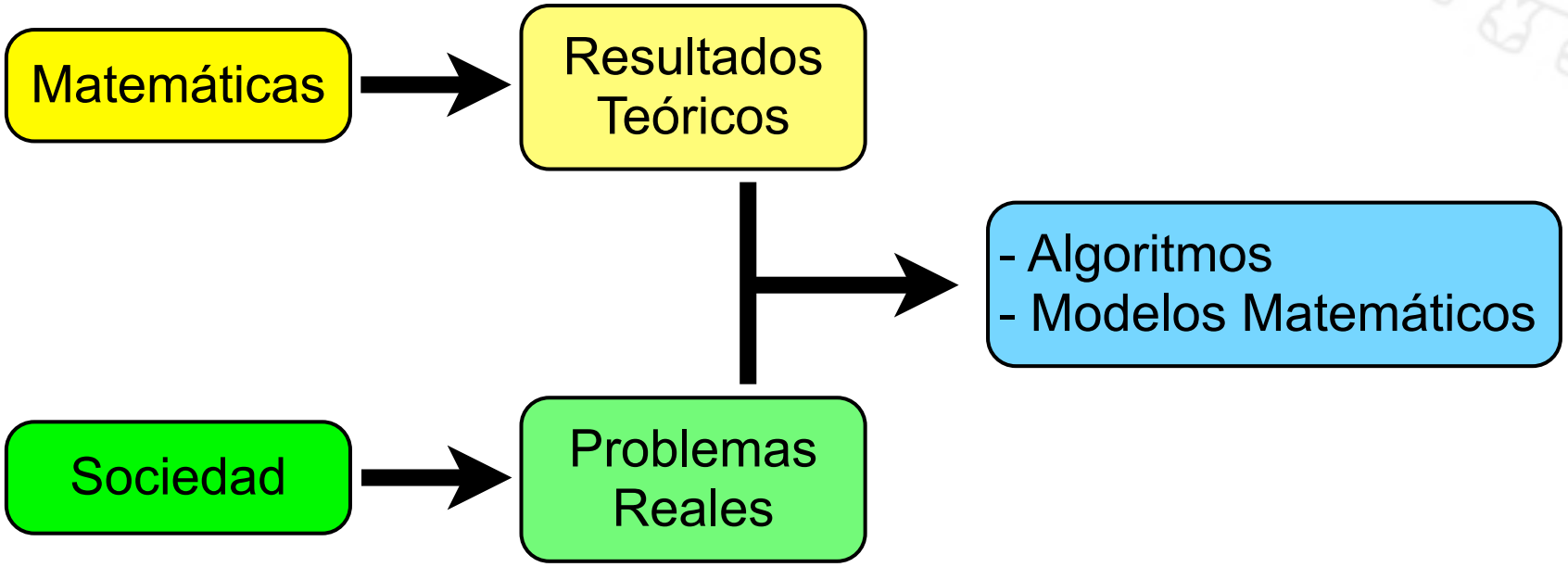
Aplicaciones de las Matemáticas

Ángel Martín del Rey
Departamento de Matemática Aplicada
Instituto de Física Fundamental y Matemáticas
Universidad de Salamanca
delrey@usal.es

XXII Olimpiada Provincial de Resolución de Problemas (Salamanca, 3 de mayo de 2014)

Introducción

La **Matemática Aplicada** consiste en...



