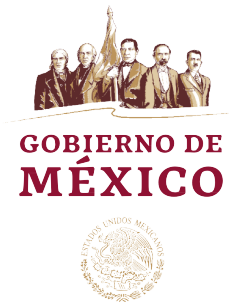
INTRODUCCIÓN A LA CRIPTOGRAFÍA

Escuela de Verano

[2019]

Luis J. Dominguez Perez



Lecture 4

Contenido, sección 1

Firma electrónica

Tendencias

La firma electrónica en México

CIMAT

- Es un paso hacia la transformación de la gestión pública.
- Coadyuva en la erradicación de la corrupción
- Provee una mayor productividad
- Reduce los costos de la ciudadanía al ejercer sus derechos y obligaciones.

Una fórmula para mejorar México

CIMAT

Ley que garantice la equivalencia entre:
firma autógrafa y de tipo digital

+

Esquema que fomente la productividad

=

Economía más competitiva
un México más fuerte
más próspero
con mejor futuro.

Inicios de la firma electrónica

CIMAT

- En un principio, el SAT instruyó el proyecto “Tu firma” (2004)
- Banxico intentó autorizar a terceros para validar las firmas
- SAT crea la CIEC - Clave de Identificación Electrónica Confidencial
- Nace la “FEA” - Firma Electrónica Avanzada (2005)
- Se instrumenta un esquema de PKI

Inicios de la firma electrónica - 2

- Se renombra la FEA por “FIEL” (2007)
- Entran la Secretaría de Economía, la Secretaría de la Función Pública, y el Servicio de Administración Tributaria (2008 – 2012)

Legislación

- Ley Federal de Protección de Datos en Posesión de los Particulares
  - **Año:** 2010
  - **Reforma:** 2010
  - **Alcance:** Particulares
  - **Aspectos relevantes:** Establece que para el caso de las solicitudes en general, la firma electrónica u otro medio se pueden utilizar para las autorizaciones.

Legislación - 2

- Ley Federal de Transparencia y Acceso a la Información Pública
  - **Año:** 2002
  - **Reforma:** 2010
  - **Alcance:** Agencias gubernamentales
  - **Aspectos relevantes:** Exige mecanismos de verificación de la integridad de la información, se puede hacer uso de la firma electrónica para tal efecto.

Legislación - 3

- Código de Comercio
  - **Año:** 1889
  - **Reforma:** 2012
  - **Alcance:** Operaciones mercantiles
  - **Aspectos relevantes:** Contiene un título extensivo sobre el comercio electrónico, que incluye el uso de la firma electrónica

Legislación - 4

- Código Fiscal de la Federación
  - **Año:** 1984
  - **Reforma:** 2005
  - **Alcance:** Operaciones fiscales
  - **Aspectos relevantes:** Establece cómo se rigen los procedimientos relacionados a los impuestos

Legislación - 5

- Ley de Firma Electrónica Avanzada
  - **Año:** 2012
  - **Reforma:** 2012
  - **Alcance:** Particulares, operaciones no fiscales ni mercantiles
  - **Aspectos relevantes:** Hace equivalente a la firma digital con la firma autógrafa. Define las características de los certificados digitales

Legislación - 6

- Decreto de Austeridad 2012
  - **Año:** 2012
  - **Reforma:** 2012
  - **Alcance:** Gobierno federal, operaciones no fiscales ni mercantiles
  - **Aspectos relevantes:** Hace obligatorio y extensivo el uso de la firma electrónica, y busca reducir el consumo del papel

Infraestructura Extendida de Seguridad

CIMAT

- El Banco de México, como Banco Central del país, establece los mecanismos de comunicación para las transacciones financieras
- Define una infraestructura PKI que hace uso extensivo de los certificados digitales
- Delega ciertas actividades a los diferentes actores del mercado financiero

