La **criptografía** se ha definido, tradicionalmente, como el ámbito de la [criptología](https://es.wikipedia.org/wiki/Criptolog%C3%ADa" \o "Criptología) que se ocupa de las técnicas de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) o [codificado](https://es.wikipedia.org/wiki/C%C3%B3digo_(criptograf%C3%ADa)) destinadas a alterar las [representaciones lingüísticas](https://es.wikipedia.org/wiki/C%C3%B3digo_(comunicaci%C3%B3n)) de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el [arte](https://es.wikipedia.org/wiki/Arte) como en la [ciencia](https://es.wikipedia.org/wiki/Ciencia) y en la [tecnología](https://es.wikipedia.org/wiki/Tecnolog%C3%ADa). Por tanto, el único objetivo de la criptografía era conseguir la [confidencialidad](https://es.wikipedia.org/wiki/Confidencialidad) de los mensajes, para lo cual se diseñaban [sistemas de cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) y [códigos](https://es.wikipedia.org/wiki/C%C3%B3digo_(criptograf%C3%ADa)), y la única criptografía existente era la llamada [criptografía clásica](https://es.wikipedia.org/wiki/Cifrado_cl%C3%A1sico).

La aparición de la [informática](https://es.wikipedia.org/wiki/Inform%C3%A1tica) y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas, y por tanto, la seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la [criptología](https://es.wikipedia.org/wiki/Criptolog%C3%ADa" \o "Criptología) que se encarga del estudio de los algoritmos, protocolos (se les llama [protocolos criptográficos](https://es.wikipedia.org/wiki/Protocolo_criptogr%C3%A1fico)), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

Para ello los criptógrafos investigan, desarrollan y aprovechan técnicas [matemáticas](https://es.wikipedia.org/wiki/Matem%C3%A1ticas) que les sirven como herramientas para conseguir sus objetivos. Los grandes avances producidos en el mundo de la criptografía, han sido posibles gracias a la evolución que se han producido en el campo de la [matemática](https://es.wikipedia.org/wiki/Matem%C3%A1tica) y la [informática](https://es.wikipedia.org/wiki/Inform%C3%A1tica).

Objetivos de la criptografía

La criptografía actualmente se encarga del estudio de los [algoritmos](https://es.wikipedia.org/wiki/Algoritmo), protocolos y sistemas que se utilizan para dotar de [seguridad](https://es.wikipedia.org/wiki/Seguridad) a las comunicaciones, a la información y a las entidades que se comunican.[1](https://es.wikipedia.org/wiki/Criptograf%C3%ADa#cite_note-1)​ El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto el tipo de propiedades de las que se ocupa la criptografía son, por ejemplo:[2](https://es.wikipedia.org/wiki/Criptograf%C3%ADa#cite_note-2)​

* [Confidencialidad](https://es.wikipedia.org/wiki/Confidencialidad). Es decir, garantiza que la información sea accesible únicamente a personal autorizado. Para conseguirlo utiliza [códigos](https://es.wikipedia.org/wiki/C%C3%B3digo_(criptograf%C3%ADa)) y técnicas de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)).
* [Integridad](https://es.wikipedia.org/wiki/Integridad_del_mensaje). Es decir garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo [funciones hash criptográficas MDC](https://es.wikipedia.org/wiki/C%C3%B3digo_de_detecci%C3%B3n_de_manipulaciones), [protocolos de compromiso de bit](https://es.wikipedia.org/wiki/Protocolos_de_compromiso), o [protocolos de notarización electrónica](https://es.wikipedia.org/w/index.php?title=Protocolos_de_notarizaci%C3%B3n_electr%C3%B3nica&action=edit&redlink=1).
* [Vinculación](https://es.wikipedia.org/wiki/Vinculaci%C3%B3n). Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado. Cuando se trata de una persona, se trata de asegurar su conformidad respecto a esta vinculación (content commitment) de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona. Antiguamente se utilizaba el término "No repudio" que está abandonándose, ya que implica conceptos jurídicos que la tecnología por sí sola no puede resolver. En relación con dicho término se entendía que se proporcionaba protección frente a que alguna de las entidades implicadas en la comunicación, para que no pudiera negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo [firma digital](https://es.wikipedia.org/wiki/Firma_digital). En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Por ejemplo cuando se usa un servicio de [mensajería instantánea](https://es.wikipedia.org/wiki/Mensajer%C3%ADa_instant%C3%A1nea) y no queremos que se pueda demostrar esa comunicación. Para ello se usan técnicas como el [cifrado negable](https://es.wikipedia.org/wiki/Cifrado_negable).
* [Autenticación](https://es.wikipedia.org/wiki/Autenticaci%C3%B3n). Es decir proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo [función hash criptográfica MAC](https://es.wikipedia.org/wiki/Message_Authentication_Code) o [protocolo de conocimiento cero](https://es.wikipedia.org/wiki/Prueba_de_conocimiento_cero).
* Soluciones a problemas de la falta de simultaneidad en la telefirma digital de contratos. Para conseguirlo puede usar por ejemplo [protocolos de transferencia inconsciente](https://es.wikipedia.org/w/index.php?title=Transferencia_trascordada&action=edit&redlink=1).

