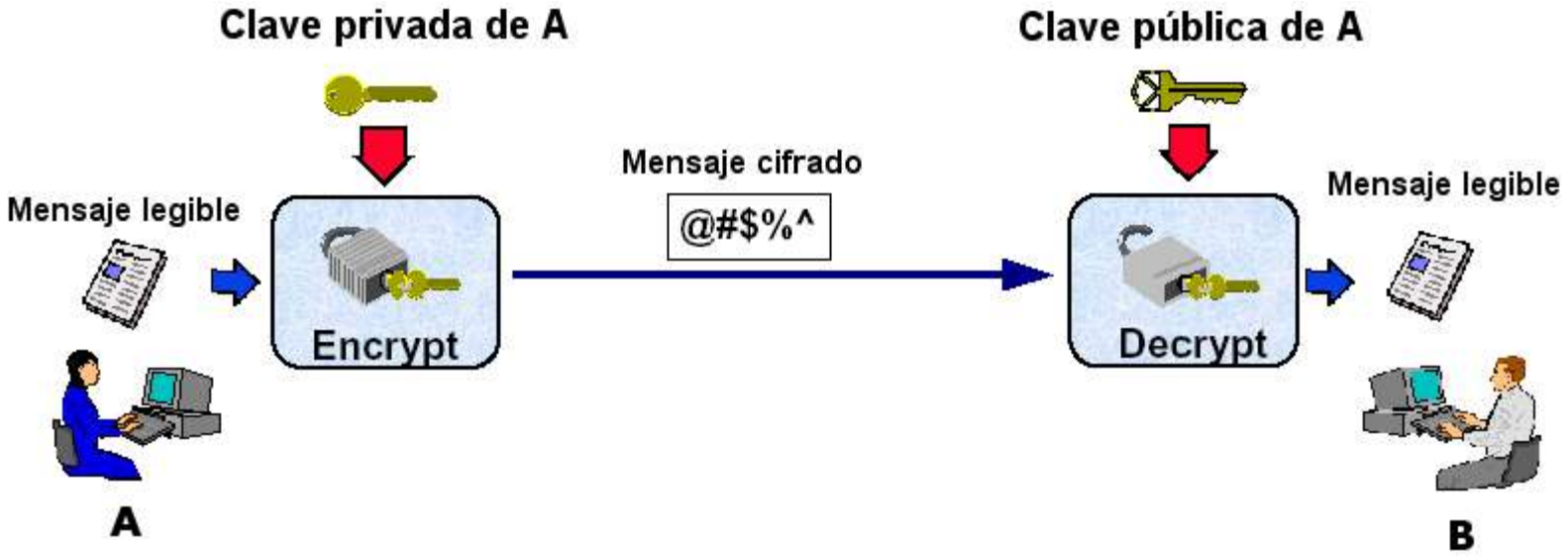
- RSA (Rivest, Shamir y Adleman)
- Diffie – Hellman
- DSS (Digital Signature Standard)
- ECC (Elliptic Curve Cryptography)

# Funciones Hash


## Requisitos para las funciones hash

- **H** puede aplicarse a un bloque de datos de cualquier tamaño
- **H** produce una salida de tamaño fijo
- **H(x)** es relativamente fácil de computar para cualquier **x**
- Para cualquier valor **h** dado es computacionalmente imposible encontrar **x** tal que **H(x) = h**. ***(Unidireccional)***
- Para cualquier **x** dado, es computacionalmente imposible encontrar **y** $\neq$ **x** tal que **H(y) = H(x)**. ***(Resistencia débil a la colisión)***
- Es computacionalmente imposible encontrar un par **(x,y)** tal que **H(x) = H(y)**. ***(Resistencia fuerte a la colisión)***