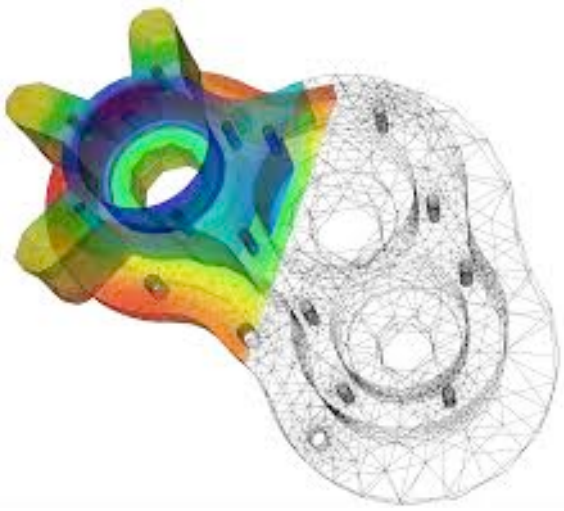
Introducción

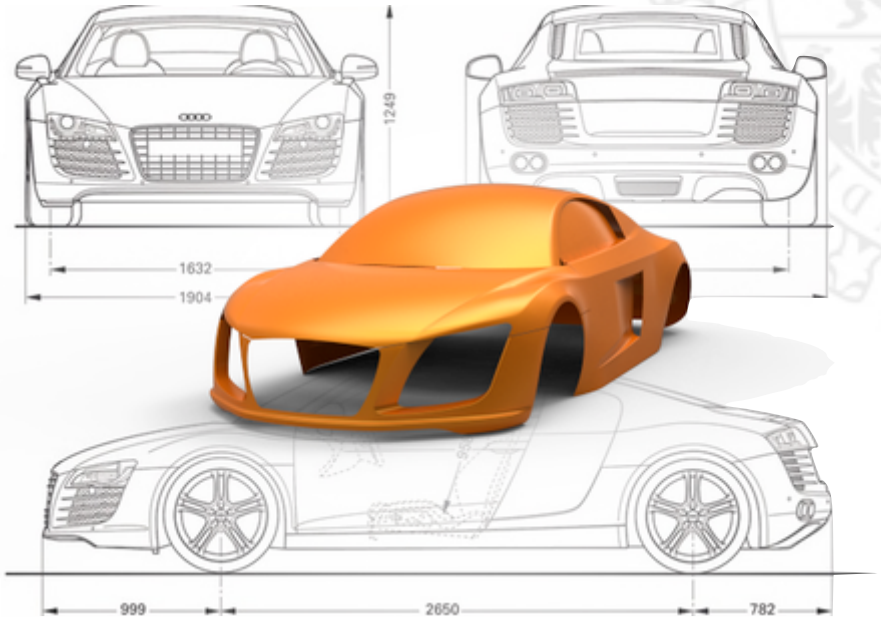
Se han desarrollado algoritmos y modelos para dar respuesta a múltiples retos planteados en diferentes situaciones...

- Ingeniería
- Economía
- Medio Ambiente
- Medicina y Salud
- Sociedad de la Información
- etc.

Aplicaciones: Ingeniería

- Diseño de superficies





Aplicaciones: Economía

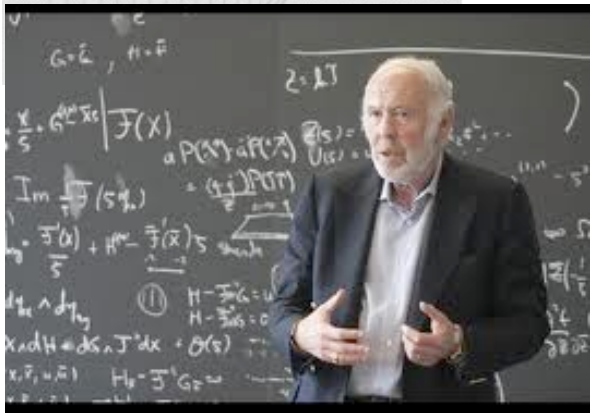
- Asesoría fiscal
- Operaciones en el mercado financiero

