VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

Criptografía: Matemáticas para proteger la información

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

16 de diciembre de 2015
Bachillerato de Investigación y Excelencia, I.E.S. “Vaguada de la Palma”, Salamanca

MoACIS

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

Introducción

- El gran desarrollo de las TIC en los últimos años ha dado lugar a una sociedad totalmente dependiente de ellas.
- Caminamos de manera inexorable hacia el pleno establecimiento de la Internet de las Cosas.

Introducción

- Hoy en día los Sistemas Informáticos controlan el buen funcionamiento de multitud de procesos y tareas.

- Cobra especial relevancia la protección de las Infraestructuras Críticas.

Introducción

- Peligros ya existentes 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

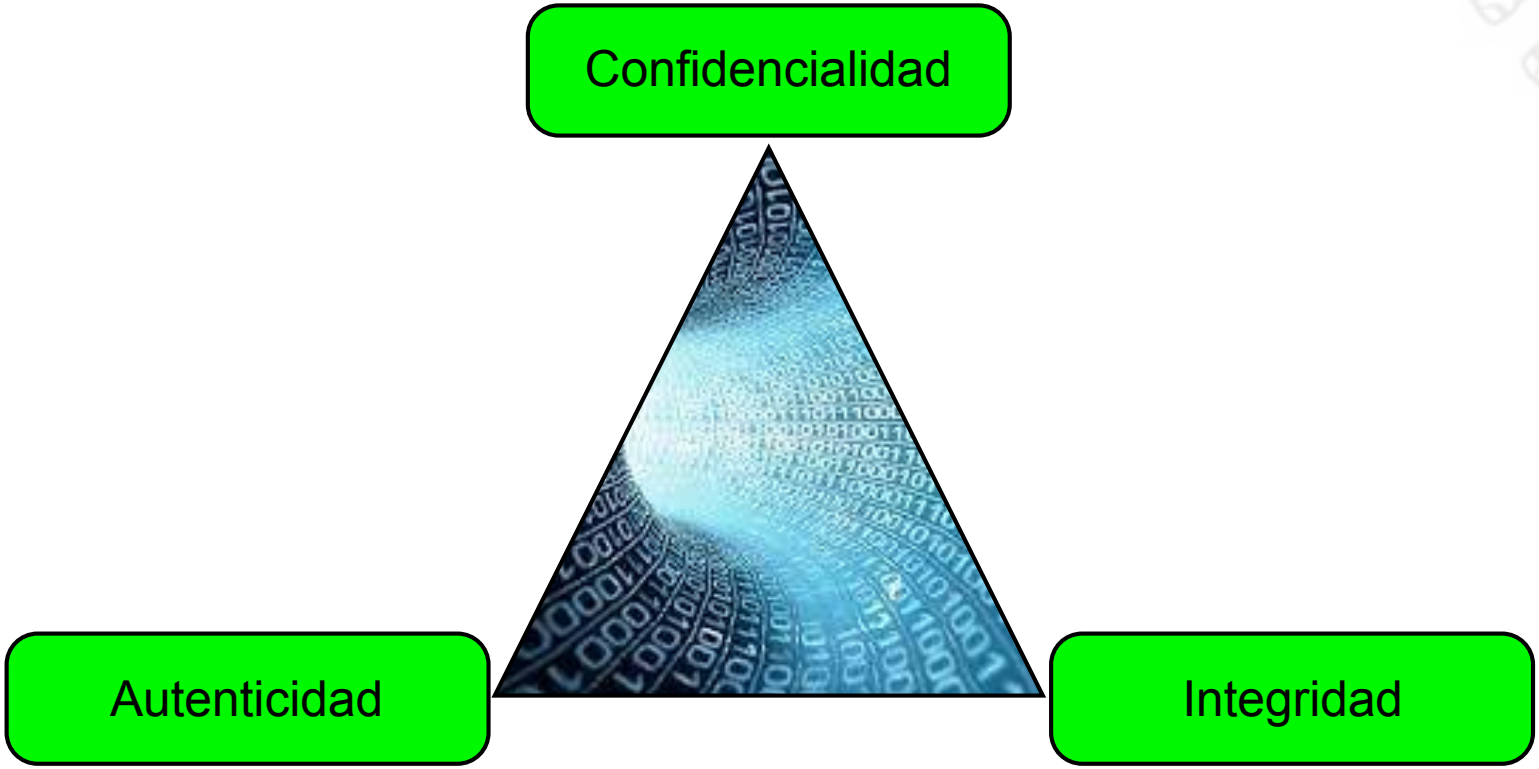
- Las Matemáticas ofrecen herramientas que permiten analizar, evaluar y gestionar dichas amenazas con el objetivo de minimizar su impacto:
  - Algoritmos criptográficos para proteger la información (confidencialidad, integridad, autenticidad, etc.)
  - Modelos matemáticos para detectar, evaluar y gestionar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

