2 Criptografía

A **criptoloxía** é a práctica e o estudo da ocultación de información. É a ciencia de cifrar e descifrar información mediante técnicas especiais, empregándose para facer inintelixibles mensaxes para receptores non autorizados. Búscase facer un intercambio de mensaxes que só poidan ser lidos por persoas ás que van dirixidos e que posúen os medios para descifralos.

A criptoloxía pode dividirse en dúas ramas:

- Criptografía: centrada nas técnicas para cifrar a información.
- Criptoanálise: centradas nas técnicas e mecanismos para decodificar a información, rompendo os procedementos de cifrado e recuperar a mensaxe orixinal.

Poden atoparse exemplos de uso de técnicas criptográficas na antigüidade, como a 'escítala' empregada polos espartanos. Sen embargo, a criptografía utilizada na actualidade data dos anos 70. Estas técnicas aplícanse cada día no mundo da tecnoloxía en multitude de usos como as comunicacións militares, protocolo https, protocolo ssh, envío de correos electrónicos cifrados ou as telecomunicacións en xeral.

Fig. Escítala. Fonte: Wikipedia. Licenza CC BY-SA 3.0

A información orixinal que debe protexerse denomínase texto plano (texto en claro) e o cifrado é o proceso de converter o texto plano nun texto imposible de ler chamado texto cifrado ou criptograma. Para obter un texto cifrado, aplícase ó texto plano un algoritmo de cifrado utilizando unha clave:

Fig. Cifrado dun texto

Para recuperar a mensaxe orixinal, collerase o criptograma (texto cifrado), a clave e aplicarase o algoritmo de descifrado:

Fig. Descifrado dun criptograma

Os principais obxectivos que busca a criptografía son:

- **Confidencialidade**: a información revélase unicamente ós usuarios autorizados. Por exemplo, ó usar https ó acceder a un sistema de webmail, os datos de usuario/contrasinal irán cifrados por un tunel de comunicacións establecido entre o navegador do usuario e o servidor. Conséguese que o navegador e o servidor poidan intercambiar información pero que esa información non sexa lexible para os demais (se un sniffer capturase os paquetes da comunicación veríanse os datos cifrados).
- **Integridade**: garantiza a exactitude da información contra a alteración, perda ou destrucción da información. Por exemplo, cando se firma electrónicamente un documento, apórtase un 'resumo' que garantiza que se o documento orixinal fose modificado, poderíase detectar a manipulación ó non coincidir o resumo do documento orixinal co resumo do documento modificado.
- **Autenticación**: comprobación da identidade. Por exemplo, ó usar ssh para conectarse a un equipo remoto, o cliente comproba a identidade dixital do servidor ssh para asegurarse que se está conectando ó servidor de verdade e non cun impostor.
- **Non repudio** (**irrenunciabilidade ou vinculación**): vincula un documento ou transacción a unha persoa ou equipo. Por exemplo, na firma electrónica de documentos garántese o non repudio no emisor; é dicir, empréganse mecanismos que garanten que un documento firmado electrónicamente por unha persoa usando a súa identidade dixital está asociado a esa persoa, non sendo posible que fose asinado por outra.

Dependendo do número de claves utilizadas polos algoritmos de cifrado/descifrado, existen dous tipos de métodos criptográficos:

- **Criptografía de clave simétrica**, que utiliza unha única clave para cifrar/descifrar.
- **Criptografía de clave asimétrica**, que utiliza dúas claves.

Como se verá máis adiante, existen sistema chamados de **criptografía híbrida**, que empregan os dous sistemas (simétrico e asimétrico) procurando escoller o mellor de cada un (seguridade e rendemento).

2.1 Criptografía de clave simétrica

Úsase **unha única clave para cifrar e descifrar** mensaxes. Unha vez que as dúas partes que se van a comunicar posúen a mesma clave, o remitente cifra unha mensaxe con ela, envíaa ó destinatario e este a descífra coa mesma.