Un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.

Los espartanos utilizaron, hacia el 400 a.C., la **Escitala**, que puede considerarse el primer sistema de criptografía por **transposición**, es decir, que se caracteriza por ocultar el significado real de un texto alterando el orden de los signos que lo conforman. Los militares de la ciudad-estado griega escribían sus mensajes sobre una tela que envolvía una vara. El mensaje sólo podía leerse cuando se enrollaba la tela sobre un bastón del mismo grosor, que poseía el destinatario lícito del mensaje (¿el origen del "bastón de mando"?).

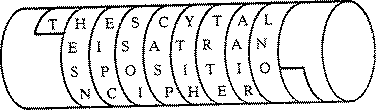


Fig. A- Representación del método de la escitala

El método de la escitala era extremadamente sencillo, como también lo era el que utilizó Julio César, basado en la sustitución de cada letra por la situada tres puestos después en el alfabeto latino. A este cifrado por **sustitución** sencilla se le conoce como **cifrado César**.

#### Los cifrados polialfabéticos

La criptografía resurgió en la Europa de la Edad Media y el Renacimiento, impulsada por las intrigas del papado y las ciudades-estado italianas. Fue un servidor del Papa Clemente VII, *Grabiele de Lavinde*, quien escribió el primer manual sobre la materia en el viejo continente. En 1466, *León Battista Alberti*, músico, pintor, escritor y arquitecto, concibió el sistema de **sustitución polialfabética** que emplea varios abecedarios, saltando de uno a otro cada tres o cuatro palabras. El emisor y el destinatario han de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinará la correspondencia de los signos.

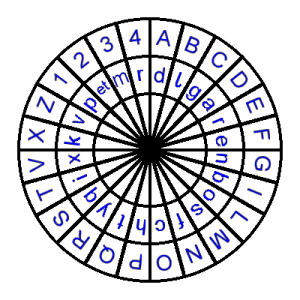


Fig. B- Discos de Alberti

Un siglo después, *Giovan Battista Belaso de Brescia* instituyó una nueva técnica. La clave, formada por una palabra o una frase, debe transcribirse letra a letra sobre el texto original. Cada letra del texto se cambia por la correspondiente en el alfabeto que comienza en la letra clave. Este cifrado ha llegado hasta nuestros días como *"****Cifrado Vigenère****"*, ya que su invención fue atribuida incorrectamente al diplomático francés Blaise de Vigenère, contemporáneo de Belaso y autor de famosos tratados sobre criptografía en el S. XVI.

Pero los métodos clásicos mono y polialfabéticos distan mucho de ser completamente seguros. En algunos casos, basta hacer un simple cálculo estadístico para desentrañar los mensajes ocultos. Si se confronta la frecuencia habitual de las letras en el lenguaje común con la de los signos del criptograma, puede resultar relativamente sencillo descifrarlo. Factores como la longitud del texto, el uso o no de más de una clave o la extensión de esta juegan un papel muy importante, así como la intuición, un arma esencial para todo criptoanalista (rompedor de cifrados). En el siglo XIX *Friederich Kasiski*, un militar prusiano, publicó un ataque basado en métodos estadísticos que rompía los cifrados por sustitución polialfabética.