Introducción

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

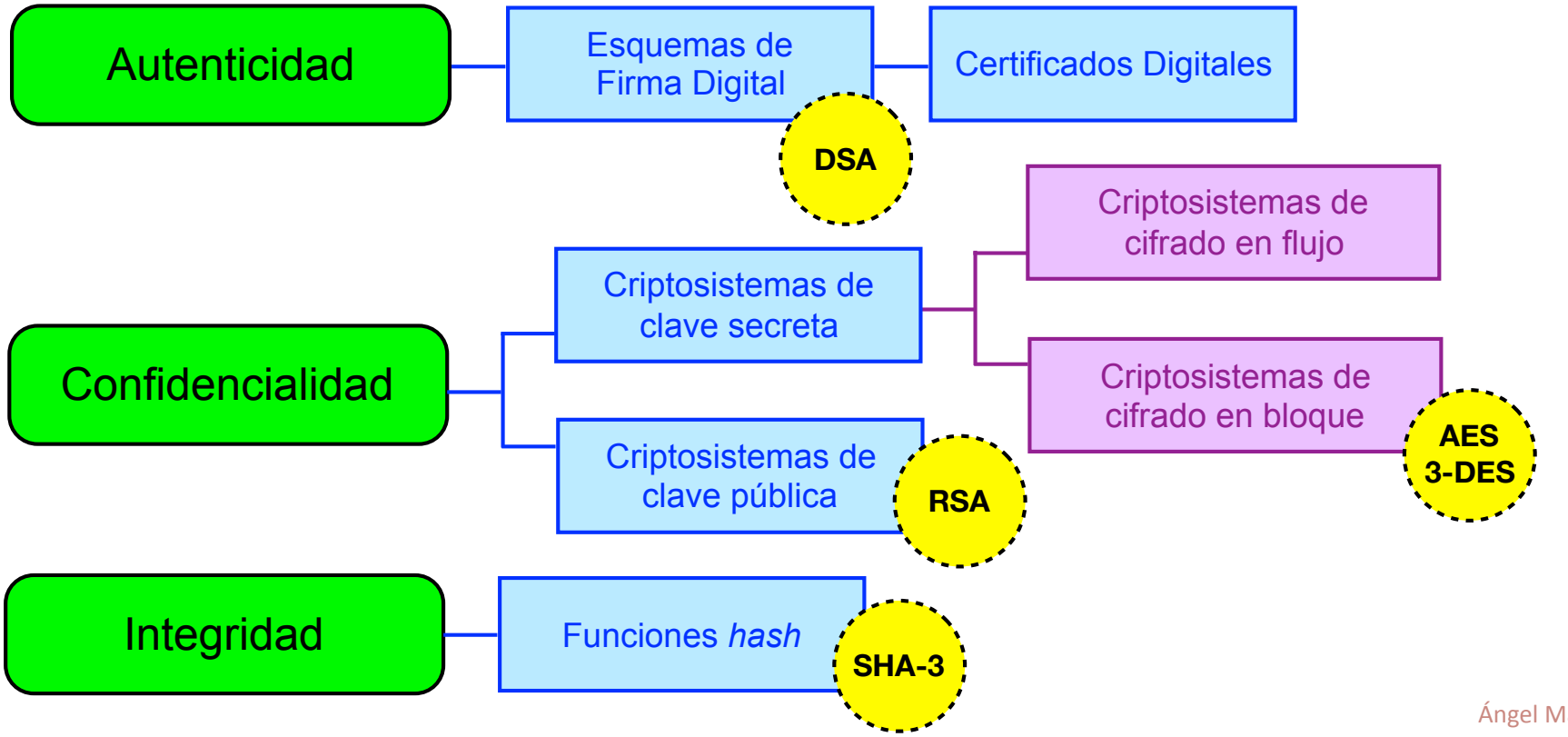
Introducción

- Proteger la información es una prioridad en nuestros días



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.



Confidencialidad

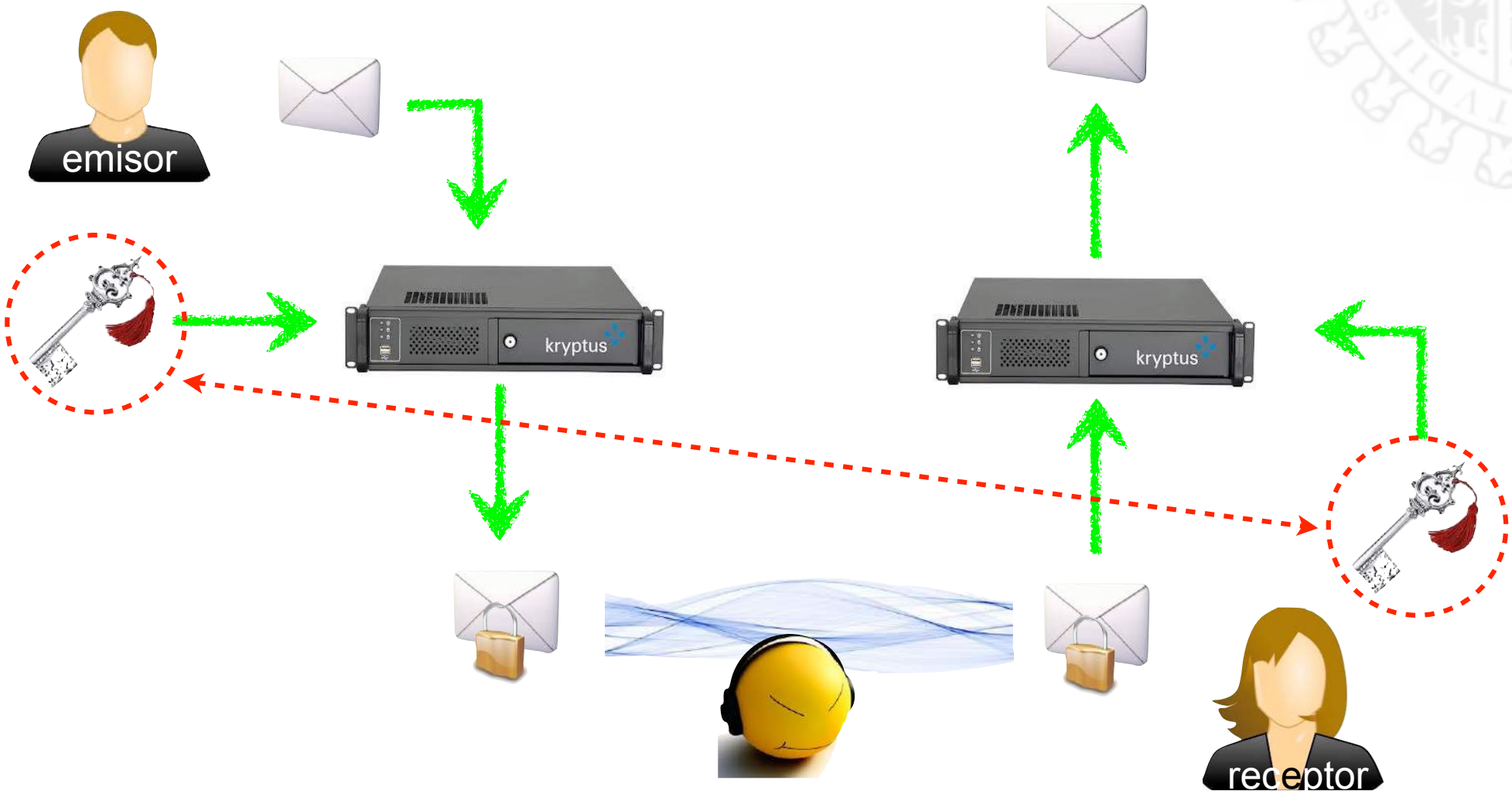
- Confidencialidad: el mensaje sólo puede ser leído por su legítimo destinatario.
- La confidencialidad se garantiza cifrando los datos mediante...
  - Criptosistemas de clave secreta.
  - Criptosistemas de clave pública.

