VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Modelos Matemáticos en Ciberseguridad

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

Bachillerato de Investigación, I.E.S. “Vaguada de la Palma”, 17 de diciembre de 2014

Introducción

- El gran desarrollo de las TIC en los últimos años ha dado lugar a una sociedad totalmente dependiente de las mismas: en paralelo a nuestra vida en el mundo físico desarrollamos también una vida en el ciberespacio.

Introducción

- Hoy en día la Información es uno de los bienes más preciados y los Sistemas Informáticos controlan el buen funcionamiento de multitud de procesos y tareas.

Introducción

- Peligros existentes anteriormente se han adaptado al nuevo escenario y otros han aparecido:

Amenazas contra la información

- Espionaje.
- Robo y publicación de información clasificada.
- Robo y publicación de datos personales.
- Robo de la identidad digital.
- Fraude.

CIBERATAQUES CONTRA LA SEGURIDAD »

España sufre un récord de asaltos cibernéticos desde Rusia y China

JOAQUÍN GIL | Madrid 173

Los cuatro ministerios vinculados a la seguridad reciben ataques de 'hackers' con los virus más sofisticados que se conocen. Los servicios secretos sufrieron 100 tentativas de infiltración en 2014

Amenazas contra los sistemas

- Amenazas Persistentes Avanzadas.
- Ataques contra infraestructuras críticas.
- Ataque contra las redes y sistemas de control.
- Infecciones por malware.

Introducción

- Las Matemáticas ofrecen herramientas que permiten analizar, evaluar y gestionar dichas amenazas con el objetivo de minimizar el impacto de las mismas:
  - Algoritmos criptográficos para proteger la información (confidencialidad, integridad, autenticidad, etc.)
  - Modelos matemáticos para simular la propagación de malware.
  - Modelos matemáticos para detectar, evaluar y gestionar potenciales amenazas en la red.
  - Etc.