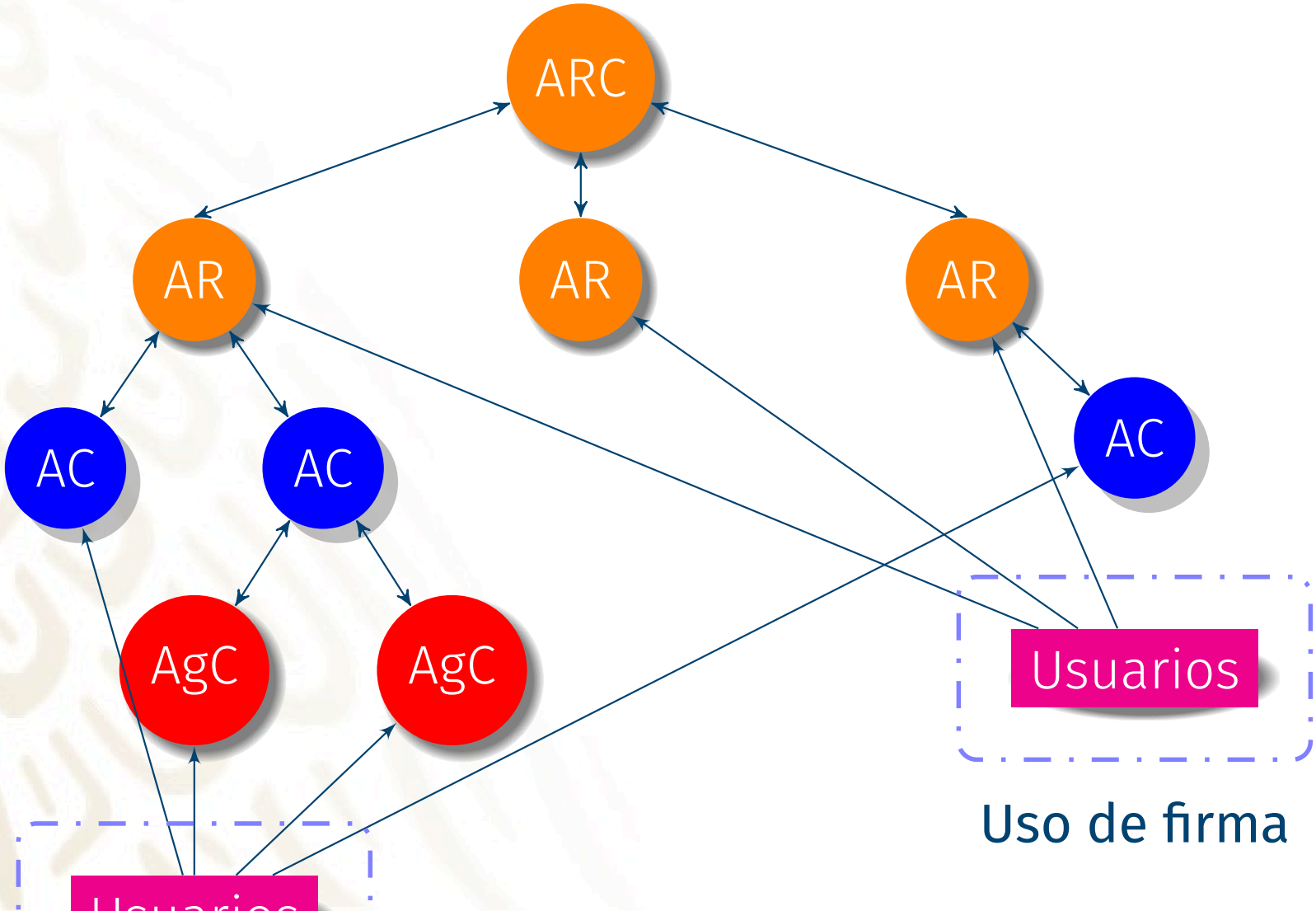
Elementos en la infraestructura de Banxico

La IES, infraestructura extendida de seguridad, contiene los siguientes actores:

- ARC - Agencia Registradora Central
- AR - Agencia Registradora
- AC - Agencia Certificadora
- AgC - Agente Certificador
- Usuario