Confidencialidad

- Los criptosistemas de clave secreta se caracterizan por el uso de una única clave que se utiliza para cifrar y descifrar mensajes.
- Dicha clave debe ser compartida (y mantenida en secreto) por el emisor y por el receptor.
- Consecuentemente antes de enviar un mensaje cifrado deben de haberse puesto de acuerdo en la clave secreta a utilizar.

Confidencialidad

- Esquema de los criptosistemas de clave secreta:



Confidencialidad

- Ventajas de los criptosistemas de clave secreta:
  - Gran rapidez en el cifrado.
  - Cifrado de gran cantidad de datos.
  - Tamaño de las claves pequeño (128-256 bits).
  - Los algoritmos se basan en sencillas operaciones matemáticas.
- Desventajas de los criptosistemas de clave secreta:
  - Distribución y gestión en red de la clave secreta.
  - La clave secreta se debe cambiar con cierta frecuencia.

Confidencialidad

- Criptosistemas de clave secreta: cifrado en flujo

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Codificación

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

$\oplus$

Generador de Secuencias pseudolaeatorias de bits criptográficamente seguras

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

=

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

Confidencialidad

- El cifrado en flujo en la actualidad:
  - Telefonia móvil GSM: algoritmo A5.

  - Bluetooth: algoritmo E0.

  - WEP (WiFi): algoritmo RC4.

Confidencialidad

- El cifrado en flujo en el futuro: el proyecto eSTREAM

  - El proyecto eSTREAM se inició en 2004 con la finalidad de seleccionar un algoritmo de cifrado en flujo que pudiera ser considerado con el estándar de cifrado en flujo en el futuro.

  - En 2008 se seleccionaron los siguientes algoritmos:

    ✓ Perfil software: HC-128, Rabbit, Salsa20/12, Sosemanuk.

    ✓Perfil hardware: Grain, MICKEY, Trivium.

ECRYPT II http://www.ecrypt.eu.org/stream/

Confidencialidad

- Criptosistemas de clave secreta: cifrado en bloque

Codificación y Rotura en bloques

- Transformación inicial
- Aplicación reiterada de una función
- Transformación final

Generador de Secuencias pseudolaeatorias de bits criptográficamente seguras

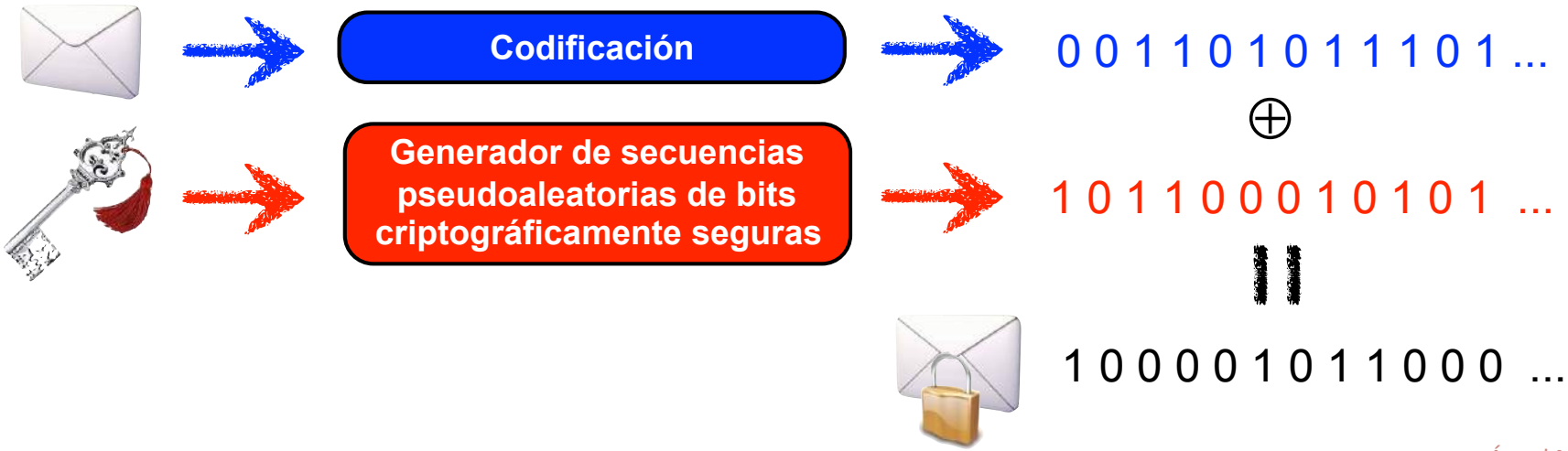
Confidencialidad

- El cifrado en bloque en la actualidad:
  - Triple DES (Data Encryption Standard).
  - AES (*Advanced Encryption Standard*).
    - ✓Aparece en 2001 para sustituir al DES con una vida útil estimada de 20-30 años.
    - ✓Utiliza claves de longitud 128, 192 o 256 bits y los bloques tienen un tamaño de 128 bits.
    - ✓Se usa para cifrar el material sensible (no clasificado) de las agencias gubernamentales de EE.UU.

Confidencialidad

¿Qué Matemáticas se utilizan en el 3-DES?

