



XIII Congreso Regional de Matemáticas de Castilla y León
Ávila, 15-16 de abril de 2016

Matemáticas: Ciberseguridad y Contraterrorismo



Ángel Martín del Rey
Departamento de Matemática Aplicada
Universidad de Salamanca
delrey@usal.es

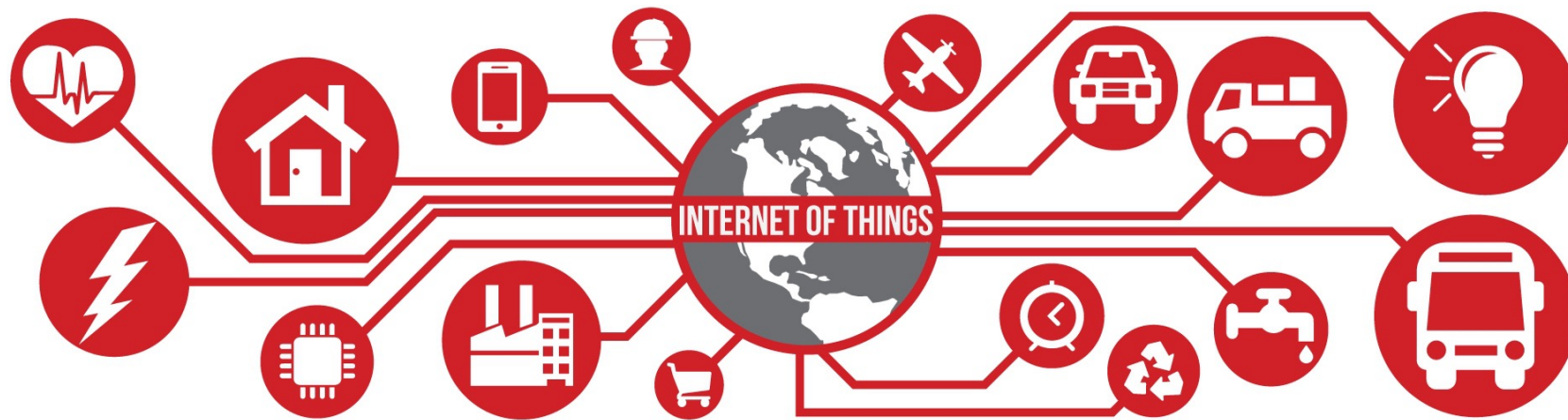


VNIVERSIDAD
D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL



Introducción

- El gran reto en el siglo XXI en el ámbito de las TIC es el pleno establecimiento de la **Internet de las Cosas**.



Introducción

- Actualmente los **Sistemas Informáticos** controlan el funcionamiento de multitud de procesos y tareas, entre los que se incluye el control de las **Infraestructuras Críticas**.



Introducción

- Peligros ya existentes se han adaptado al nuevo escenario y otros han aparecido:
 - ▶ Amenazas a la información
 - ▶ Amenazas a los sistemas informáticos.

Informe sobre ciberamenazas del CCN

El CNI prevé más ciberataques en 2016

Carlos Hidalgo  @carloshidalgo  carlos.hidalgo@bez.es 08 de abril de 2016

Seguridad

 seguir tema

Sociedad red

Tecnología

Terrorismo

↓ El CCN ha tenido que hacer frente a 18.232 incidentes, de los cuales 430 han sido considerados de peligrosidad muy alta

↓ España fue especialmente atacada por grupos de ciberespionaje rusos y chinos, orientados al sector de Defensa

↓ Se prevé un incremento en los ataques al Internet de las Cosas, debido a que los fabricantes descuidan la seguridad

Introducción

- Las **Matemáticas** ofrecen herramientas que permiten analizar, evaluar y gestionar dichas amenazas con el objetivo de minimizar su impacto:
 - ▶ Algoritmos criptográficos para proteger la información (confidencialidad, integridad, autenticidad, etc.)
 - ▶ Modelos matemáticos para detectar, evaluar y gestionar potenciales amenazas en la red.
 - ▶ Modelos matemáticos para el análisis y comportamiento de redes terroristas.

Introducción

¿Cuál es el organismo, agencia o empresa que más matemáticos contrata?