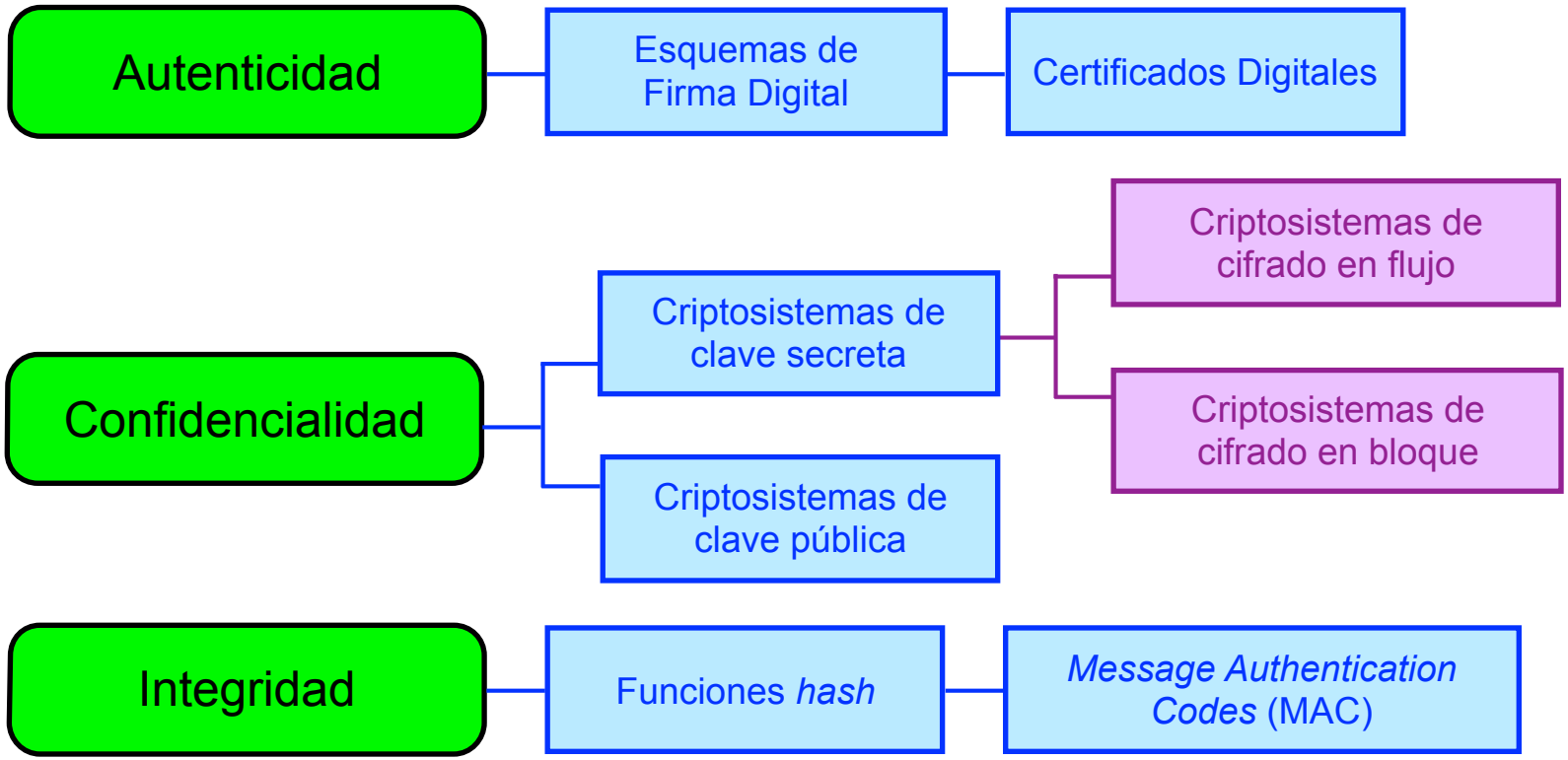
Introducción

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

Algoritmos criptográficos para proteger la Información

Algoritmo criptográficos: Introducción

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



Algoritmos criptográficos: El DNI electrónico

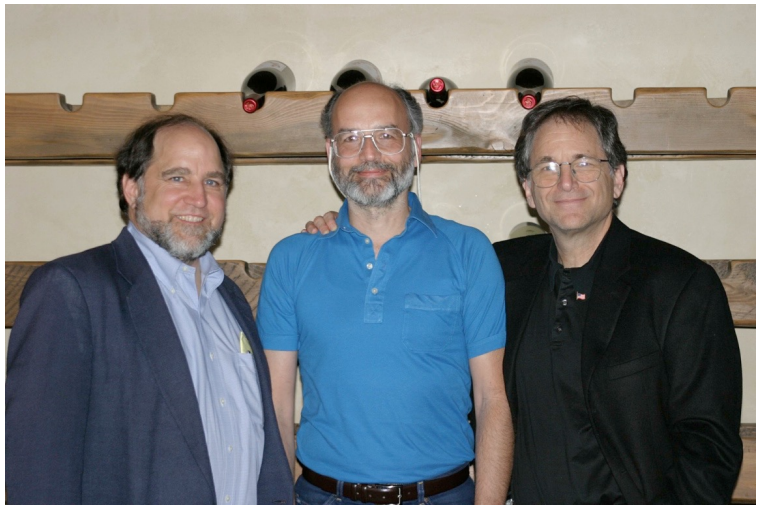
- En marzo de 2006 comienza la expedición del DNIe.

dni electrónico

- Los algoritmos que tiene implementados son los siguientes:
  - Esquema de firma digital RSA.
  - Función resumen SHA-1.
  - Cifrado en bloque: Triple DES.

Algoritmos criptográficos: El DNI electrónico

¿Qué Matemáticas se utilizan en el protocolo de cifrado RSA?



Rivest, Shamir y Adleman

- Cálculo de potencias: m^e
- Cálculo del m.c.d.: $\mathrm{m.c.d.}\left(e,\phi\right)$
- Cálculo de congruencias: $c = m^e \left(\mathrm{mod}\, n\right)$

