Lección 3: Sistemas de Cifra con Clave Pública

intypedia

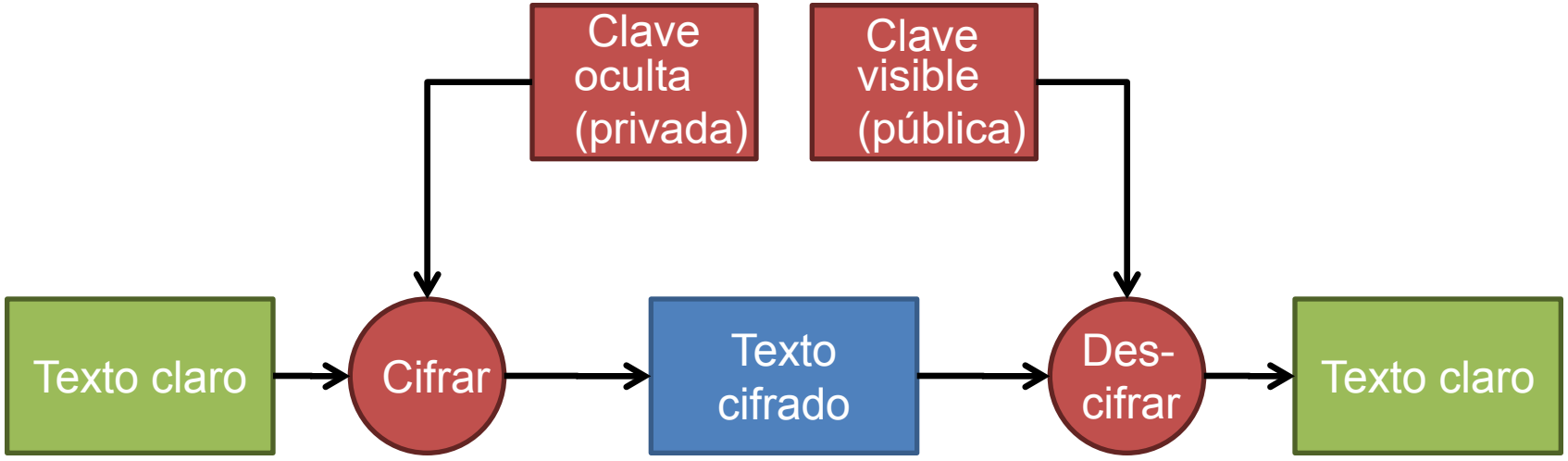
INFORMATION SECURITY ENCYCLOPEDIA

Gonzalo Álvarez Marañón
gonzalo@iec.csic.es

Consejo Superior de Investigaciones Científicas
Científico Titular

Funcionamiento del cifrado asimétrico

- Se utilizan dos claves diferentes: una para cifrar (pública) y otra para descifrar (privada)



Características del cifrado asimétrico I

- La clave visible (pública) debe ser conocida por todo el mundo, pero la clave oculta (privada) sólo debe conocerla su propietario.
- A partir del conocimiento de la clave visible o del texto cifrado no se puede obtener la clave oculta.
- Lo que se cifra con una clave, sólo puede descifrarse con su pareja.

Características del cifrado asimétrico II

- Cualquiera puede cifrar un mensaje con la clave visible de un usuario, pero sólo el propietario de la clave, quien posee la clave oculta, puede descifrarlo (confidencialidad)
- Si un usuario cifra con su clave oculta un mensaje, cualquiera puede descifrarlo con la correspondiente clave visible (integridad, autenticación y no repudio).

Fundamento del cifrado asimétrico

- Usa funciones unidireccionales:
  - Su cálculo directo es viable, pero el cálculo de la función inversa tiene tal complejidad que resulta imposible
- Problemas matemáticos difíciles de resolver:
  - Factorización: descomponer un número grande en sus factores primos
  - Logaritmo discreto: obtener el exponente al que ha sido elevado una base para dar un resultado
  - Mochila tramposa: obtener los sumandos que han dado origen a una suma