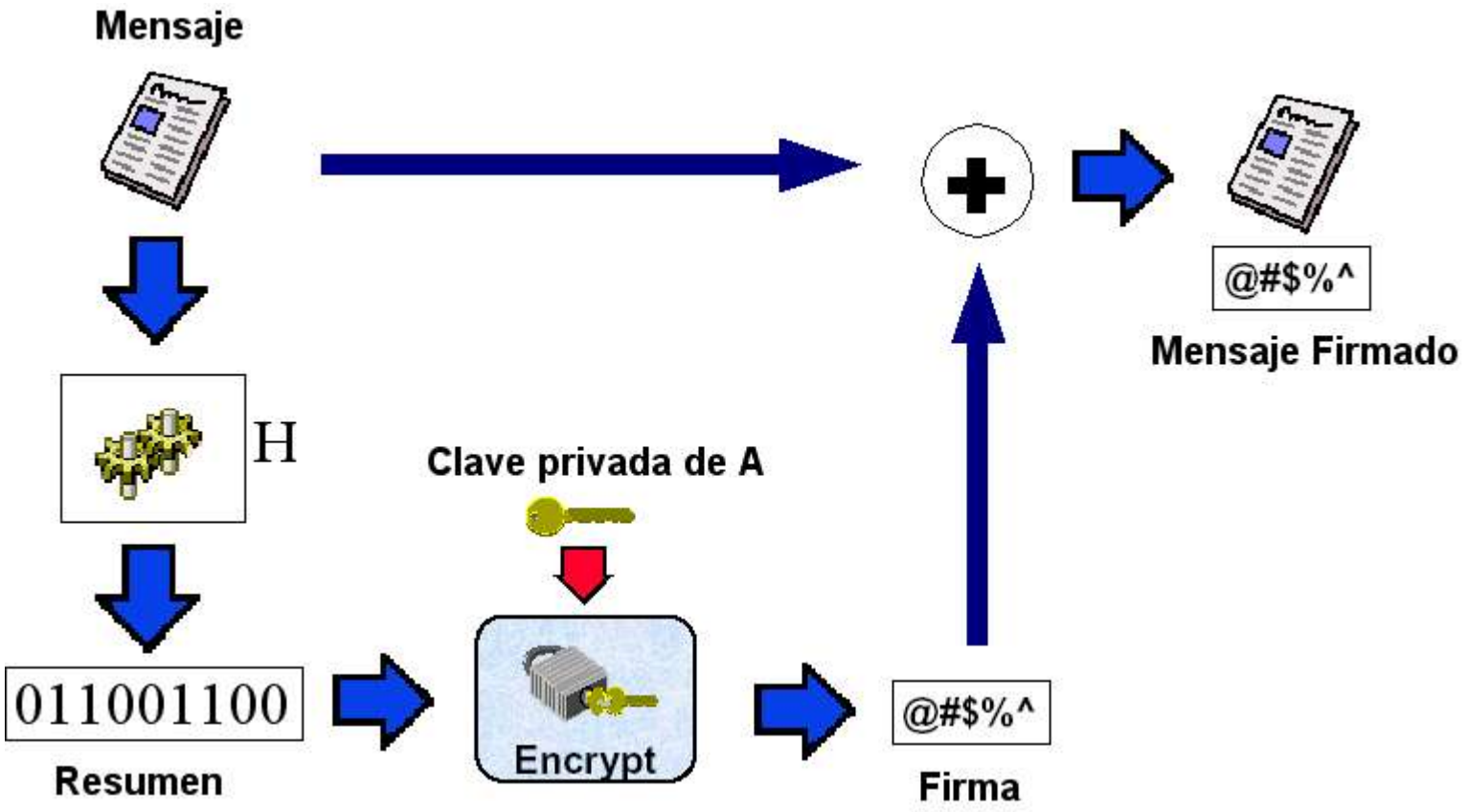
# Autenticación con Criptografía de Clave Pública