Diagrama IES

Infraestructura IES



Elementos en la infraestructura de Banxico

CIMAT

- ARC - Agencia Registradora Central
  - Establece la normatividad y administra la IES
  - Autoriza su inclusión a la IES a otros elementos, y define sus funciones
  - Administra el esquema de PKI
- AR - Agencia Registradora
  - Registra los certificados digitales, previa autorización de la ARC
  - Administra los certificados a su cargo

Elementos de la IES - 2

- AC - Agencia Certificadora
  - Emiten los certificados digitales
  - Son el intermedio entre los Usuarios y los Agentes Certificadores (AgC), y la Agencia Registradora (AR)
- AgC - Agente Certificador
  - Realiza labores de certificación y revocación de firmas digitales
- Usuario
  - Es quien requiere un certificado
  - Puede ser persona física o moral, nacional o extranjera

Operaciones en la IES

Existen dos protocolos de comunicación:

- Entre la Agencia Registrador (AR) y la Agencia registradora Central (ARC):
  - Conexión
  - Desconexión
  - Alta de Certificado
  - Consulta de Certificado
  - Revocación de Certificado
  - Aviso de Revocación de Certificado

Operaciones en la IES - 2

- Entre el Usuario y las diferentes entidades de la IES:
  - Conexión
  - Desconexión
  - Consulta de Certificados
  - Revocación de Certificado propio

Caso Colima

- El caso de la firma electrónica del Estado de Colima es interesante ya que se tenía un serio problema de productividad y un evidente retraso en la operación de partes clave en el estado
- El Registro Público de la Propiedad y del Comercio del Estado de Colima (RPPC) requirió que el estado hiciera cambios en la legislación, e hizo uso de la firma electrónica como solución a sus problemas
- El Estado de Colima recibió un reconocimiento por parte de la OECD por sus avances en esta materia

Legislación afectada del Estado de Colima

- Se creó la Ley de Firma Electrónica para el Estado de Colima (2009)
- Se modificaron las siguientes leyes:
  - Código Civil
  - Código de Procedimientos Civiles
  - Código Penal
  - Código de Procedimientos penales
  - Ley de Catastro
  - Ley del Notariado del Estado de Colima
  - Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Colima

Resultados en el Estado de Colima

CIMAT

- Reducción dramática de los procesos relacionados con el RPPC
- Eliminación o absorción de procedimientos redundantes
- Automatización de ciertos procesos
- Generación de nuevos y ágiles servicios
- Aumento de la productividad
- Reconocimiento de la OECD

Distrito Federal

- En el Distrito Federal también se generó una Ley en materia de firma electrónica (2009). En este caso se buscó:
  - Transparentar la función pública
  - Combatir la corrupción
  - Eficientizar la gestión administrativa
  - Brindar mejores servicios
- En este caso, se dejó a la Asamblea Legislativa hacer los ajustes pertinentes en materia legal
- También se dispuso al Departamento de la Administración Pública de proveer los medios a la ciudadanía (incluyendo la brecha digital)

UNAM

- Otro caso interesante es el de la UNAM. (2005)
  - El objetivo de la firma electrónica es facilitar la autenticación de los miles de alumnos que se tienen
  - Facilitar el resguardo de la documentación (digitalización de documentos)
  - Incrementar la seguridad de los datos
- Dado que no existe urgencia del cambio en este caso, se ha ido incorporando el uso de la firma electrónica a diversos módulos de atención a alumnos, pero ha sido uno a uno, y no se procede a incluir otro hasta que se haya terminado el cambio en el módulo anterior.

