Criptografía

Contenidos

1. Introducción.
2. Criptografía clásica.
3. Criptografía moderna.
    1. Algoritmos simétricos.
    2. Algoritmos asimétricos.
    3. Funciones resumen o hash.
    4. Infraestructura de clave pública.
4. Criptografía cuántica.
5. Recursos de aprendizaje y CTFs

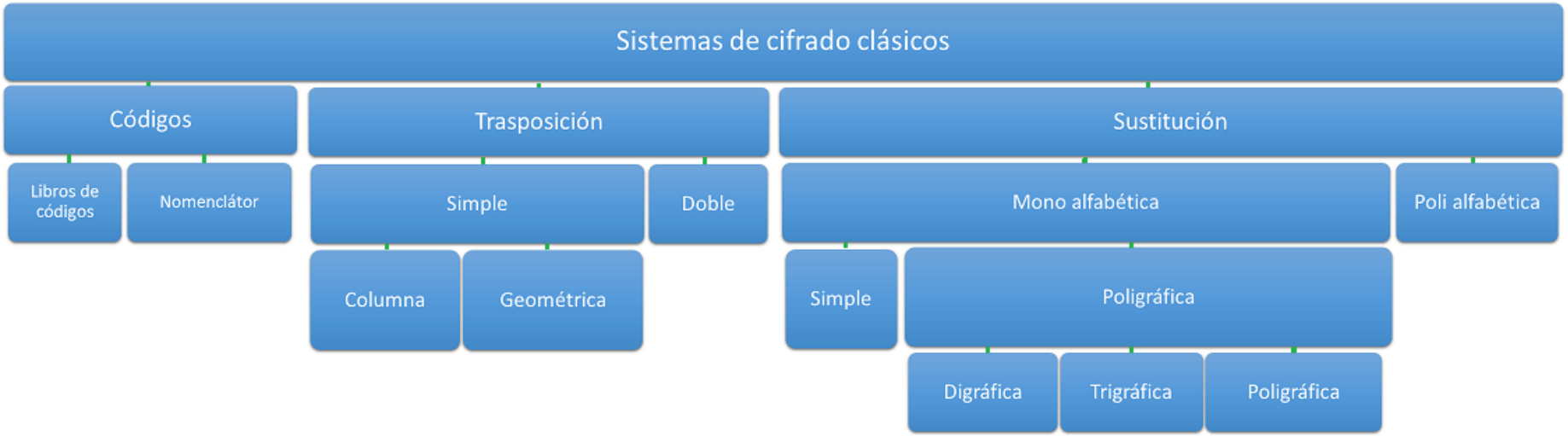
Introducción

- **Criptología**: ciencia que estudia la forma de ocultar información.
- **Criptografía**: técnicas utilizadas para ocultar información.
- **Criptoanálisis**: estudia los métodos para acceder a información cifrada sin conocer los secretos.

Necesidad de proteger información sensible y privada (comunicaciones políticas, militares, etc.)

Confidencialidad, Integridad, Autenticación, No Repudio

Criptografía clásica



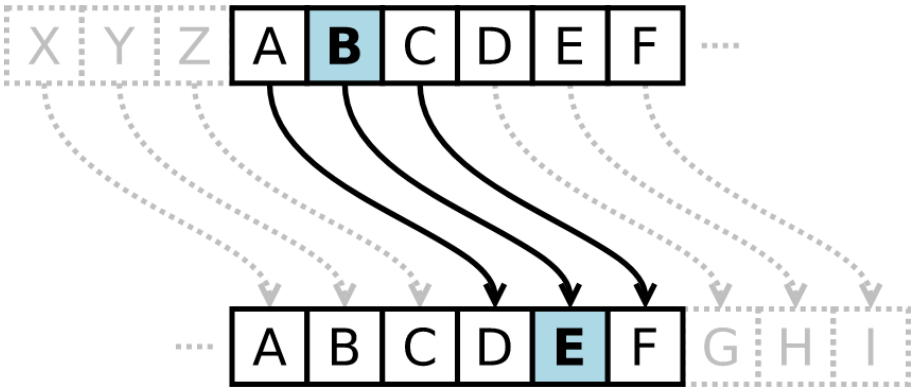
http://numerentur.org/criptografia-clasica/

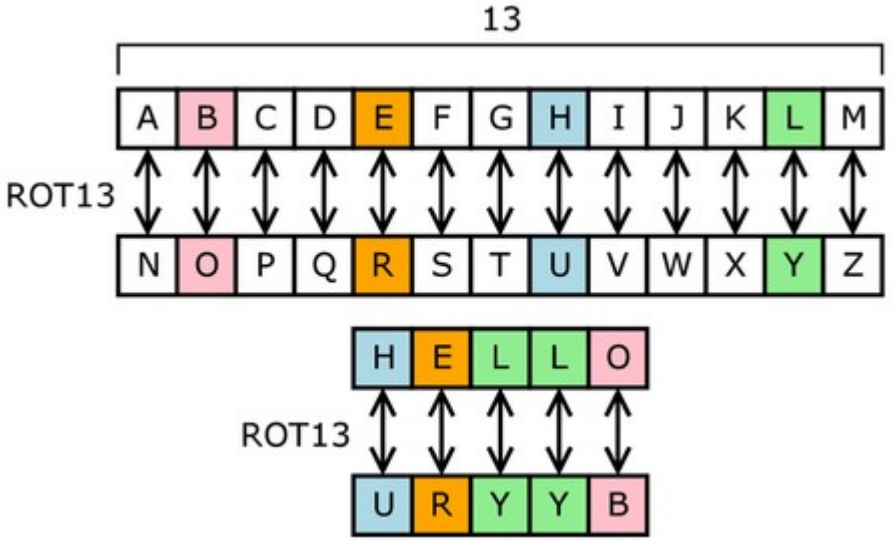
Criptografía clásica

- **Sustitución**. Los símbolos del alfabeto se sustituyen por otros.
  - **Monoalfabética**. Equivalencia entre los alfabetos signo a signo. Ej: Cesar, Atbash, Polybios, ROT13.
  - **Polialfabética**. Cada carácter se sustituye por otro en función de su posición. Ej: Alberti, Vigenère.
- **Trasposición**. Los símbolos del mensaje original se cambian de posición.
  - **Columnas**. Se escribe el texto por filas en una matriz y luego se reordena por columna. Ej. Escítala.
  - **Filas**. Método inverso al anterior.

Criptografía clásica

- Ejemplo: **Cesar**, **ROT13**





Criptografía clásica

- Ejemplo: **Polybios**
  - HOLA → 23 34 31 11
  - HOLA → BC CD CA AA

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Criptografía clásica

- Ejemplo: **Escítala**.

E	n		u	n		l	u	g	a
r		d	e		l	a		M	a
n	c	h	a	,		d	e		c
u	y	o		n	o	m	b	r	e
	n	o		q	u	i	e	r	o
	a	c	o	r	d	a	r	m	e

Criptografía clásica

- **Criptógrafos mecánicos**: aparatos que mediante el movimiento combinado de determinados elementos son capaces de cifrar de forma automática.
  - 1867. Disco Wheatstone.
  - 1900. Kriha.
  - 1920. Enigma.
  - 1936. Hagelin.
  - 1942. SZ42.