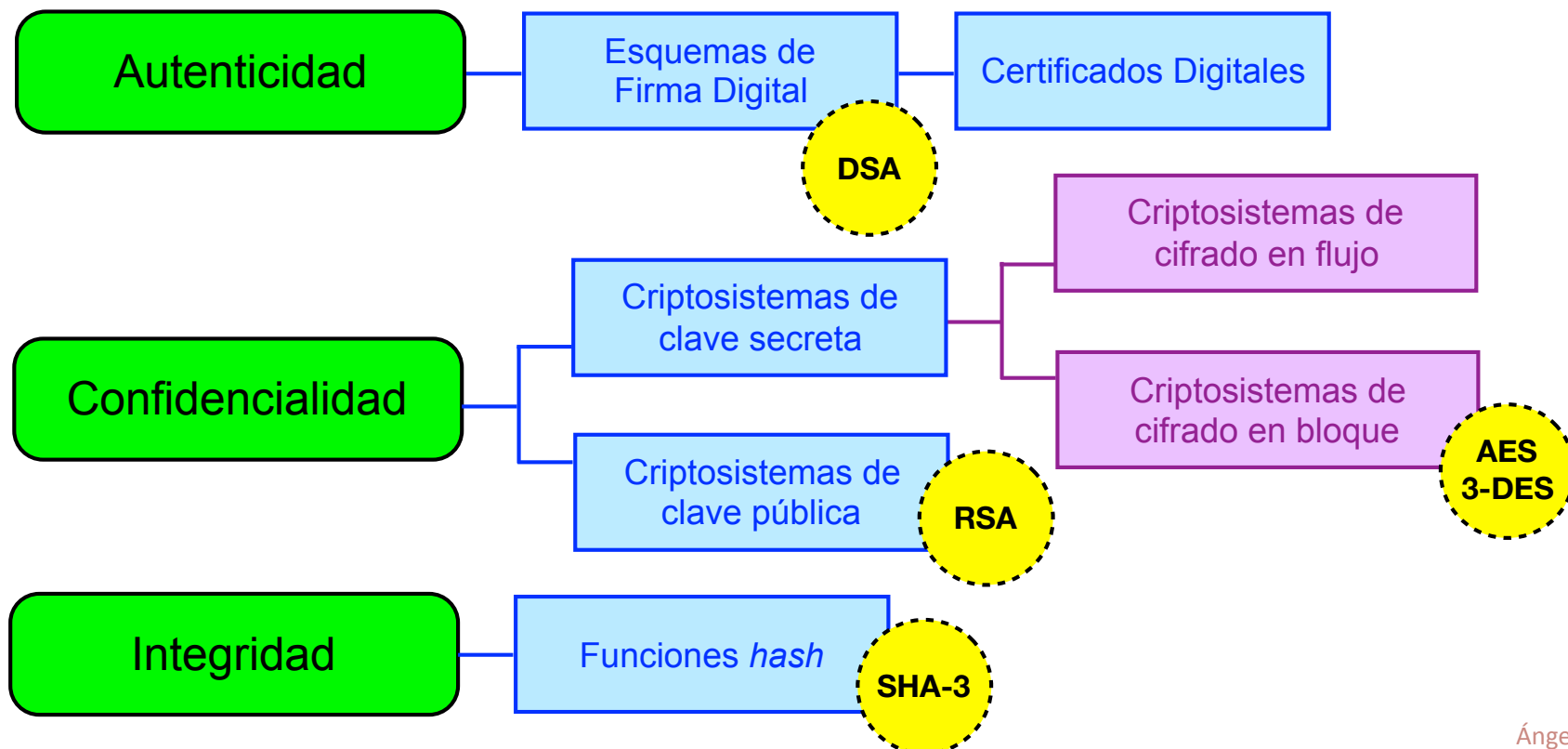


Criptografía: diseño de algoritmos matemáticos para proteger la Información



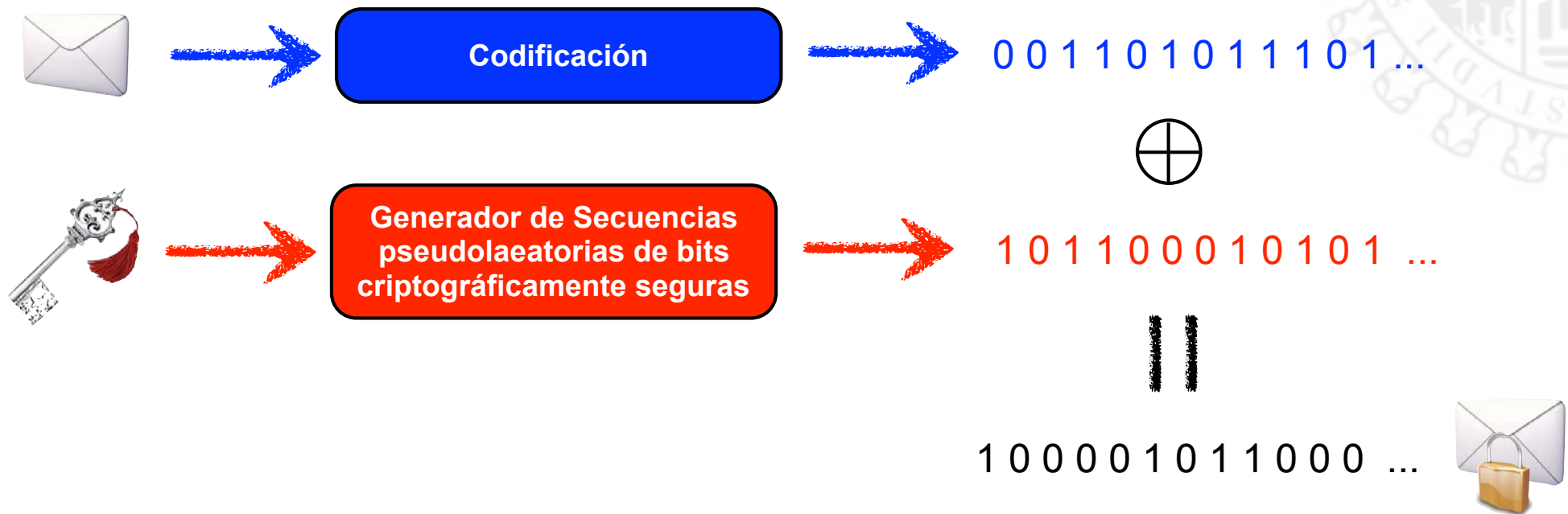
Algoritmos criptográficos: Introducción

- A lo largo de la historia se han utilizado diferentes técnicas para proteger la información.
- El uso de algoritmos matemáticos surge fundamentalmente en el siglo XX en paralelo al desarrollo de los ordenadores.



