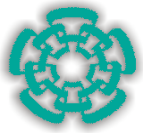
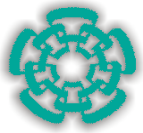


Propuestas de Temas de Tesis

Francisco Rodríguez-Henríquez
francisco@cs.cinvestav.mx
http://delta.cs.cinvestav.mx/~francisco/

CINVESTAV-IPN
Departamento de Ingeniería Eléctrica
Sección de Computación

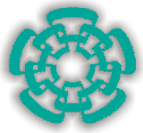


Estadísticas y Datos Personales

Julio 2005

Francisco Rodríguez Henríquez

Datos Generales



Posición actual:	Investigador Titular CINVESTAV 3A y Coordinador Académico de la Sección de Computación.
Antigüedad:	3 años [fecha de ingreso: 2 de mayo de 2002].
Edad:	37 años
Nacionalidad:	salvadoreña y mexicana
Experiencia profesional:	acumula una experiencia de más de 3 años de trabajo en compañías IT de Alemania y EUA, en donde colaboró como investigador y arquitecto de diseño criptográfico.

Formación Académica

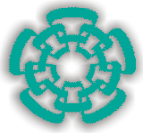
Doctorado: Departamento de Ingeniería Eléctrica y Computacional, Universidad Estatal de Oregon, EUA, Junio 2000.

Con Sub-especialidad (*minor area*) en Matemáticas.

Maestría: Maestría en Ciencias con especialidad en Electrónica, INAOE, Puebla, abril 1992.

Licenciatura: Licenciatura en Electrónica, Facultad de Ciencias Físico-Matemáticas, Universidad Autónoma de Puebla, Septiembre 1989

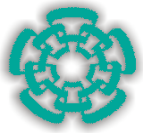
Líneas de Investigación



- Aplicaciones de Seguridad Informática
  - Sistema de Elecciones Electrónicas
  - Monedero digital
  - Notaría digital.
- Seguridad en dispositivos móviles e inalámbricos
  - Autentificación
  - Confidencialidad
- Criptografía
  - Diseño de algoritmos criptográficos
  - Diseño de protocolos de Seguridad
- Cómputo Reconfigurable
  - Algoritmos
  - Técnicas de diseño en paralelo.

Formación de Recursos Humanos

- 1 Tesis Doctoral finalizada: "Efficient Implementation of Cryptographic Algorithms on Reconfigurable Hardware Devices", Nazar Abbas Saqib, CINVESTAV 3 de Septiembre de 2004 [co-dirigida con el Dr. Arturo Díaz-Pérez] [tiempo promedio de graduación 3.5 años]
- 3 Tesis de Maestría finalizadas [tiempo promedio de graduación 2.6 años]
- 5 Tesis de Maestría en prrogreso [se estima finalizar las 5 tesis este año]