**Solo A tiene la clave privada, solo A pudo haber encriptado el mensaje**

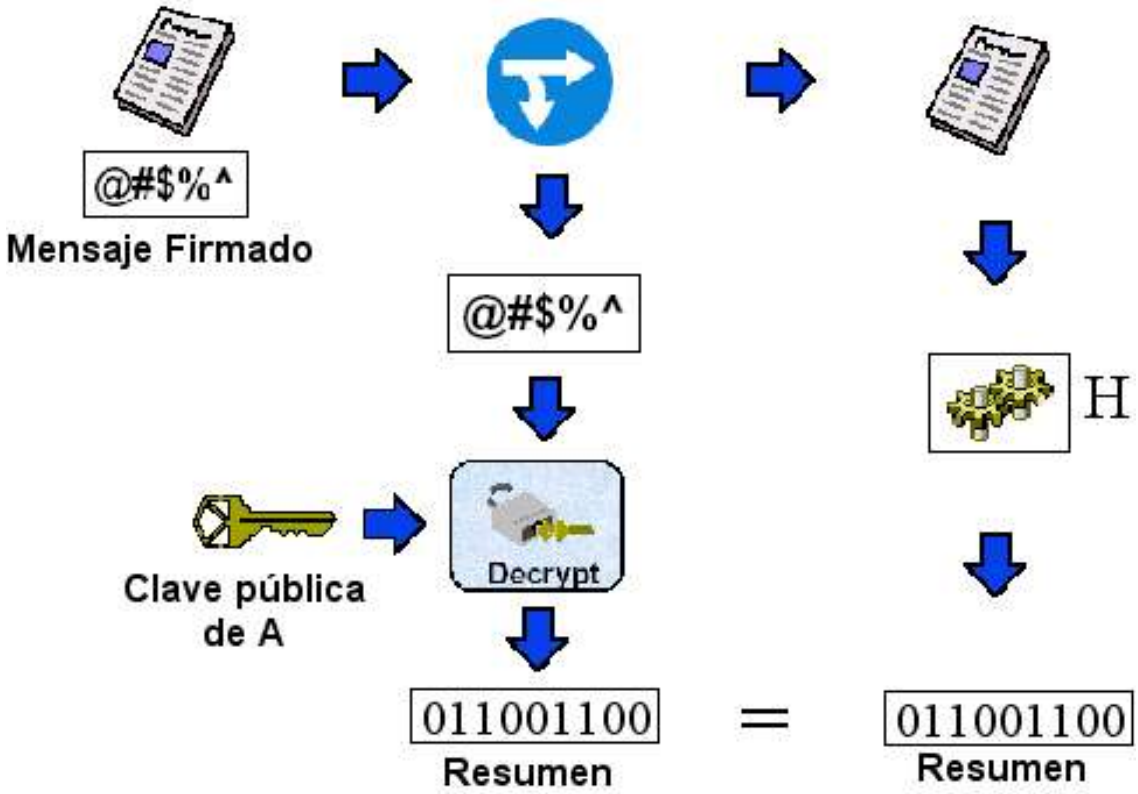
# Firmas Digitales

Cuando A envía mensaje firmado a B



# Firmas Digitales

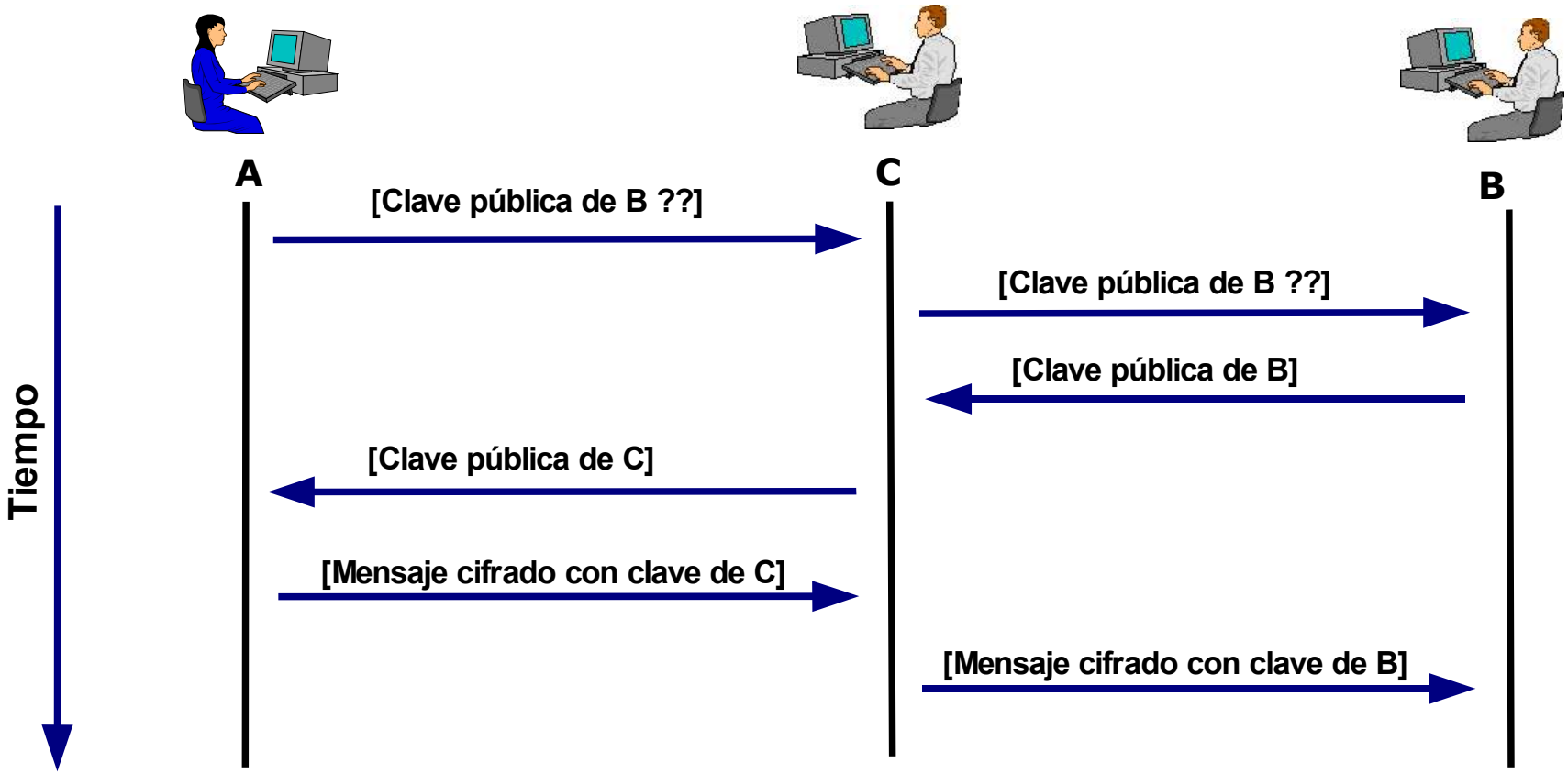
Cuando B recibe el mensaje y verifica su origen