Algoritmos criptográficos: Cifrado en flujo

- Criptosistemas de clave secreta: **cifrado en flujo**

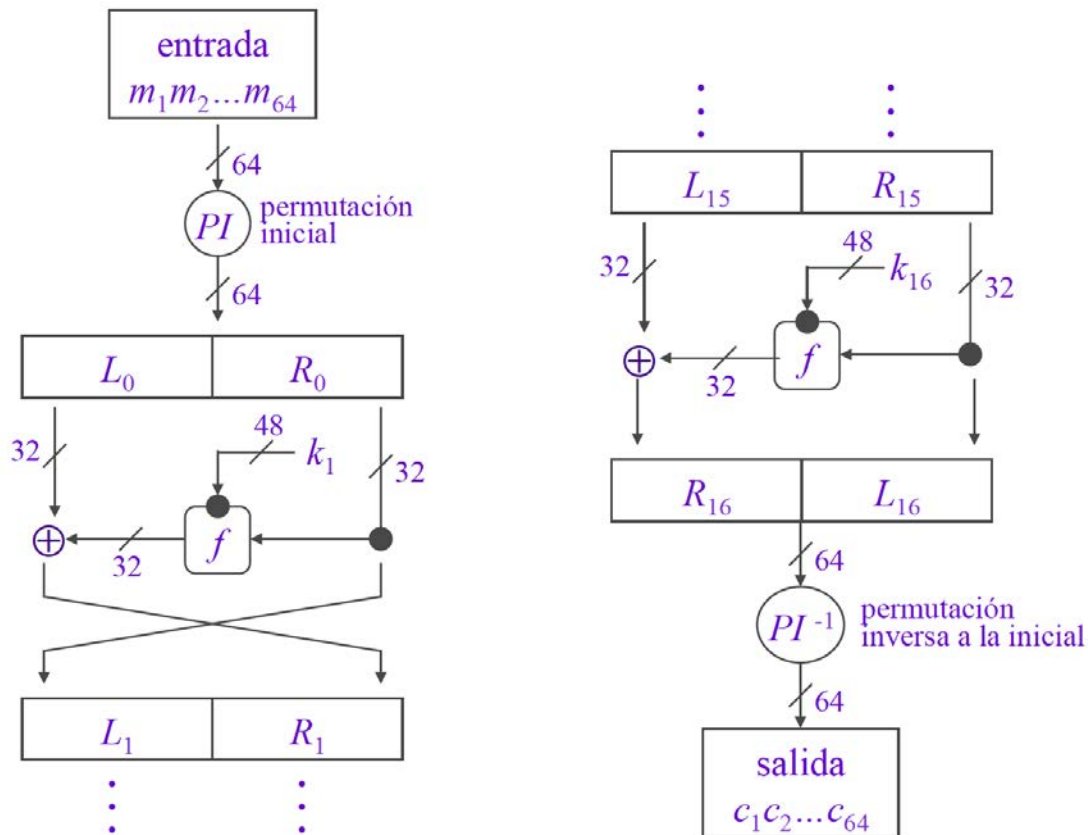


- ▶ Telefonía móvil GSM: algoritmo A5.
- ▶ Bluetooth: algoritmo E0.
- ▶ WEP (WiFi): algoritmo RC4.

$$\begin{array}{ll} 0 \oplus 0 = 0 & 1 \oplus 0 = 1 \\ 0 \oplus 1 = 1 & 1 \oplus 1 = 0 \end{array}$$

Algoritmos criptográficos: Cifrado en bloque

- Criptosistemas de clave secreta: **3-DES**



- Permutaciones.
- Sustituciones: S-boxes.
- Suma XOR:

Algoritmos criptográficos: Clave pública

- Criptosistemas de clave pública: **RSA**



Rivest, Shamir y Adleman

- Cálculo de potencias: m^e
- Cálculo del m.c.d.: $\text{m.c.d.}(e, \phi)$
- Cálculo de congruencias: $c = m^e \pmod{n}$
(c es el resto de dividir m^e entre n)

- n es el producto de dos números primos de 2.048 bits (617 cifras decimales).
- La seguridad del RSA reside en la enorme dificultad que supone factorizar el número n .

Algoritmos criptográficos: El DNI electrónico

- Funciones resumen: **Familia SHA**
 - ▶ La función resumen SHA-256 asigna a una cadena de bits de longitud arbitraria (Gb, Mb,...) una secuencia de 256 bits (resumen) de manera que:
 - Es muy sencillo calcular la secuencia de 256 bits.
 - Es computacionalmente muy difícil encontrar dos mensajes que tengan el mismo resumen.



Algoritmos criptográficos: El DNI electrónico

- En marzo de 2006 comienza la expedición del DNle.



- En septiembre de 2015 se empieza a expedir la versión 3.0 del DNI electrónico.



Algoritmos criptográficos: El DNI electrónico

- Los algoritmos que tiene implementados la versión 3.0 son los siguientes:
 - ▶ Esquema de firma digital RSA (claves de 1024 ó 2048 bits).
 - ▶ Función resumen SHA-256.
 - ▶ Cifrado de clave secreta:
 - 3-DES CBC (claves de 192 bits)
 - AES (claves de 128 bits)



Algoritmos criptográficos: Seguridad

Ataques al algoritmo

- “Romper” un criptosistema de clave pública conlleva resolver un problema matemático muy difícil (seguridad computacional):
 - ▶ factorización de números enteros (RSA)
 - ➡ se ha conseguido factorizar un RSA-768
- Un ordenador cuántico sería capaz de romper el RSA y, en menor medida ECC (criptosistemas de curvas elípticas: *el plan B*).
 - ▶ El algoritmo cuántico de Shor consigue factorizar números muy grandes en tiempo polinómico.