Propuestas de Temas de Tesis

Julio 2005

Francisco Rodríguez Henríquez

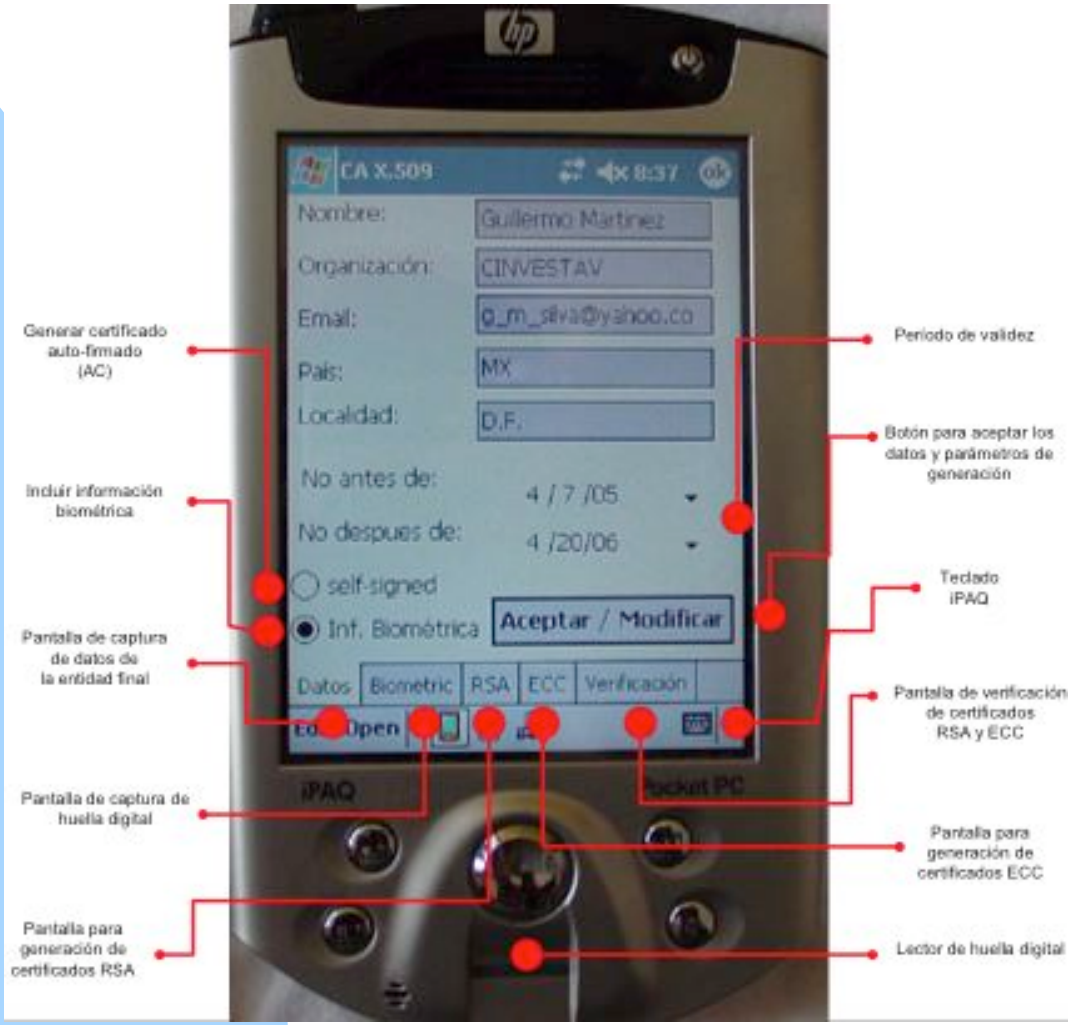
Tema 1: Autenticación Biométrica

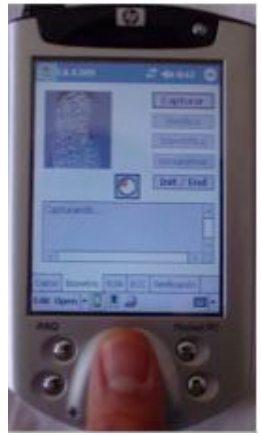
Francisco Rodríguez Henríquez

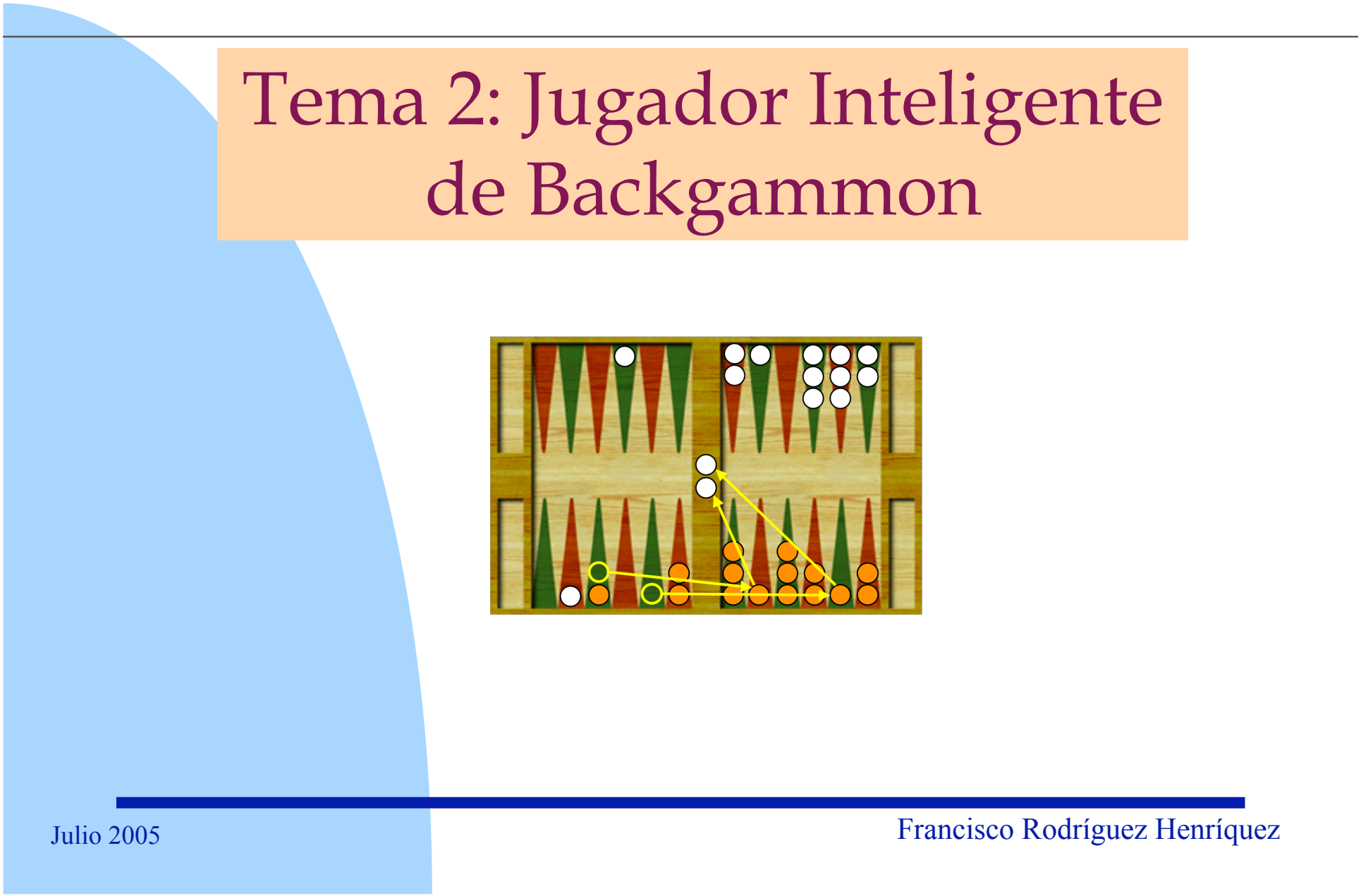
Tema 1: Autenticación Biométrica [Descripción]

- Plataforma Sugerida: C combinado con BIOAPI [http://www.bioapi.org/] PDA Sharp Zaurus y HP IPAQ.
- Breve Descripción: En la actualidad, existen tres principios para autenticar usuarios/nodos: a) Prueba que uno posee algo [típicamente un certificado digital]; b) Prueba que uno sabe algo [típicamente contraseñas secretas o códigos NIP]; c) Prueba que uno es algo.
- La autenticación biométrica estudia cómo realizar en la práctica el tercer objetivo, existiendo diversos mecanismos propuestos a la fecha, tales como: huellas digitales, dinámica en la forma de teclear, iris, retina, dinámica en la firma, etc.
- Objetivo: Implementar mecanismos de autenticación basado en biometría.

Autenticación Biométrica





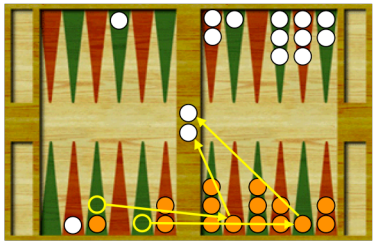


Tema 2: Jugador Inteligente de Backgammon

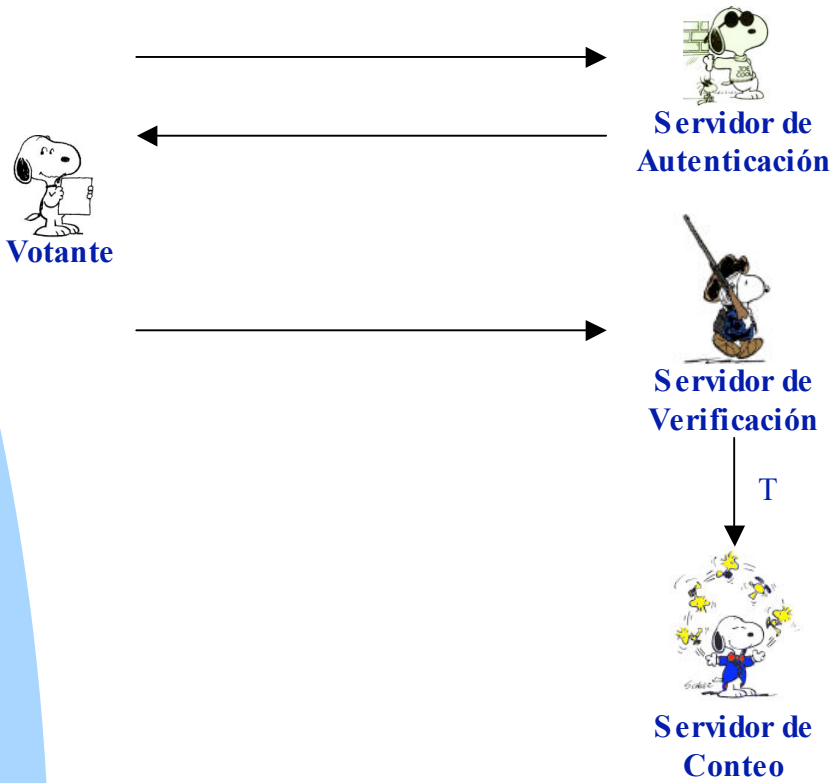
Francisco Rodríguez Henríquez

Tema 2: Jugador Inteligente de Backgammon [Descripción]

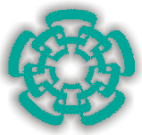
- Nota: Trabajo ofrecido en colaboración con la doctora Nareli Cruz Cortés [Cinvestav] y el Dr. Daniel Ortiz Arroyo [Universidad de Aalborg, Dinamarca].
- Plataforma Sugerida: C# C Sharp.
- Breve Descripción: Diversas heurísticas para desarrollar jugadores autómatas *inteligentes* de juegos de mesa tipo ajedrez, damas, backgammon y otros, han sido reportadas en la literatura especializada. En particular, el juego de Backgammon ofrece un reto especial debido a su naturaleza estocástica [se juega con dados] mezclado con estrategias y reglas bien definidas para vencer al oponente. Actualmente, nuestro grupo ha desarrollado un jugador de backgammon cuyo módulo *inteligente* fue implementado con lógica difusa y redes neuronales.
- Objetivo: Desarrollar un jugador autómata inteligente de backgammon utilizando heurísticas evolutivas tales como algoritmos genéticos o sistema inmune artificial.
- Reto: Jugar competitivamente [i.e, con porcentajes de victoria superiores al 50%]en contra del campeón mundial autómata.



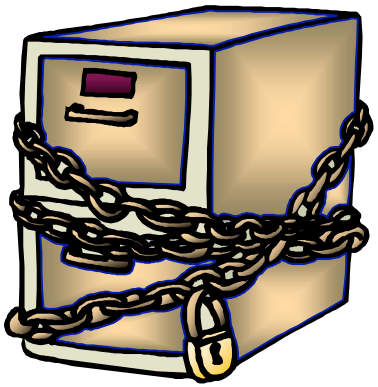
Tema 3: Elecciones Electrónicas con protocolos de curvas elípticas



Tema 3: Elecciones Electrónicas con protocolos de curvas elípticas [Descripción]



- Escenarios
  - Elecciones electrónicas
  - Reuniones de accionistas
  - Distribución segura de software
- Objetivos
  - anonimato
  - Sistema justo y auditable
  - Conteo rápido
- Herramientas
  - Matemáticas basadas en DSA, RSA y curvas elípticas
  - Firmas a ciegas
  - Protocolos no rastreables.
- Objetivo
  - Se cuenta con un sistema de elecciones electrónicas que implementa un protocolo basado en DSA y RSA. Se desea implementar un esquema basado en criptografía de curvas elípticas exclusivamente.