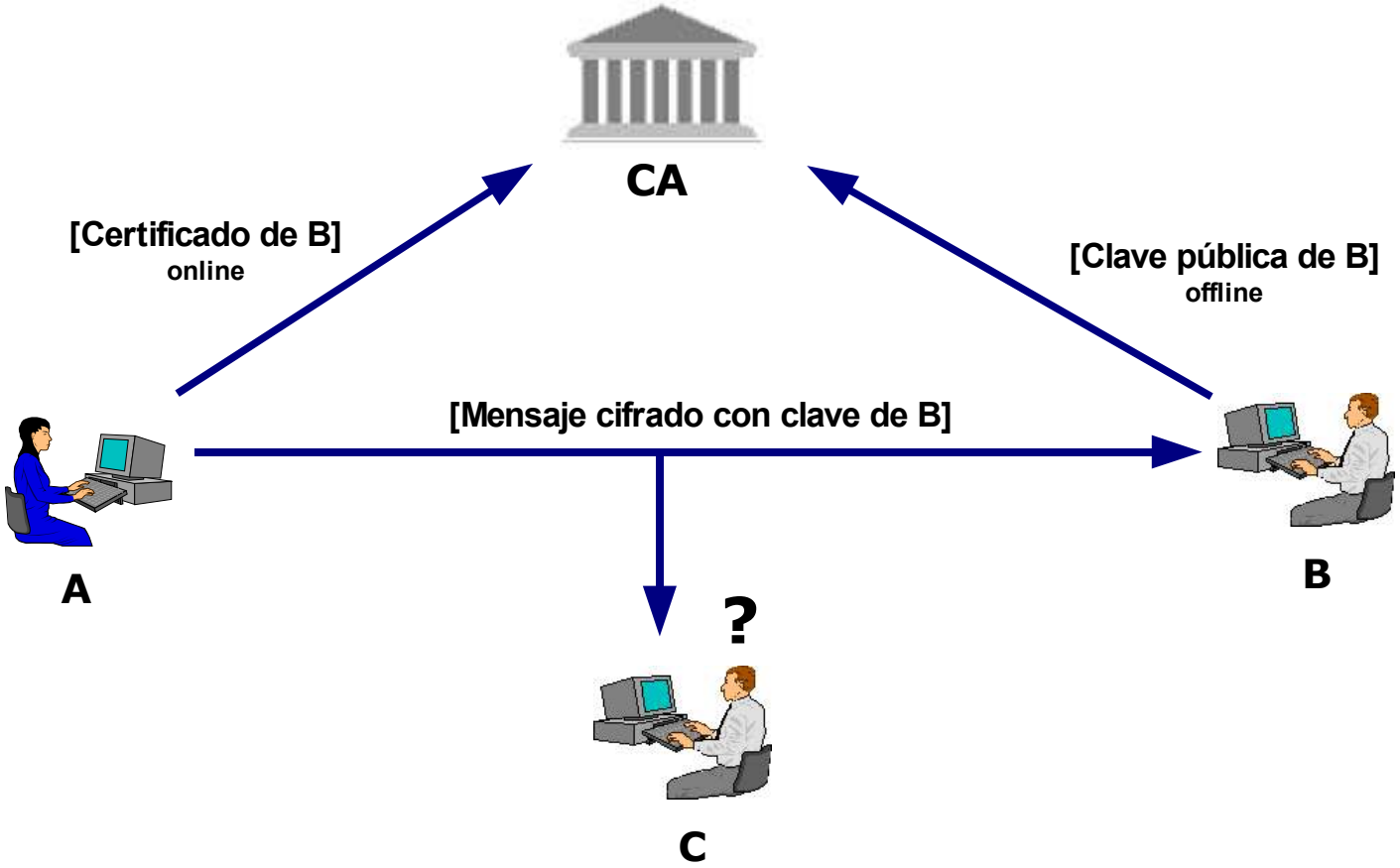
# Servicios de seguridad proveídos por la Criptografía de Clave Pública

