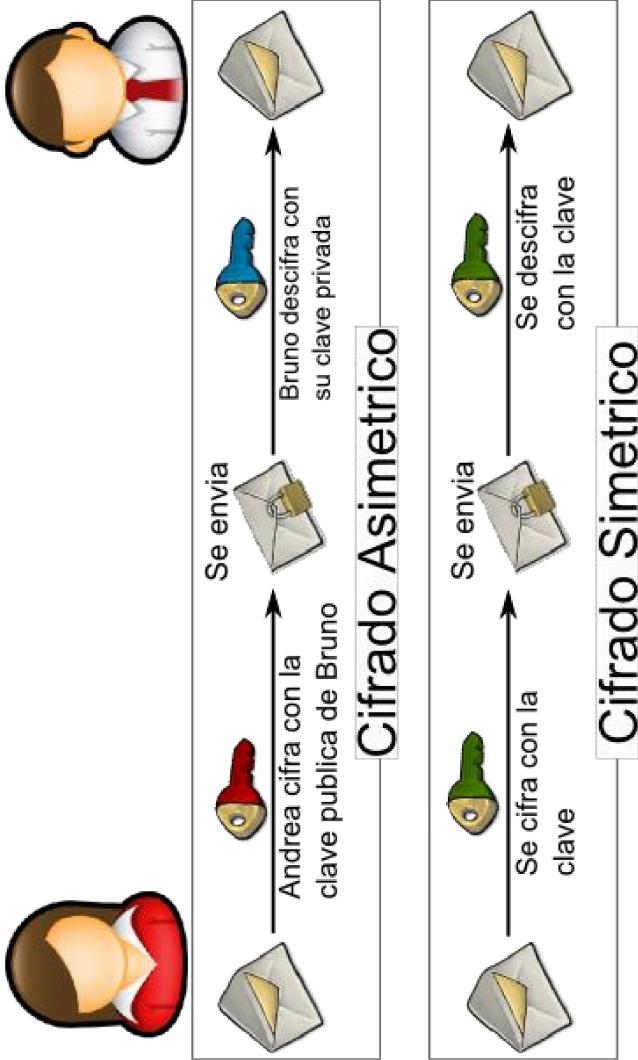


3. CIFRADO DE CLAVE ASIMÉTRICA

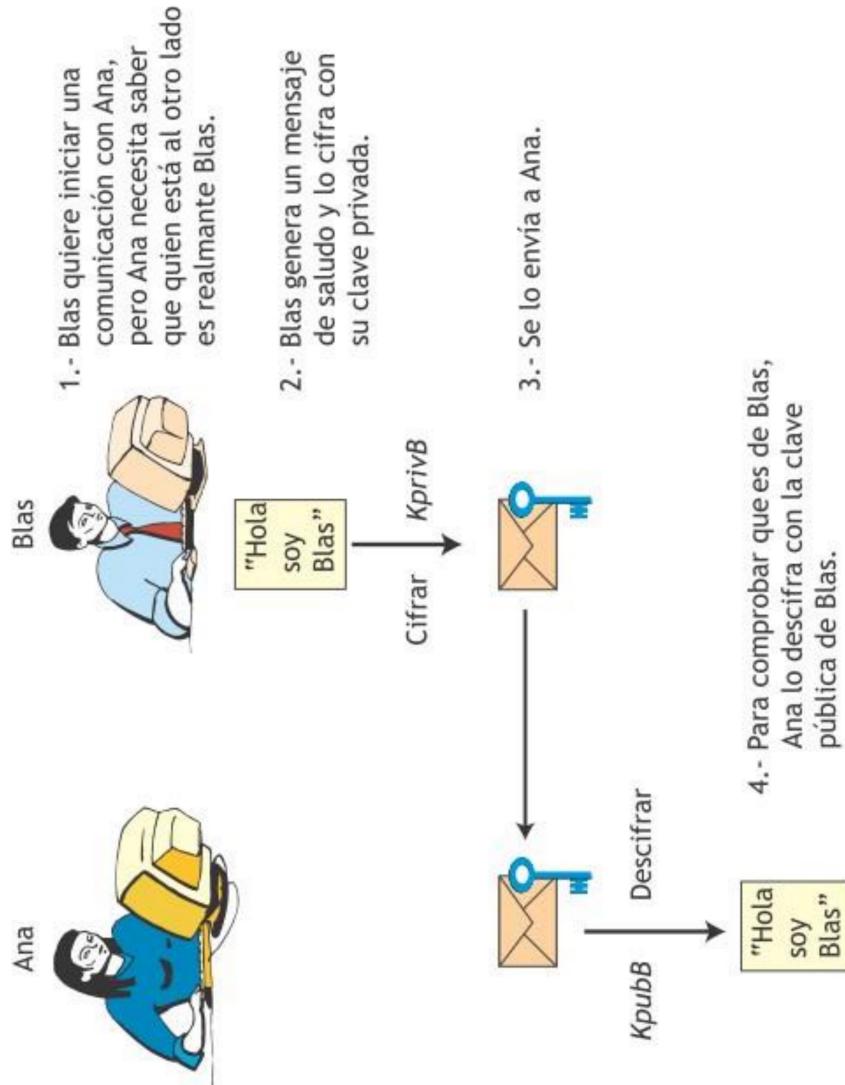
Estos sistemas utilizan un par de claves: **una privada** (que solo conoce su propietario) y otra pública. La criptografía asimétrica tiene dos usos principales: **Autenticación** y **Confidencialidad**.