Algoritmos criptográficos: Seguridad

Ataques por canal lateral

- Aprovechan las debilidades de las implementaciones de los algoritmos matemáticos.
- En 2013, Genkin, Shamir y Tromer consiguieron romper una clave RSA-4096 en 1 hora gracias al análisis del sonido emitido por el portátil mientras descifraba algunos mensajes.



Algoritmos criptográficos: Otras aplicaciones

- Identificación amigo/enemigo.
- Póquer *on-line*.
- Venta o intercambio de secretos.
- Reparto de secretos.
- Votación electrónica.
- Descubrimiento mínimo o nulo.



Algoritmos criptográficos: Los servicios secretos

- Inventores *públicos* de la “Criptografía de Clave Pública”



- Ralph Merkle.
- Martin Edward Hellman. 1976
- Bailey Whitfield Diffie.

- Inventores *reales* de la “Criptografía de Clave Pública”



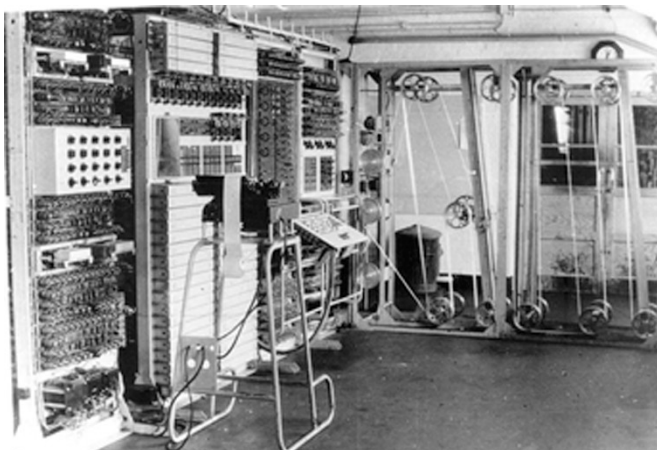
- Clifford Christopher Cocks.
- Malcolm John Williamson. 60's
- James Henry Ellis

Algoritmos criptográficos: Los servicios secretos

- El GCHQ es el homólogo británico a la NSA americana



Government Communications Headquarters
(Reino Unido)



Algoritmos criptográficos: Los servicios secretos

- No solo Estados Unidos y el Reino Unido poseen una agencia de este tipo...



Special Communications Service
(Rusia)



Agence Nationale de la sécurité des systèmes d'information
(Francia)