- ***Confidencialidad***. Cifrado del mensaje con clave pública del destinatario.
- ***Autenticación***. Firmas digitales
- ***No repudio***. Firmas digitales
- ***Integridad***. Firmas digitales

# Problemas en la distribución de claves



# Autoridad de Certificación (CA)



# Certificados Digitales

- El Certificado Digital es un documento firmado por una Autoridad Certificadora (AC). El documento contiene, principalmente, el nombre de un sujeto y su clave pública.
- Si el Certificado es auténtico y confiamos en la CA, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado.

# Certificados Digitales

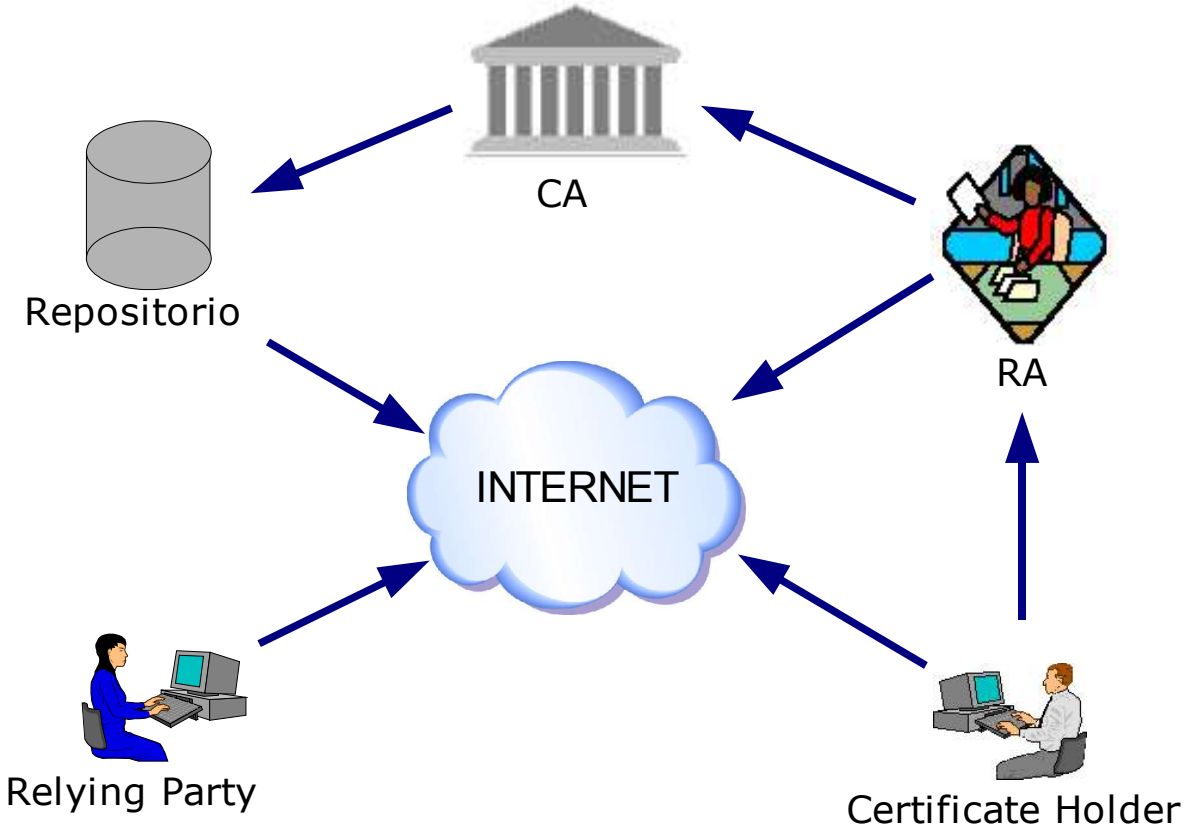
## Contenido de los certificados X.509v3 (RFC 3280)

| | |
|---|---|
| Versión (del formato del certificado) | |
| Número de serie del certificado | |
| Identificador del algoritmo de firma (para la firma de la CA) | |
| Nombre de la CA, formato X.500 | |
| Periodo de validez del certificado | |
| Nombre del sujeto, formato X.500 | |
| Información sobre clave del sujeto | Identificador del algoritmo |
| Clave pública del sujeto | |
| Firma digital de la Autoridad de Certificación | |