3. CIFRADO DE CLAVE ASIMÉTRICA

Autenticación con claves asimétricas

Para garantizar que el remitente de un mensaje es quien dice ser, este cifra el mensaje con su clave privada. Todo equipo que posea la clave pública de ese remitente podrá descifrar el mensaje y comprobar que procede de esa persona porque solo él, que es quien posee la clave privada, ha podido generar el mensaje. Un ejemplo de este uso es el intercambio de claves SSH entre servidores.



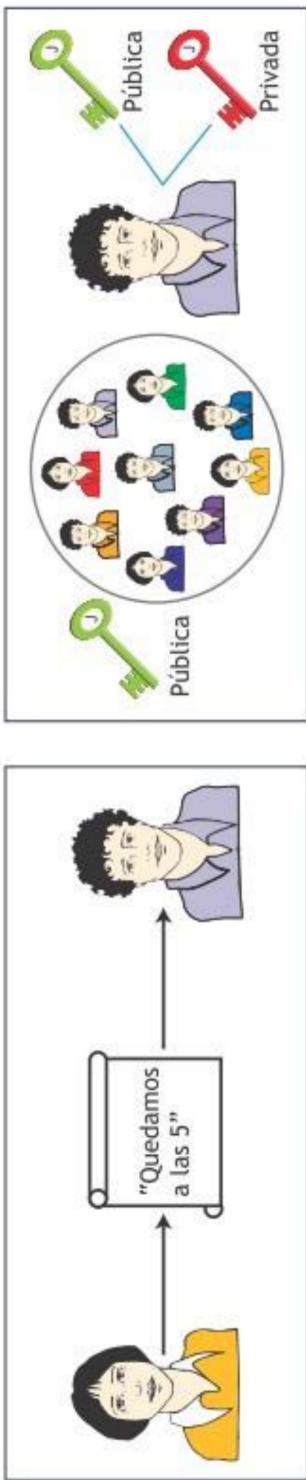
3. CIFRADO DE CLAVE ASIMÉTRICA

Confidencialidad con claves asimétricas

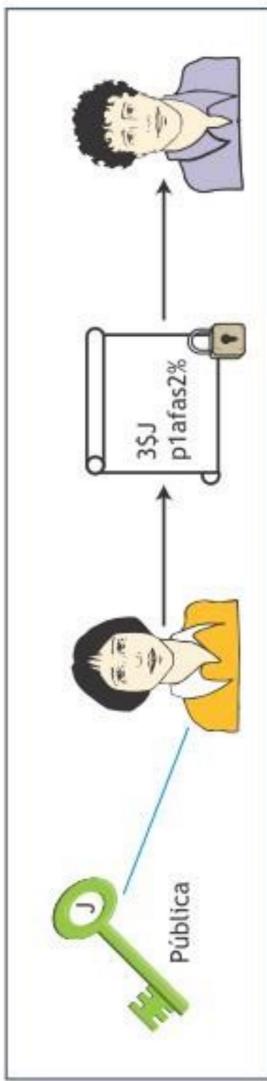
Los sistemas de cifrado con claves asimétricas sirven para garantizar la confidencialidad del mensaje, al igual que la criptografía simétrica. Cuando alguien