Renaissance

- Locations
- Job Openings

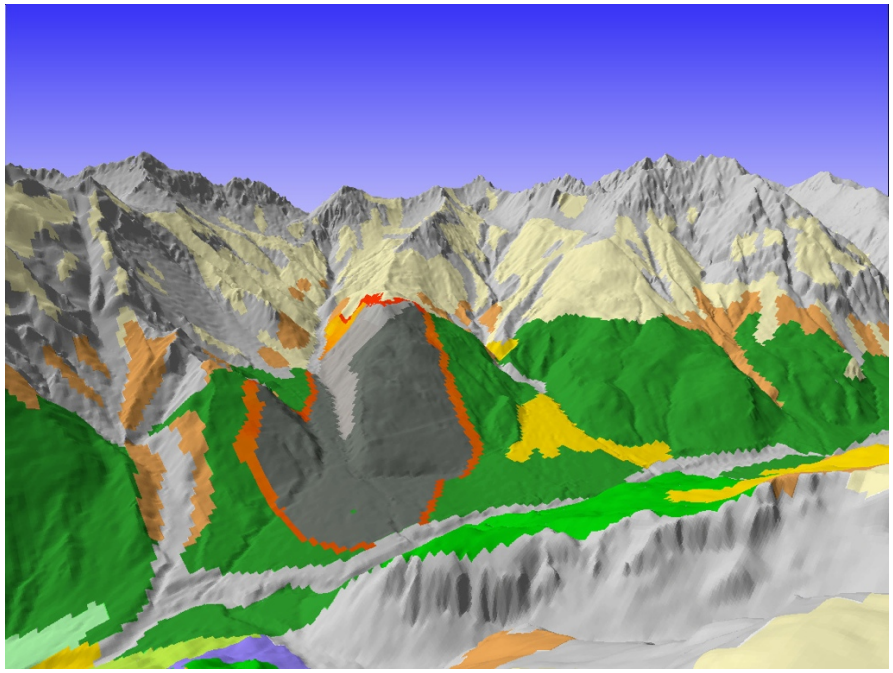
About Renaissance

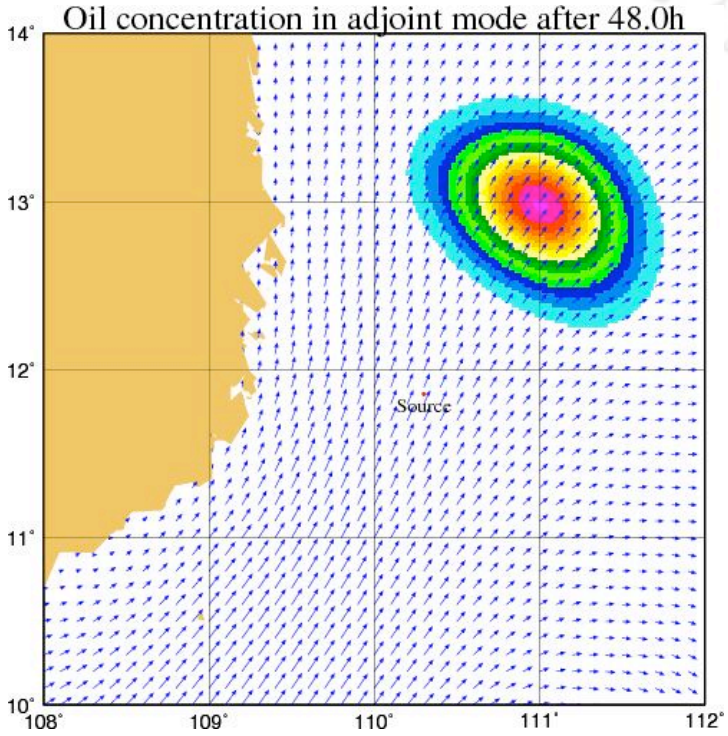
Renaissance Technologies LLC is an investment management company dedicated to producing superior returns for its clients and employees by adhering to mathematical and statistical methods.