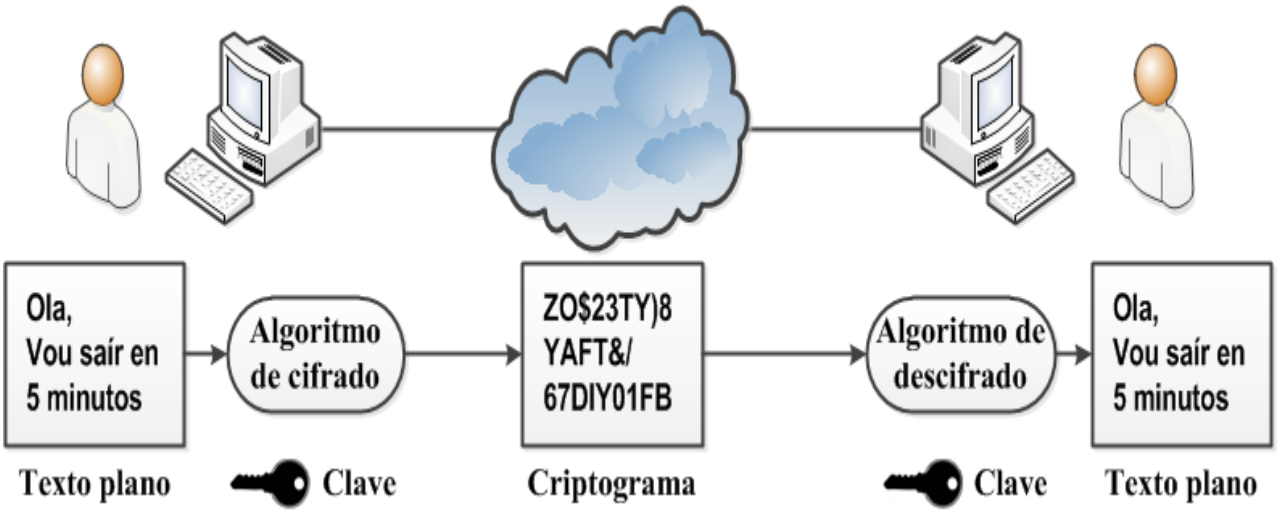

Fig. Cifrado de información mediante criptografía de clave simétrica

Un problema que teñen os sistemas de clave simétrica é o intercambio de claves; xa que, antes de poder enviar información, os participantes teñen que intercambiarse a clave. Se a clave cae en malas mans toda comunicación que use esa clave comprometida non será segura; por que, persoas non autorizadas poderán acceder ós contidos transmitidos. Se se atopa un sistema seguro para intercambiar a clave, este sistema é o máis eficiente.

Un bo sistema de cifrado centra toda a seguridade na clave e non no algoritmo; é dicir, non debería ser de ningunha axuda para un atacante coñecer o algoritmo que se está usando. Só se o atacante obtivese a clave, serviríalle coñecer o algoritmo. Dado que toda a seguridade está na clave, é importante que sexa moi difícil adiviñar o tipo de clave. Isto quere dicir que o abanico de claves posibles (espazo de posibilidades de claves) debe ser amplo. Na seguinte táboa pode compararse a lonxitude de clave e o número de claves posibles:

Tamaño (lonxitude da clave)	Número de claves posible
8	$2^8 = 256$
40	$2^{40} = 1.099.511.627.776$
56	$2^{56} = 72.057.594.037.927.900$
64	$2^{64} = 18.446.744.073.709.600.000$
128	$2^{128} =$ 340.282.366.920.938.000.000.000.000.000.000.000.000
256	$2^{56} = 1,16E+077$

512	2^{512} = 1,34E+154

Os computadores modernos poden descifrar claves con extrema rapidez, e esta é a razón pola cal o tamaño da clave é importante nos criptosistemas modernos. O algoritmo de cifrado DES usa unha clave de 56 bits, o que significa que hai 2^{56} claves posibles. Aínda que pode parecer un número moi grande de posibles claves, un computador xenérico pode comprobar o conxunto posible de claves en cuestión de días e un equipo especializado en horas.

Algoritmos de cifrado de deseño máis recente como AES, 3DES, Blowfish e IDEA usan claves de maior lonxitude, o que dificulta enormemente os ataques ó prolongalos no tempo. A modo de exemplo, o algoritmo AES (Advanced Encryption Standard) permite o uso de claves de 128, 192 e 256 bits. AES é un estándar de cifrado no Goberno dos Estados Unidos de América e para os documentos clasificados como TOP SECRET é obrigatorio o uso de claves de 192 ou 256 bits.

2.2 Criptografía asimétrica

Os sistemas criptográficos de clave simétrica teñen o problema da distribución da clave entre os participantes da comunicación. Nos sistemas de clave asimétrica non existe este problema e cada participante ten un parella de claves propias:

- **Clave privada**:
  - O seu propietario debe mantela en segredo a toda costa.
  - Permite cifrar mensaxes (que poderán ser descifrados coa clave pública).
  - Permite descifrar mensaxes cifrados coa clave pública do propietario.
- **Clave pública**:
  - Debe repartirse a todos os usuarios cos que se queira comunicar.
  - Úsase para enviar mensaxes cifradas ó propietario, que só el poderá descifrar usando a súa clave privada.
  - Úsase para descifrar mensaxes enviadas polo propietario e cifrados coa clave privada.