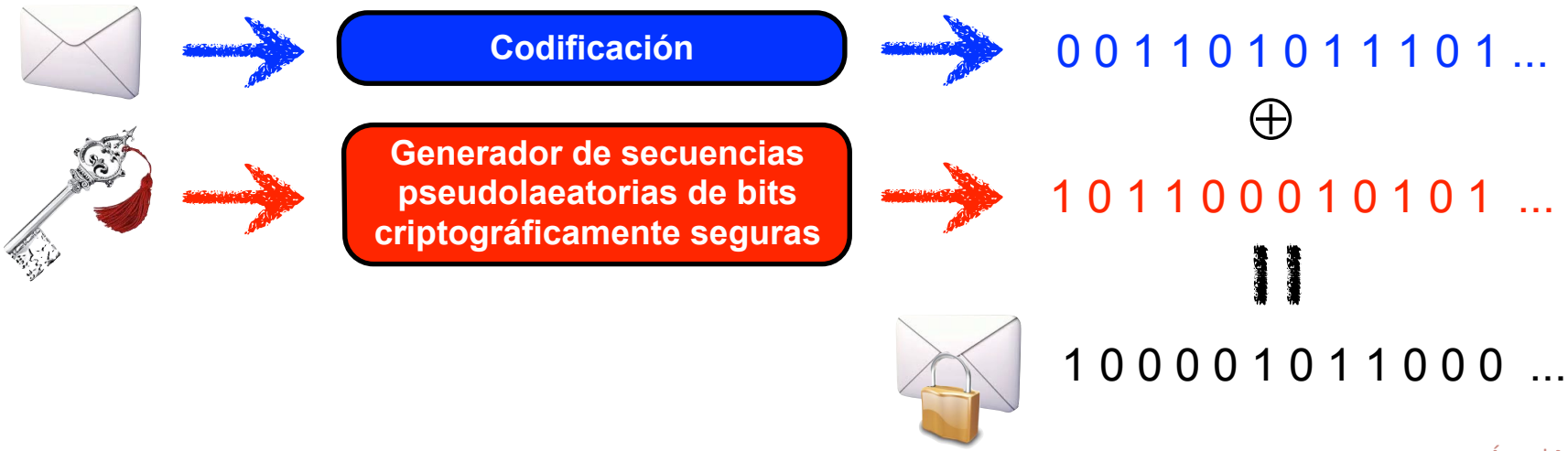
(c es el resto de dividir m^e entre n)

- 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

¿Qué Matemáticas se utilizan en el Triple DES?

- Permutaciones.
- Sustituciones: S-boxes.
- Suma XOR: $0 \oplus 0 = 0 \quad 1 \oplus 0 = 1$
  $0 \oplus 1 = 1 \quad 1 \oplus 1 = 0$



Algoritmos criptográficos: El DNI electrónico

¿En qué se basan las funciones resumen?

- Las funciones resumen son funciones de la forma:

$$f : M \rightarrow H$$

$$m \mapsto h = f(m)$$

de manera que:

- Es muy sencillo calcular la imagen de un mensaje: $f(m)$.
- El tamaño de m es variable (Gb, Mb,...) mientras que el de h es fijo (128-512 bits).
- Es computacionalmente muy difícil encontrar dos mensajes que tengan la misma imagen (resumen).

Algoritmos criptográficos: El DNI electrónico

DOCUMENTO FIRMADO ELECTRÓNICAMENTE Identificador: 0WFW4SQ8IW1NH

Nº Registro: 20149000207491 Fecha Registro: 27/03/2014 16:26:37 Fecha copia: 27/03/2014 16:26:40

Firmado por: ANGEL MARIA MARTIN DEL REY

Acceda a la página web: https://www.ae.jcyl.es/verDocumentos/ver?idDOE=0WFW4SQ8IW1NH para visualizar el documento original

Junta de Castilla y León
Consejería de Educación

D) DATOS DE LOS INVESTIGADORES.			
1º. INVESTIGADOR PRINCIPAL.			
NIF/NIE: 07953200F	Sexo: Hombre	Nombre: ÁNGEL MARÍA	
1er. Apellido: MARTÍN		2º Apellido: DEL REY	
Teléfono de contacto: 669144059		Correo electrónico: delrey@usal.es	

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.

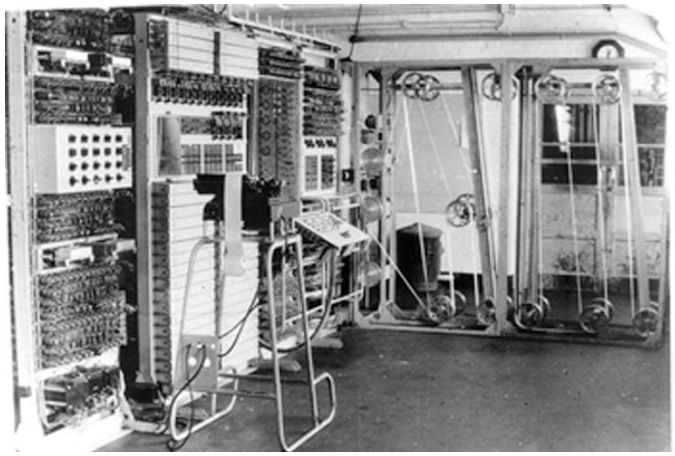
- Inventores *reales* de la "Criptografía de Clave Pública"

  - Clifford Christopher Cocks.
  - Malcolm John Williamson. 1973
  - James Henry Ellis

Algoritmos criptográficos: Los servicios secretos

- El GCHQ es el homólogo británico a la NSA americana

Government Communications Headquarters
(Reino Unido)



Aplicaciones: Sociedad de la Información

- 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)

Modelos matemáticos para simular la propagación del malware

Simulación de la propagación de malware

- El malware es una de las principales amenazas a la seguridad de la información.
  - Su impacto social, económico, político, etc. es muy alto.
  - Un porcentaje significativo de dispositivos están infectados.