#### El siglo XX y la II Guerra Mundial

El siglo XX ha revolucionado la criptografía. Retomando el concepto de las ruedas concéntricas de Alberti, a principios del siglo se diseñaron teletipos equipados con una secuencia de **rotores** móviles. éstos giraban con cada tecla que se pulsaba. De esta forma, en lugar de la letra elegida, aparecía un signo escogido por la máquina según diferentes reglas en un código polialfabético complejo. Estos aparatos, se llamaron traductores mecánicos. Una de sus predecesoras fue la Rueda de Jefferson, el aparato mecánico criptográfico más antiguo que se conserva.

La primera patente data de 1919, y es obra del holandés *Alexander Koch*, que comparte honores con el alemán *Arthur Scherbius*, el inventor de **Enigma** una máquina criptográfica a rotor que los nazis creyeron inviolable, sin saber que aceleraría su derrota. En efecto, en el desenlace de la contienda, hubo un factor decisivo y apenas conocido: los aliados eran capaces de descifrar todos los mensajes secretos alemanes.



Fig. C- Una máquina Enigma original de la S.G.M.

Una organización secreta británica, en la que participó *Alan Turing*, uno de los padres de la informática y de la inteligencia artificial, había logrado desenmascarar las claves de **Enigma** y de su "hermana mayor" **Lorenz**, desarrollando más de una docena de artilugios -llamados las bombas- que desvelaban los mensajes cifrados. La máquina alemana se convertía así en el talón de Aquiles nazi, un topo en el que confiaban y que en definitiva, trabajaba para el enemigo. Paralelamente, Los códigos de la versión japonesa de Enigma (llamados Purple, violeta) se descifraron por un grupo de analistas, dirigidos por el comandante Joseph J. Rochefort. Su criptoanálisis fue vital para la victoria americana en la batalla de Midway.

La existencia de Enigma y el hecho de que los aliados conociesen sus secretos fueron, durante mucho tiempo, dos de los secretos mejor guardados de la II Guerra Mundial. ¿La razón? Querían seguir sacándole partido tras la guerra potenciando su uso en diversos países, que, al instalarla, hacían transparentes sus secretos para las potencias anglosajonas.

#### La criptografía en la era de la informática

Finalizada la contienda, las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas. Se dieron así los primeros pasos hacia los sistemas criptográficos más modernos, mucho más fiables que la sustitución y transposición clásicas. Hoy por hoy, se utilizan métodos que combinan los dígitos del mensaje con otros, o bien algoritmos de gran complejidad como el **DES** (inventado por IBM) y sus posteriores sucesores.

Una de las aportaciones del último cuarto del s. XX son los sistemas de cifrado **asimétrico** o de **clave pública** (como **RSA**), en contraposición con todos los anteriores, que son criptosistemas **simétricos** o de **clave privada**, que usaban la misma clave para el cifrado y el descifrado del mensaje. La ventaja de estos sistemas es que permiten solucionar uno de los problemas de la criptografía clásica, la distribución de las claves secretas a los participantes en la comunicación. En la criptografía de clave pública, una de las claves puede hacerse pública sin que por ello la seguridad de la clave secreta se vea afectada. Lo cifrado con la clave secreta puede descifrarse con la pública y viceversa. Esta propiedad de los criptosistemas asimétricos permite también otras aplicaciones de estos criptosistemas, como la **firma digital** que es tan importante en las redes de telecomunicaciones hoy.

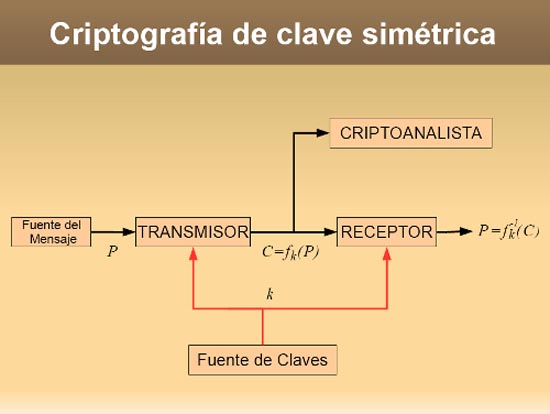
Existen dos trabajos fundamentales sobre los que se apoya prácticamente toda la teoría criptográfica actual. Uno de ellos, desarrollado por *Claude Shannon* en sus artículos "A Mathematical Theory of Communication" (1948) y "Communication Theory of Secrecy Systems" (1949), sienta las bases de la Teoría de la Información y de la Criptografía moderna. El segundo, publicado por *Whitfield Diffie* y *Martin Hellman* en 1976, se titulaba "New directions in Cryptography", e introducía el concepto de Criptografía de Clave Pública, abriendo enormemente el abanico de aplicación de esta viejísima disciplina.