Esquema de Votación

Votante

$\{V, AS, Cert_v, z_1, z_2, (z_1||z_2||t)^{dv} \bmod n_v\}$

$\{AS, V, z_3, (z_4||z_5||z_6||t)^{ev} \bmod n_v\}$

Servidor de Autenticación

$T = \{s_1 \| s_2 \| s_3 \| s_4 \| s_5 \| y \| \mathbf{pr_1} \| \mathbf{pr_2} \| m\}$

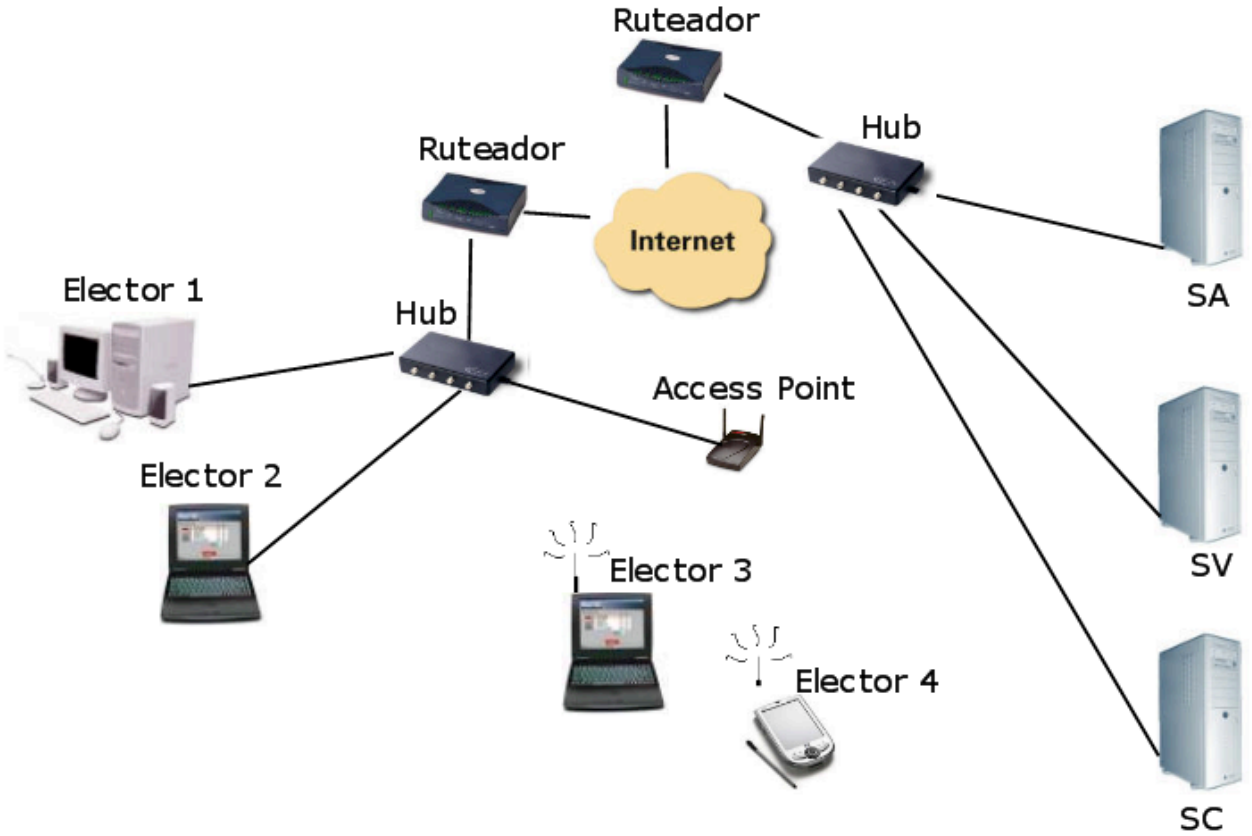
Servidor de Verificación

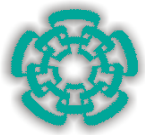
T

Servidor de Conteo

- ✓**Las firmas s4, s5 son hechas con DSA.**
- ✓**Para la construcción de pr_1 y pr_2 se hace uso del teorema del residuo chino.**