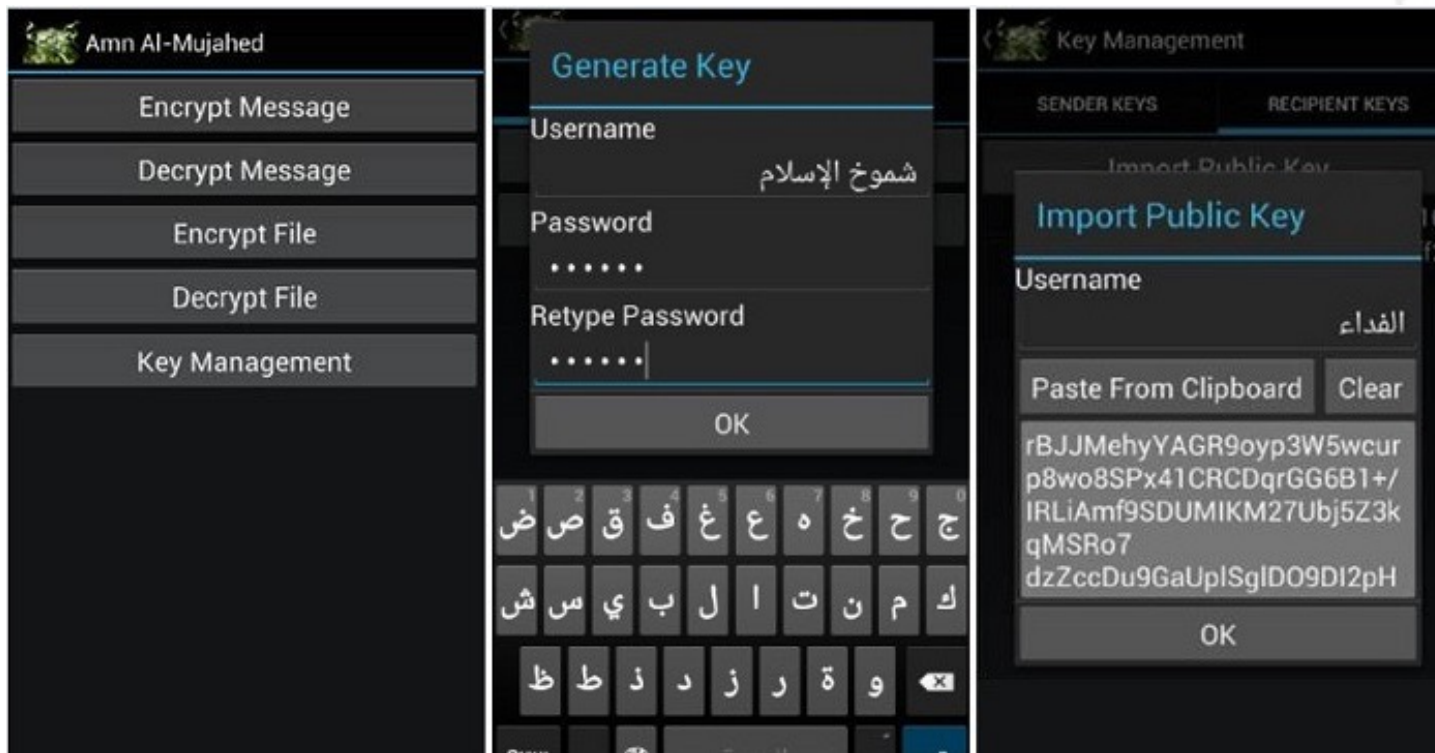


Centro Criptológico Nacional
(España)



Algoritmos criptográficos: Usos maliciosos

- Los terroristas también usan estas tecnologías...



Aplicación *Amn Al-Mujahed* (AES, RSA-4096)

Algoritmos criptográficos: más posibilidades

- **Criptosistemas homomórficos:**

- ▶ Permiten realizar operaciones entre los textos en claro usando los mensajes cifrados.

- ▶ Aplicaciones en...

- * Voto electrónico.
 - * Computación en la nube.
 - * Big Data.
 - * etc.



Algoritmos criptográficos: más posibilidades

- Criptosistemas que preservan el formato:
 - ▶ Permiten que tanto el texto en claro como el criptograma tengan el mismo formato (tipo, tamaño, etc.)
 - ▶ Aplicaciones en...
 - * Información cifrada en bases datos.
 - Números de tarjetas de crédito.
 - Números de la seguridad social.
 - * Computación en la nube.
 - * Cifrado de imágenes digitales.
 - * etc.



Algoritmos criptográficos: ¡Últimas noticias!

- A mediados de agosto de 2015, la NSA (National Security Agency) presenta nuevas directivas en las que recomienda...
 - ▶ No migrar los sistemas funcionando bajo RSA a ECC.
 - ▶ Diseñar nuevos estándares resistentes a los algoritmos cuánticos (*criptografía post-cuántica*).
- Muchas elucubraciones en la comunidad científica...
 - ▶ ¿Han roto el RSA?
 - ▶ ¿Han construido un ordenador cuántico?
 - ▶ ¿Han roto la ECC?
 - ▶ ...



Algoritmos criptográficos: Criptografía post-cuántica

- Posibles algoritmos criptográficos post-cuánticos...
 - ▶ AES: se cree que claves de 256 bits ofrecen una seguridad de 128 bits frente a ataques de naturaleza cuántica.
 - ▶ *Lattice-based cryptography*: NTRU.
 - ▶ *Hash-based cryptography*: se estima que tienen el mismo nivel de seguridad frente a los ataques cuánticos que frente a los convencionales. No es posible desarrollar protocolos de clave pública basados en funciones hash.
 - ▶ *Code-based cryptography*: McEliece. Tienen como desventaja las deficiencias presentadas por los esquemas de firma digital basados en ellos.
 - ▶ *Isogeny-based cryptography*: curvas elípticas isogenas supersingulares sobre \mathbb{F}_{p^2} .

Recursos On-line

- National Security Agency (USA):
<https://www.nsa.gov/kids/index.htm>



Recursos On-line

- Crypto Club (University of Illinois, USA):

<http://cryptoclub.org>





Redes terroristas: análisis matemático de redes complejas

Análisis de redes complejas

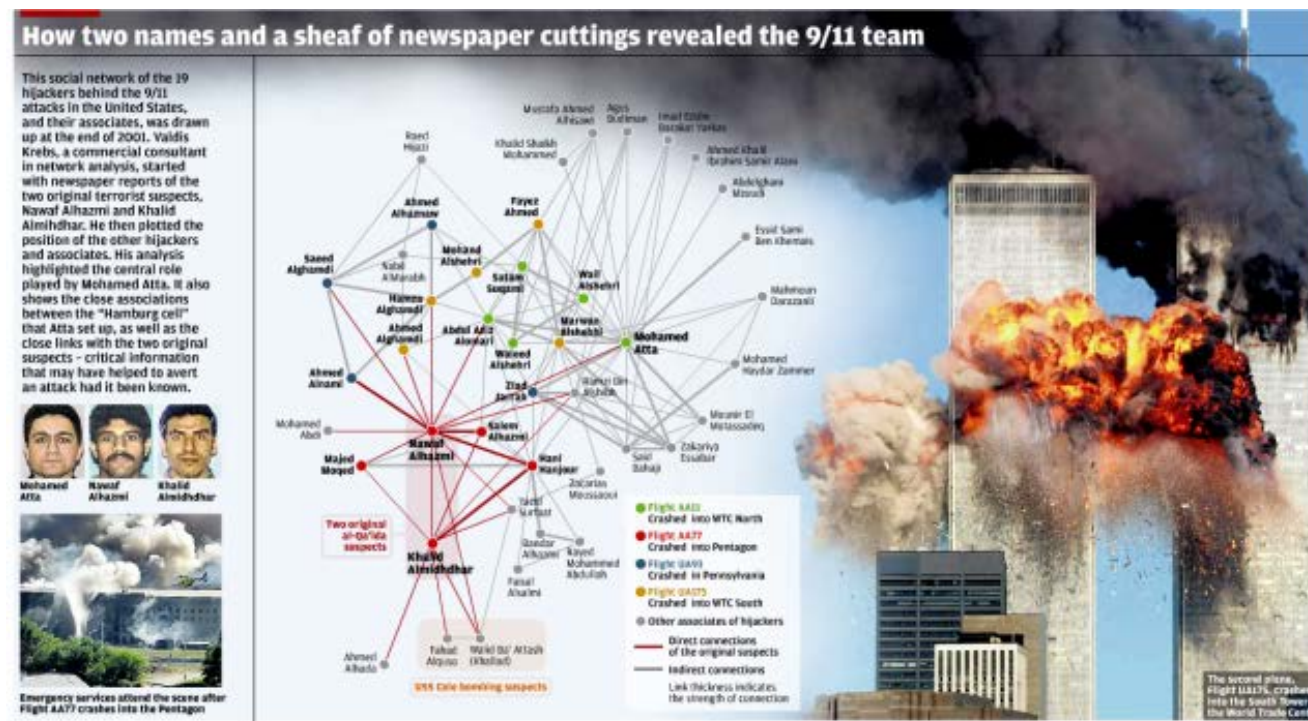
- La estructura organizativa y de interacción de muchos sistemas y fenómenos se pueden describir por medio de **redes complejas**.
- Una red compleja es una colección de actores (de diferente naturaleza) que interactúan entre sí a lo largo del tiempo.
- Matemáticamente son grafos con características dinámicas:

- ▶ Vértices
- ▶ Aristas
- ▶ Topología variable



Estudio de amenazas en redes complejas

- Algunos de los desafíos a los que se enfrenta el Contraterrorismo pueden ser modelizados matemáticamente y resueltos algorítmicamente usando el Análisis de Redes Complejas.



Estudio de amenazas en redes complejas

- Podemos estudiar sus características, obtener e interpretar datos y resultados, realizar simulaciones, etc.
- En redes con miles de participantes y una gran cantidad de interacciones de todo tipo (redes sociales, contactos personales, uso de aplicaciones,...), ¿es posible detectar anomalías, características, conexiones ocultas o patrones temporales? ¿sería posible predecir la dinámica de los mismos?

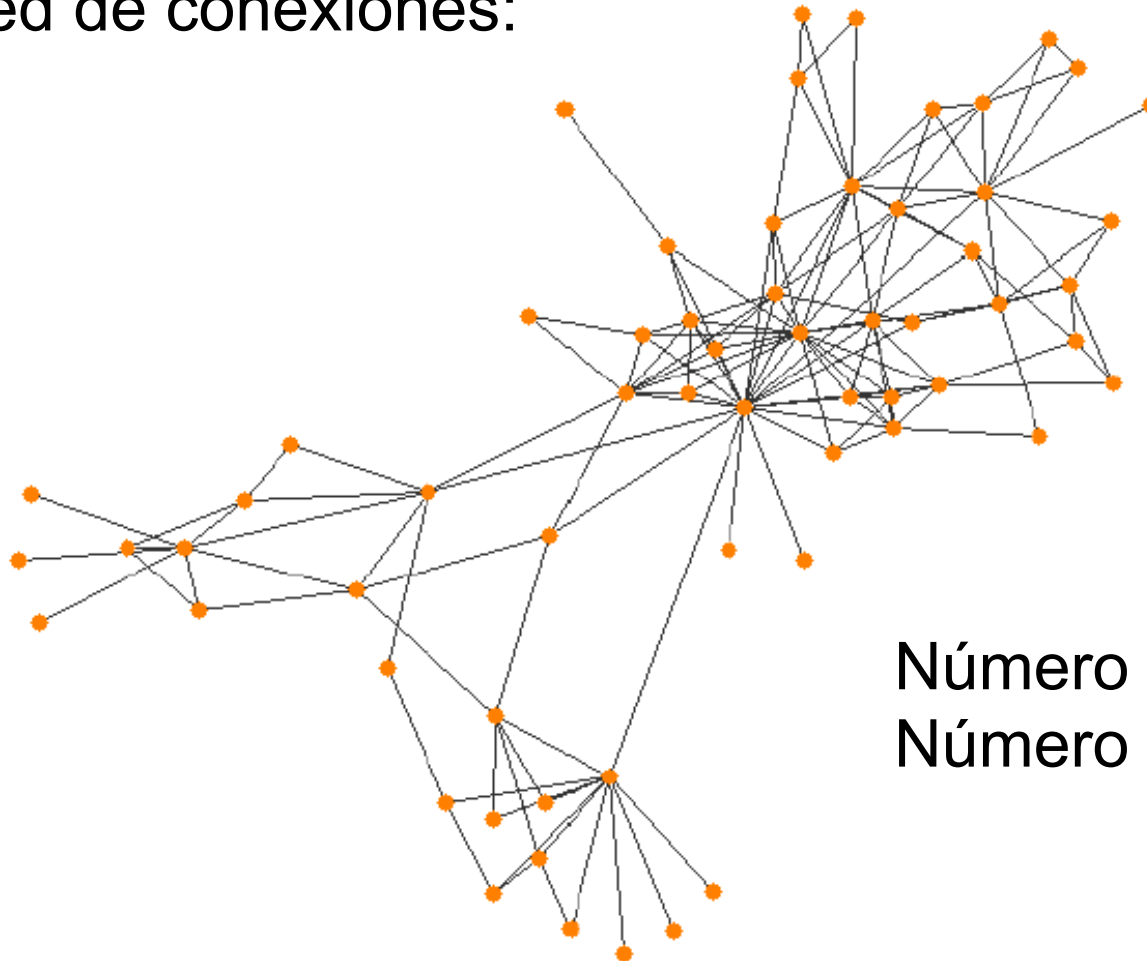
Estudio de amenazas en redes complejas

- En el estudio matemático de las redes terroristas cobran especial importancia las **medidas de centralidad**:
 - ▶ **Centralidad de grado**: nº de contactos de cada terrorista.
 - ▶ **Intermediación**: mide la importancia de un terrorista teniendo en cuenta el nº de veces que actúa como enlace entre otros dos.
 - ▶ **Centralidad de vector propio**: indica la influencia de un terrorista en la red teniendo en cuenta el número de terroristas en posiciones privilegiadas a los que tiene acceso.
 - ▶ **Cercanía**: indica cómo de “cercano” está un terrorista al centro de la red.