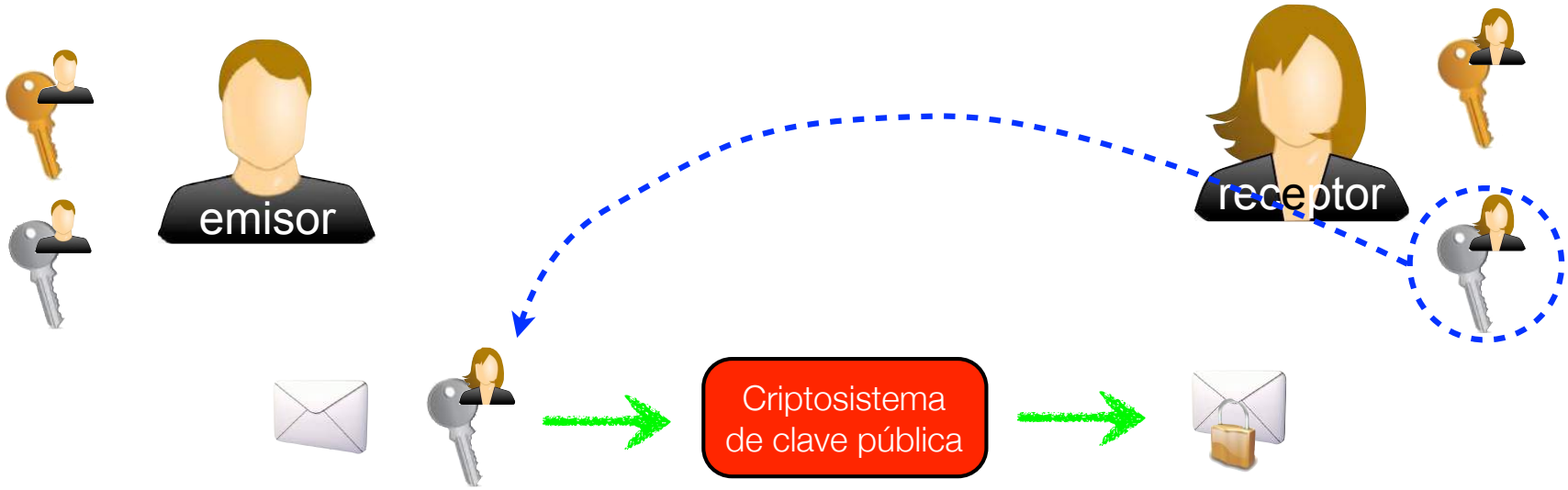
- Permutaciones.
- Sustituciones: S-boxes.
- Suma XOR: $0 \oplus 0 = 0 \quad 1 \oplus 0 = 1$
  $0 \oplus 1 = 1 \quad 1 \oplus 1 = 0$



Confidencialidad

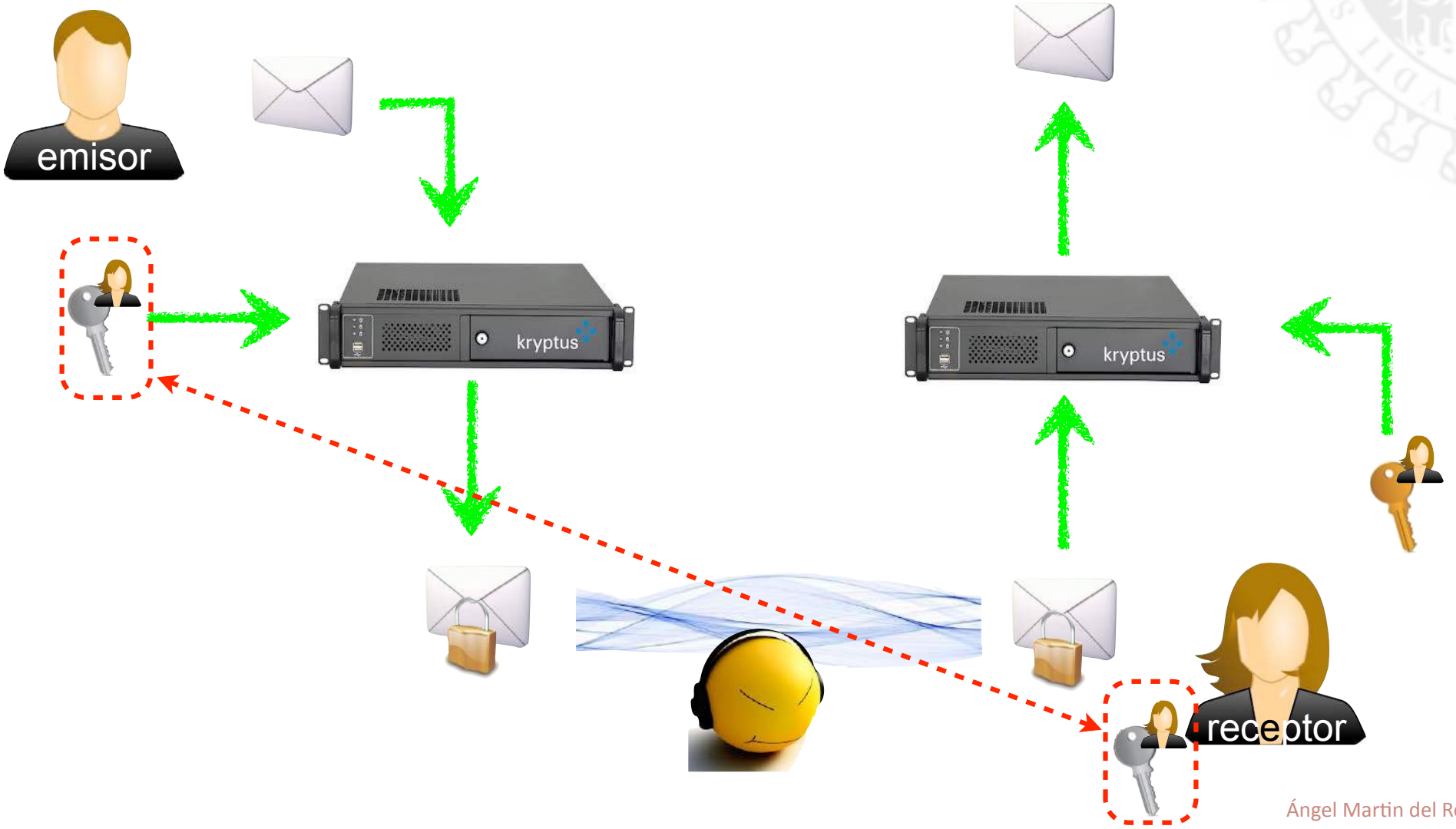
- Los criptosistemas de clave pública se caracterizan por el uso de dos claves: una *clave pública* (que conoce todo el mundo y que se utiliza para cifrar mensajes) y una *clave privada* (que sólo conoce el propietario y que se utiliza para descifrar los mensajes).

- Estas dos claves estar relacionadas entre sí matemáticamente.