**X.509**, estándar emitido por la **ITU** (International Telecommunication Union) que define el formato de los certificados para el servicio de directorios X.500, la versión 3 es la adaptación por la **IETF** (Internet Engineering Task Force) para su uso en Internet conocida también como **PKIX**.

# Infraestructura de Clave Pública (PKI)

PKI – Public Key Infrastructure



# Componentes de una PKI

- **Certificate holder**, entidad cuyos datos personales están asociados a su clave pública en un certificado digital.
- **Relaying Party**, entidad que confía en el contenido de un certificado por estar este firmado por una CA de confianza.
- **CA**, Certification Authority, entidad encargada de generar los certificados a partir de las solicitudes, firmarlos y almacenarlos en un repositorio de acceso público.
- **Repositorio**, lugar en donde se almacenan los certificados y listas de revocación.
- **RA**, Registration Authority, entidad encargada de verificar los datos de quienes solicitan un certificado, generar la solicitud de certificación y enviarla a la CA.

# Algunos estándares para PKIs

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 2510: Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC 2511: Internet X.509 Certificate Request Message Format
- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 2585: Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

# Aplicaciones que requieren de una PKI

- SSL (Secure Socket Layer), permite enviar información encriptada, así como autenticar a uno o ambos extremos de un canal de comunicación. Es la base para HTTPS, FTPS, SMTPS, POPS, etc.
- S/MIME (Secure/Multipurpose Internet Mail Extensions), permite el envío de correo electrónico encriptado y firmado.
- SET (Secure Electronic Transaction), protocolo para compra y pago con tarjetas de crédito a través de Internet. Comercio electrónico.
- IPSec, extensiones de seguridad para el protocolo IP, implementa autenticación y confidencialidad a nivel de red, permite crear túneles seguros a través de redes inseguras para comunicar redes remotas.
- WTLS (Wireless Transport Layer Security), componente opcional de la pila de protocolos WAP, similar a SSL con consideraciones especiales para dispositivos wireless.

# PKIs en países de la región

## Brasil

El ICP-Brasil es la infraestructura de clave pública del Brasil. El ITI (Instituto Nacional de Tecnologías de Información) es la autoridad certificadora raíz, el ITI es dependiente de la Casa Civil de la Presidencia de la República. El ITI tiene certificada a varias otras CAs privadas, es una cadena de certificación plenamente operante en la actualidad.

En cuanto a legislación, tienen reguladas las políticas y prácticas de certificación, las auditorías de las CA, políticas referentes a tarifas de las CAs, etc.

# PKIs en países de la región

## Argentina

La ley argentina reconoce los documentos electrónicos firmados digitalmente, en cualquier caso que la ley requiera un documento firmado en forma manuscrita, también se aceptan documentos firmados en forma digital. Se encuentran reguladas por la ley todas las actividades de una PKI.

En cuanto a infraestructura de clave pública, actualmente el gobierno, ofrece un servicio experimental de firma digital para correo electrónico, es un servicio que asocia una clave a una cuenta de correo, pero no ofrece garantía en cuanto a la identidad del propietario de la cuenta.

# PKIs en países de la región

## Uruguay

Para la legislación uruguaya una firma manuscrita y una digital tienen el mismo valor legal, también están reglamentados los requisitos mínimos para la validez de los certificados, procedimientos de certificación, etc.

En cuanto a infraestructura, la Administración Nacional de Correos tiene una PKI operante y reconocida por el gobierno.

# PKIs en países de la región

## Bolivia

El Banco Central de Bolivia reconoce como válidos los documentos electrónicos firmados digitalmente, el único requisito para la validez legal de los documentos con firma digital es el acuerdo contractual de ambas partes de utilizar este medio de comunicación.

Existe un proyecto de ley que reglamentará la utilización de la firma digital y lo relativo a infraestructuras de clave pública. Actualmente no existe una PKI mantenida por el gobierno.

# PKIs en países de la región

## Paraguay

No existe un marco legal que haga posible la utilización de documentos electrónicos firmados digitalmente, pero se están elaborando proyectos de ley que reglamenten la utilización de este medio.