Módulos UNAM

Los módulos a los que se le incluyeron la firma electrónica son:

- 2005 - Actas de calificaciones de bachillerato, vale de abastecimientos, presupuestos, mantenimiento, viáticos
- 2006 - Firma de actas de calificaciones
- 2007 - Programación de eventos culturales
- 2011 - Cartas de no adeudo para titulación, calificaciones extracurriculares, Archivo General
- 2012 - Sistema interno

Diferencias

- Caso Colima
  - Mejora de productividad
  - Nuevas leyes
  - Contratación de personal
- Caso UNAM
  - Autenticar y digitalizar
  - Aviso en la Gaceta universitaria
  - Cambio escalonado
- Caso D.F.
  - Corrupción y mejores servicios
  - Nuevas leyes
  - Delegación de trabajo

Diferencias - 2

- Caso SAT
  - Productividad y mejor recaudación
  - Nuevas leyes
  - Cambio escalonado
- Caso Banxico
  - Proporcionar una infraestructura
  - Nuevas leyes
  - Concientizar al gobierno

PKCS #1

- El PKCS #1 se refiere a los procesos alrededor de la firma electrónica.
- Actualmente se tiene la firma electrónica tipo RSA y DSA
- El SAT utiliza la firma tipo RSA
- En el 2016/2017 la firma tipo RSA tuvo una mejora en el estándar, versión 2.2
- La mejora toma nota de avances de 1996. . .
- Actualmente el SAT seguirá utiliando la firma RSA tradicional.

Firma RSA con SHA-1 y certificado del SAT

El procedimiento para firmar un documento utilizando el certificado del SAT con la combinación del cripto-esquema RSA y la función de resumen SHA-1, consiste de los siguientes pasos:

- Un ciudadano mexicano que realice sus declaraciones de impuestos tiene un certificado digital del SAT
- El contribuyente necesita el archivo de su llave privada
- La biblioteca OpenSSL u otra similar
- Si se desea firmar un cierto documento que ha sido almacenado como “archivo.txt”

Firma RSA con SHA-1 con Certificado

```
openssl pkcs8 -inform DER
  -in Claveprivada_RFC_FIRMANTE.key
  -out Claveprivada_RFC_FIRMANTE.pem
openssl dgst -sha1 -sign
   Claveprivada_RFC_FIRMANTE.pem
  archivo.txt > firmabinaria.txt
rm Claveprivada_RFC_FIRMANTE.pem
openssl base64 -in firmabinaria.txt -out
   firma.txt
```

Verificación de firma

```
1 Descargar Certificado FIEL del Signatario
     desde el SAT: https://portalsat.
    plataforma.sat.gob.mx/
    RecuperacionDeCertificados/faces/
    recuperaRFC.xhtml
2 openssl x509 -inform DER -in RFC_FIRMANTE.
    cer -pubkey -noout > RFC_FIRMANTE.pem
3 openssl base64 -d -in firma.txt -out
    firmabinaria.txt
4 openssl dgst -sha1 -verify RFC_FIRMANTE.
    pem  -signature firmabinaria.txt
    archivo.txt
```