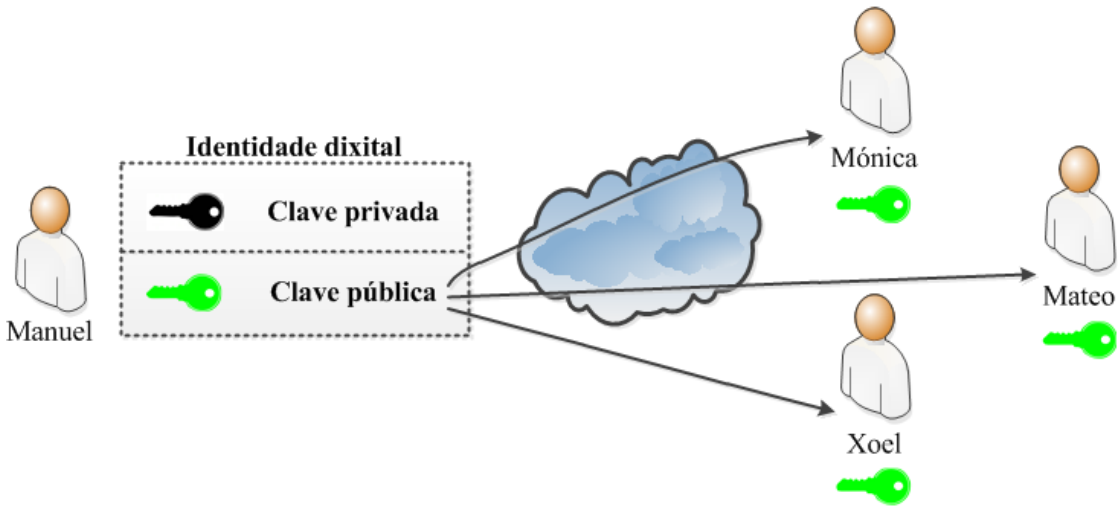

Fig. Reparto da clave pública na criptografía de clave asimétrica

Na seguinte imaxe pode verse o que sucede se Mónica envía unha mensaxe a Manuel cifrándoa coa clave pública de Manuel. O que consegue é que únicamente Manuel póidaa descifrar usando a súa clave privada (a de Manuel). Ninguén, agás o que teña a clave privada de Manuel poderá descifrar a mensaxe; polo tanto, conseguiuse a confidencialidade.