 - ▶ **Coeficiente de agrupamiento**: indica en qué medida un terrorista se encuentra conectado a la red.

Estudio de amenazas en redes complejas

- Red terrorista del 11 de septiembre

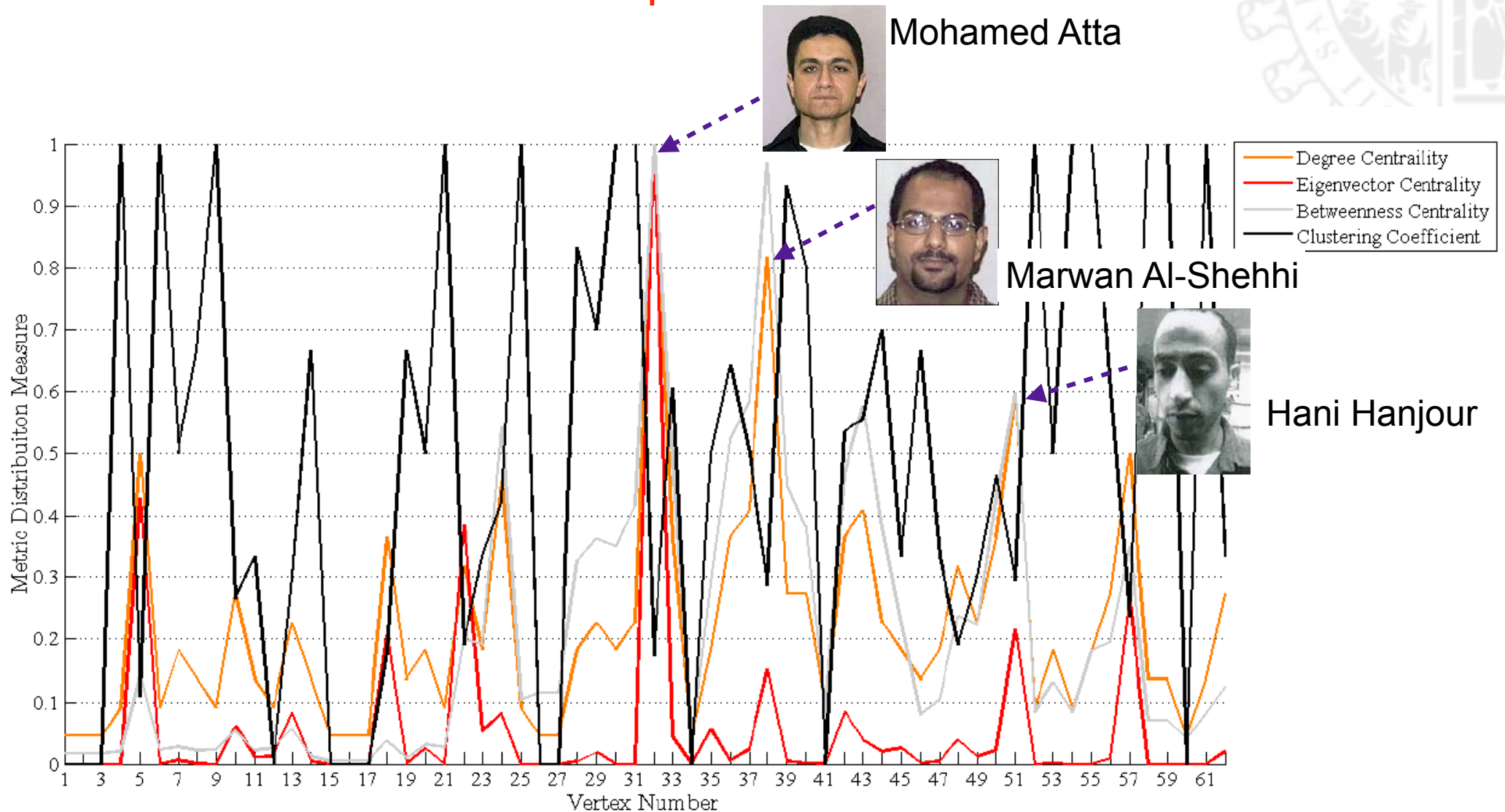
- ▶ Red de conexiones:



Número de nodos: 62
Número de aristas: 152

Estudio de amenazas en redes complejas

- Red terrorista del 11 de septiembre



Estudio de amenazas en redes complejas

- El análisis de redes complejas permite demostrar de manera científica certezas obtenidas fruto de la investigación “sobre el terreno”: *comprobación a posteriori*.
- La gran ayuda de este análisis a la lucha contrterrorista es la capacidad para detectar variables ocultas y dinámicas “invisibles” en las redes terroristas.
 - ▶ **Determinación de la estructura y funcionamiento de la red terrorista a partir de información parcial de la misma.**
 - ▶ **Teorema de Takens.**

Estudio de amenazas en redes complejas

- Existen también modelos matemáticos para simular el comportamiento (crecimiento/decrecimiento) del número de individuos en las redes terroristas.
- Usualmente son modelos compartimentales:
 - ▶ Dividen la población en tres clases:
 - Terroristas: $x(t)$.
 - Susceptibles de ser reclutados: $y(t)$.
 - No susceptibles de ser reclutados: $z(t)$.
 - ▶ La dinámica viene regida por un sistema de ecuaciones diferenciales ordinarias.