- La lucha contra el malware se lleva a cabo en diferentes frentes:
  - Concienciación del usuario.
  - Desarrollo de software anti-malware.
  - Simulación de la propagación del malware.

Simulación de la propagación de malware

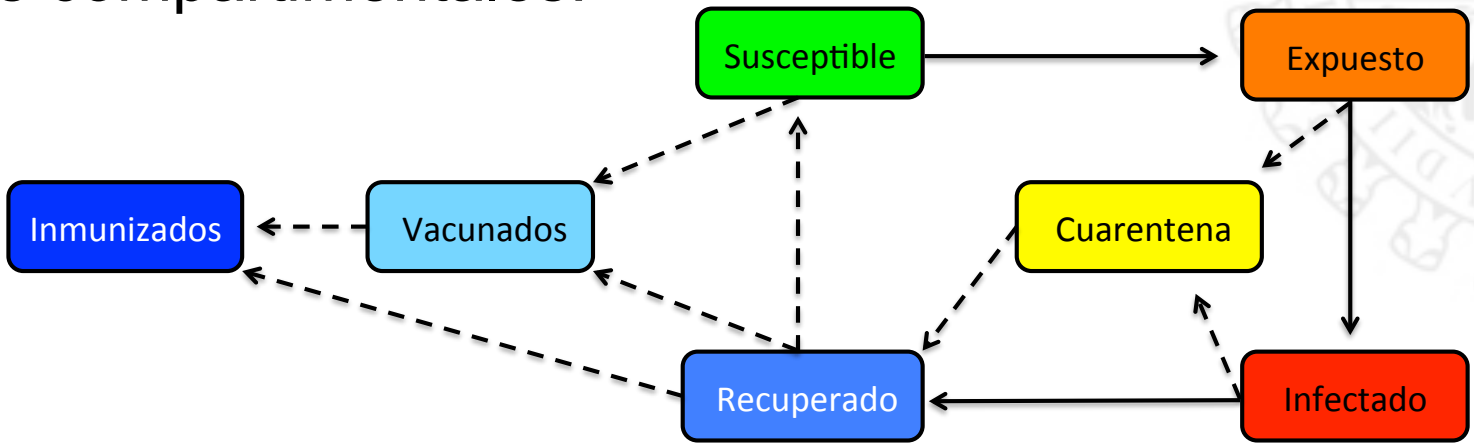
- Los simuladores se basan en la implementación computacional de un determinado modelo matemático.

- Su importancia radica en:
  - Modelización del comportamiento de la epidemia.
  - Probar la efectividad de las posibles contramedidas.
  - Tomar decisiones adecuadas para controlar la epidemia.
  - Herramienta de análisis forense.

- La modelización matemática de la propagación de malware se basa en la Epidemiología Matemática.

Simulación de la propagación de malware

- Son modelos compartimentales:



- Deterministas o estocásticos.
- Continuos o discretos.
- Globales o individuales.
- La mayoría son deterministas, continuos (EDOs) y globales: se basan en el modelo de Kermack y McKendrick (1927).