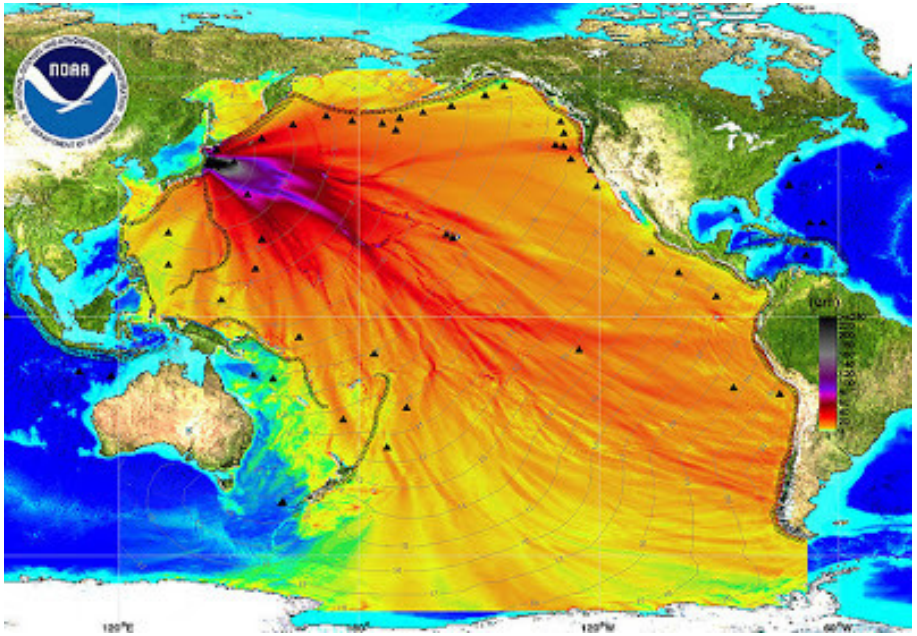
Aplicaciones: Medio ambiente

- Propagación de incendios forestales
- Contaminación





Aplicaciones: Medio ambiente



MEDIO AMBIENTE

Radiactividad de Fukushima en un atún de Oregón

La central de Fukushima tras el accidente Efe

Hace 3 horas

Reuters/EP. Portland.

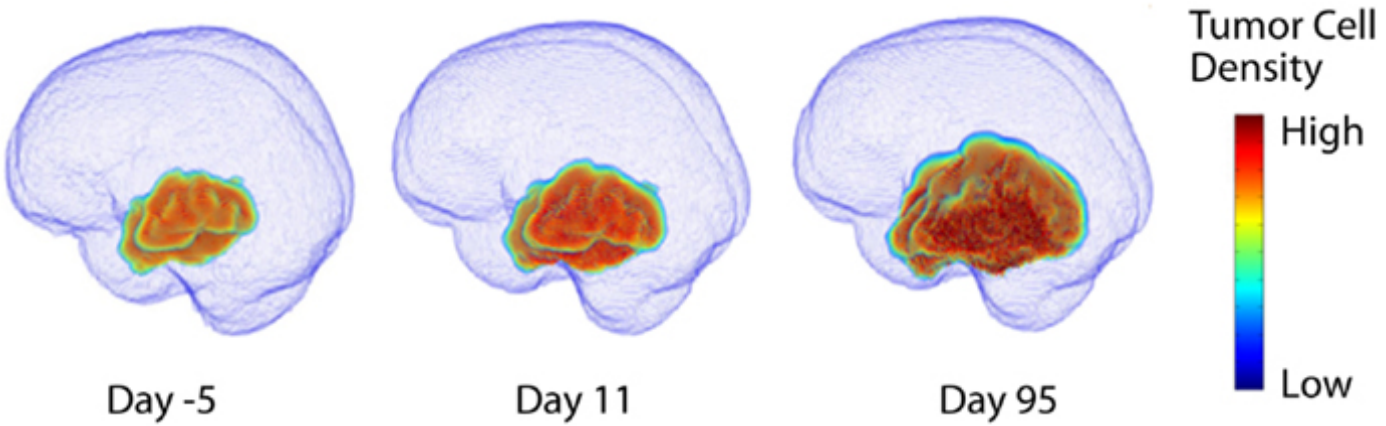
Una muestra de atún blanco capturada **frente a las costas de los estados de Oregon y Washington, en Estados Unidos,** contiene pequeños **niveles de radiactividad provenientes del desastre nuclear de Fukushima** en Japón de 2011, según un estudio de la Universidad Estatal de Oregón, que aclara que estos niveles son «mínimos» y no pueden tener ningún impacto sobre las personas.