Contenido, sección 2

Firma electrónica

Tendencias

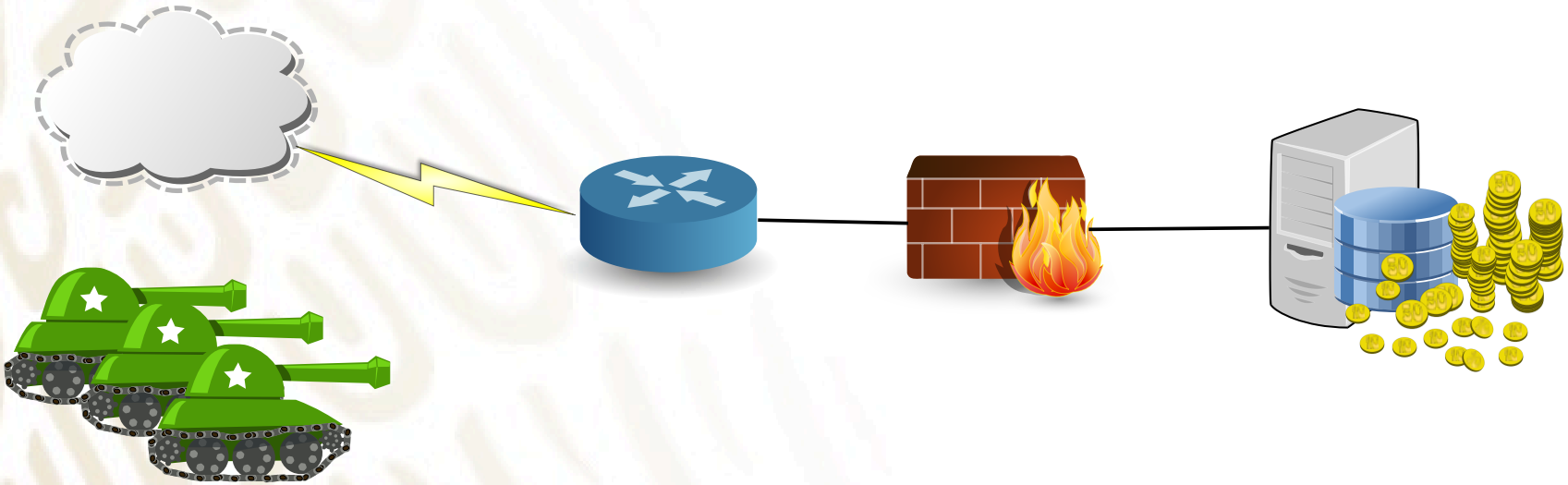
Sistemas desplegados

- Supuestos de intratabilidad convencionales:
  - Factorización entera (IFP): RSA
  - Logaritmo Discreto (DLP): Diffie-Hellman (DHP), y sus variantes bilineares: ECC y PBC

- Estos supuestos se reducen a lo que se conoce como El Problema del Subgrupo Escondido (HSP).

Balance entre la protección y lo protegido

- La principal preocupación de un sistema de seguridad es cuánto tiempo le tomará a un atacante romperlo, y cuántos recursos le son necesarios.
- El costo de romper un sistema, medido tanto en tiempo y en dinero invertido en recursos computacioneales, debe de ser mayor a el valor de la información protegida



Beneficios y tiempos

- Cuando un atacante necesitase 100 millones de USD para obtener un beneficio de 100 mil USD, un atacante típicamente desistirá
- Cuando se dice que a un atacante le tomará alrededor de 100 años en romper un sistema, es calculado al inicio del ataque.
  - Con el tiempo, nuevos métodos y mejores recursos están disponibles
  - Un atacante podría ir actualizando sus recursos y reducir drásticamente los 100 años inicialmente estimados

Calculando el costo

- En un sistema simétrico, el tiempo de vida de la protección de los datos puede ser calculado con el tiempo que nos tomaría romper el esquema mediante fuerza bruta, utilizando un diccionario de llaves, u otro método
- En “Using the cloud to determine key strengths”, Kleinjung et al. popusieron un esquema de medición para comparar el costo de romper un esquema criptográfico utilizando los servicios de Amazon.
  - Romper un esquema de 128 bits de seguridad utilizando los servidores cloud de Amazon costaría 10^{27} USD.

Algoritmo de Shor

- Factoriza un entero no primo en tiempo polinomial
- Son dos partes principales:
  - Reducción del problema de factorización a un problema de búsqueda ordenada (cómputo clásico)
  - Resolver el problema de búsqueda ordenada (cómputo cuántico)

Consecuencias: RSA podría ser roto ya que su fuerza recae en la dificultad de encontrar los dos factores primos de un número entero grande.