Simulación de la propagación de malware

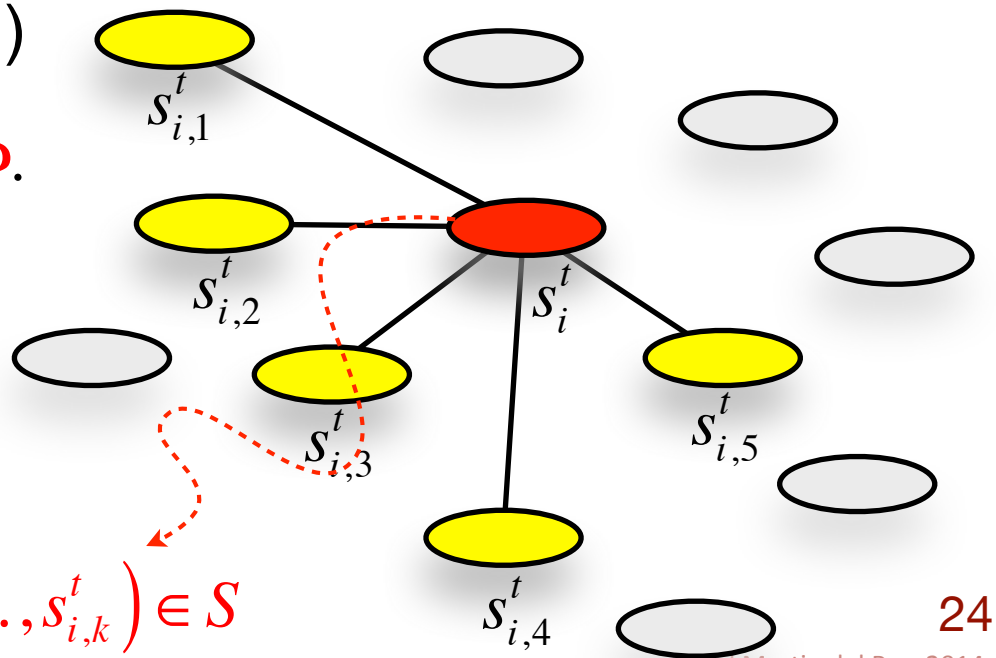
- Los modelos basados en ecuaciones diferenciales...
  - son rigurosos y matemáticamente bien fundamentados.
  - sus propiedades matemáticas son estudiadas:
    - ✓ Número reproductivo básico R_0 (si $R_0 < 1$ no hay propagación, si $R_0 > 1$ hay propagación).
    - ✓ Disease-free equilibrium (ausencia de individuos infectados).
    - ✓ Endemic equilibrium (existencia perpetua de individuos infectados).
  - su interés fundamental es puramente académico.

Simulación de la propagación de malware

- Presentan los siguientes inconvenientes:
  - Los dispositivos se encuentran homogéneamente distribuidos y conectados.
  - No se tienen en cuenta las características particulares de los dispositivos y de sus usuarios.
  - No es posible simular la dinámica individual de cada dispositivo.
- Como alternativa proponemos el uso de modelos individuales y discretos basados en agentes, y más concretamente en autómatas celulares.

Simulación de la propagación de malware

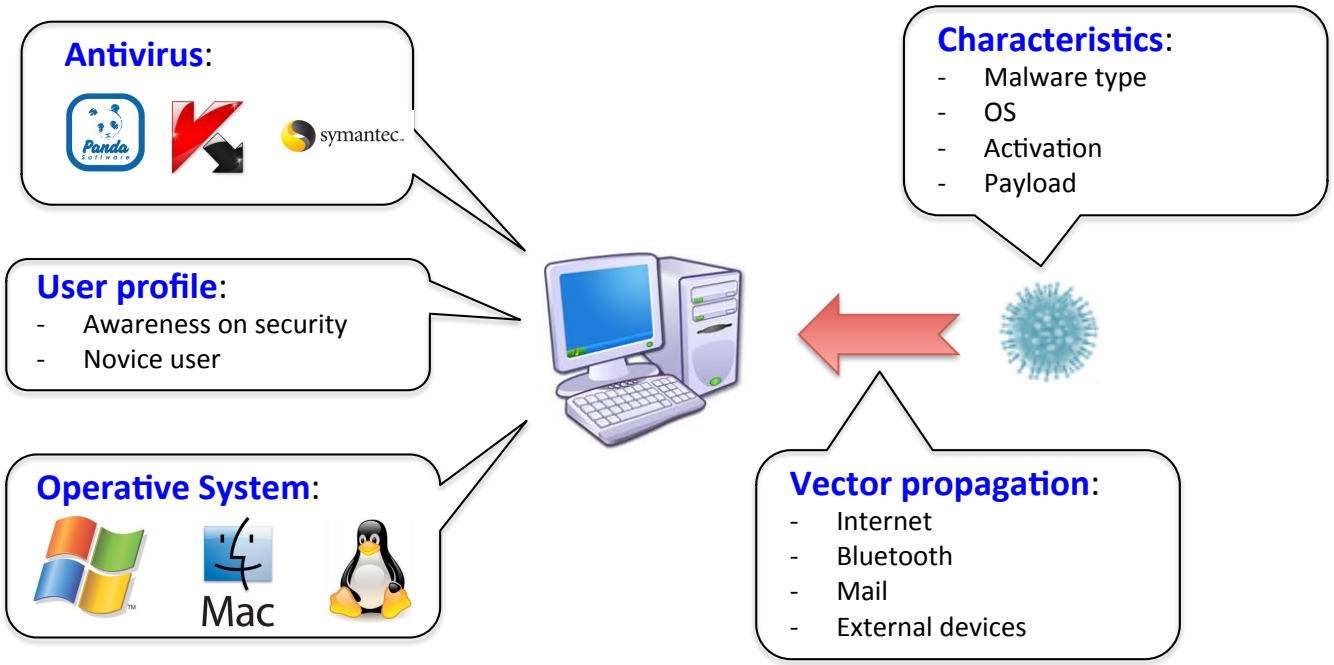
- Un autómata celular (AC) es un modelo simple de computación que es capaz de simular sistemas muy complejos.
- Un autómata celular viene definido por:
  - El espacio celular (topología, vecindades)
  - El conjunto de estados *S* (finito)
  - La función de transición local Φ.