Arquitectura propuesta



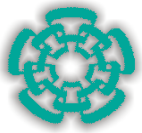


Tema 4: Notaría Digital

Julio 2005

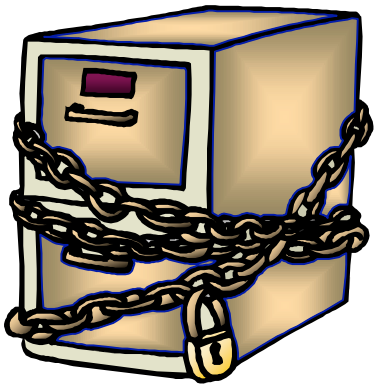
Francisco Rodríguez Henríquez

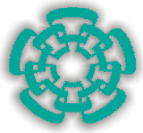
Tema 4: Notaría Digital [Descripción]



- Escenarios
  - Firma de Contratos
  - Firma de escrituras
  - Aval de Documentos importantes
- Objetivos
  - Verificación de fecha y hora de la firma de documentos
  - Sistema justo y auditable
  - Firmas válidas a largo plazo o por tiempo indefinido
- Herramientas
  - Autoridad certificadora y certificados digitales
  - Reloj de tiempo real y Autoridad de estampas de tiempo [timestamps]
  - Criptografía de llave pública

- Objetivo
  - Se desea implementar una notaría digital de acuerdo al RFC de la IETF disponible en: http://www1.ietf.org/proceedings_new/04nov/ltans.html.



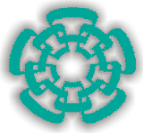


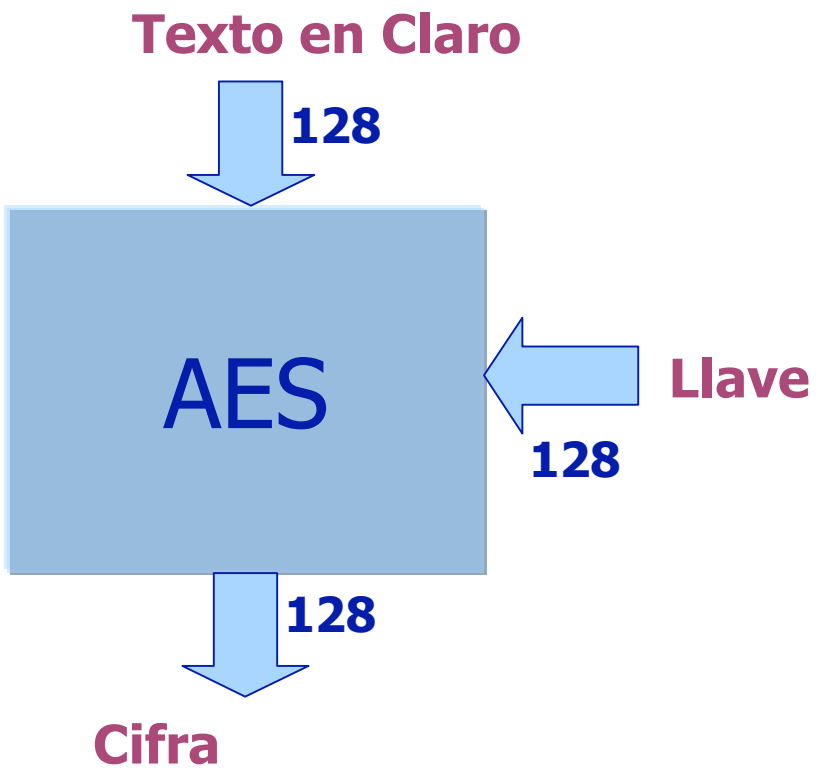
Temas 5 y 6: Cripto algoritmos implementados en hardware reconfigurable

Julio 2005

Francisco Rodríguez Henríquez

AES: Estándar de Cifrado Avanzado (Rijndael)