Ataques

- El algoritmo cuántico de Shor permite resolver en tiempo polinomial aleatorios ciertos esquemas del problema del subgrupo escondido para grupos finitos *abelianos*.
- En particular, este algoritmo puede romper los esquemas:
  - RSA
  - DSA
  - ECDSA

  en un tiempo $\mathcal{O}(\log N)^3$

Algoritmo de Shor

Algorithm 1 Algoritmo de Shor

Require: $N \in \mathbb{N}$ no primo

Ensure: un factor de N

1: Escoja un x aleatorio entre el rango $[2..N]$
2: Si el $\text{MCD}(x, N) \neq 1$ terminar
3: Encontrar el orden r de x mod $N (x^r \equiv 1 \bmod N)$
4: **if** r es par y $x^{r/2} \neq \pm 1 \bmod N$ **then**
5: $\quad \text{MCD}(x^{r/2} + 1, N)$ es un factor no trivial de N
6: **else**
7: $\quad$ intentar con otra x
8: **end if**

Alcance

- Los algoritmos criptográficos basados en la dureza de problemas en los que el algoritmo de Shor no se puede aplicar, se conocen como **sistemas criptográficos poscuánticos**
- Estos esquemas están basados en problemas computacionalmente **NP**-completos o **NP**-duros:
  - Funciones picadillo
  - Códigos
  - Retículas
  - Ecuaciones cuadráticas multivariables
  - Llave secreta
  - Isogenias sobre curvas elípticas supersingulares
  - Grupos no abelianos
  - etc.

Mecánica cuántica

- Física a nivel atómico y subatómico
- Requiere teoría precisa
- El estado del sistema no es dado por observaciones físicas
- Es imposible conocer el estado actual del sistema
- Se pueden hacer predicciones probabilísticas

Definición

Notación $|\cdot\rangle$, se conoce como *ket*, y es un vector en el espacio de todos los estados posibles.

Principios cuánticos

- Una cantidad observable se representa como una matrix Hermitiana $\mathcal{A}$. Los posibles valores de una medición son el eigen-vector de $\mathcal{A}$. Esta matriz puede ser unitariamente diagonalizada.
  - Los eigenvectores de $\mathcal{A}$ generan una base ortogonal, tal que, cada vector $|\psi\rangle$ puede ser representado por una combinación lineal de estos eigen-vectores $|\phi_i\rangle$.

$$|\psi\rangle = c_1|\phi_1\rangle + \ldots + c_n|\phi_n\rangle$$

- Dada una matiz $\mathcal{A}$ observable, su medición nos arroja un $|\phi_i\rangle$ con una probabilidad $|c_i|^2$

CIMAT

Definición

Entrelazado cuántico. Es el fenómeno en el cual los estados cuánticos de dos objetos se describen como referencia entre sí, por ejemplo:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|B_1C_2\rangle + |B_2C_1\rangle)$$

Definiciones

- **Qubit**. Un qubit es la unidad de información cuántica. Sus dos estados computacionales clásicos son:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ y } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  Un qubit puede ser representado por la combinación lineal de estos dos estados.

- **Registro de qubit**. Un número de qubits entrelazados a analizar, o el producto tensorial de los qubits.

- **Compuerta cuántica**. Es un circuito cuántico que opera sobre un determinado número de qubits

Quantum-safe Cryptography

Dado que aún no existe una máquina cuántica lo suficientemente poderosa para romper un cryptosystema, ¿porqué preocuparse?

- Costo de re-implementación
- Sistemas desplegados obsoletos, pero funcionales
- Perfect Forward Secrecy
- Eficiencia

Progreso en máquinas cuánticas para atacar a la criptografía

CIMAT

- Inicios: Factorizar 15 = 3 . 5 (en el 75% de las veces)
- 2012: Factorizar: 143
- 2014: Factorizar: 56,153

Para factorizar una clave RSA de 2048 se necesitan 8 horas!!!...

Progreso en máquinas cuánticas para atacar a la criptografía

CIMAT

- Inicios: Factorizar 15 = 3 . 5 (en el 75% de las veces)
- 2012: Factorizar: 143
- 2014: Factorizar: 56,153

Para factorizar una clave RSA de 2048 se necesitan 8 horas!!!...pero 20 millones de qubits. Eso tardará unos 25 años con la tecnología actual.

Concurso NIST

FIN

- Si desdeas profundizar sobre el tema.

Luis J. Dominguez Perez, luis.dominguez@cimat.mx / luisjdominguezp@gmail.com