$$s_i^{t+1} = \Phi\left(s_i^t, s_{i,1}^t, \ldots, s_{i,k}^t\right) \in S$$

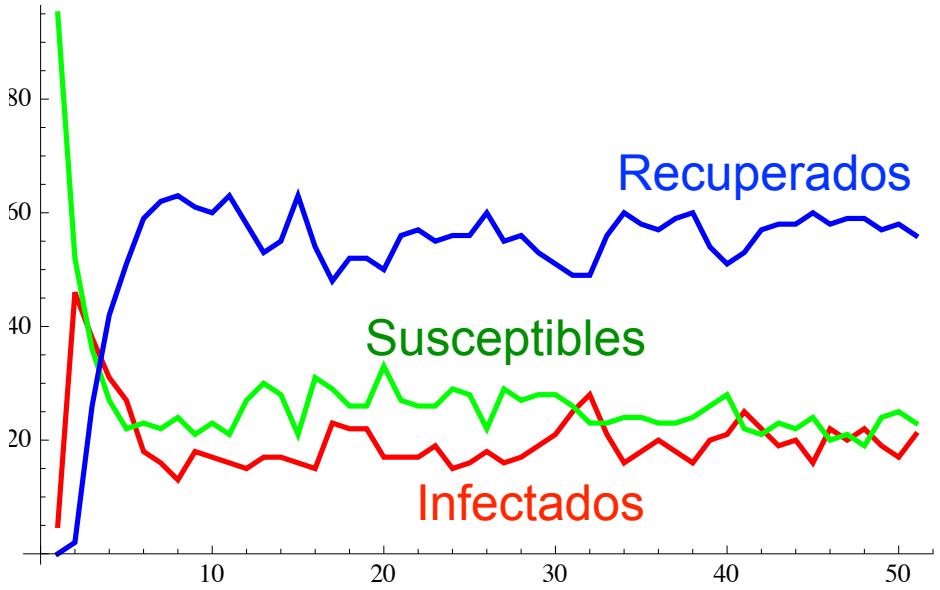
Simulación de la propagación de malware

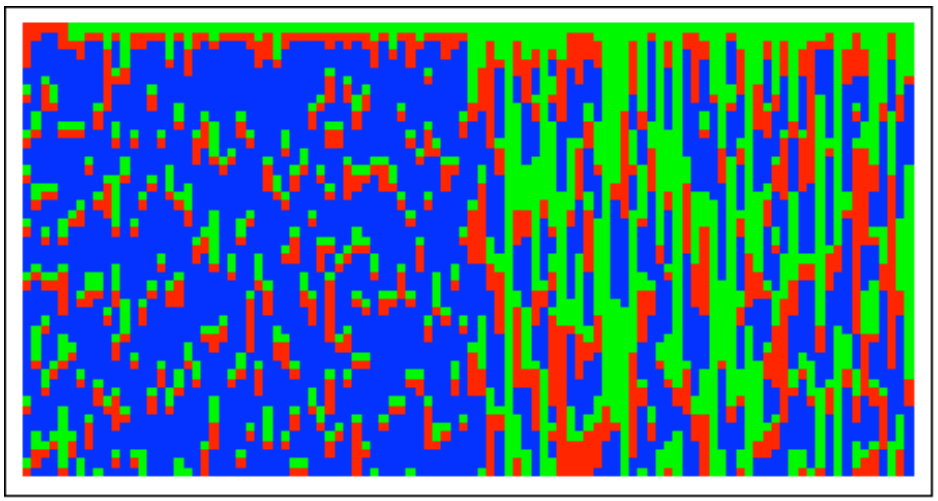
- Los ACs nos permiten capturar las características individuales de los actores del sistema.