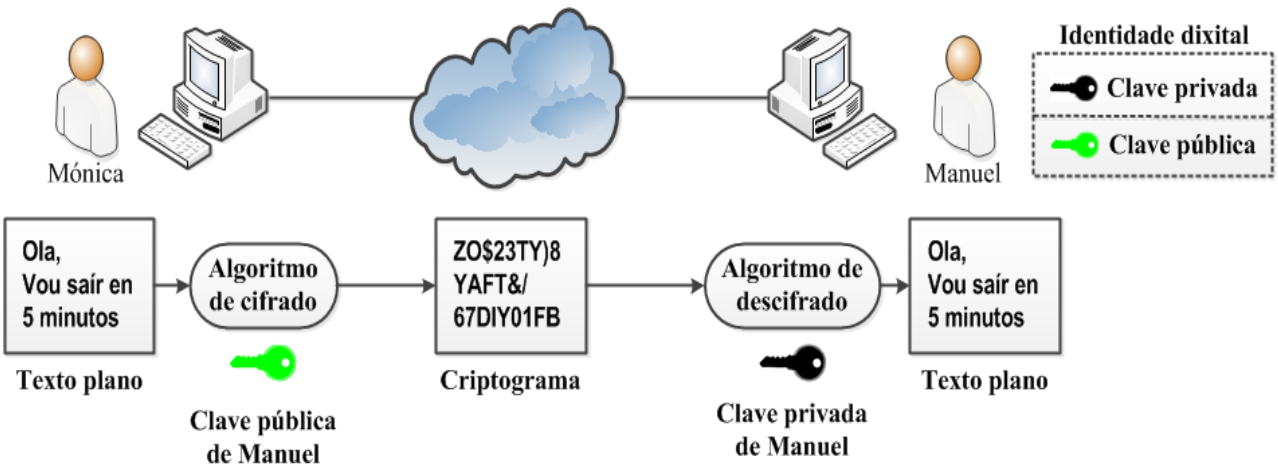

Fig. Confidencialidade da información mediante criptografía de clave asimétrica

Agora Manuel envía unha mensaxe cifrada coa súa clave privada a Mónica. Mónica, usando a clave pública de Manuel, será capaz de descifrar a mensaxe e terá a seguridade de que a mensaxe foi enviada por Manuel; xa que, ninguén agás Manuel posúe a clave privada (de Manuel). Conséguese a identificación e a vinculación (non repudio) do remitente.

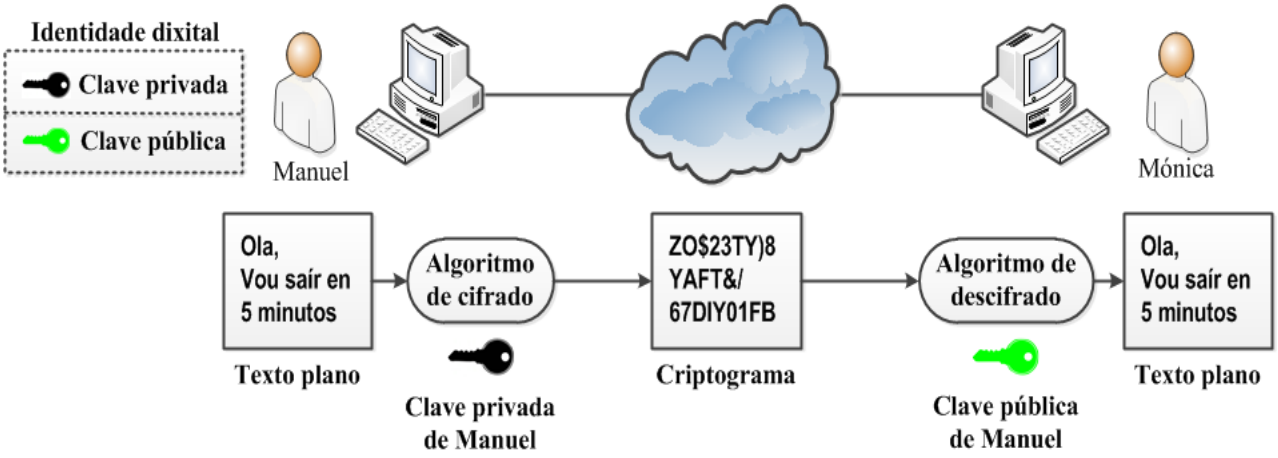

Fig. Identificación e vinculación do remitente mediante criptografía de clave asimétrica

Unha vez entendidas as posibilidades que ofrece o uso das claves privadas e públicas de Manuel, plantéxase a situación onde Manuel e Mónica queren comunicarse buscando á vez confidencialidade, identificación e vinculación. Para acadalo:

- Manuel ten a súa clave privada que non comparte con ninguén.
- Manuel envía a súa clave pública a Mónica.
- Mónica ten a súa clave privada que non comparte con ninguén.
- Mónica envía a súa clave pública a Manuel.
- Mensaxes de Manuel a Mónica:
  - Manuel cifra a mensaxe coa súa clave privada e despois a cifra coa clave pública de Mónica.
  - A mensaxe dobremente cifrada envíase a Mónica.
  - Unha vez que lle chega a mensaxe a Mónica, ésta descifra a mensaxe coa súa clave privada e o resultado procede a descifralo coa clave pública de Manuel. Unha vez aplicado este procedemento, Mónica recupera a mensaxe orixinal de Manuel.
- Mensaxes de Mónica a Manuel:
  - Mónica cifra a mensaxe coa súa clave privada e despois a cifra coa clave pública de Manuel.
  - A mensaxe dobremente cifrada envíase a Manuel.
  - Unha vez que lle chega a mensaxe a Manuel, éste descifra a mensaxe coa súa clave privada e o resultado procede a descifralo coa clave pública de Mónica. Unha vez aplicado este procedemento, Manuel recupera a mensaxe orixinal de Mónica.

O que se consegue con este sistema é:

- Ó cifrar en primeiro lugar coa clave privada do remitente, o destinatario poderá estar seguro que a mensaxe realmente procede do remitente; e polo tanto, garántese a identificación e vinculación do remitente.