Con la publicación del algoritmo **RSA** en 1977 por parte de los matemáticos *Ron Rivest*,*Adi Shamir* y *Len Adleman* la criptografía "moderna" o de clave pública alcanza su consolidación.

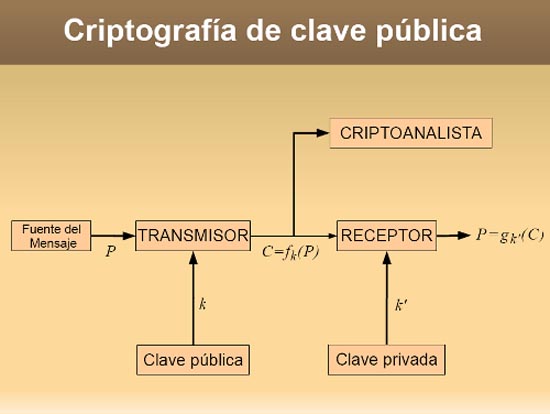
### Tipos de criptosistemas

Existen dos tipos fundamentales de criptosistemas o sistemas de cifrado:

* **Criptosistemas simétricos o de clave privada**. Son aquellos que emplean una misma clave **k** tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitirles a los participantes en la comunicación esa clave de forma segura.



* **Criptosistemas asimétricos o de clave pública**, que emplean una doble clave (**kp,kP**). **kp** se la conoce como clave privada y **kP** se la conoce como clave pública. Una de ellas sirve para la transformación o función **E** de cifrado y la otra para la transformación **D** de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.



## HASH

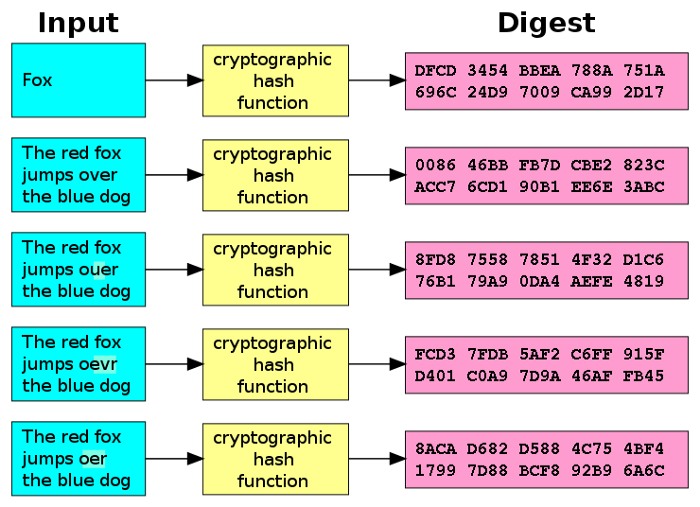
Por último, para poder entender un poco mejor todo los elementos criptográficos que se utilizan en la tecnología blockchain, hablaremos del hash.

Un hash es un elemento que se obtiene mediante una función hash. A estas funciones también se las conoce como “digestivas”, porque transforman la información a un elemento de tamaño fijo y con unas ciertas características, como si se tratase un “digerido” de la información.

Para entender un poco mejor los hashes, pensemos en el ADN. El ADN es un conjunto de elementos (casi siempre con el mismo número de elementos en todos los seres humanos) que todos tenemos, pero que con pequeñas variaciones es capaz de crear de forma única a todos y cada uno de nosotros. El hash de cualquier archivo es un conjunto de caracteres que se forma de manera única para ese archivo. De esta modo, si se hace el hash de dos archivos distintos, se obtendrán dos hashes distintos (de la misma longitud).

Este mecanismo es muy potente, pues nos permite, siempre y cuando utilicemos la misma “receta” (algoritmo) para crear el hash de un elemento, obtener un identificador único para dicho elemento. Esto nos permite también saber si un elemento ha sido modificado, es decir, si el elemento cambia, no puede mantener el mismo ADN.

Esto es muy potente y es uno de los elementos claves utilizados en la tecnología blockchain, permitiendo crear un ADN único para toda la información, asegurando así su inmutabilidad.



Videos varios

<https://es.khanacademy.org/computing/computer-science/cryptography>