Aplicaciones: Medicina y Salud

- Los modelos matemáticos son de gran utilidad en múltiples disciplinas de la Medicina y la Salud:
  - Propagación de enfermedades infecciosas.
  - Farmacocinética.
  - Diseño de prótesis.
  - Planificación y evaluación de planes de control y prevención.
  - Control y análisis de experimentos clínicos.
  - Impacto económico de las medidas sanitarias.
  - Etc.

Aplicaciones: Medicina y Salud

- Análisis de los niveles de biomarcadores cancerígenos en sangre.
- Simulación del crecimiento de tumores.
- Planificación de la medicación anticancerígena.



Aplicaciones: Medicina y Salud

- Diseño de prótesis.

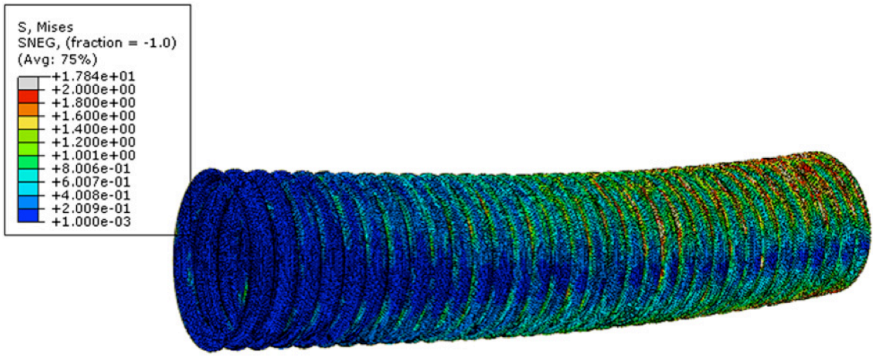
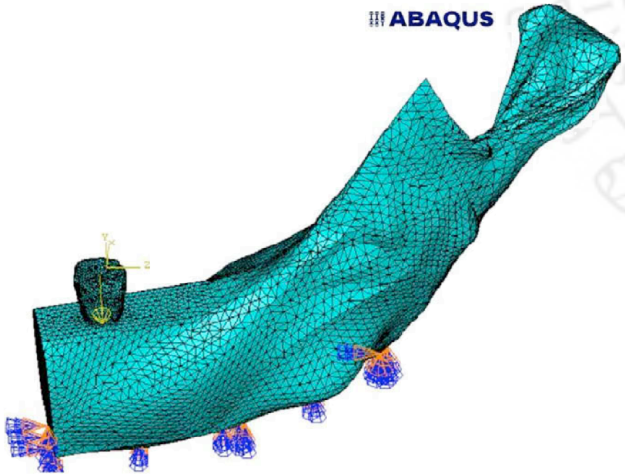
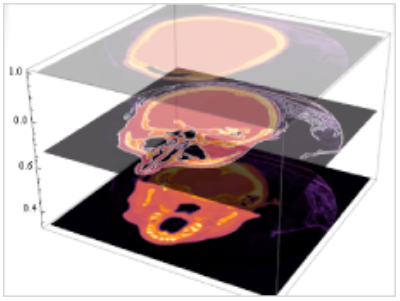