- Ó cifrar en segundo lugar coa clave pública do destinatario, asegúrase que únicamente o destinatario pode ver o contido da mensaxe (grazas a que a única clave que pode descifrar a mensaxe é a privada do destinatario); e polo tanto, garántese a confidencialidade do envío.

Na seguinte imaxe pode verse o proceso a seguir no envío de mensaxes de Manuel a Mónica:

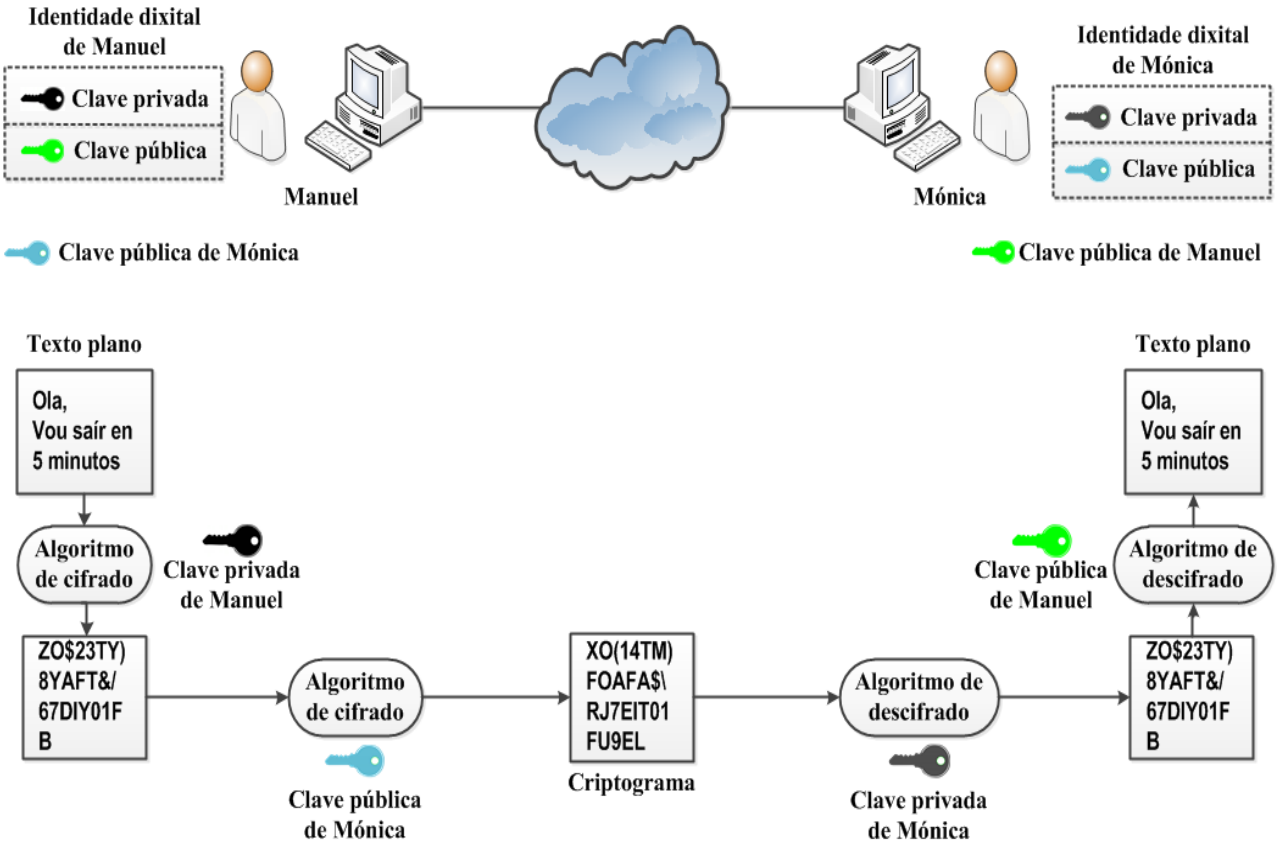

Fig. Confidencialidade da información, identificación e vinculación do remitente mediante criptografía de clave asimétrica

Os métodos criptográficos garanten:

- Que esa parella de claves só se poida xerar unha vez, de modo que se pode asumir que non é posible que dúas persoas obtivesen casualmente a mesma parella de claves.
- Que a partir da clave pública non se pode deducir nada da clave privada.
- Que o que cifra a clave pública só pode ser descifrado coa privada e o que cifra a clave privada só o descifra a pública.