Actualmente no existe una PKI operante en el país.

# Proyecto de PKI en el Centro Nacional de Computación

- El CNC como Autoridad de Certificación
- Software utilizado en la PKI
- Integración del NIC-PY con la PKI
- Utilización del DNS como repositorio de certificados
- Inicialmente en forma experimental en la red de la UNA
- Luego se ofrecerán los servicios a nivel nacional

# El CNC como Autoridad de Certificación

- Otorgar certificados digitales firmardos con su clave privada
- Establecer las políticas y procedimientos de certificación
- Mantener el servicio de repositorio de certificados y CRLs
- Autoridad de Registro, en el CNC y/o delegado a otras instituciones

# Software en la infraestructura

- Gestor de base de datos (PostgreSQL)
- Aplicación de gestión (OpenCA)
- Módulo criptográfico (OpenSSL)
- Servidor web (Apache)
- Servidor LDAP (OpenLDAP)
- Sistema operativo (Unix FreeBSD)

***"Software 100% Open Source"***

# Integración del NIC-PY con la PKI

- Integración de procedimientos de solicitud

NIC-PY (Network Information Center - Paraguay), Administración de base de datos del DNS y delegación de dominios ".py".

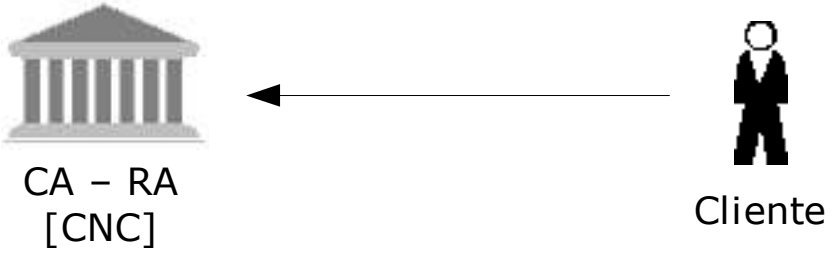
Conformado por:

**Laboratorio de Electrónica Digital (LED)**
**Universidad Católica de Asunción**

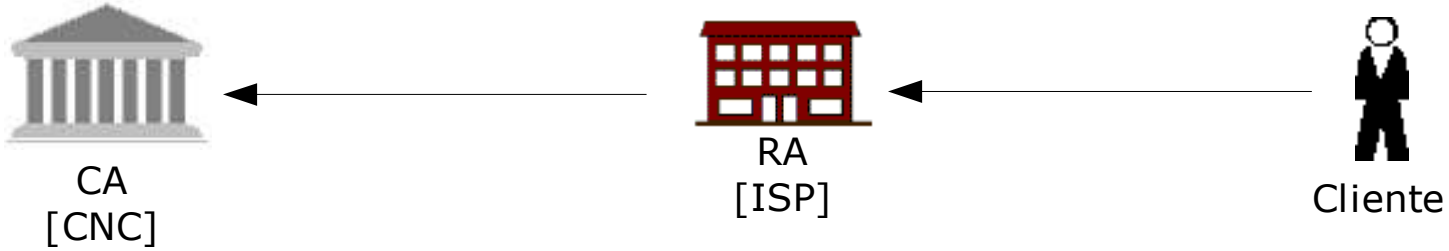
**Centro Nacional de Computación (CNC)**
**Universidad Nacional de Asunción**

# Modelos de Autoridad de Registro

- Centralizado




- Delegado




**ISP**, Internet Service Provider. Empresas que ofrecen servicios de acceso a Internet a sus clientes.

# Utilización de servidores DNS como repositorios de certificados

Protocolos generalmente utilizados para la obtención de certificados digitales:

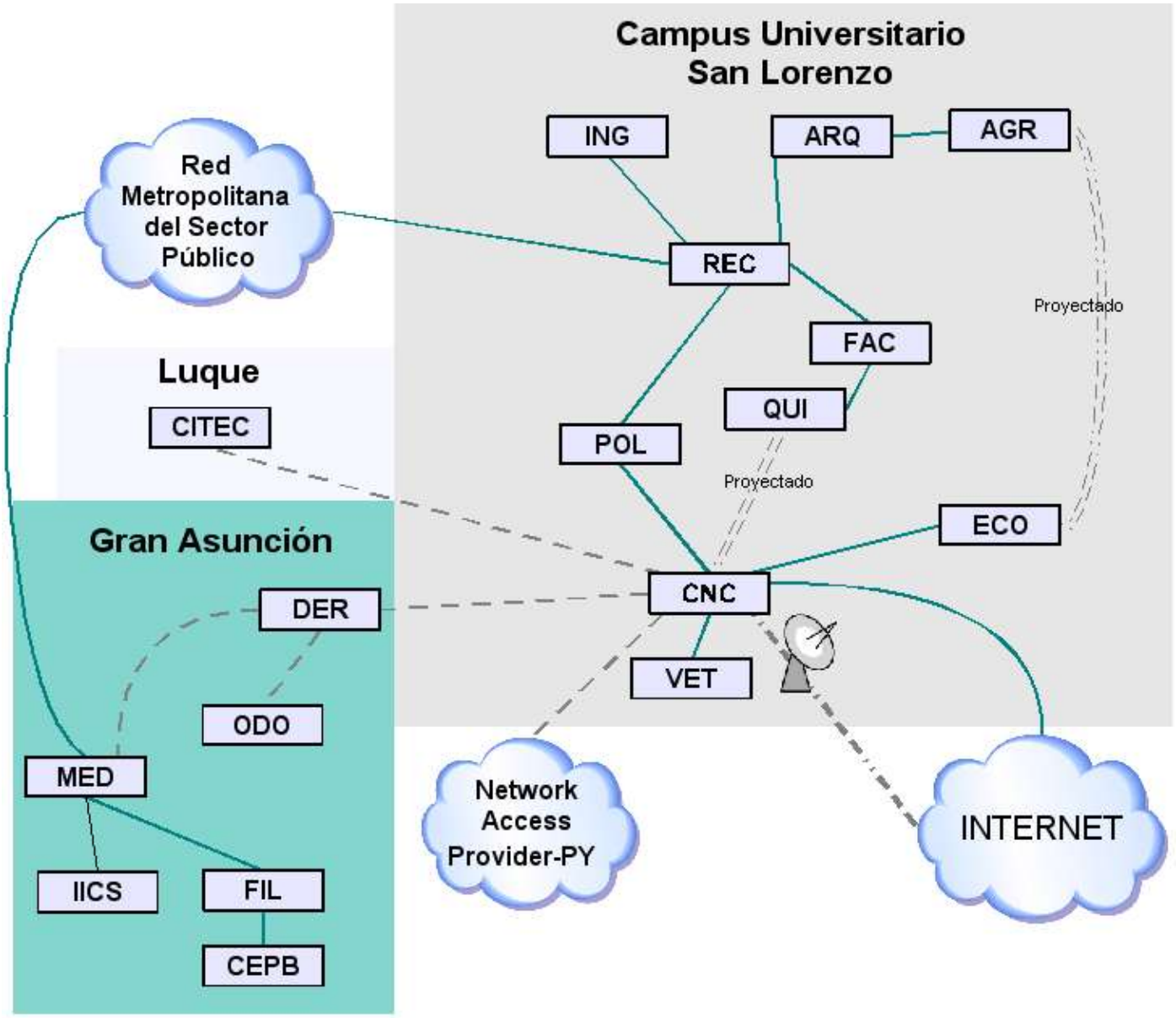
- LDAP, Lightweight Directory Access Protocol
- HTTP, Hypertext Transfer Protocol
- FTP, File Transfer Protocol

En nuestra implementación también usaremos al:

- DNS, Domain Name System

***"Primera PKI operante haciendo uso del DNS como repositorio de certificados"***

# Inicialmente en la Red de la UNA




Experimentalmente con los protocolos:

- IPSec
- DNSSec
- SSL
- HTTPS
- FTPS
- S/MIME

# Servicios a nivel nacional

Para posibilitar o facilitar la implementación segura de servicios como:

- Comercio electrónico (SET)
- Sitios web seguros (HTTPS)
- Correo electrónico seguro (S/MIME)
- Redes Privadas Virtuales (IPSec)
- Trasmisión de archivos segura (FTPS)
- Autenticación de usuarios (SSL, Otros)

# Trabajos Futuros

- Implementación de módulos para obtención de certificados desde el DNS. Necesario para aplicaciones como exploradores web, clientes de email, administradores de certificados, etc.
- Proyectar la infraestructura necesaria para la utilización del protocolo para transacciones electrónicas SET.

# ¿Preguntas?

Juan Talavera
jtalavera@cnc.una.py

Para mayor información:

- The Open–source PKI Book.
  Symeon Xenitellis
- Infraestructura de Clave Pública empleando el DNS.
  Pablo Greenwood
- http://www.openca.org
- http://www.pkiforum.org
- http://www.iti.gov.br