Estudio de amenazas en redes complejas

- Ejemplo:

reclutamiento
(directo)



contraterrorismo
(actuaciones)



$$x'(t) = a \cdot x(t) \cdot y(t) - b \cdot x(t)^2 + (c - 1) \cdot x(t)$$

$$y'(t) = -a \cdot x(t) \cdot y(t) - e \cdot x(t)^2 \cdot y(t) + f \cdot x(t) + g \cdot y(t)$$

$$z'(t) = e \cdot x(t)^2 \cdot y(t) - h \cdot x(t) + l \cdot z(t)$$



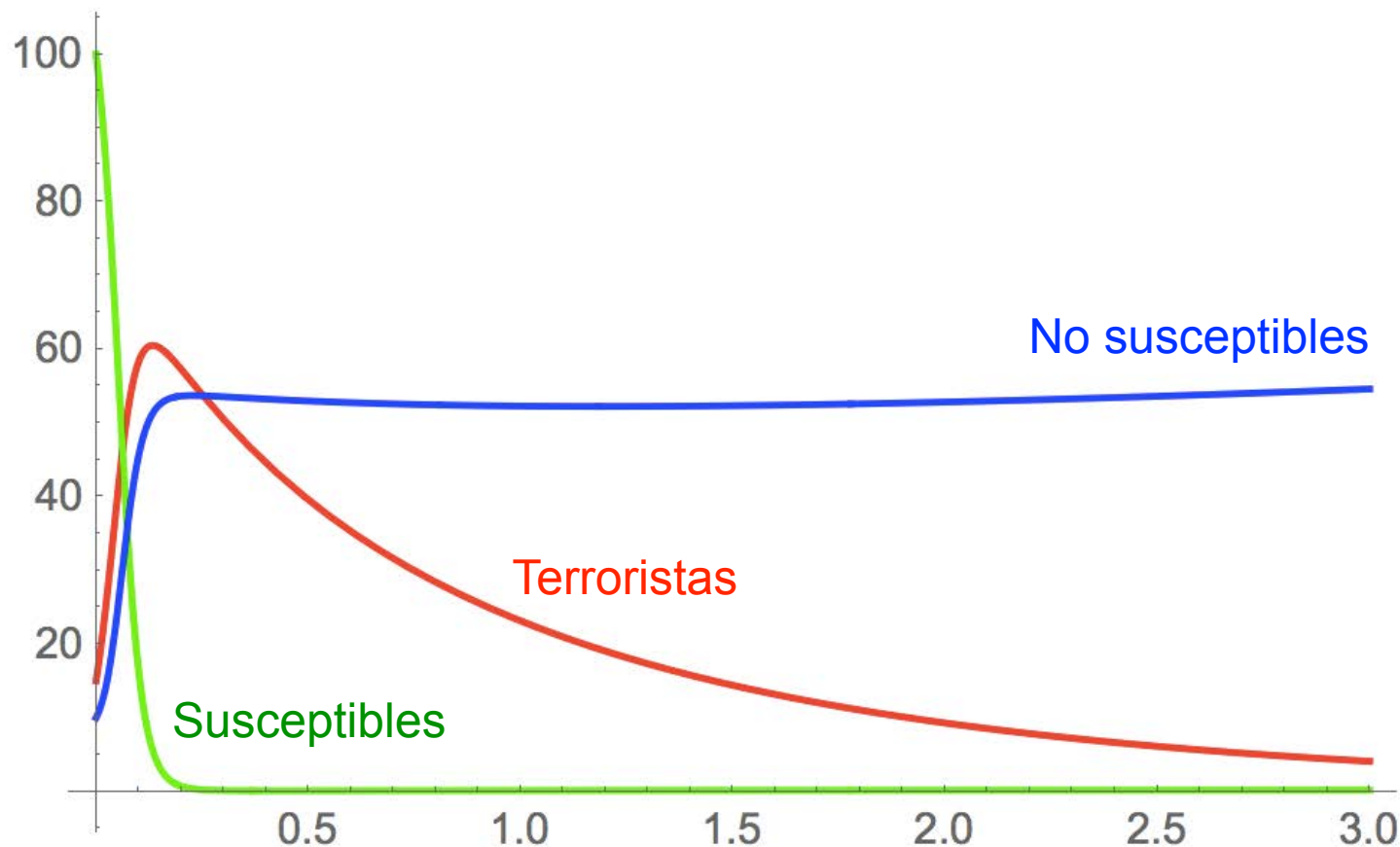
contraterrorismo
(persuasión)



reclutamiento
(fascinación)

Estudio de amenazas en redes complejas

- Ejemplo:





¡ Muchísimas gracias por vuestra atención !

¿alguna pregunta o comentario?