Agora o intercambio de claves xa non é problema xa que a pública está pensada para repartirse. O que si é crítico é manter a clave privada a bo recaudo. Exemplos de métodos de cifrado asimétricos son Diffie-Hellman, RSA, DSA e ElGamal.

2.3 Criptografía híbrida

Debido a que os sistemas de cifrado asimétricos son computacionalmente máis custosos que os simétricos e que estes últimos teñen o problema de intercambio de claves, inventáronse os sistemas de criptografía híbrida. Nestes sistemas híbridos, ó comezo da comunicación úsase un sistema de claves asimétricas para intercambiar de forma segura unha clave simétrica de sesión, que se usará para cifrar o resto da comunicación de forma máis eficiente. Un exemplo de implementación práctica deste tipo de sistema pode atoparse nos protocolos SSH e https.

Na seguinte figura pode verse un resumo do proceso:

- Paso 1: Manuel envía a clave pública a Mónica.
- Paso 2: Mónica xera unha clave de sesión que é cifrada usando a clave pública de Manuel e a envía a Manuel. Este procede a descifrala usando a súa clave privada.
- Paso 3: unha vez que os dous participantes da comunicación xa coñecen a clave de sesión, poden proceder a enviar mensaxes cifradas e descifralas usando a mesma clave (criptografía simétrica).

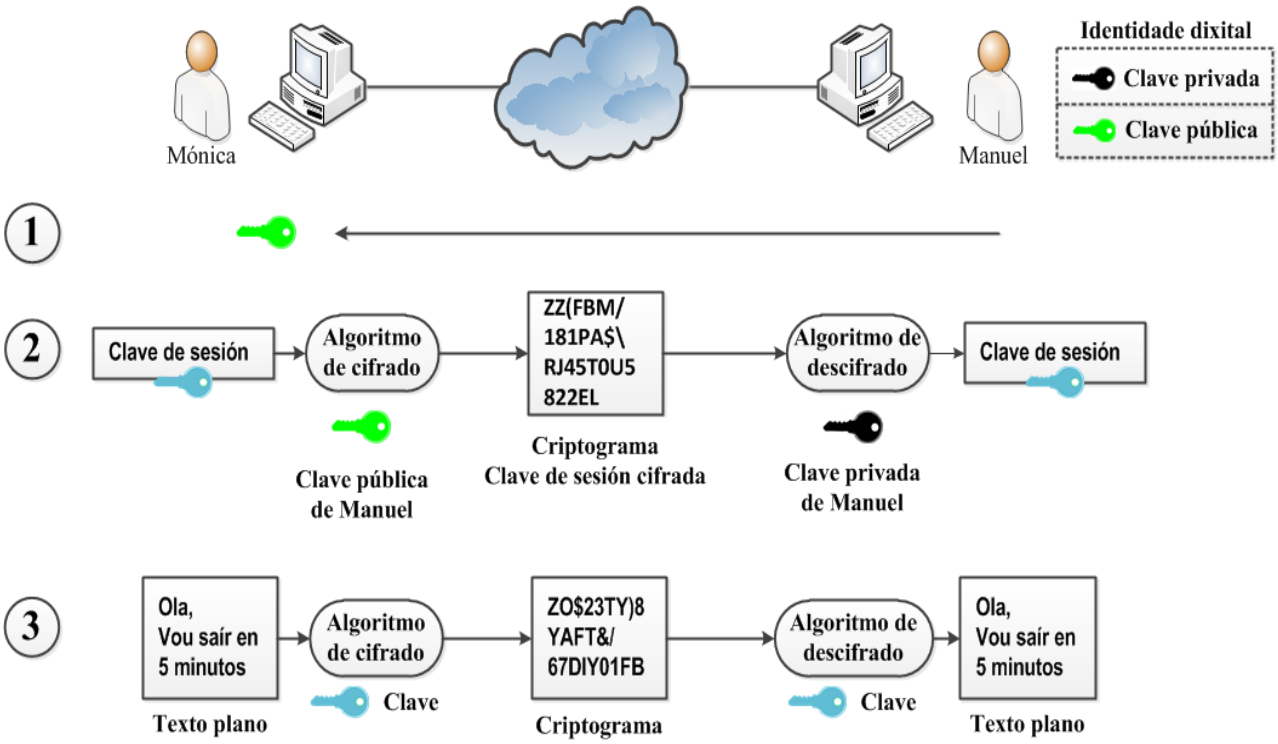

Fig. Funcionamento dun sistema de criptografía híbrida