Confidencialidad

- Esquema de los criptosistemas de clave pública:



Confidencialidad

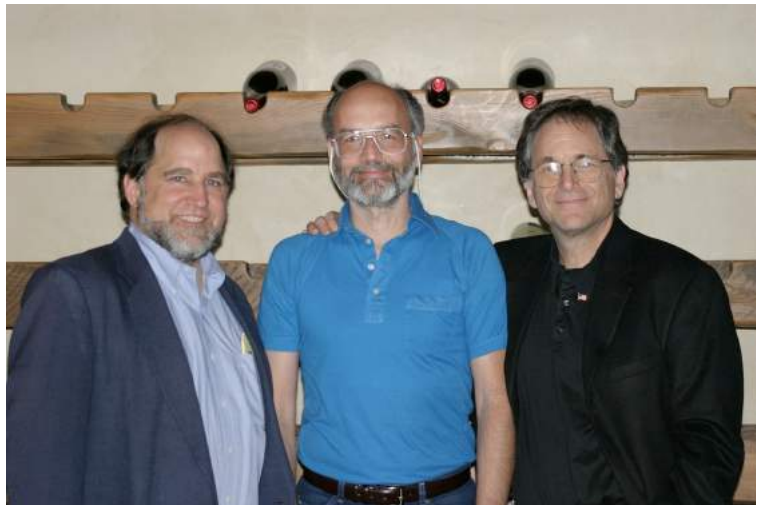
- La clave pública en la actualidad:
  - Criptosistema RSA: se basa en la dificultad computacional de la factoriación de números enteros muy grandes.
  - Criptosistema ElGamal: se basa en la dificultad computacional que supone resolver el problema del logaritmo discreto.
  - Criptosistemas basados en curvas elípticas: variante mejorada y más eficiente del criptosistema ElGamal (la seguridad que proporciona ElGamal con claves de longitud 1024 bits no es superior a la generada por las curvas elípticas con longitudes de clave de 160 bits).

Confidencialidad

- Ventajas de los criptosistemas de clave pública:
  - Eficacia en la gestión y distribución de claves.
  - La vida útil de las claves es de unos 2 años (aprox.), superior a la de las claves utilizadas en los criptosistemas de clave secreta.
  - Se pueden diseñar a partir de ellos esquemas de firma digital.
- Desventajas de los criptosistemas de clave pública:
  - La longitud de las claves (1024-4096 bits) es superior a la utilizada en los criptosistemas de clave secreta.
  - Lentitud en el proceso de cifrado/descifrado.
  - Poco eficaces a la hora de cifrar grandes cantidades de datos.
  - Los algoritmos se basan en complejos resultados matemáticos.

Confidencialidad

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



Rivest, Shamir y Adleman

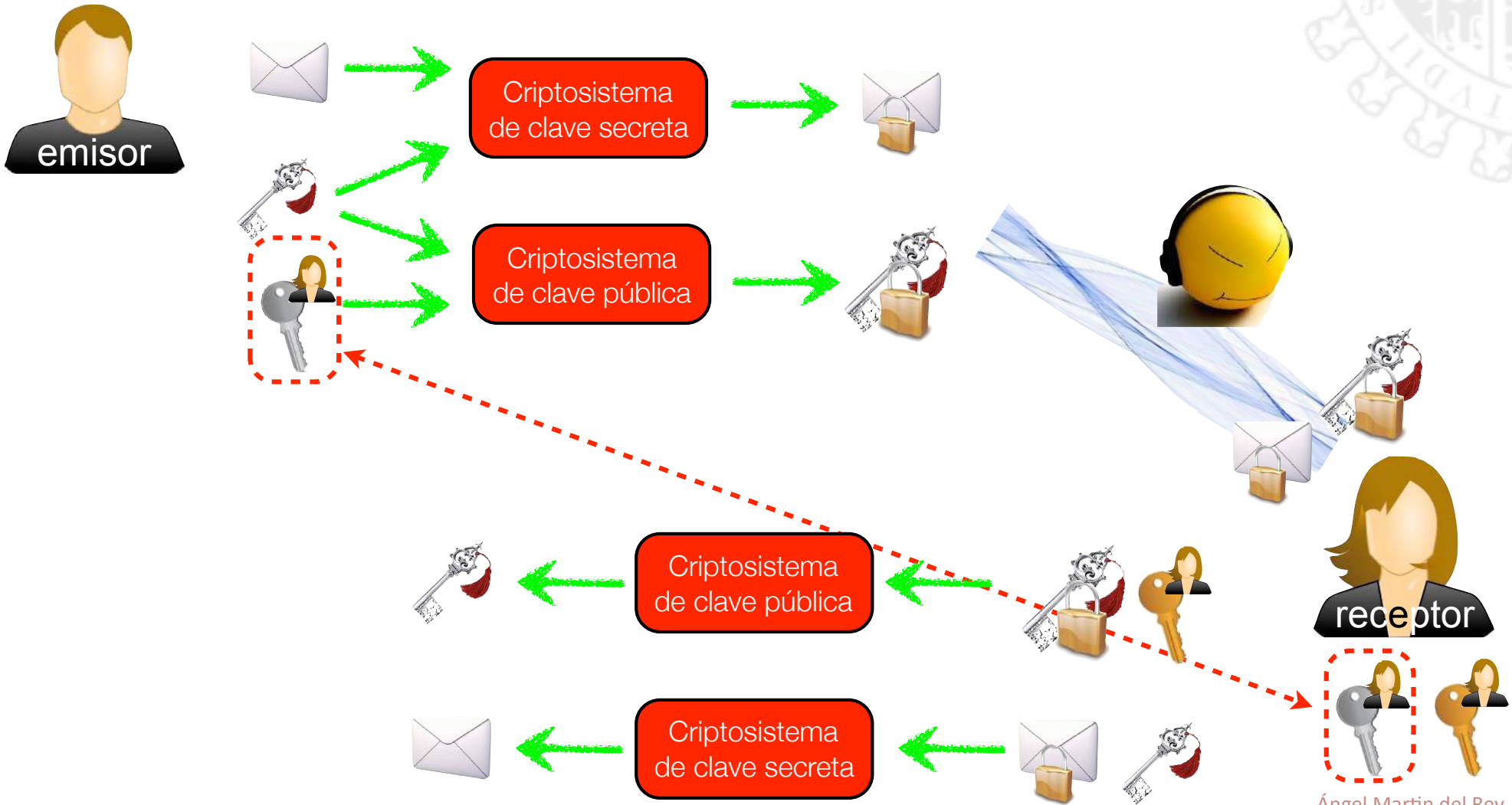
- Cálculo de potencias: m^e
- Cálculo del m.c.d.: $\mathrm{m.c.d.}(e,\phi)$
- Cálculo de congruencias: $c = m^e \pmod{n}$

(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.