quiera cifrar un mensaje dirigido a mí, utilizará mi clave pública (que es conocida) para cifrarlo, pero únicamente yo lo podré leer, ya que soy el único que posee la clave privada. Funcionaría de forma similar a un candado, cualquiera puede cerrarlo, pero solo quien tenga la llave de ese candado puede abrirla.

3. CIFRADO DE CLAVE ASIMÉTRICA

Ana quiere enviar un mensaje secreto a Juan cifrándolo mediante una clave asimétrica. Juan dispone de una pareja de claves pública y privada y ha distribuido su clave pública de forma que cualquiera que quiera enviarle un mensaje pueda usarlo para cifrarlo.



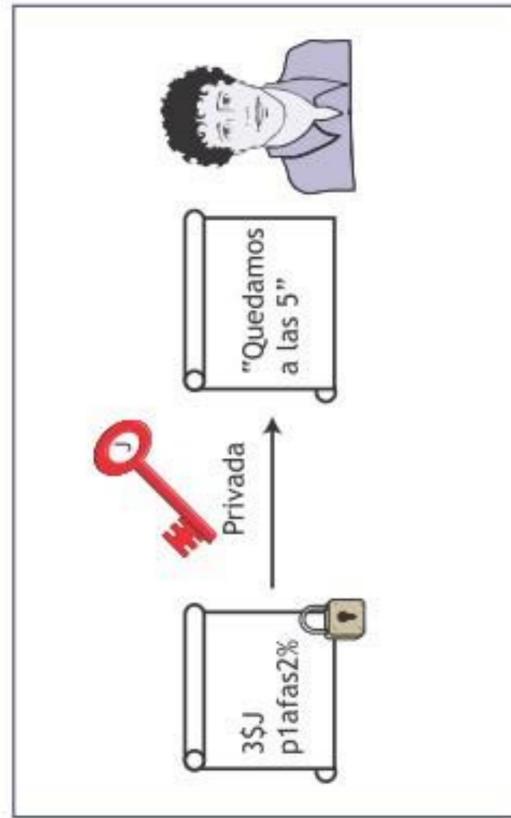
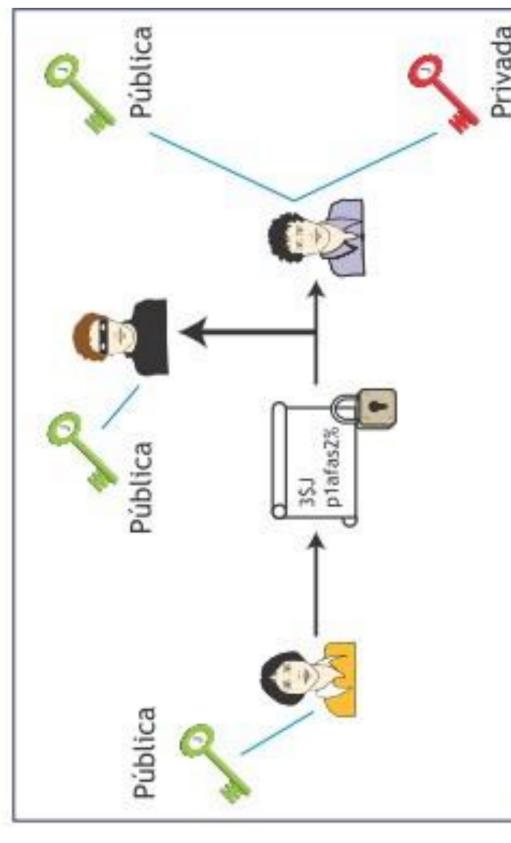
Como la clave pública de Juan es conocida, Ana la utilizará para cifrar el mensaje.



