Módulo 1:
Criptografía y Esteganografía

Hacking Ético

2023 / 2024

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Definiciones

La criptografía es la ciencia dedicada al estudio de la escritura secreta. Compuesta de los siguientes campos:

- **Criptografía**: Estudio de las técnicas que alteran las representaciones lingüísticas para hacerlas inteligibles a los potenciales ‘intrusos’.
- **Criptoanálisis**: Estudio de los métodos para intentar obtener el sentido de una información cifrada, sin tener acceso a la información secreta requerida para ello.
- **Esteganografía**: Estudio de las técnicas para el ocultamiento de mensajes (No los transforma, los oculta).

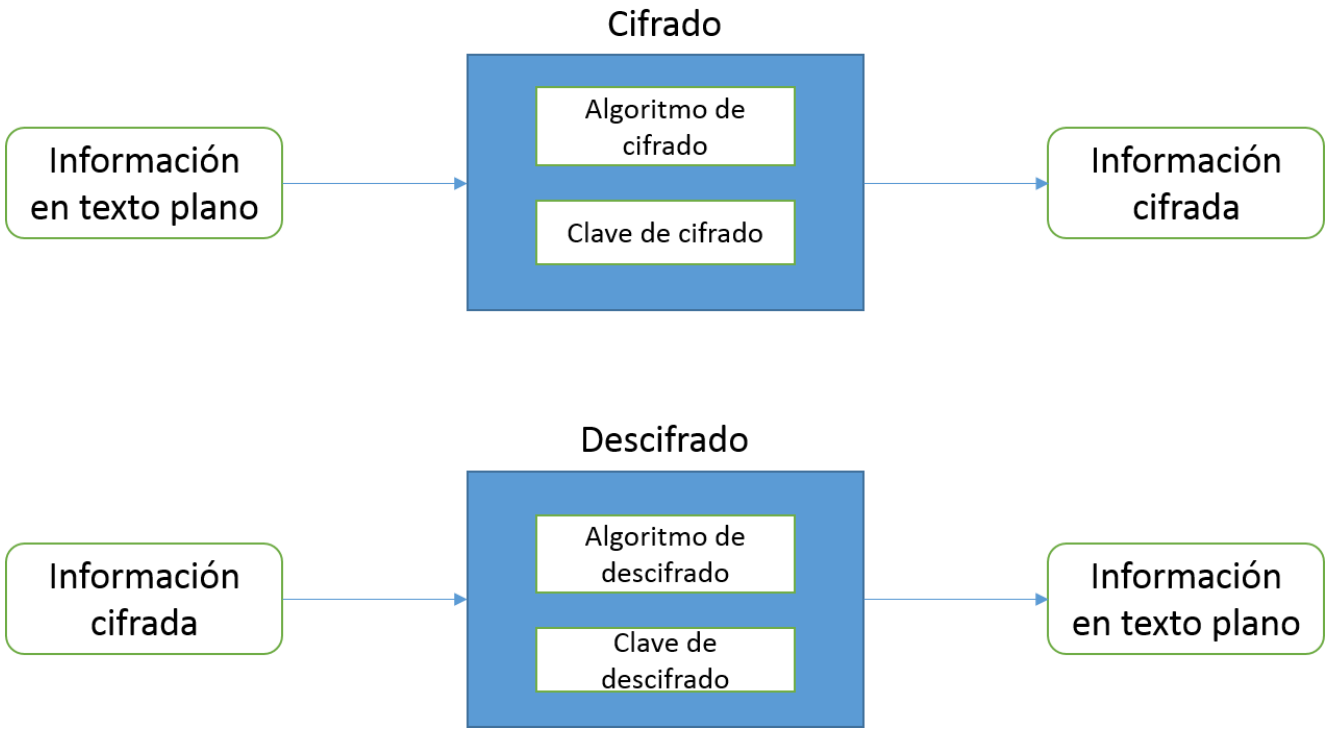
Sistemas de cifrado

El **cifrado** es un procedimiento que hace uso de un **algoritmo** de cifrado con una determinada **clave** para **transformar un mensaje**, sin prestar atención a la estructura lingüística o significado.

El objetivo es convertir el **texto** que se quiere ocultar en algo **incomprensible** o al menos, difícil de comprender para toda persona que no tenga la clave.

Sistemas de cifrado

Los elementos clásicos de un sistema de cifrado son los siguientes:



1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Principios criptográficos

En la criptografía clásica se utilizaban dos métodos de cifrado:

- **Transposición**: Se basa en cambiar la posición de los caracteres.

  Ejemplo: gato → OTAG

Existen múltiples formas de implementar el algoritmo de transposición entre los que destacan por carácter o por bloques.

Plain Text:	p r o b	h a t d	e u r i	g o t h	e r e k
Key:	3 2 0 1	3 2 0 1	3 2 0 1	3 2 0 1	3 2 0 1
Cipher Text:	o b r p	t d a h	r i u e	t h o g	e k r e
Positions:	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
Key:	3 2 0 1	3 2 0 1	3 2 0 1	3 2 0 1	3 2 0 1
Plain Text:	p r o b	h a t d	e u r i	g o t h	e r e k

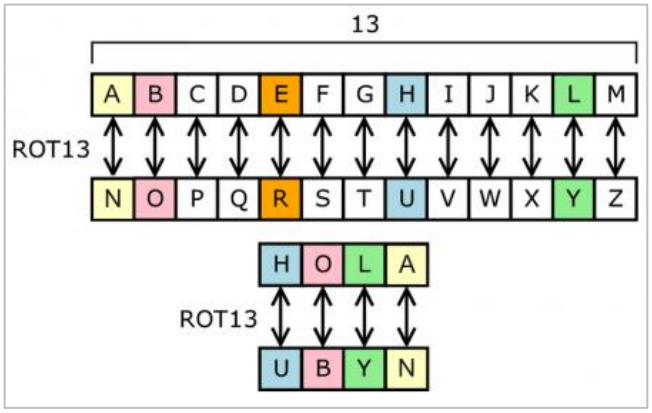
Principios criptográficos

En la criptografía clásica se utilizaban dos métodos de cifrado:

- **Sustitución**: Se basa en sustituir los caracteres por otros. Mantienen la posición pero son modificados. Los métodos de sustitución pueden ser:
  - Monoalfabéticos: Uso de un único alfabeto. Carácter A → Carácter B siempre!
  - Polialfabéticos: Uso de varios alfabetos. Cambia de forma periódica.

Pudiendo ser la sustitución:

- Monograma: Carácter a carácter.
- Poligrama: Por grupos de caracteres.



Modelos de descifrado (Ataques)

- **Ataque basado solo en texto cifrado**: El atacante tiene el texto cifrado para analizar
  - Probar todas las claves posibles distinguiendo texto real de incoherencias.
  - Análisis estadístico.

- **Ataque basado en texto legible conocido**: el atacante tiene algo de texto legible correspondiente a texto cifrado
  - Por ejemplo, en cifrado monoalfabético el atacante determina pares.

- **Ataque por texto legible seleccionado**: el atacante se las ingenia para conseguir que transmisor envíe un texto conocido que el vera en su forma cifrada

Tipos de criptografía

La criptógrafa normalmente usa un algoritmo conocido por todos y solo las claves son secretas.

- **Criptografía de clave simétrica**: Usa una única clave, utilizada tanto para cifrar como para descifrar.
- **Criptografía de calve pública**: Usa dos claves que pueden ser usadas de forma desordenada para cifrar o descifrar.
- **Funciones Hash**: No hace uso de claves.

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Cifrado Simétrico

Es un método de cifrado que utiliza la **misma clave para cifrar y descifrar**. Las dos partes han de ponerse de acuerdo de antemano para utilizar dicha clave conocida por ambos.

Misma clave de cifrado

Cifrado Simétrico

Existen dos tipos de cifrado simétrico:

- **Cifrado de flujo**

Cifrado de un bit cada vez. Combina cada bit del flujo de clave con el texto legible y obtiene el texto cifrado. Ejemplo: RC4.

- **Cifrado de bloques**

Se divide el mensaje legible en bloques de igual tamaño y se cifra cada bloque como una unidad. El mensaje es procesado en bloques de k bits (p.e., bloques de 64 bit).

Cifrado Simétrico - DES

Data Encryption Standard (DES)

- Es un estándar americano de creado en 1993.
- Hace uso de una clave de 56 bit + 8 bit de paridad.
- Toma bloques de texto plano de 64 bits en cadena (Cifrado por bloques)
- De forma analítica es muy complejo. Por fuerza bruta en menos de un día es posible romperlo.

3DES: Es una algoritmo que se publico de forma posterior y consiste en cifrar 3 veces utilizando el algoritmo DES con diferente valor de clave (en realidad el algoritmo cifra, descifra y vuelve a cifrar).

Cifrado Simétrico - AES

Advanced Encryption Standard (AES o Rijndael)

- Es un estándar estadounidense de clave simétrica publicado en Noviembre de 2001 para remplazar al algoritmo roto DES.
- Utiliza cifrado de bloques de datos de 128 bits.
- Puede hacer uso de claves de 128, 192, o 256 bits.
- Si el descifrado de DES a través de fuerza bruta durase 1 segundo, en AES serán necesarios 149 trillones de años.

Actualmente AES es el estándar utilizado para cifrado simétrico, que cuenta con un nivel de seguridad suficiente, siendo además el algoritmo mas robusto.

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Cifrado Asimétrico

Es un método de cifrado donde **se requiere que transmisor y receptor compartan un secreto** pero… ¿Como ponerse de acuerdo si no se conocen?

Dos claves distintas

Clave pública **Clave privada**

Cifrado Asimétrico

A través del cifrado asimétrico o cifrado de clave pública:

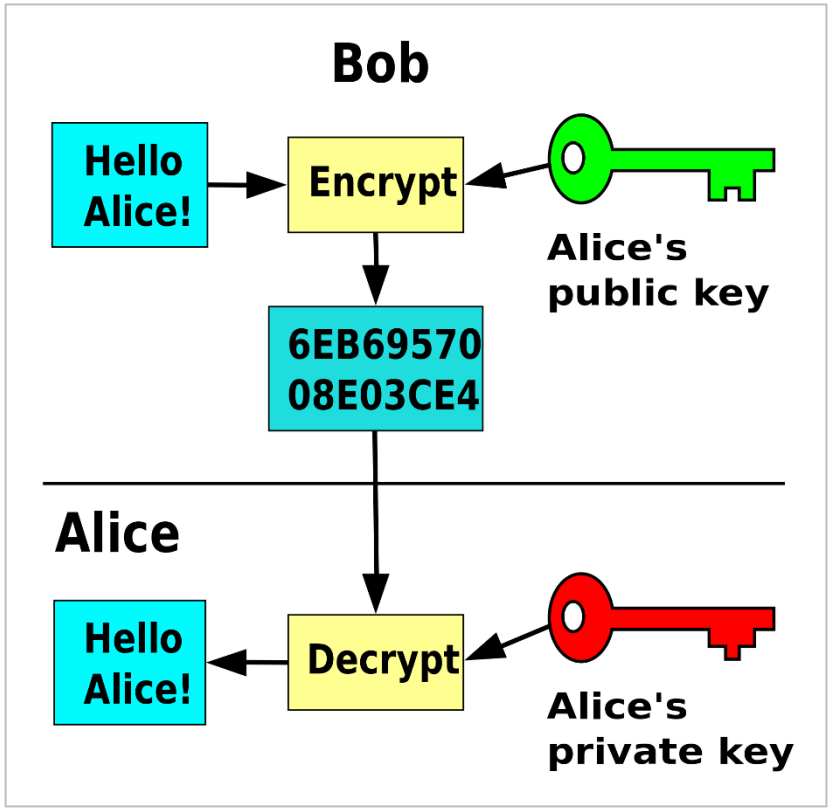
- Transmisor y receptor **no comparten ningún secreto.**
- La **clave publica** es conocida por todos ya que el propietario la publica.
- La **clave privada** solo la conoce el propietario y es secreta.

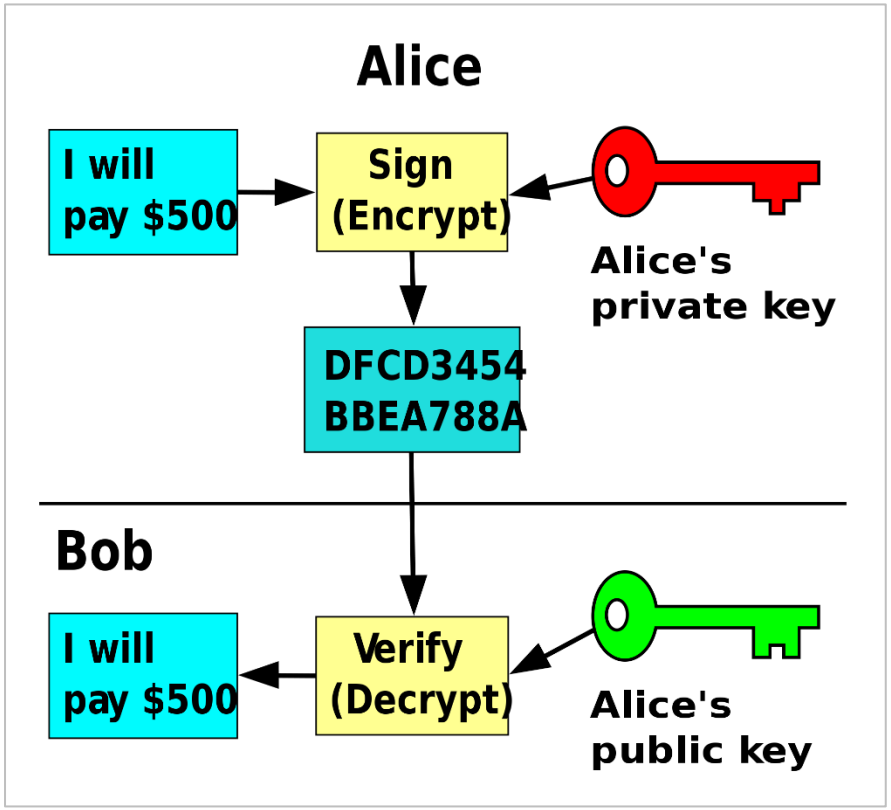
Permite mantener la confidencialidad y autenticidad entre dos personas que previamente no comparten información.

PROPIEDAD IMPORTANTE:

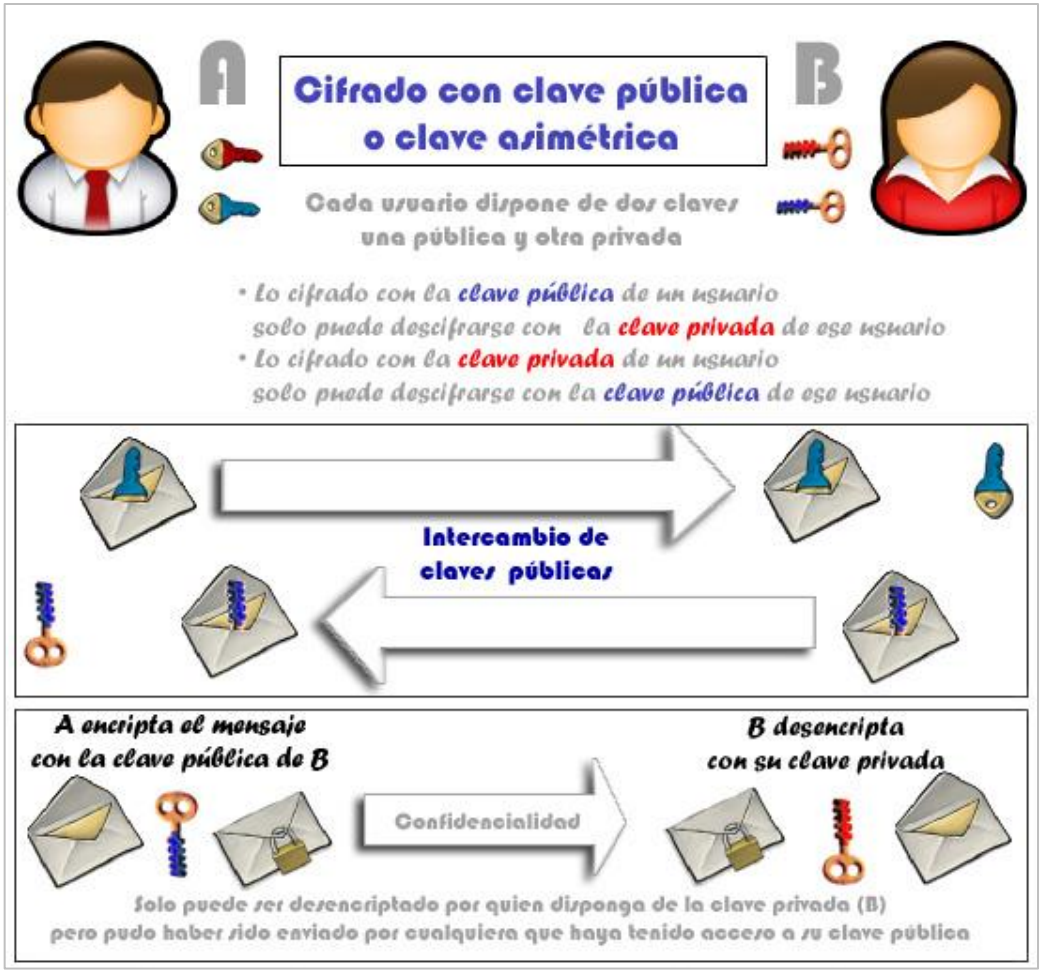
El resultado es el mismo independientemente de si se usa primero la clave privada o la pública.

Cifrado Asimétrico – Funcionamiento Básico





Cifrado Asimétrico – Propiedades



Cifrado Asimétrico – Propiedades

Cifrado Asimétrico - RSA

RSA (Rivest, Shamir y Adleman)

- Considera un mensaje como un patrón de bits.
- A su vez, un patrón de bits puede ser unívocamente interpretado por un numero entero.
- De esta forma, asume que cifrar un mensaje es como cifrar un numero.
- Para cifrar un mensaje, ciframos el numero o conjunto de números correspondiente.

Cifrado Asimétrico - RSA

Funcionamiento:

- Se eligen 2 números primos (*p* y *q*) suficientemente grandes.
- Se calculan $n = pq$ y $z = (p - 1)(q - 1)$.
- Se elige un valor $e < n$ primo relativo con z.
- Se elige un valor d tal que $ed \bmod z = 1$.
- La clave publica es (n, e) y la privada (n, d)

En Linux se puede generar el par de claves publica y privada mediante los siguientes comandos:

- *openssl genrsa -out mykey.pem*
- *openssl rsa -in mykey.pem -pubout*

Cifrado Asimétrico - RSA

Cifrado: $c \equiv m^e \pmod{n}$

Descifrado: $m \equiv c^d \pmod{n}$

Ejemplo:

p = 61	1º nº primo privado
q = 53	2º nº primo privado
n = pq = 3233	producto p×q
e = 17	exponente público
d = 2753	exponente privado

$$\text{encrypt}(m) = m^e \pmod{n} = m^{17} \pmod{3233}$$

$$\text{decrypt}(\text{c}) = c^d \pmod{n} = c^{2753} \pmod{3233}$$

$$\text{encrypt}(123) = 123^{17} \pmod{3233} = 855$$

$$\text{decrypt}(855) = 855^{2753} \pmod{3233} = 123$$

Funciones Asimétrico - RSA

¿Por qué es seguro RSA?

Supongamos que conocemos la clave publica de alguien (n, e). ¿Sería difícil determinar d?

- Se requiere encontrar factores de *n* sin conocer los factores *p y q.*
- Hechos importantes a tener en cuenta:
  - Factorizar grandes números es difícil.
  - RSA implica exponenciación que es algo computacionalmente intensivo.
  - DES es al menos 100 veces mas rápido que RSA.

Lo normal es que en el inicio de una comunicación segura se utilice el algoritmo RSA para intercambiar una clave simétrica. Posteriormente se usa cifrado simétrico con la clave intercambiada.

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Funciones Hash

Las funciones Hash cumple las siguientes condiciones:

- Una función *H(m)* toma como entrada un mensaje de largo arbitrario y genera un string de largo fijo denominado hash o firma del mensaje.

- La función *H(m)* es una aplicación suprayectiva; en otras palabra, hay mas secuencias de entrada que de salida debido a su limitación de generar una cadena de caracteres de largo fijo.

- *H()* es conocida como “función hash“ y cuyas propiedades deben ser*:
  - Fácil de calcular.
  - Irreversible: No se pueda determinar *m* a partir de *H(m)*.
  - Resistencia a colisiones: que sea difícil generar *m* y *m0* tal que *H(m) = H(m0)*.
  - Salida de apariencia aleatoria.

Funciones Hash

MD5

Es una función hash ampliamente utilizada descrita en el RFC 1321.

- Genera un resumen del mensaje de 128 bits en un proceso de 4 pasos.
- Funciones en Linux para el calculo automático: md5sum y md5pass.

SHA-1

Actualmente sustituye a MD5, debido a que este algoritmo esta roto.

- Genera un resumen del mensaje de 160 bits.
- Funciones en Linux para el calculo automático: sha1sum, sha1pass.

Existen otros como algoritmos más modernos y robustos como SHA-256, MAC, HMAC, etc.

1. Introducción
2. Principios Criptográficos
3. Cifrado Simétrico
4. Cifrado Asimétrico
5. Funciones Hash
6. Firma Digital

Firma Digital

Es una técnica criptográfica análoga a las firmas a mano.

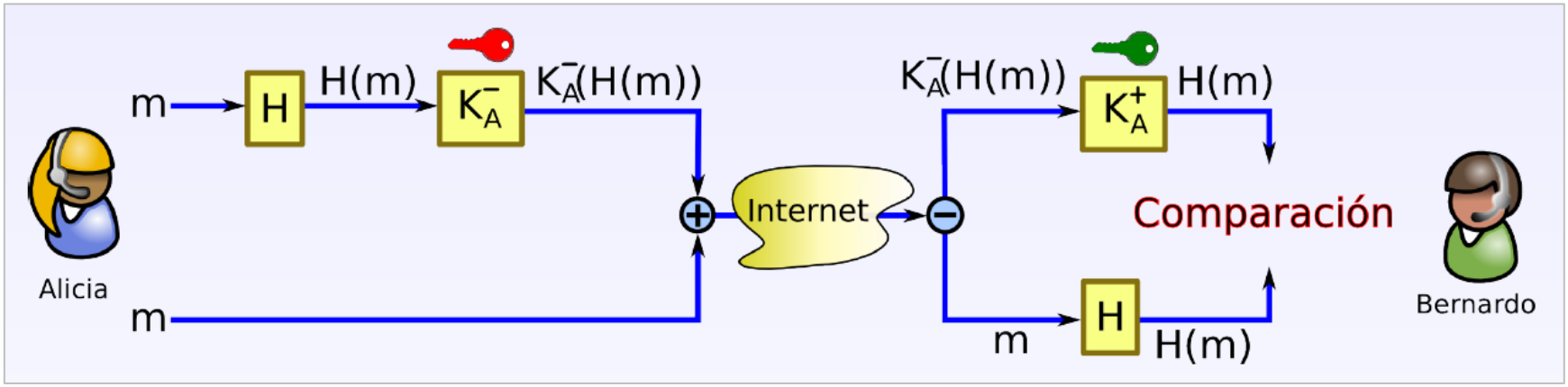
- El transmisor firma digitalmente un documento, estableciendo así que el es su dueño/creador. Para ello se hace uso de la clave privada.
- Es verificable y no repudiable: el receptor puede probar que el emisor es el correcto.

Una forma simple de firmar digitalmente es cifrar todo el mensaje con la clave privada, aunque es una solución computacionalmente cara.

Permite mantener la Integridad del mensaje, la Autenticidad de la fuente y la Confidencialidad de los datos.

Firma Digital

En la realidad únicamente se firma el resumen (hash) del mensaje, ya que es algo mucho más corto y computacionalmente más barato.



Se verifica que:

- El emisor firmo el mensaje (Clave privada)
- Solo el emisor pudo firmar el mensaje (Clave privada)
- El mensaje enviado no ha sido modificado (Hash)