Confidencialidad

- Esquema de la **envoltura digital**:



Integridad

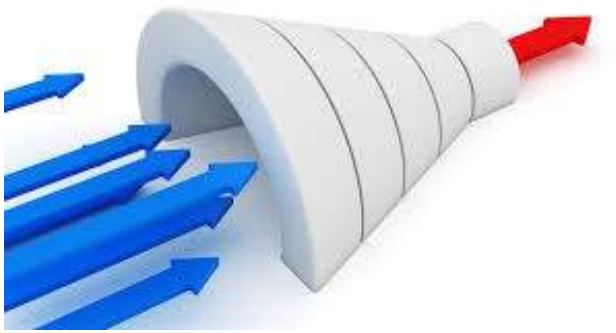
- Integridad: el mensaje no puede ser alterado.
- La integridad se garantiza mediante el uso de funciones resumen (*hash functions)* o MAC.
  - función MD5
  - funciones SHA (SHA-1, SHA-2, SHA-3)
  - función RIPEMD-160
  - función Tiger

Integridad

- 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 varible (Gb, Mb,...) mientras que el de *h* es fijo (128-512 bits)
  - Es computacionalmente muy difícil determinar *m* conociendo *f*(*m*), a no ser que se conozca una determinada información adicional denominada *trampilla*.

Integridad

- Las funciones resumen deben verificar las siguientes condiciones:
  - Si se cambia un único bit del mensaje *m*, el resumen *h*=*f*(*m*) debería cambiar (por término medio) en la mitad de los bits.
  - *Resistencia a la preimagen*: dado un resumen, debe ser computacionalmente muy dificil obtener el mensaje.
  - *Resistencia a la segunda preimagen*: dado un mensaje, debe ser computacionalmente difícil encontrar otro mensaje diferente de manera que sus resúmenes coincidan.
  - *Resistencia a colisiones*: debe ser computacionalmente dificil encontrar dos mensajes distintos con el mismo resumen.

Integridad

- En el caso de que no se cumplieran estas condiciones, la función resumen sería vulnerable.
- Su seguridad se vería comprometida por el ataque de la *paradoja del cumpleaños*...
  - *Paradoja del cumpleaños*: ¿cuántas personas debe haber en una sala para que la probabilidad de que dos de ellas celebren su cumpleaños el mismo día sea superior al 50%?

Integridad

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

Datos de registro:	
Número de registro:	**201560000089983**
Fecha de presentación:	**20-04-2015**
Hora de presentación:	**07:07:52**

PETICIÓN

Documento de Propuesta de resolución

DATOS DEL SOLICITANTE

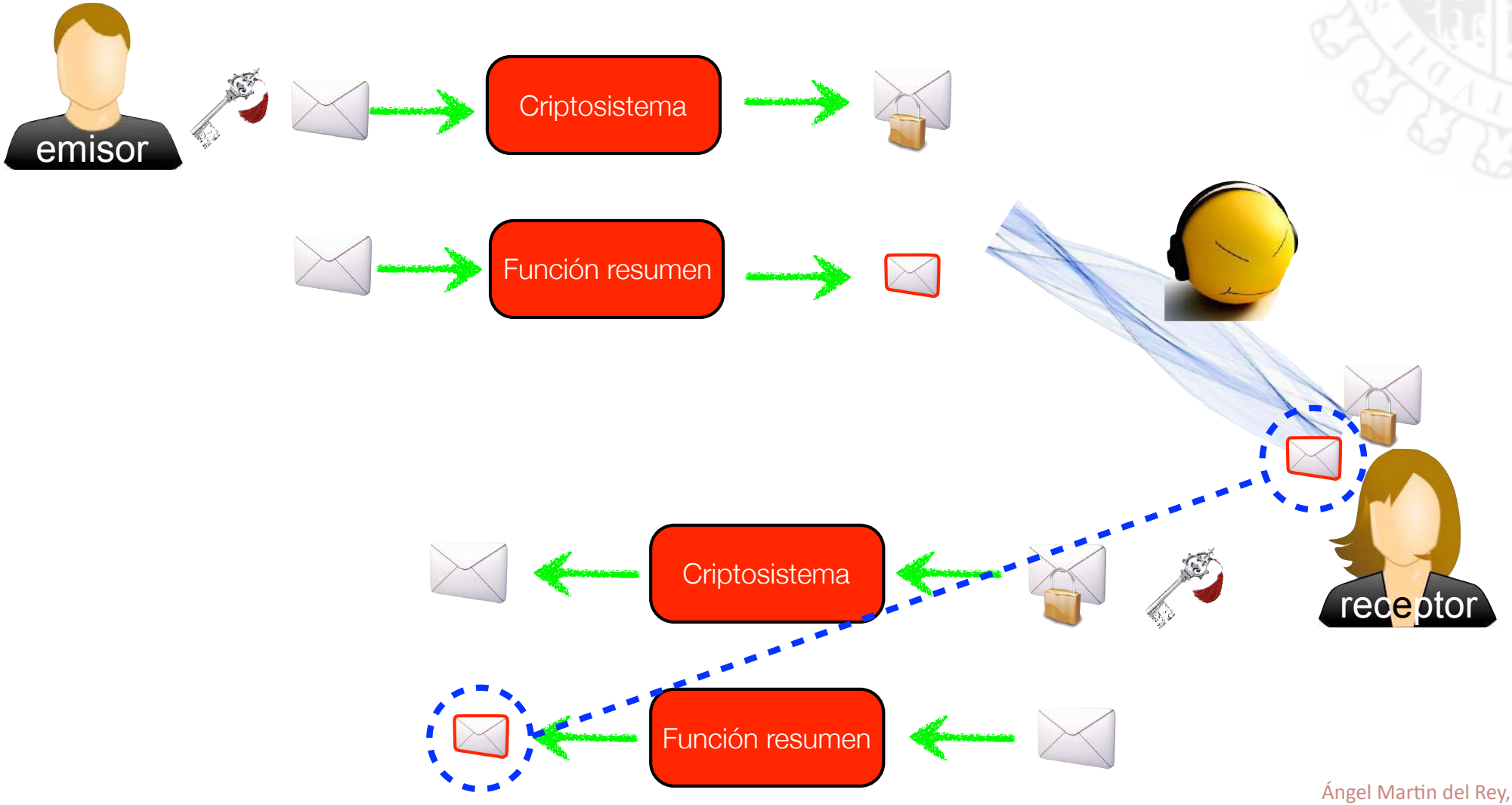
Nombre y Apellidos/Razón Social:	Angel Martín Del Rey	NIF:	[redacted]
Domicilio:	[redacted]		
Población:		Provincia: [redacted]	C.P.: [redacted]
Teléfono:		E-mail:	

DOCUMENTOS APORTADOS

DAceptacionPRPTIN2014-55325-C2-2-R.pdf (PDF de la petición) Huella digital: d3de77647759f4e0d230f88bc9016cfa.