3. CIFRADO DE CLAVE ASIMÉTRICA

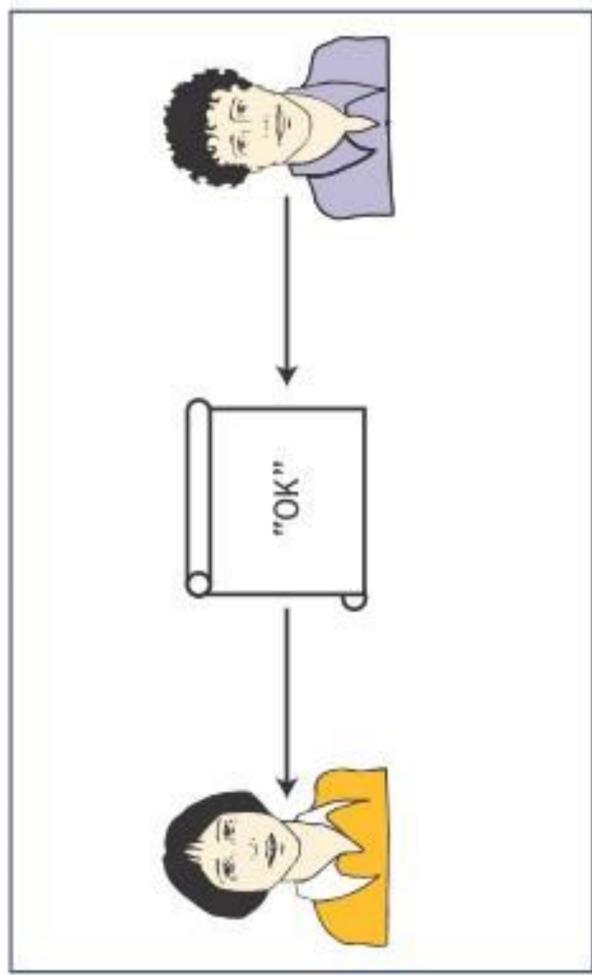
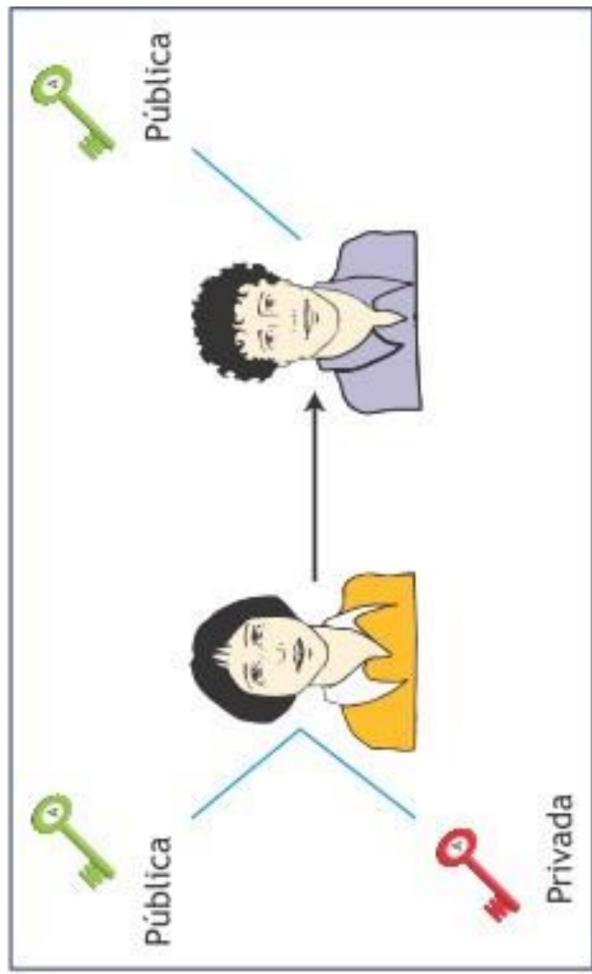
Una vez cifrado el mensaje con la clave pública, solo Juan podrá leerlo, porque él es la única persona que tiene su clave privada. Al estar cifrado con la clave pública, la privacidad del mensaje para Juan está garantizada, puesto que solo quien conozca la clave privada podrá descifrar el mensaje.