Criptografía clásica

- Ejemplo: **Enigma**
  - Hackaday: How the enigma machine works
  - Simulador: http://enigmaco.de/enigma/enigma.html

Criptografía clásica

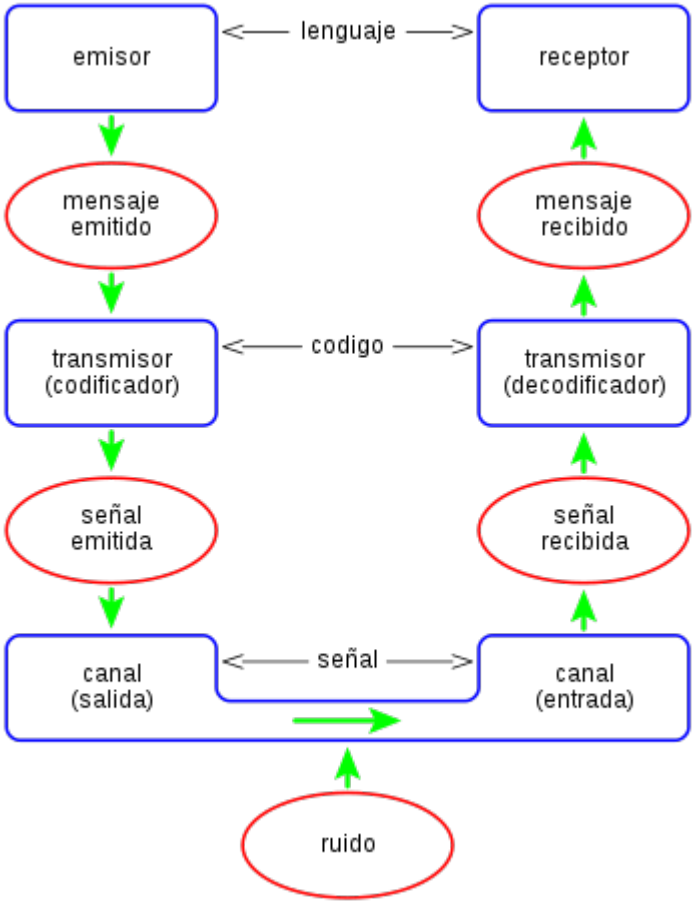
- **Ataques - Criptoanálisis**:
  - **Fuerza bruta**. Búsqueda de la clave utilizando todas las combinaciones posibles.
  - **Análisis de frecuencias**. Método estadístico que se basa en comparar la distribución de frecuencias de los caracteres en el texto cifrado con la del idioma correspondiente. http://numerentur.org/analisis-de-frecuencias/
  - **Método Kasiski**. Método de ataque a cifrados por sustitución polialfabéticos que no pueden ser atacados por el análisis de frecuencias. Desarrollado por Friedrich W. Kasiski contra el cifrado Vigenère. http://numerentur.org/metodo-kasiski/

Criptografía moderna

- Surge con el desarrollo de los ordenadores.
- 1883 - **Principios de Kerckhoffs** (6):
  - La seguridad del sistema debe depender solo de la clave (evitar la seguridad por oscuridad).
- 1948 - **Teoría de la Información de Shanon**.
  - Establece las bases que rige la transmisión y procesamiento de la información.
  - Aplicación: compresión, robótica, criptografía, etc.

Criptografía moderna

- Teoría de la Información de Shanon.

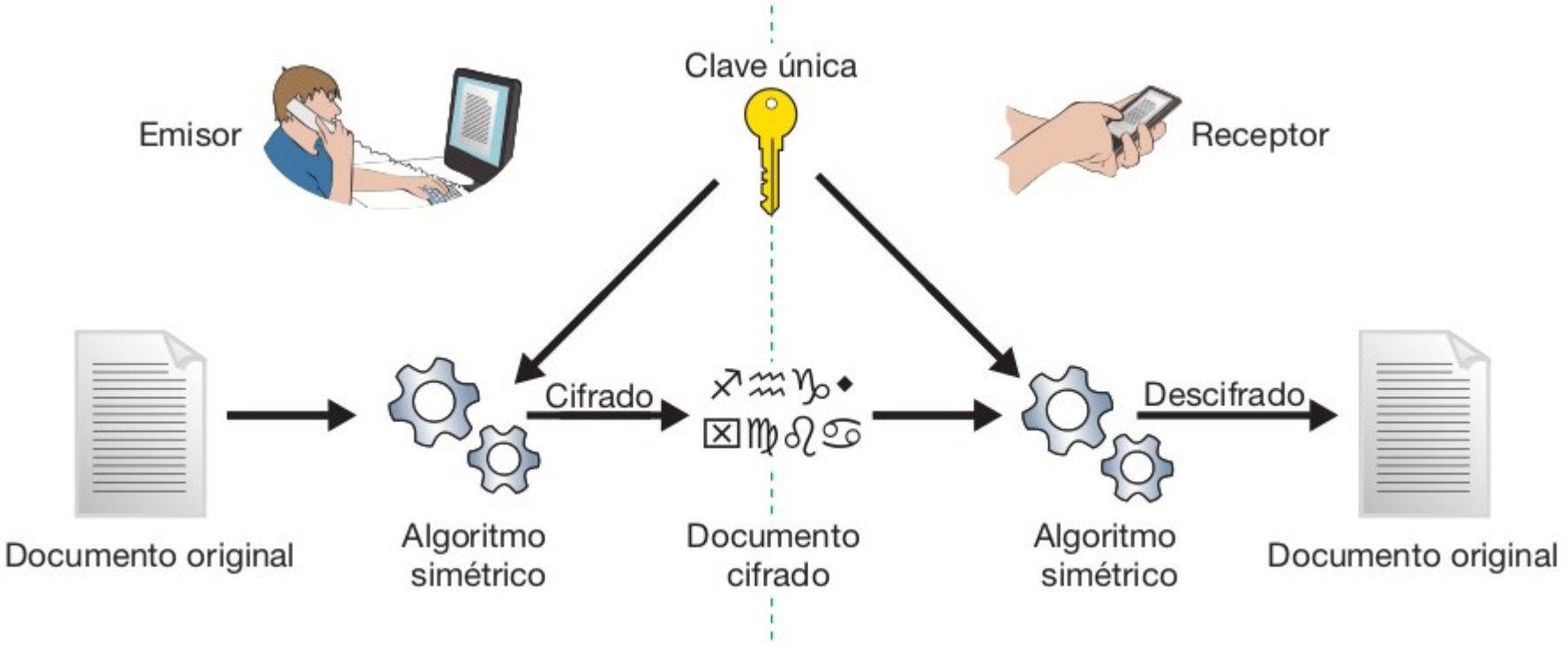


Criptografía moderna

- **Criptografía simétrica o de clave secreta**.
  - Misma clave para cifrar y descifrar.
  - Dos tipos:
    - Cifrado en serie o flujo.
    - Cifrado en bloque.
- **Criptografía asimétrica o de clave pública**.
  - Dos claves: pública y privada. Cifrado y firma digital.
  - Infraestructura de clave pública (PKI).
- **Funciones de resumen o *hash***.
  - Unidireccionales.
  - Se genera un resumen “único” del mensaje.

Algoritmos simétricos o clave secreta

- Misma clave para cifrar y descifrar.
- Problema: ¿cómo se intercambia la clave?



Algoritmos simétricos o clave secreta

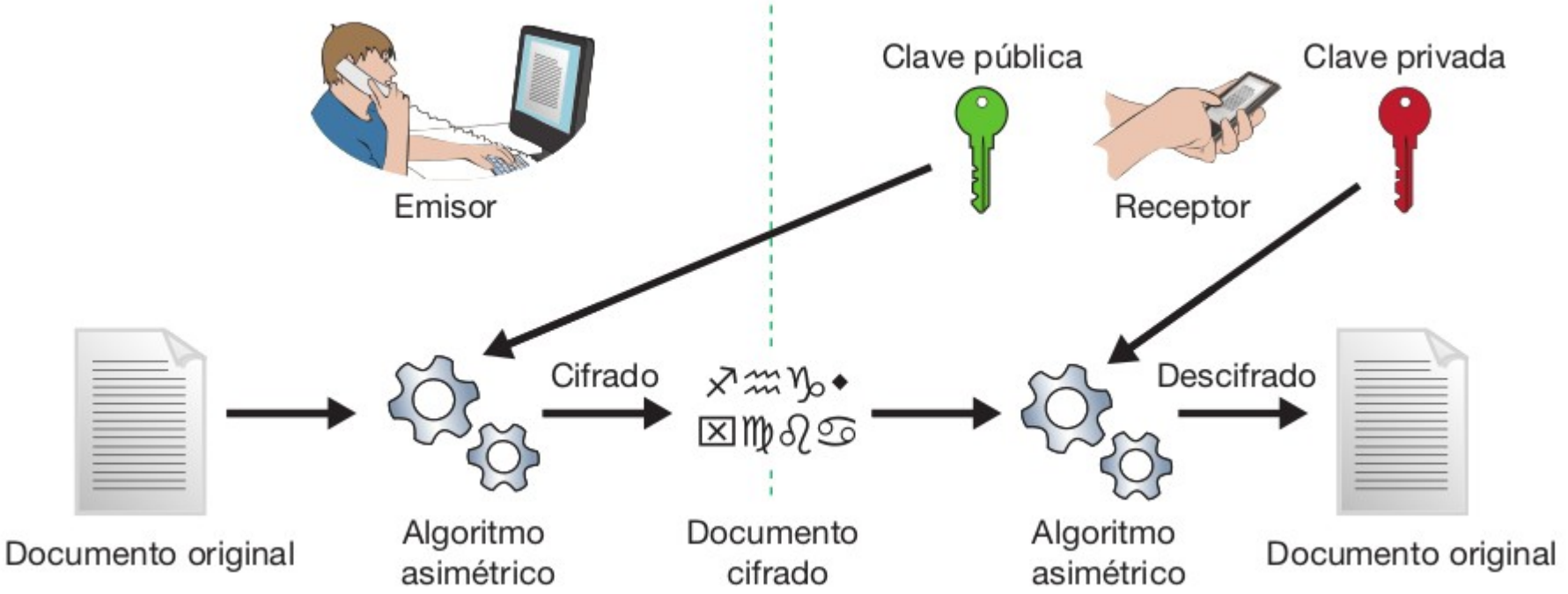
- **Cifradores de flujo** (*stream cipher*). La transformación se realiza a cada símbolo del mensaje (Ej: GSM A51 y A52).
- **Cifradores de bloque** (*block cipher*). La transformación se aplica sobre bloques (64, 128, 256 bits) del mensaje.
  - **DES** (*Data Encryption Standard*). Bloque de 64 bits, (clave de 56 bits más 8 de paridad).
  - **Triple DES** o **3DES**. Consiste en usar tres algoritmos DES encadenados.
  - **AES** (*Advanced Encryption Standard*) o **Rijndael** (por sus autores Joan Daemen y Vincent Rijmen). Bloque y claves de 128, 192 y 256 bits (o múltiplo de 32).
  - **Blowfish**, **Twofish** (256 bits) y **Threefish** (hasta 1024).

Algoritmos asimétricos o clave pública

- Es posible **cifrar** y/o **firmar** la información.
  - **Cifrado**. El emisor emplea la clave pública del receptor. El descifrado solo se puede realizar conociendo la clave privada.
  - **Firma**. El emisor utiliza su clave privada para firmar el mensaje. El receptor utiliza la clave pública del emisor para comprobar que la firma es correcta.
- Resuelven el problema del **intercambio de claves secretas** en los algoritmos simétricos.
- Origen en el artículo de W. Diffie y M.E. Hellman "New directions in Cryptography" de 1976.

Algoritmos asimétricos o clave pública

- **Clave pública** conocida por todo el mundo y **clave privada** conocida solo por su propietario.



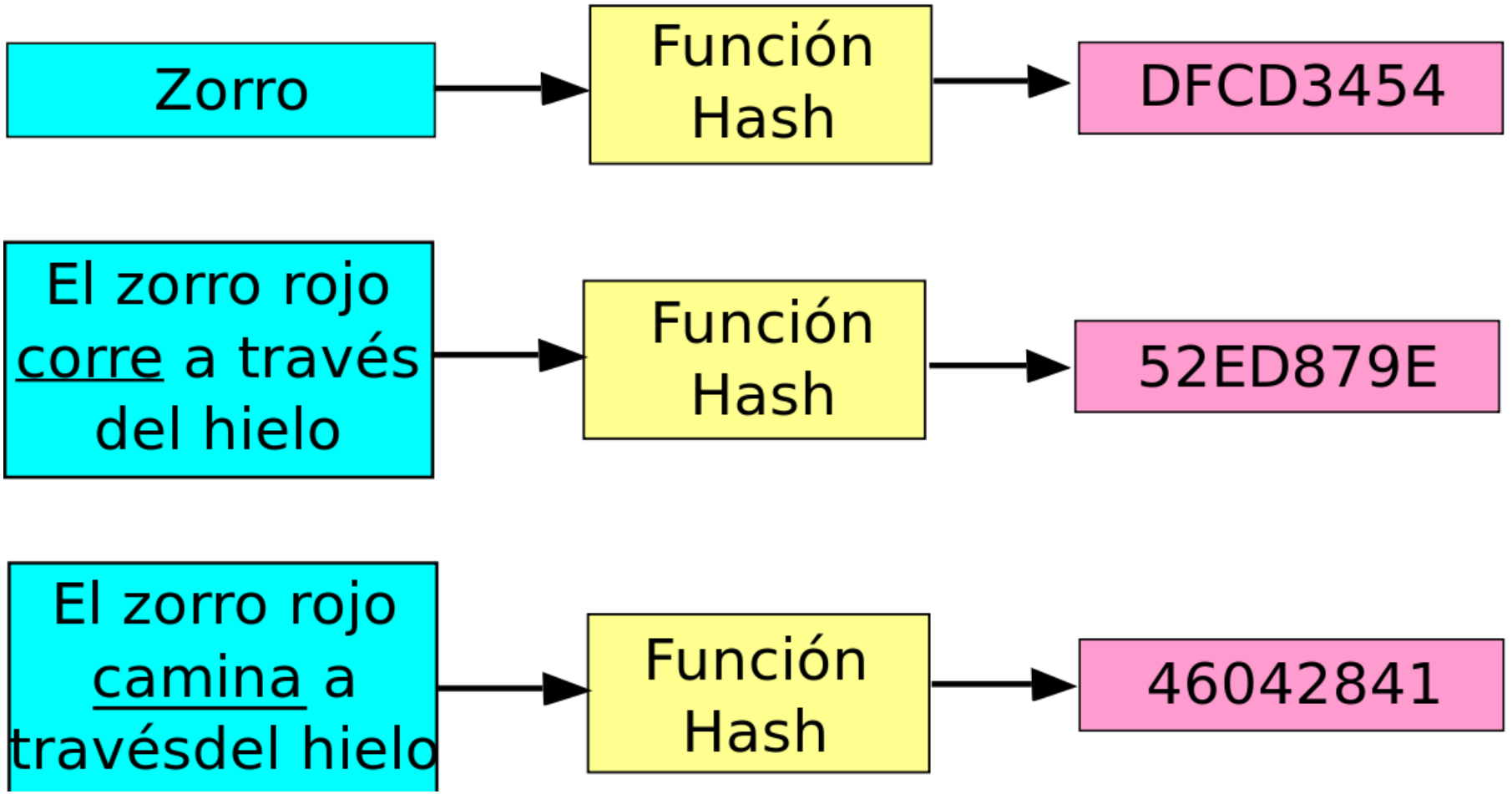
Algoritmos asimétricos o clave pública

- Algunos algoritmos de este tipo:
  - **RSA** (*Rivest-Shamir-Adleman*). Se basa en el problema de la **factorización** de números enteros. No existe ningún algoritmo que pueda resolver este problema en un tiempo polinomial. La empresa RSA Laboratories obtuvo la patente del algoritmo RSA y en 1991 comenzó a desarrollar una serie de estándares de criptografía de clave pública conocidos como **PKCS** (*Public-Key Cryptography Standards*).
  - **ElGamal**. Es el primer algoritmo que propuso el empleo de **curvas elípticas**, y al igual que la propuesta de Diffie-Hellman se basa en el problema del **logaritmo discreto**.

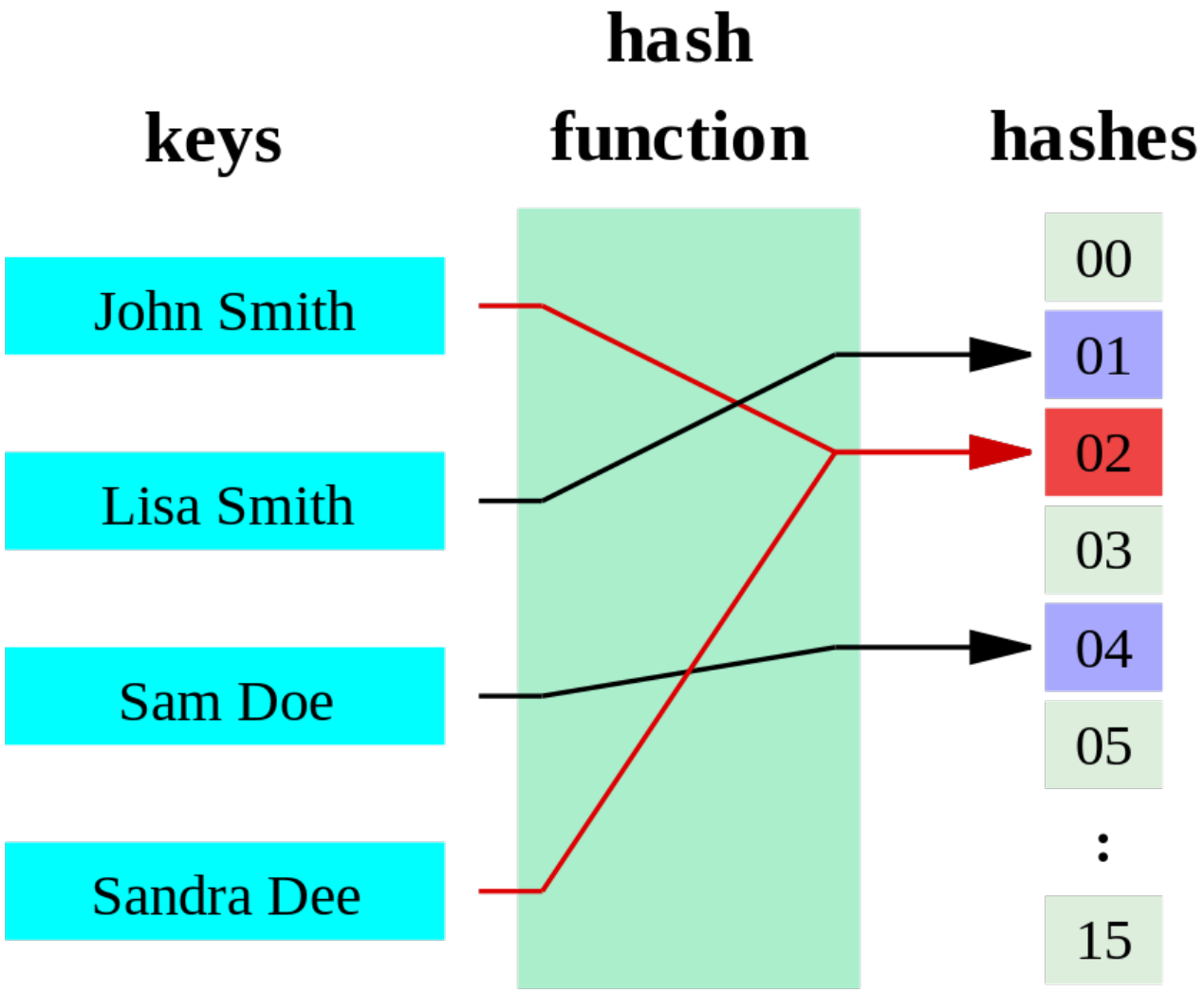
Funciones de resumen o hash

- Calculan un **resumen de longitud fija** de un mensaje que puede ser de cualquier longitud.
- La **seguridad** radica en que:
  - Sea imposible obtener el mensaje original a partir del resumen.
  - Sea imposible obtener un mensaje cuyo resumen sea idéntico (**colisión**).
- Son usados para **almacenar contraseñas**, para comprobar la **integridad de ficheros** y en la **firma electrónica**.

Funciones de resumen o hash



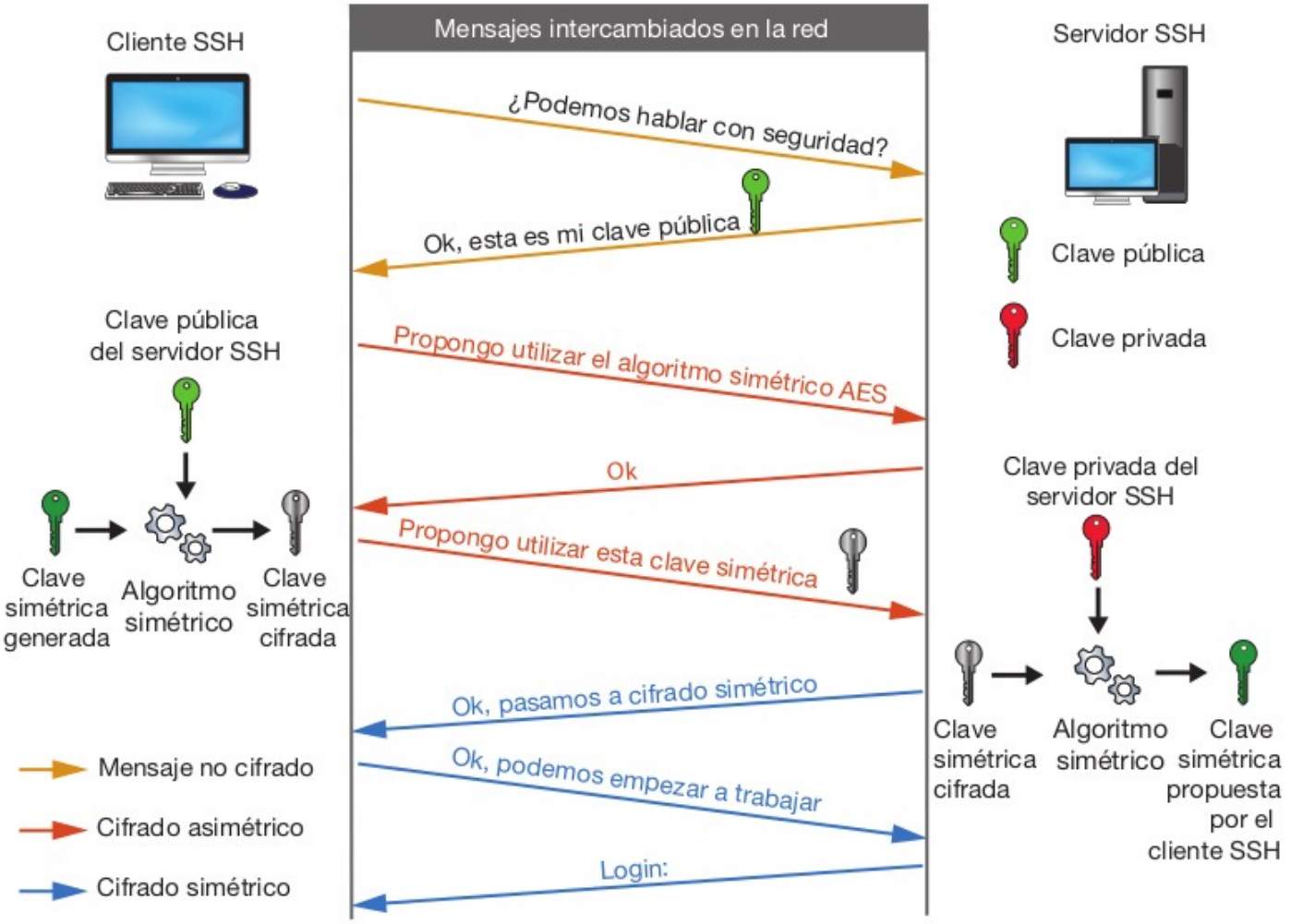
Funciones de resumen o hash



Funciones de resumen o hash

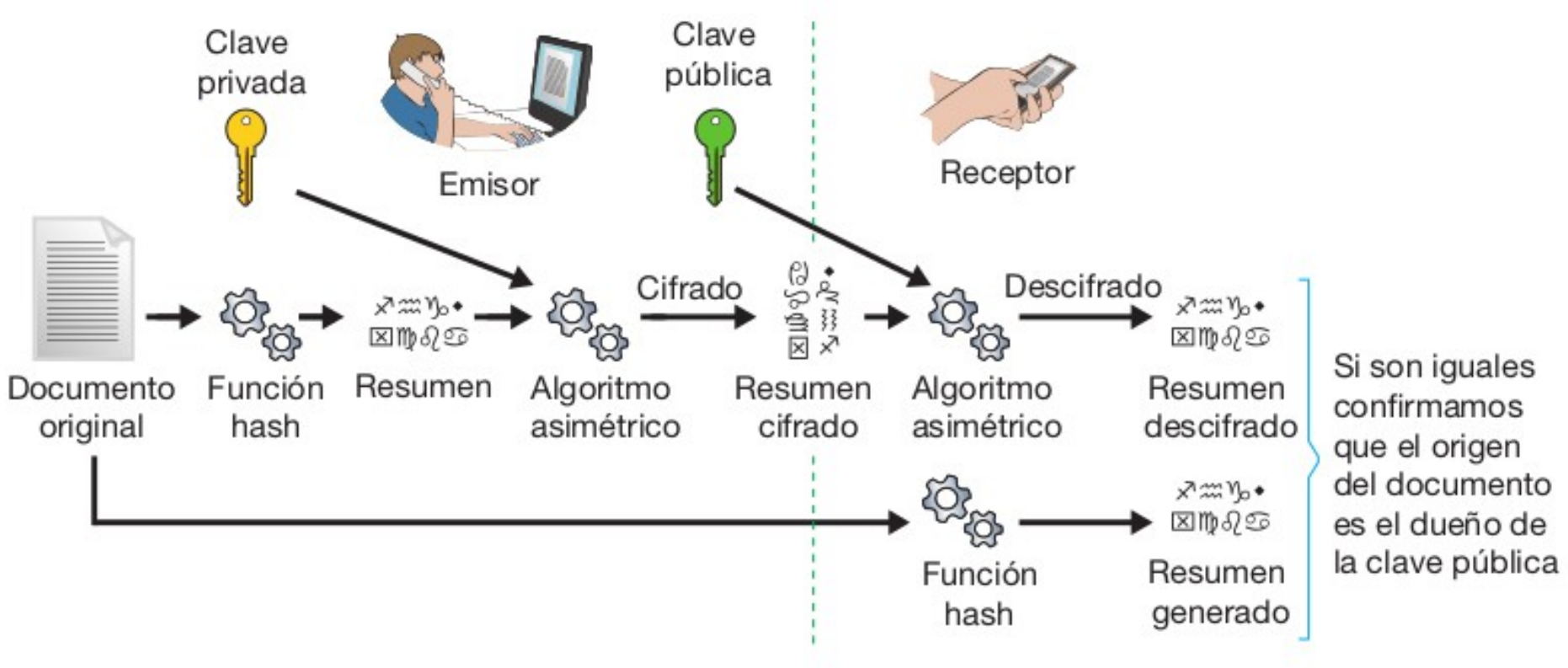
- Ejemplos de funciones *hash*:
  - **MD** (*Message Diggest*). Creado por Ronald Rivest, la R de RSA. Existen diversas versiones, MD2, MD4, MD5 y MD6. La seguridad de MD5 está comprometida actualmente y su uso está desaconsejado, su longitud de resumen es de 128 bits. MD6 puede tener una longitud variable de resumen hasta 512 bits.
  - **SHA** (*Secure Hash Algorithm*). Conjunto de funciones hash publicadas por el NIST. Series SHA-0, SHA-1, SHA-2 y SHA-3. La seguridad de SHA-2 está empezando a ser comprometida y muchas de sus versiones (según la longitud de resumen que emplean) son inseguras por lo que **se recomienda usar SHA-3**.

Intercambio de clave secreta



Firma digital

- Criptografía de clave pública + función *hash*.



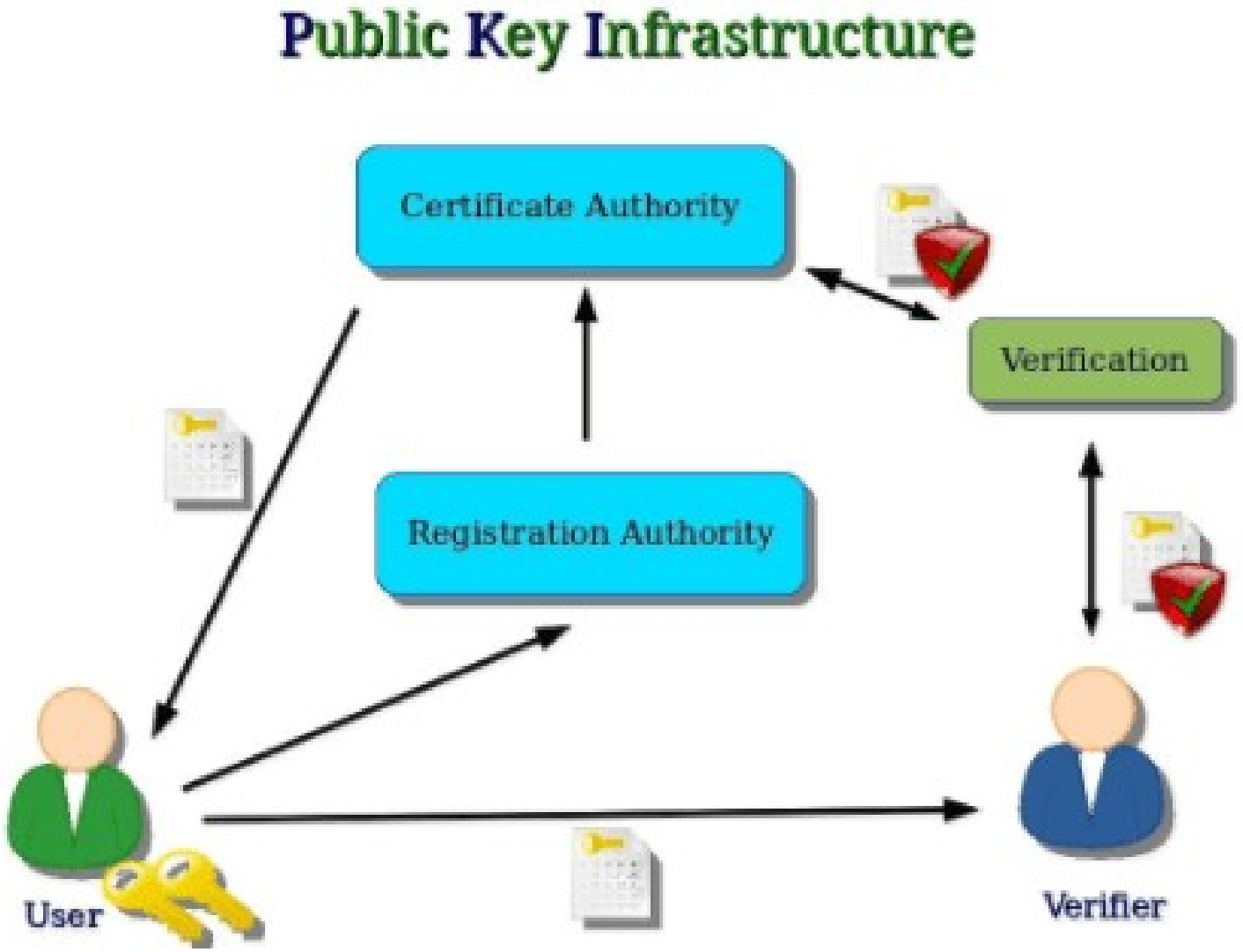
Infraestructura de Clave Pública

- **PKI** (***Public Key Infraestructure***) permite la ejecución con garantías de operaciones criptográficas basadas en clave pública. En ella intervienen:
  - **Autoridad de Certificación** (CA – Certification Authority).
  - **Autoridad de Validación** (VA – Validation Authority).
  - **Autoridad de Registro** (RA – Registration Authority).
  - **Certificado electrónico** X.509.
- Hace posible la **firma electrónica**. Misma validez que la firma manuscrita (Ley 6/2020).
- Protocolos seguros con certificados de confianza (HTTPS, SSH, etc.).

Infraestructura de Clave Pública

- **Certificado electrónico**. Documento electrónico emitido por una **autoridad de certificación** que permite cifrar y firmar documentos e identificarse de forma electrónica.
- **Autoridad de Certificación**. Organismo (público o privado) encargado de emitir certificados electrónicos.
- **Autoridad de Validación**. Comprueba la validez de un certificado digital.
- **Autoridad de Registro**. Comprueba la validez de los datos del certificado y del usuario que lo está tramitando.

Infraestructura de clave pública



Infraestructura de clave pública

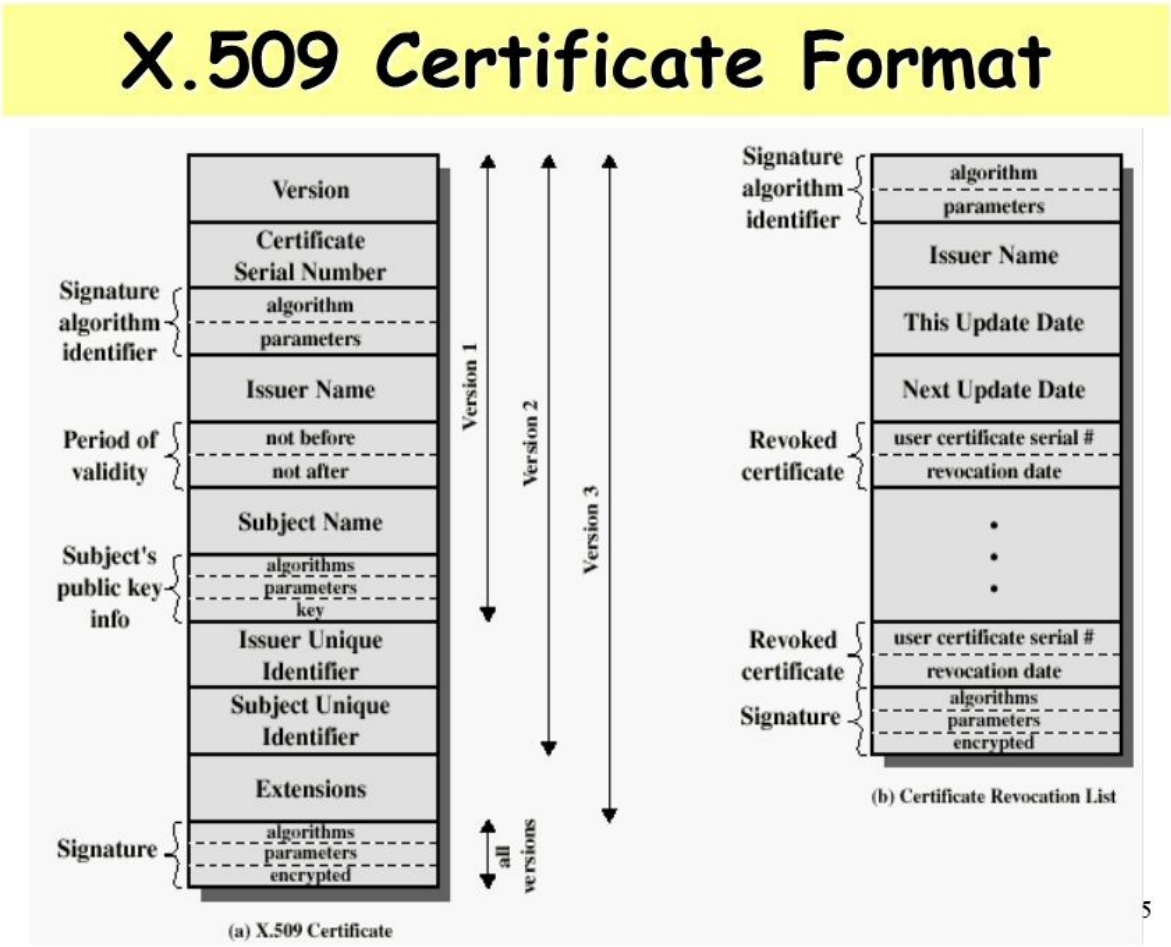
1. Para obtener un certificado digital debemos solicitarlo a una CA.
2. La propia CA o una RA comprobará nuestros datos e identidad para validarlos antes de emitir el certificado.
3. La CA emite el certificado firmado con su clave privada.
4. La CA debe disponer de un certificado emitido por otra autoridad de certificación de rango superior: **CA raíz.**
5. La CA raíz puede firmar su propio certificado.
6. ¿Cómo confiar en una CA? Sello **Webtrust**.

Infraestructura de clave pública

7. Hay que comprobar la validez del certificado (VA).
8. Un certificado puede ser no válido porque haya expirado o su clave privada esté comprometida.
   - En este caso **el certificado se revoca** y se añade a una **lista de revocación de certificados** (CRL – *Certification Revocation List*).
   - Una alternativa a CRL es el **protocolo OCSP** (*Online Certificate Status Protocol*).

Certificado electrónico

- Fichero que cumple el **protocolo X.509** (RFC 5280. Última versión v3).



Certificado electrónico

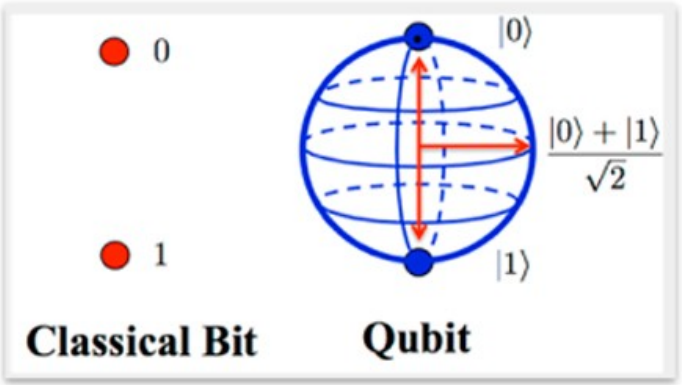
- Campos de un documento **X.509 v3.**
  - **Número de versión**: (v1, v2 o v3).
  - **Número de serie**: Identifica de manera única un certificado digital emitido por una CA.
  - **Algoritmo de firma del certificado**: Algoritmo utilizado por la CA para firmar el certificado.
  - **Emisor**: Entidad que ha emitido el certificado.
  - **Validez**. Periodo durante el cual el certificado es válido. Contiene una fecha de inicio y caducidad.
  - **Asunto**. Datos del propietario del certificado.
  - **Información de la clave pública del sujeto**. Clave pública y algoritmos de clave pública asociados a la misma.
  - **Extensiones**. Información adicional del certificado.
  - **Firma digital de la autoridad de certificación**. Firma digital real del certificado, realizada por la entidad emisora utilizando el algoritmo de firma indicado.

Certificado electrónico

- La Fábrica Nacional de Moneda y Timbre (FNMT), a través de su departamento CERES (CERtificación ESpañola) es una CA de confianza con el sello Webtrust.
- También disponemos del DNIe cuyo chip lleva almacenado un certificado digital emitido por la Dirección General de la Policía que actúa como CA.
- Firma electrónica de documentos:
  - Web VALIDe.
  - Software Sinadura.
  - Software Autofirma.

Criptografía cuántica

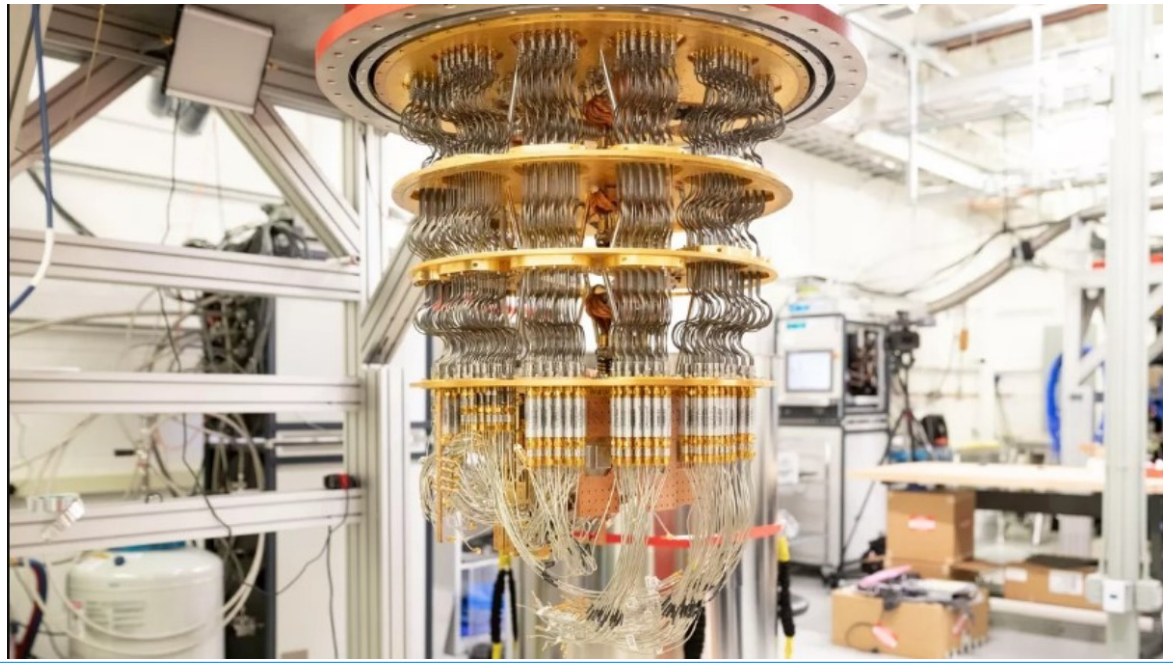
- **Ordenador cuántico**.
  - Bits cuánticos: **qubits** (x qubits = 2^x bits).
  - Puede llegar a ser más potente que 100 millones de ordenadores actuales.
  - IBM Q, Google, Microsoft.



Hola Mundo en 7 lenguajes de programación cuánticos
https://ionq.com/posts/june-24-2021-hello-many-worlds

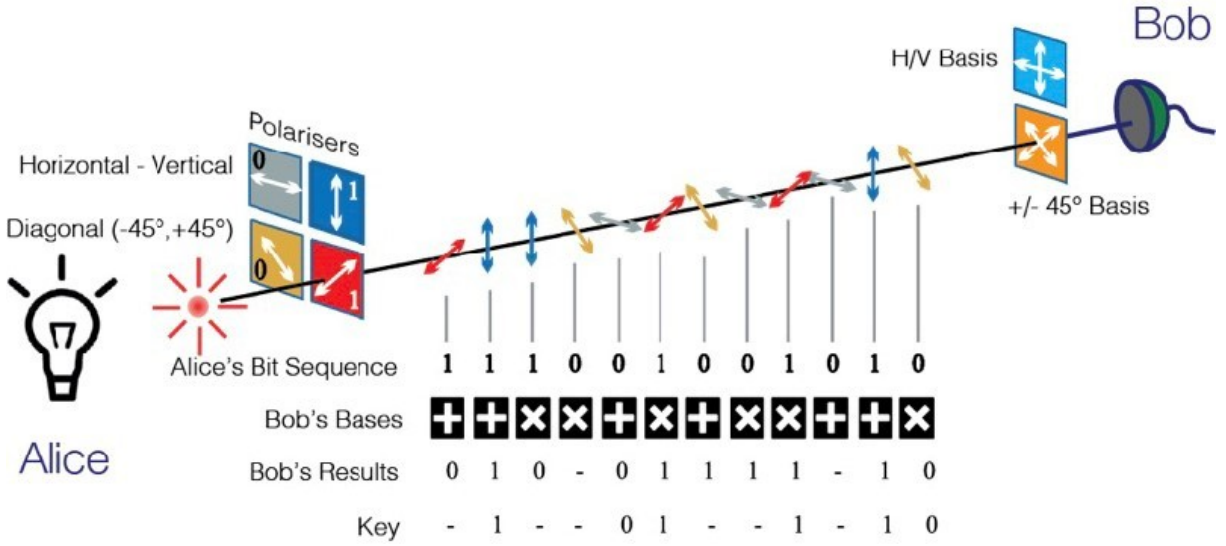
Criptografía cuántica

- **Supremacía cuántica**.
  - Ordenador cuántico que haga algún cálculo que un superordenador no puede hacer.
  - Con 40 qubits puedo realizar 2^{40} operaciones: no es suficiente.
  - Romper claves actuales (2048 bits) requeriría 4 días con 7 millones de qubits. En el año 2030.



Criptografía cuántica

- **Protocolo cuántico: QKD**
  - Distribución cuántica de claves (*Quantum Key Distribution*).
  - Único protocolo propuesto. No se necesita un ordenador cuántico. Ejemplos:
    - Bennett y Brassard (1984): BB84.
    - Ekert (1991): E91.



Criptografía cuántica

- **Criptografía cuántica**.
  - Utiliza los principios de la física cuántica y no necesita un ordenador cuántico: QKD.
  - Problemas: distancia máxima y se necesita un canal clásico para comprobar la información intercambiada.

TECNOLOGÍA • Puede servir para construir una red de comunicaciones globales imposibles de ser hackeadas

China consigue la primera comunicación cuántica entre un satélite y la Tierra

ISMAEL ARANA | Hong Kong 21 JUN. 2017 | 09:40

China crea un sistema de comunicación cuántica desde el espacio imposible de espiar

El país asiático transmite claves secretas desde un satélite a dos estaciones terrestres separadas por más de 1.000 kilómetros, 10 veces más que lo conseguido hasta ahora

Criptografía cuántica

- **Criptografía cuántica**.
  - Utiliza los principios de la física cuántica y no necesita un ordenador cuántico: QKD.
  - Problemas: distancia máxima y se necesita un canal clásico para comprobar la información intercambiada.

Toshiba QKD system

Toshiba's prototype Quantum Key Distribution (QKD) system delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages.

Criptografía cuántica

- **Amenaza cuántica.**
  - Peter W. Shor (1997): "*Polynomial-Time algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*".
    - Los algoritmos matemáticos empleados en criptografía asimétrica se romperían en tiempo polinómico.
  - L. K. Grover (1997): "*Quantum mechanics helps in searching for a needle in a haystack*".
    - Se reduciría el tiempo en romper la criptografía simétrica a la raíz cuadrada.
    - *Estudios más recientes apuntan a aceleraciones exponenciales (paralelización del algoritmo de Simon).

Criptografía cuántica

- **Amenaza cuántica**.
  - La **criptografía asimétrica** basada en factorización de enteros (RSA) o logaritmo discreto (DSA) morirá.
  - La **criptografía simétrica** solo necesitará duplicar el tamaño de claves para mantener la seguridad (*en duda).

https://youtu.be/eudffSU51K0

Futuro: criptografía post-cuántica

- Solución: **criptografía post-cuántica** (**PQC**).
  - Criptosistemas que funcionan en ordenadores clásicos pero son seguros incluso si el adversario tiene un ordenador cuántico.
  - Tipos de **algoritmos post-cuánticos**.
    - Criptografía basada en Teoría de Códigos (*Code-based*).
    - Firmas digitales basadas en hashes (*hash-based*).
    - Criptografía multivariante cuadrática (MQC).
    - Criptografía basada en isogenias (*isogeny-based*).
    - Criptografía basada en retículos (*lattice-based*).

The race to save the Internet from quantum hackers
https://www.nature.com/articles/d41586-022-00339-5

Futuro: criptografía post-cuántica

- Solución: **criptografía post-cuántica** (**PQC**).
  - NIST (2016). *Call of papers* algoritmos asimétricos.
    - 1ª ronda: aceptados 69 algoritmos (11/2017) aunque se retiraron 5 después de numerosos comentarios.
    - 2ª ronda: Se mantienen 26 algoritmos (01/2019): 17 criptosistemas de de clave pública y protocolos de acuerdo de clave y 9 de firma electrónica.
  - El NIST no incluyó la criptografía simétrica. Publicaciones recientes (Naya-Plasencia, 2016) indican que podría no estar tan preparada para resistir la computación cuántica.

Recursos de aprendizaje y CTFs

- Cyberchef. Herramienta online para realizar múltiples cifrados/descifrados y codificaciones.
- Dcode.fr. Dispone de numerosas herramientas para códigos y criptografía.
- Cryptovenom. Herramienta de código fuente libre que dispone de numerosos criptosistemas y criptoanálisis creada por @LockedByte (Alejandro Guerrero).
- Cryptohack.org. Cursos y retos para aprender criptografía.
- Blog de Mikel García Larragan. Contiene información sobre criptografía y criptoanálisis, propuesta de retos y sus soluciones.
- Proyecto CLCript. Cuaderno de laboratorios de criptografía de la UPM, elaborados dentro del proyecto Criptored.
- CriptoCert. Primera certificación sobre criptografía para criptoanalistas.

FIN