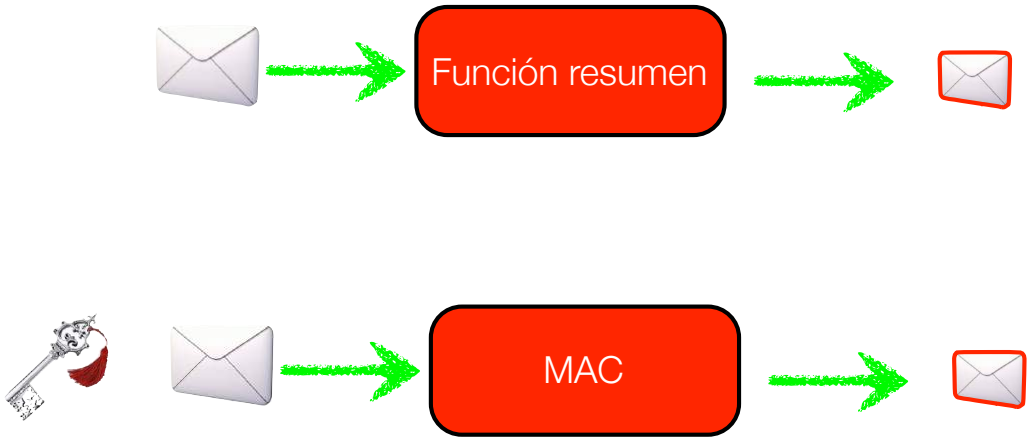
Integridad

- Esquema simple de uso de una función resumen:



Integridad

- Los *Message Authentication Codes* (MAC) son algoritmos parecidos a las funciones resumen pero con la diferencia de que hacen uso de una clave para calcular el resumen.

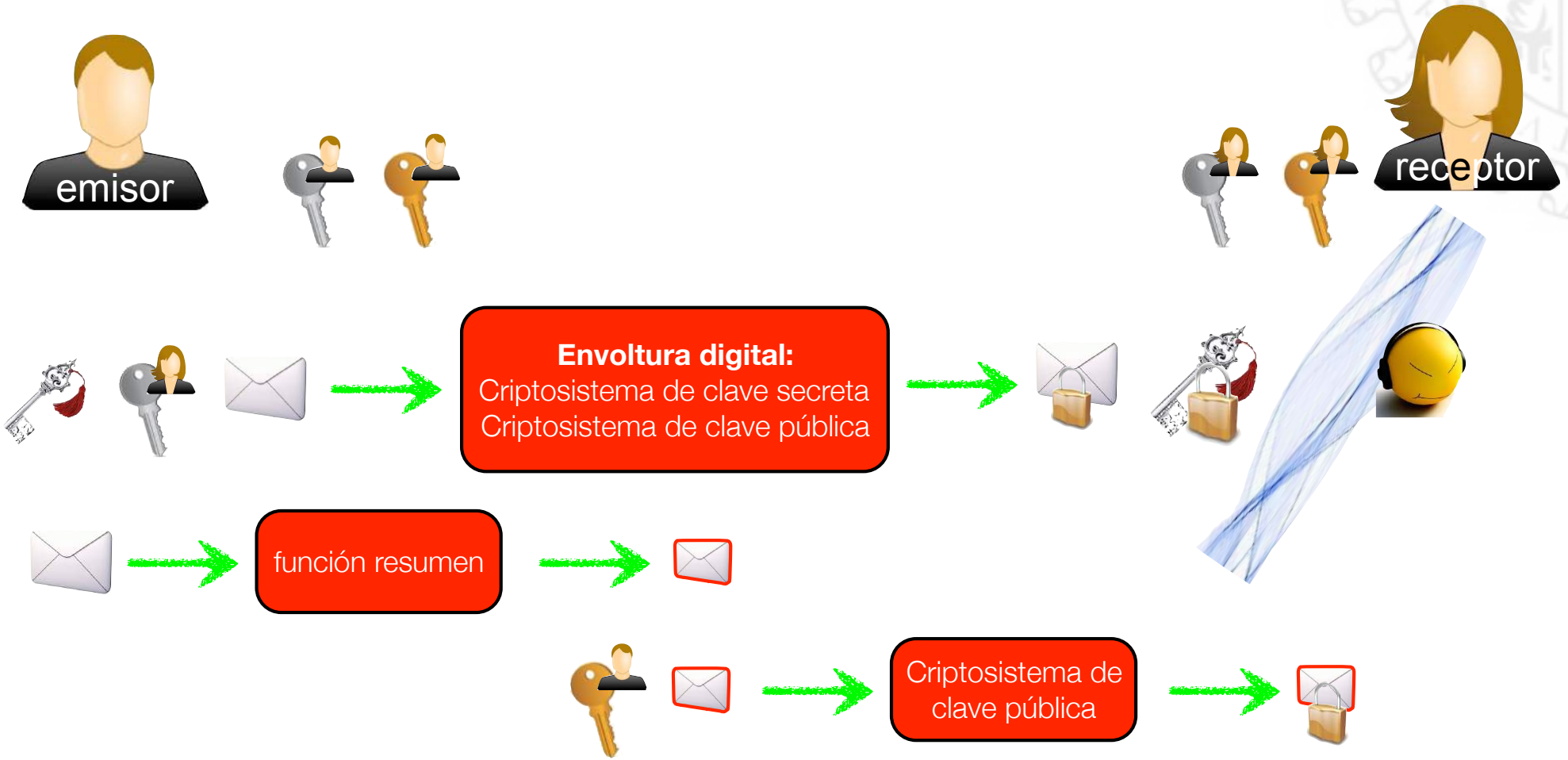


Autenticidad

- Autenticidad: el mensaje es auténtico y no se ha suplantado la personalidad del emisor.
- La autenticidad se garantiza mediante el uso de los esquemas de firma digital.
- Los esquemas de firma digital se basan en el uso de los criptosistemas de clave pública.

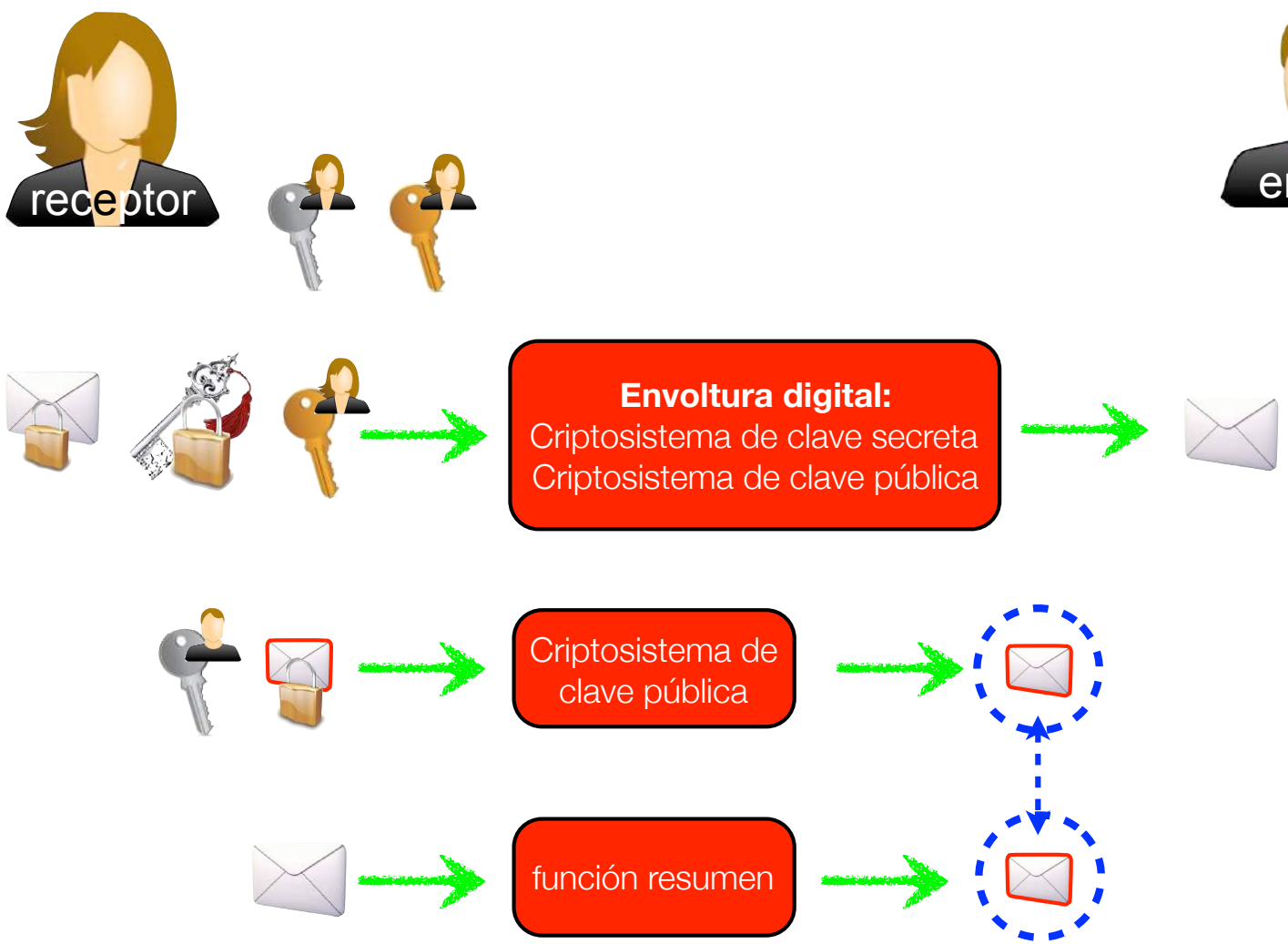
Autenticidad

- Esquema de la **firma digital (envío)**:



Autenticidad

- Esquema de la **firma digital (recepción)**:



Autenticidad

- En la actualidad se usan...
  - Firma digital DSA (*Digital Signature Algorithm*).
  - Firma digital RSA.
  - Firma digital con curvas elípticas.
  - Firma digital con curvas hiperelípticas.
  - etc.

Aplicaciones prácticas: El DNI electrónico

- En marzo de 2006 comienza la expedición del DNIe.

dni electrónico

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

Aplicaciones prácticas: 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.

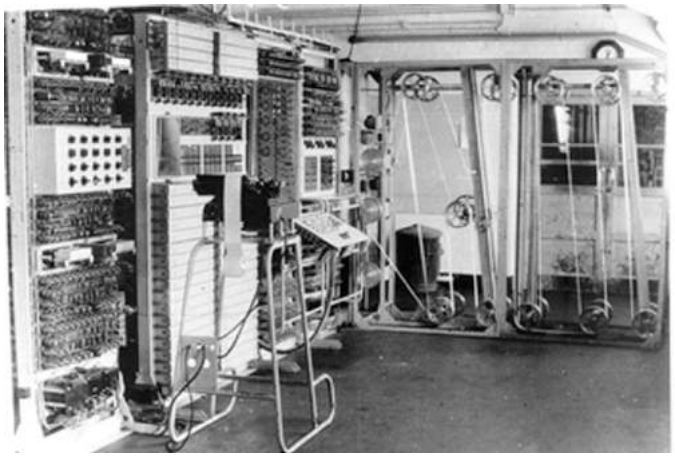
- Inventores *reales* de la "Criptografía de Clave Pública"

- Clifford Christopher Cocks.
- Malcolm John Williamson. 1973
- 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: ¡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?
  - …

¡Muchísimas gracias por vuestra atención!

¿alguna pregunta o comentario?