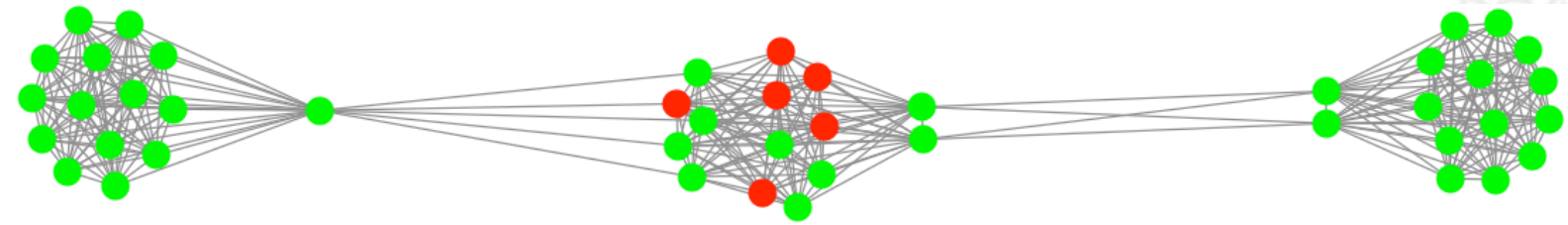
Simulación de la propagación de malware

- Los modelos matemáticos basados en ACs permiten obtener el comportamiento global e individual de los dispositivos:

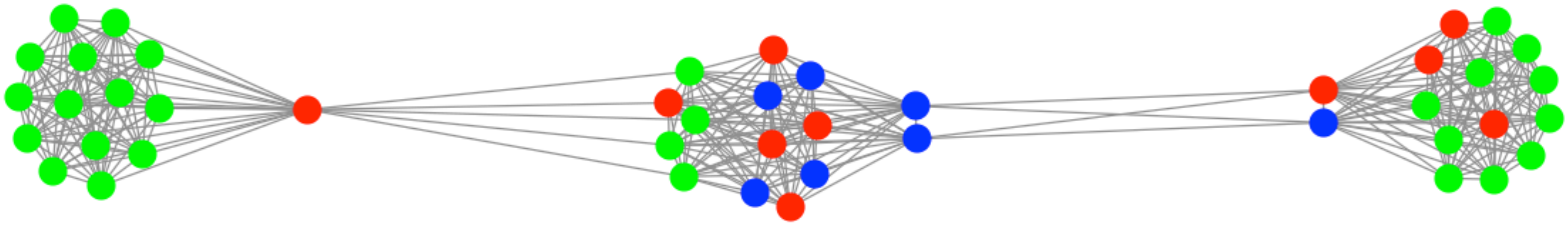




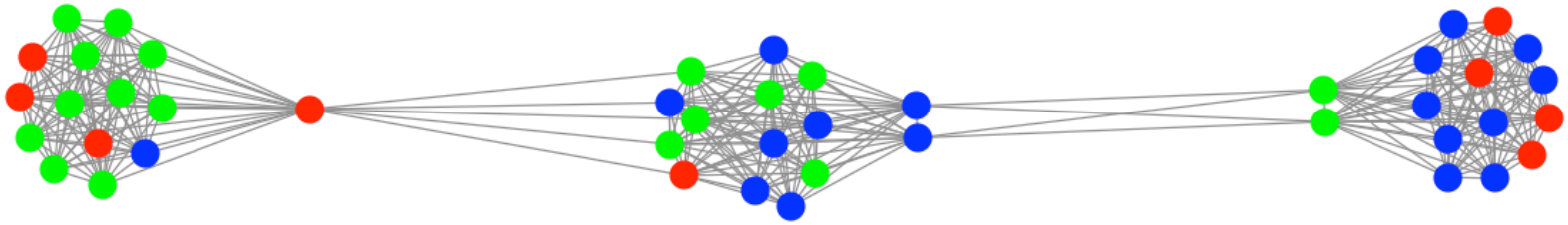
Simulación de la propagación de malware



$t = 0$

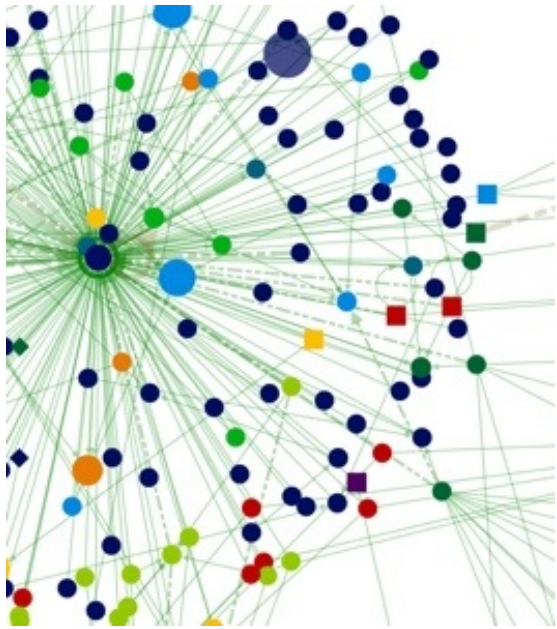


$t = 3$



$t = 6$

Modelos matemáticos para detectar, evaluar y gestionar potenciales amenazas en la red



Estudio de amenazas en redes complejas

- Los “malos” utilizan las redes sociales para sus fines.

INTERNACIONAL

El espionaje británico pide ayuda a Silicon Valley para luchar contra el ciber-yihadismo

LUIS VENTOSO / CORRESPONSAL EN LONDRES | Día 05/11/2014 - 14.12h

- Durante su asalto a la ciudad iraquí de Mosul, el Estado Islámico envió 40.000 tuits al día

Publicidad

Del 12 al 24 de dici

Las redes sociales son una herramienta clave para los grupos terroristas

Por AFP en Mundo 06/12/14 2:11pm

Las redes sociales permiten a los grupos terroristas jugar un papel más activo a la hora de alcanzar a su público. ARCHIVO GETTY

Por Rob Lever

MIDDLE EAST

Digital War Takes Shape on Websites Over ISIS

By BRIAN KNOWLTON SEPT. 26, 2014

Email

Share

Tweet

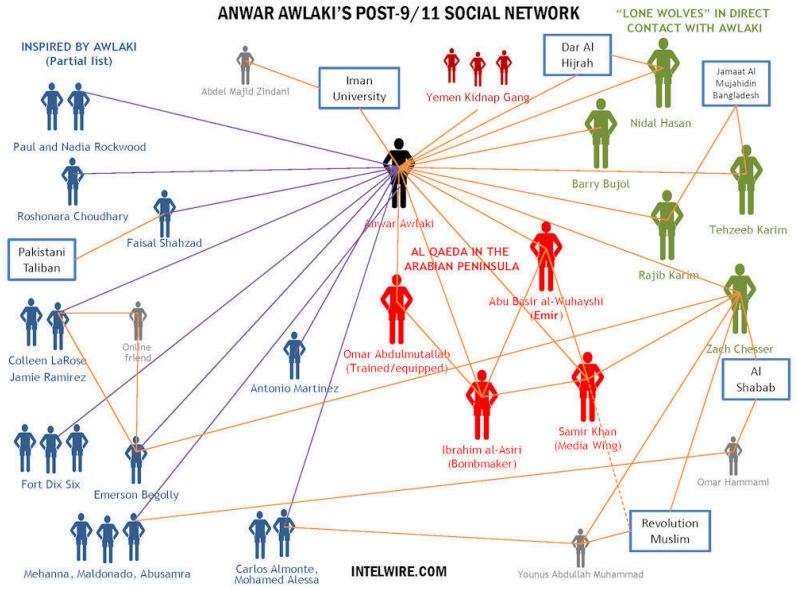
WASHINGTON — Along with its surprising military success, the Islamic State group has demonstrated a skill and sophistication with social media previously unseen in extremist groups.

And just as the United States has begun an aggressive air campaign against the militants, Richard A. Stengel, the under secretary of state for public diplomacy, believes the United States has no choice but to counter their

Estudio de amenazas en redes complejas

- Muchos de los problemas y desafíos a los que se enfrenta el Contraterrorismo pueden ser modelizados matemáticamente y resueltos algoritmicamente usando la Teoría de Grafos y las Matemáticas Discretas.

- La Teoría de Grafos nos permite analizar matemáticamente una red.



Estudio de amenazas en redes complejas

- Podemos estudiar sus características, obtener e interpretar datos y resultados, realizar simulaciones, etc.

- En grafos con más de 10^8 de nodos y más de 10^9 de interacciones por segundo, ¿es posible detectar anomalías, características, conexiones ocultas o patrones temporales? ¿sería posible predecir la dinámica de los mismos?

¡**Muchísimas gracias** por vuestra atención!