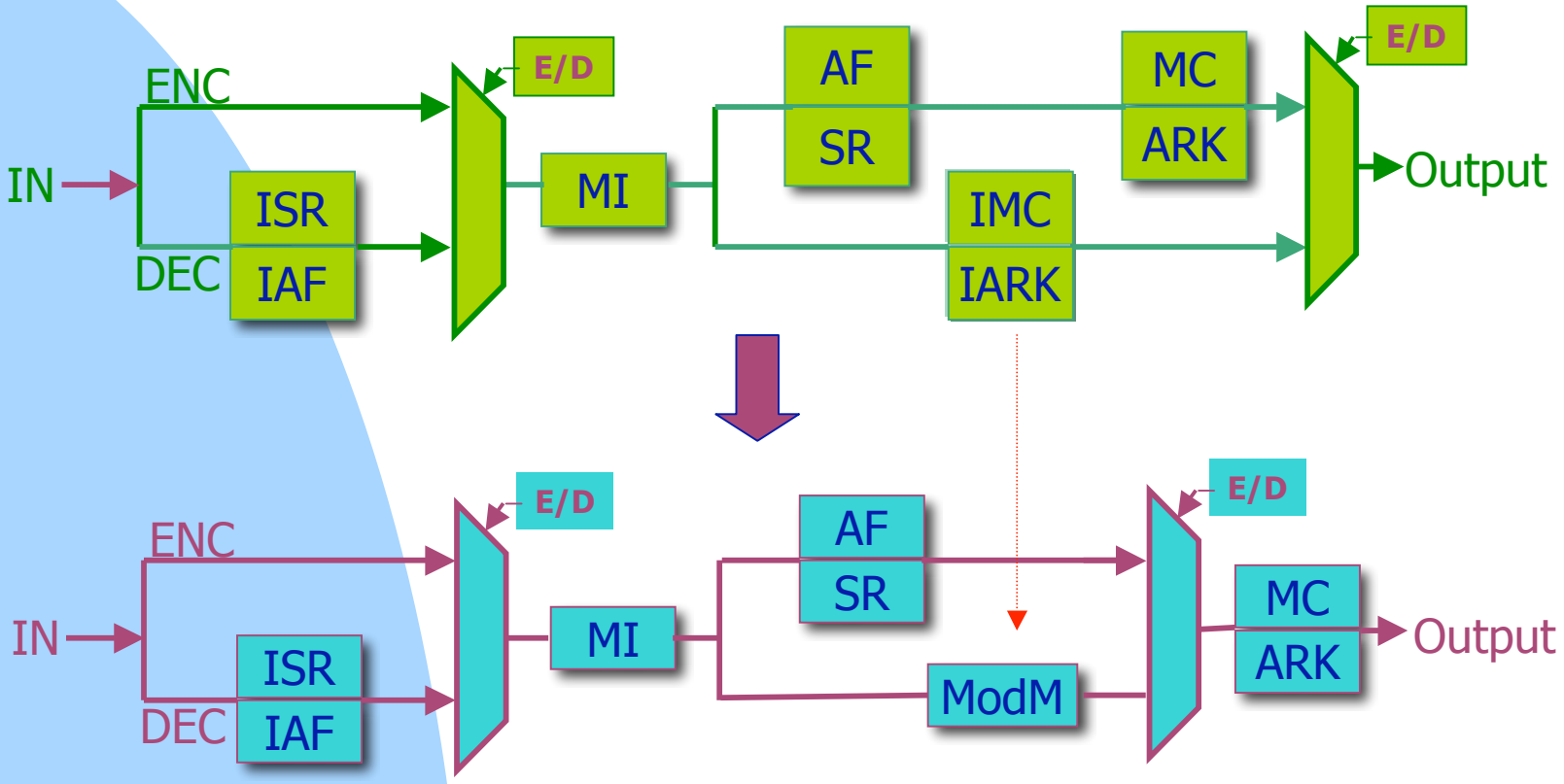




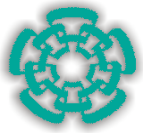
Subalgoritmos AES

- **Generación de llave**
- **Cifrado**
- **Descifrado**

AES Cifrado/descifrado en AES



Cifrado: MI + AF + SR + MC + ARK
Descifrado: ISR + IAF + MI + ModM + MC + ARK

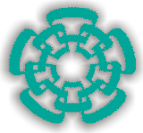


Criptografía de curva elíptica (CCE)

Julio 2005

Francisco Rodríguez Henríquez

Motivation



- Criptografía de curva elíptica: ¿cuándo usarla?
- Al menos en los siguientes tres escenarios:
  - ✓ Dispositivos con restricciones severas de cómputo: Smart Cards
  - ✓ Aplicaciones donde la Seguridad se vuelve una paranoia: Documentos de una compañía
  - ✓ Aplicaciones donde el secreto debe ser condervado a largo plazo o indefinidamente: Secretos de Estado