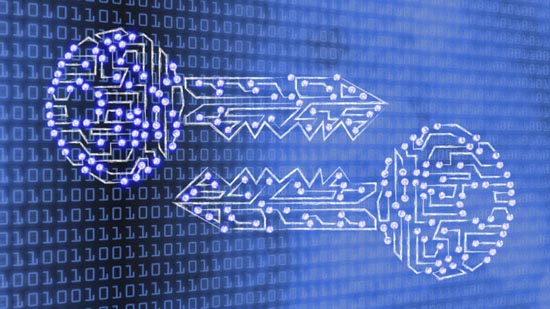
<https://tecnologia-informatica.com/que-es-la-criptografia/>

**¿Qué es la Criptografía?**

**Contenido**[[mostrar](https://tecnologia-informatica.com/que-es-la-criptografia/)]

Básicamente**, a criptografía es la técnica que protege documentos y datos.** Funciona a través de la utilización de cifras o códigos para **escribir algo secreto en documentos**y datos confidenciales que circulan en redes locales o en internet**.**Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, **la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos.** Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-1.jpg)

**Que es la Criptografía**

Criptografía es la **ciencia y arte de escribir mensajes en forma cifrada o en código.**Es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para:

* autentificar la identidad de usuarios
* autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias
* proteger la integridad de transferencias electrónicas de fondos

**Criptografía y Seguridad informática**

Un **mensaje codificado** por un método de criptografía debe ser privado, o sea, solamente aquel que envió y aquel que recibe debe tener acceso al contenido del mensaje. Además de eso, un mensaje debe poder ser suscrito, o sea, la persona que la recibió debe poder [verificar si el remitente es realmente la persona que dice ser](https://tecnologia-informatica.com/peligro-wifi-publico-precauciones-a-tomar/) y tener la capacidad de identificar si un mensaje puede haber sido modificado.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-2.jpg)

Los **métodos de criptografía** actuales son seguros y eficientes y basan su uso en una o más llaves. La llave es una secuencia de caracteres, que puede contener letras, dígitos y símbolos (como una contraseña), y que es convertida en un número, utilizada por los**métodos de criptografía para codificar y decodificar mensajes.**

**Criptografía: Claves Simétricas y Asimétricas**

Las claves criptográficas pueden ser básicamente de dos tipos:

**Simétricas:** Es la utilización de determinados **algoritmos para descifrar y encriptar** **(ocultar) documentos.**Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información.

**Asimétricas:** Es una fórmula matemática que utiliza dos llaves, una pública y la otra privada. **La llave pública es aquella a la que cualquier persona puede tener acceso,** mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-3.jpg)

Actualmente, los métodos criptográficos pueden ser subdivididos en dos grandes categorías, de acuerdo con el tipo de llave utilizado: **criptografía de llave única** y la **criptografía de llave pública y privada**.

**Tipos de claves criptográficas**

**Criptografía de llave única:** La criptografía de llave única utiliza la misma llave tanto para codificar como para decodificar mensajes. A pesar de que este método es bastante eficiente en relación al tiempo de procesamiento, o sea, el tiempo que gasta para **codificar y decodificar mensajes**, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptografiada.

**Criptografía de llaves pública y privada:** La criptografía de llaves pública y privada utiliza dos llaves distintas, una para codificar y otra para decodificar mensajes. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño**.** Los **mensajes codificados** con la llave pública solo pueden ser decodificados con la llave privada correspondiente.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-4.jpg)

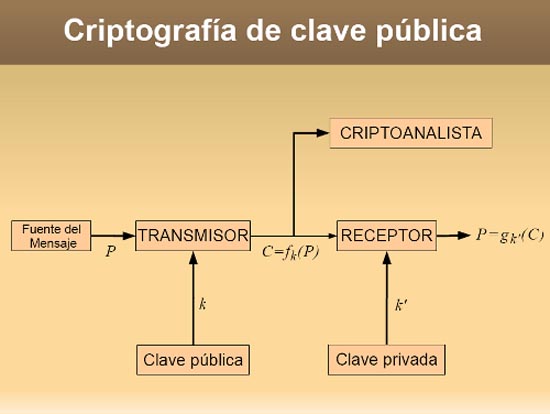
Como ejemplo, José y María quieren comunicarse de manera sigilosa. Entonces, ellos tendrán que realizar los siguientes procedimientos:

1. José codifica un mensaje utilizando la llave pública de María, que está disponible para el uso de cualquier persona.
2. Después de criptografiarlo, José envía el mensaje a María, a través de Internet.
3. María recibe y decodifica el mensaje, utilizando su llave privada, que es sólo de su conocimiento.
4. Si María quisiera responder el mensaje, deberá realizar el mismo procedimiento, pero utilizando la llave pública de José.

A pesar de que este método tiene un desempeño muy inferior en relación al tiempo de procesamiento, comparado al **método de criptografía de llave única,** presenta como principal ventaja la libre distribución de llaves públicas, no necesitando de un medio seguro para que llaves sean combinadas con antelación.