Ejemplo RSA

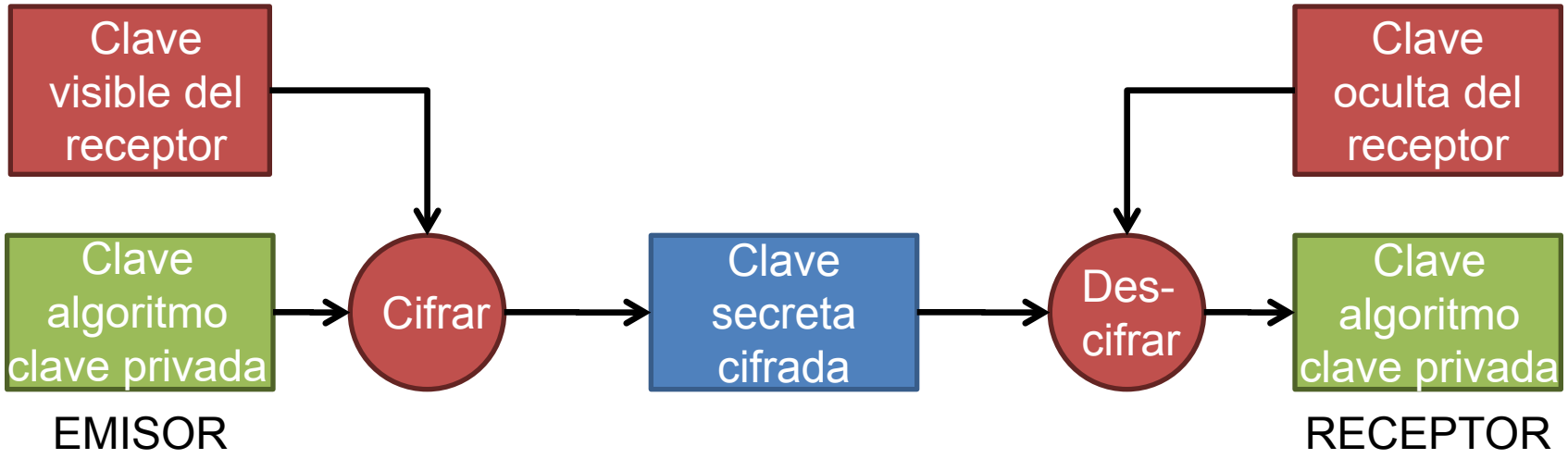
- Clave pública:
  - n = p×q, donde p y q son primos
  - e, primo con (p-1)×(q-1)

- Clave privada:
  - d, tal que d×e mod (p-1)×(q-1) = 1

- Cifrar: $c = m^e \bmod n$

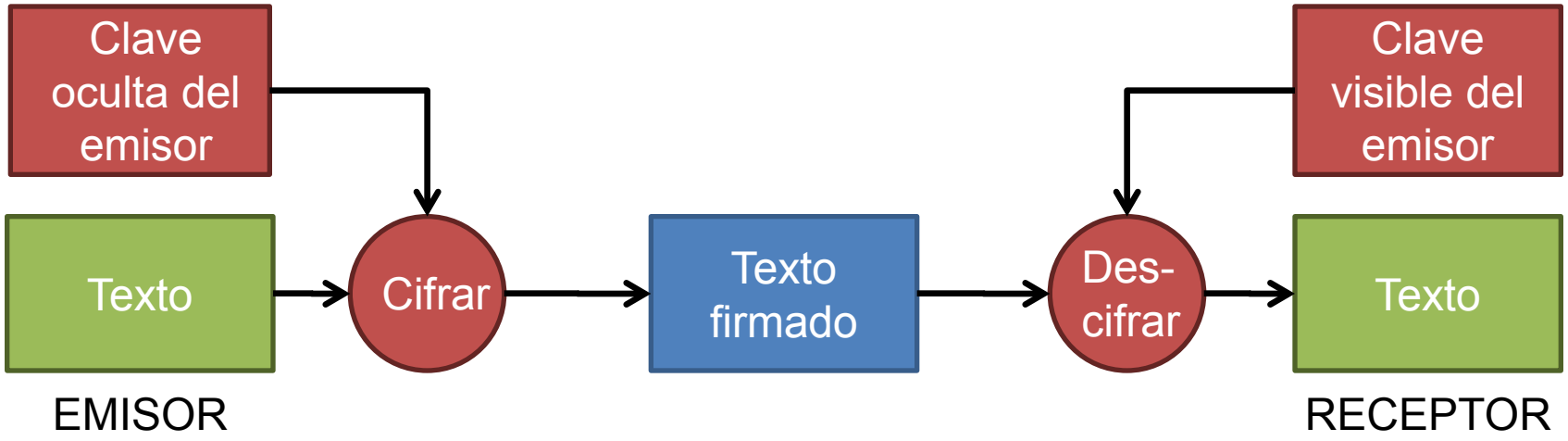
- Descifrar: $m = c^d \bmod n$

Distribución de claves secretas mediante criptografía asimétrica



- El emisor envía la clave del algoritmo de clave privada (que se utilizará en el resto de la comunicación) cifrada con la clave visible del receptor, quien será el único que podrá descifrarla con su clave oculta.

Autenticación mediante criptografía asimétrica



- El emisor cifra (firma) el mensaje con su clave privada (oculta), operación que sólo él puede realizar. Normalmente no se cifra todo el documento, sino un resumen del mismo.
- Cualquiera puede descifrarlo con la clave pública (visible) del emisor, verificando así su autoría.

Comparación entre criptografía simétrica y asimétrica

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves; firma digital
Estándar actual	DES, Triple DES, AES	RSA, Diffie-Hellman, DSA
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Oculta: sólo conocida por una persona Visible: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave visible se comparte por cualquier canal La oculta nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 – 2048 (RSA) 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio