Lección 3: Sistemas de Cifra con Clave Pública

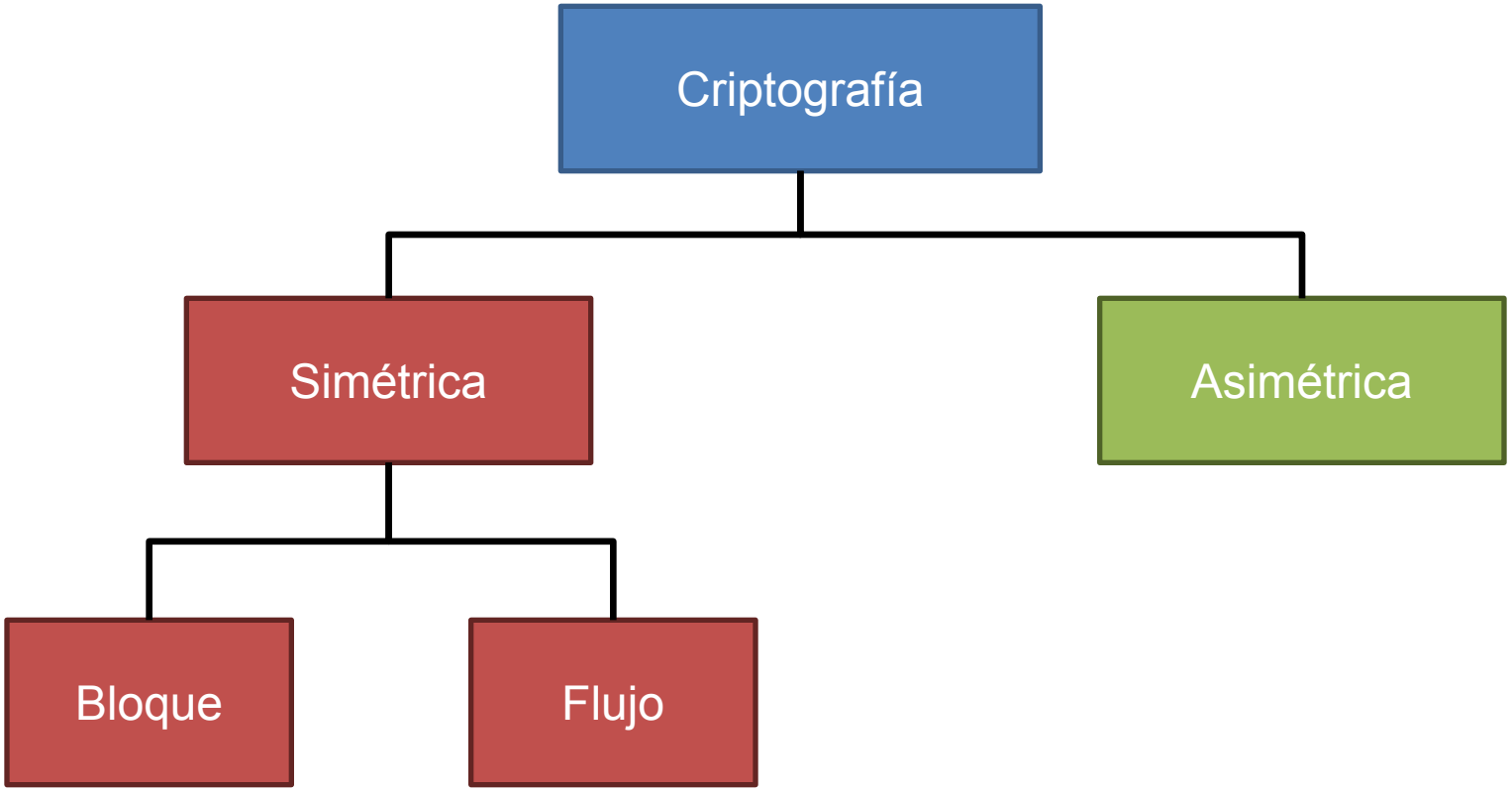
intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Gonzalo Álvarez Marañón
gonzalo@iec.csic.es

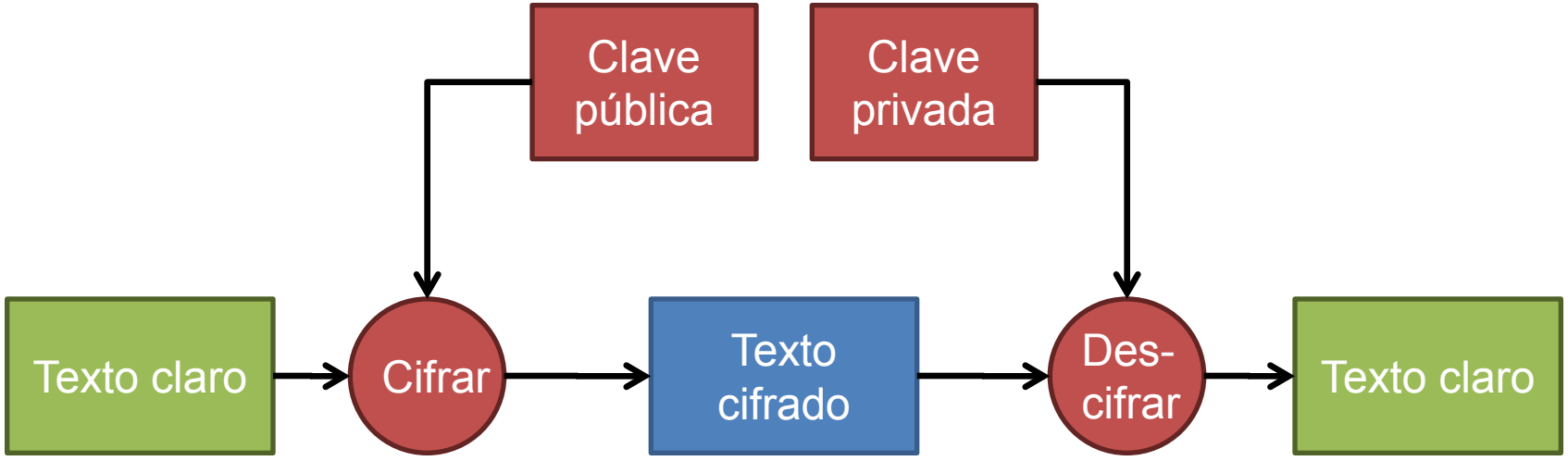
Consejo Superior de Investigaciones Científicas
Científico Titular

Los tipos de criptografía



Funcionamiento del cifrado asimétrico

- Se utilizan dos claves diferentes: una para cifrar y otra para descifrar



Características del cifrado asimétrico I

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

Características del cifrado asimétrico II

- Cualquiera puede cifrar un mensaje con la clave pública, pero sólo el propietario de la clave privada puede descifrarlo
  - Proporciona confidencialidad
- Si el propietario de la clave privada cifra con ella un mensaje, cualquiera puede descifrarlo con la correspondiente clave pública
  - Proporciona 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

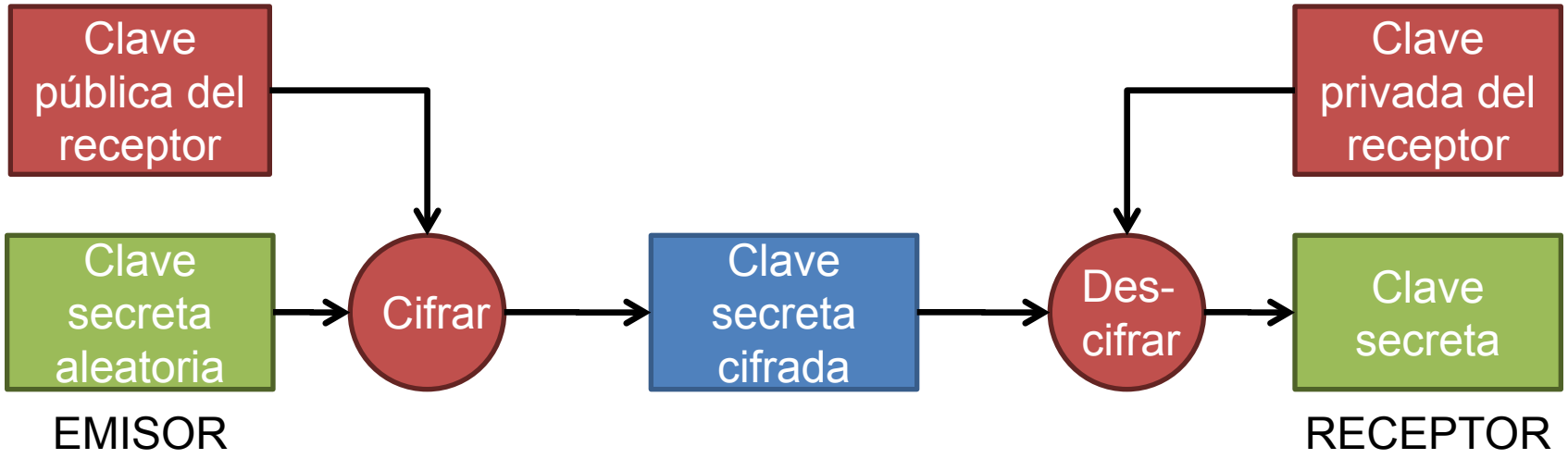
- Clave pública:
  - n = p×q, donde p y q son primos
  - e, primo con (p-1)×(q-1)

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

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

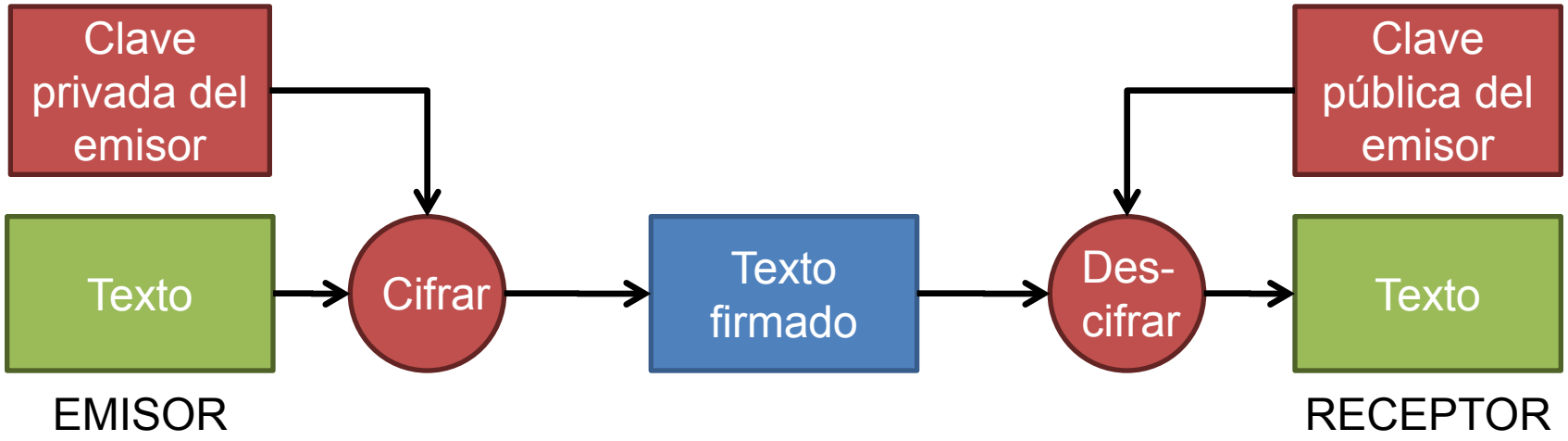
- Descifrar: $m = c^d \bmod n$

Distribución de claves secretas mediante criptografía asimétrica



- El emisor envía la clave secreta, generada aleatoriamente, cifrada con la clave pública del receptor, el único capaz de descifrarla usando su correspondiente clave privada

Autenticación mediante criptografía asimétrica



- El emisor cifra el mensaje con su clave privada, operación que sólo él puede realizar
- Cualquiera puede descifrarlo con su clave pública, verificando así su autoría
- El mensaje se comprime antes de ser firmado

Ataques sobre los criptosistemas de clave pública

- En lugar de hacer búsqueda exhaustiva de claves, se ataca el problema matemático subyacente:
  - En RSA se intenta factorizar el módulo n en lugar de probar todos los posibles valores de clave
  - Se consideran seguras longitudes de n a partir de 1024 bits
- La computación cuántica podría resolver los problemas de la criptografía de clave pública en un tiempo razonable
- Aún faltan muchos años para que se construyan los primeros ordenadores cuánticos, ¡si es que se crean alguna vez!

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	Privada: sólo conocida por una persona Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal La privada 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

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com