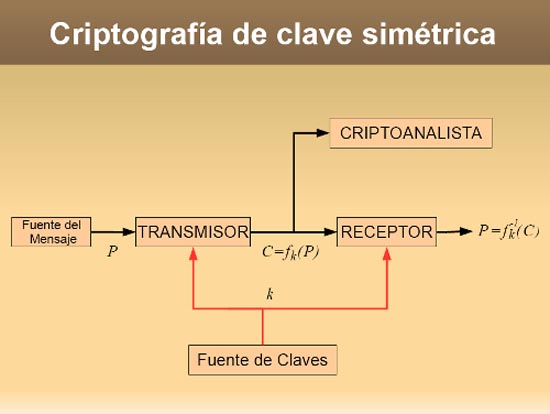
**¿Qué es firma digital?**

La firma digital consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda **verificar si el remitente es quien dice ser** e identificar cualquier mensaje que pueda haber sido modificado.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-5.jpg)

De esta forma, es utilizado el **método de criptografía de llaves pública y privada,**pero en un proceso inverso al presentado en el ejemplo anterior.

Si José quisiera enviar un mensaje suscrito a María, él codificará un mensaje con su llave privada. **En este proceso será generada una firma digital,** que será añadida al mensaje enviado a María. Al recibir el mensaje, María utilizará la llave pública de José para decodificar el mensaje. En este proceso será generada una segunda firma digital, que será comparada con la primera. Si las firmas fueran idénticas, María tendrá certeza de que el remitente del mensaje fue José y que el mensaje no fue modificado.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-6.jpg)

Es importante resaltar que la seguridad del método se basa en el hecho de que la llave privada es conocida sólo por su dueño. También es importante resaltar que [el hecho de firmar un mensaje no significara un mensaje sigiloso.](https://tecnologia-informatica.com/virus-ransomware/) Para el ejemplo anterior, si José quisiera firmar el mensaje y tener certeza de que sólo María tendrá acceso a su contenido, sería preciso codificarla con la llave pública de María, después de firmarla.

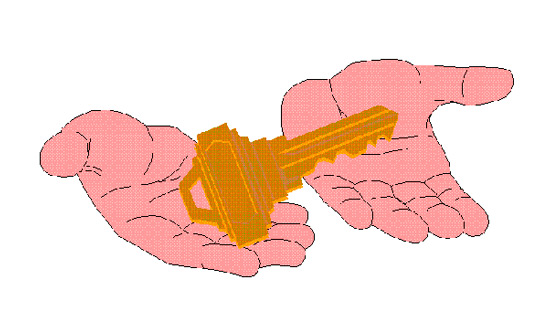
**Ejemplos de criptografía de llave única y de llaves pública y privada**

Ejemplos que combinan la **utilización de los métodos de criptografía de llave única y de llaves pública y privada**son las conexiones seguras, establecidas entre el browser de un usuario y una web, en transacciones comerciales o bancarias vía Web.

Estas conexiones seguras vía Web utilizan el método de criptografía de llave única, implementado por el protocolo **SSL (Secure Socket Layer).** El browser del usuario necesita informar a la web cual será la llave única utilizada en la conexión segura, antes de iniciar una transmisión de datos sigilosos.

Para esto, el browser obtiene la llave pública del certificado de la institución que mantiene la web. Entonces, utiliza esta **llave pública para codificar y enviar un mensaje a la web,** contiendo la llave única a ser utilizada en la conexión segura. La web utiliza su **llave privada para decodificar el mensaje**e identificar la llave única que será utilizada.

A partir de este punto, el browser del usuario y la web pueden transmitir informaciones, de forma sigilosa y segura, a través de la **utilización del método de criptografía de llave única.** La llave única puede ser cambiada a intervalos de tiempo determinados, a través de la repetición de procedimientos descritos anteriormente, aumentando así el nivel de seguridad de todo el proceso.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-7.jpg)

**¿Qué tamaño de llave criptográfica debe ser utilizado?**

Los **métodos de criptografía** actualmente utilizados, y que presentan buenos niveles de seguridad, son públicamente conocidos y son seguros por la robustez de sus algoritmos y por el tamaño de las llaves que utilizan.

Para que alguien descubra una llave necesita utilizar algún método de fuerza bruta, o sea, probar combinaciones de llaves hasta que la correcta sea descubierta. Por lo tanto,**cuanto mayor sea la llavecriptográfica, mayor será el número de combinaciones a probar,**inviabilizando así el descubrimiento de una llave en un tiempo normal. Además de eso, las llaves pueden ser cambiadas regularmente, haciendo los métodos de criptografía aún más seguros.

[](https://tecnologia-informatica.com/wp-content/uploads/2018/02/que-es-criptografia-8.jpg)

Actualmente, para obtenerse un buen nivel de seguridad en la utilización de un método de criptografía de llave única, **es aconsejable utilizar llaves de un mínimo de 128 bits.** Y para el método de criptografía de llaves pública y privada es aconsejable utilizar **llaves de 2048 bits,**siendo el mínimo aceptable de 1024 bits.

Dependiendo para los fines para los cuales los métodos criptográficos serán utilizados, se debe considerar la utilización de llaves mayores: **256 o 512 bits para llave única y 4096 o 8192 bits para llaves pública y privada.**