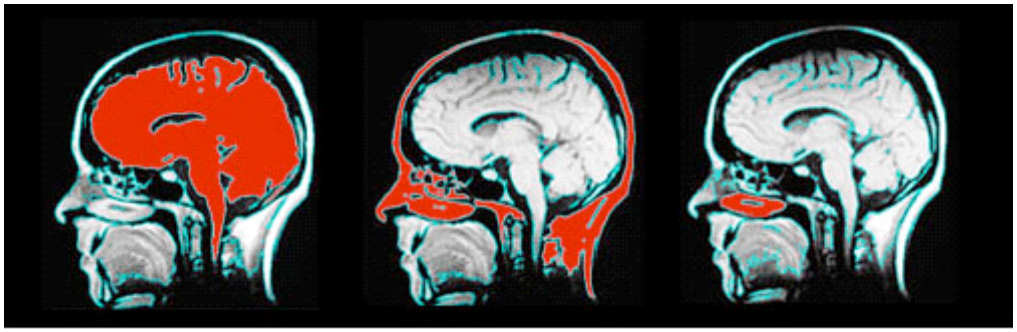
Fig. 6 – Von Mises stress distribution in bending simulations.

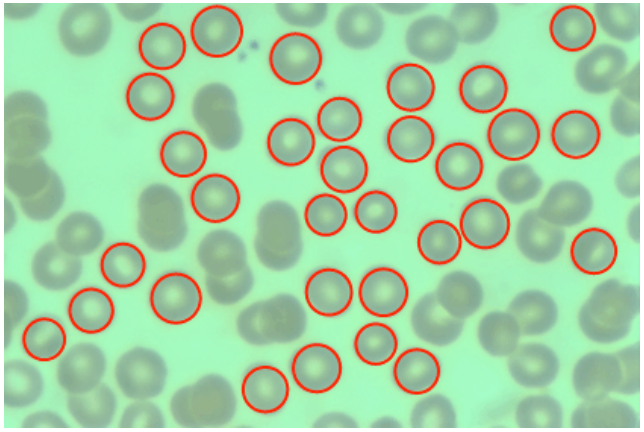


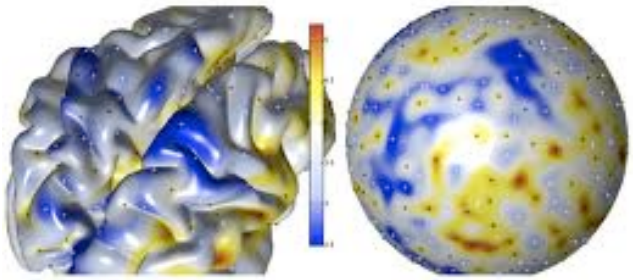
Aplicaciones: Medicina y Salud

- Análisis y procesamiento de imágenes médicas.



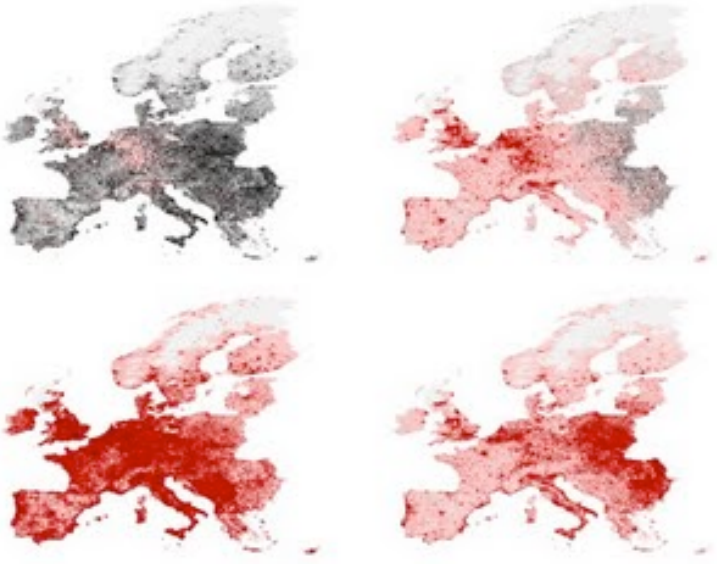


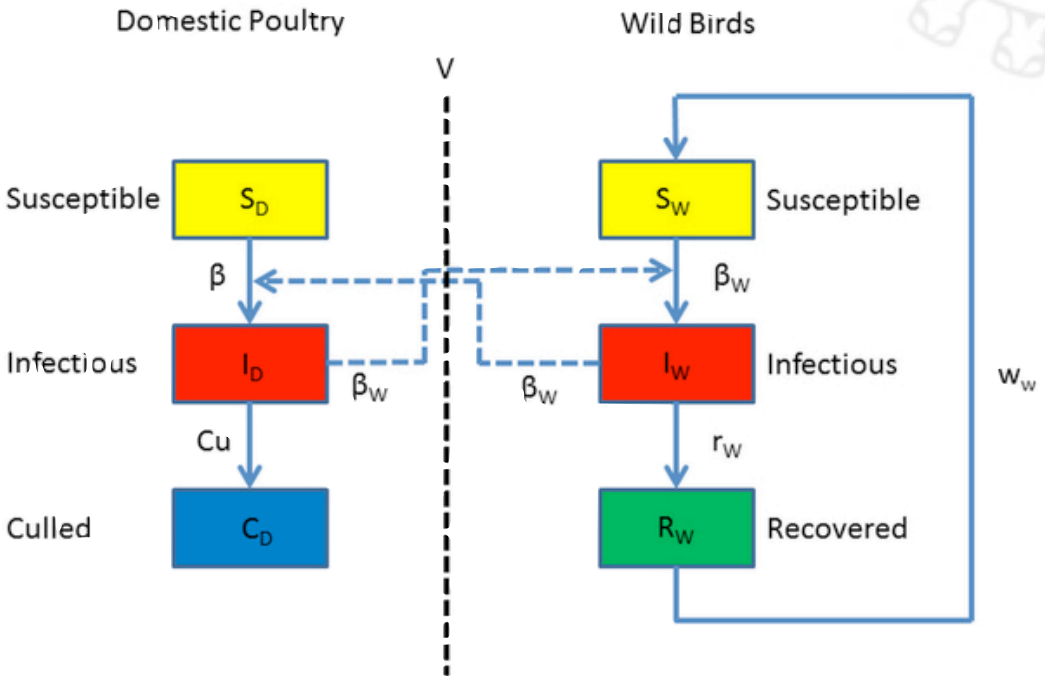




Aplicaciones: Medicina y Salud

- Propagación de enfermedades infecciosas.





Aplicaciones: Medicina y Salud

- Propagación de enfermedades infecciosas.

  - Número reproductivo básico R_0 : número de nuevos casos de pacientes infectados que un único individuo enfermo genera en una población enteramente susceptible durante el tiempo que dura la enfermedad.

Aplicaciones: Sociedad de la Información

- Algoritmo de búsqueda de Google

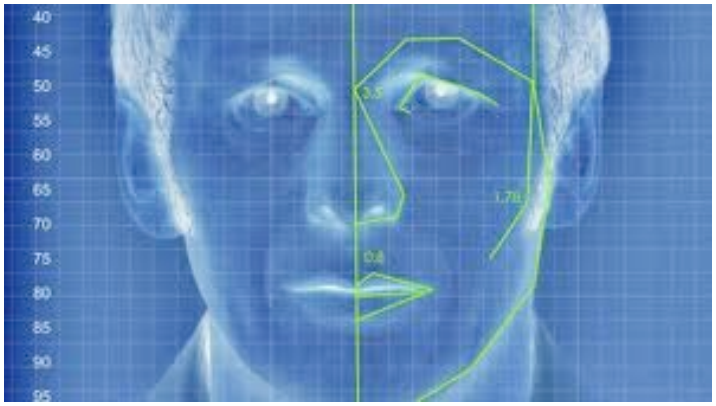
- Conexión en redes de telefonía móvil 3G

- Telecomunicaciones

- Códigos bidimensionales

Aplicaciones: Sociedad de la Información

- Biometría



- Criptografía y Seguridad de la Información

Aplicaciones: Sociedad de la Información

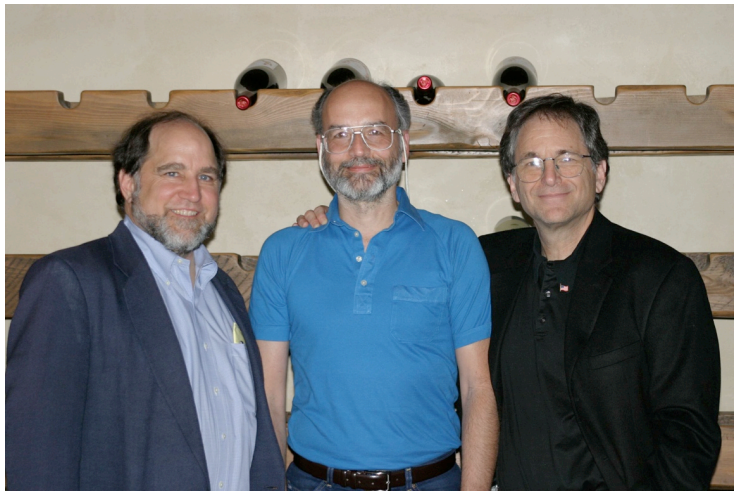
- En marzo de 2006 comienza la expedición del DNIe.

dni electrónico

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

Aplicaciones: Sociedad de la Información

¿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.

Aplicaciones: Sociedad de la Información

¿Qué Matemáticas se utilizan en el Triple DES?

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



Codificación

Generador de secuencias pseudolaeatorias de bits criptográficamente seguras

0 0 1 1 0 1 0 1 1 1 0 1 ...

$\oplus$

1 0 1 1 0 0 0 1 0 1 0 1 ...

=

1 0 0 0 0 1 0 1 1 0 0 0 ...

Aplicaciones: Sociedad de la Información

¿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).

Aplicaciones: Sociedad de la Información

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		

Aplicaciones: Sociedad de la Información

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

Aplicaciones: Sociedad de la Información

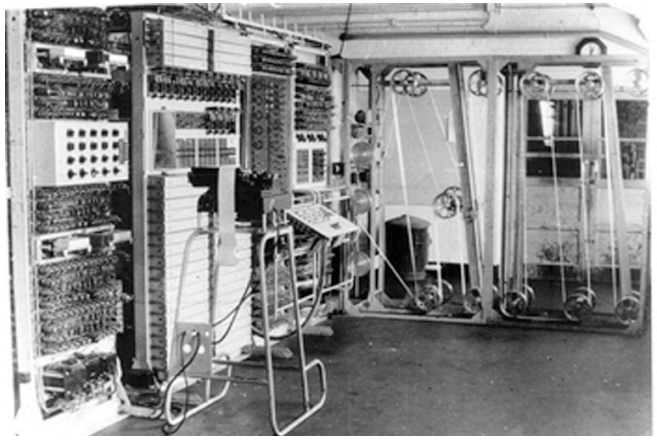
¿Cuál es el organismo, agencia o empresa que más matemáticos contrata y en el que más matemáticos trabajan?

Aplicaciones: Sociedad de la Información

- No solo Estados Unidos posee una agencia de este tipo...

Government Communications Headquarters
(Reino Unido)

Bletchely Park



Colossus

Aplicaciones: Sociedad de la Información

- 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

Aplicaciones: Sociedad de la Información

- En España también tenemos una agencia similar...

Centro Criptológico Nacional
(España)

¡**Muchísimas gracias** por vuestra atención!