Por esto no hay ningún inconveniente para que la clave pública de Juan sea públicamente conocida, pues por sí misma no será suficiente para descifrar el mensaje. Lo realmente importante es que la clave privada esté a buen recaudo, pues si un intruso la averiguara, sí que podría acceder al contenido del mensaje.



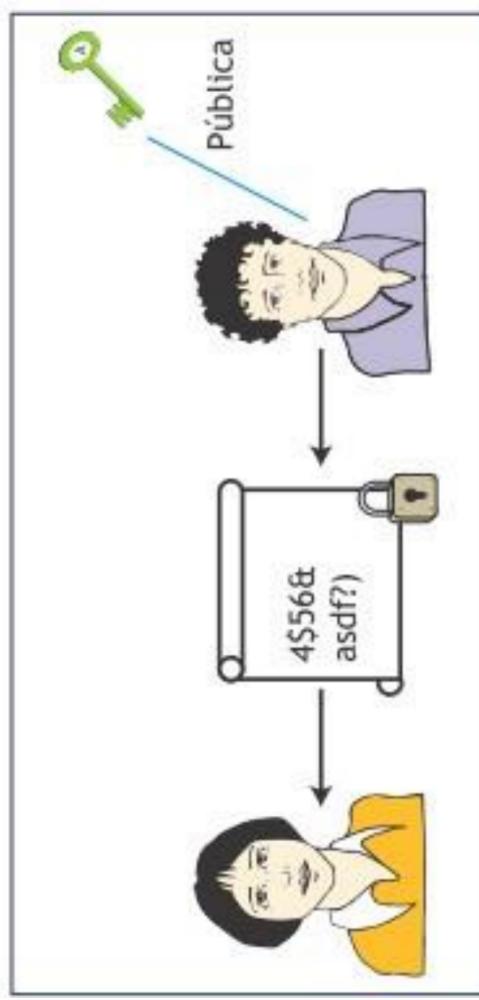
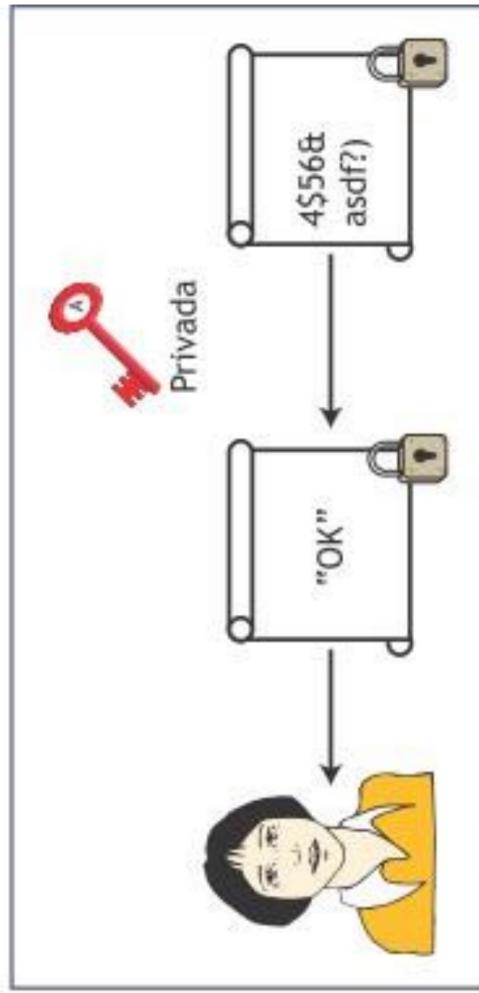
3. CIFRADO DE CLAVE ASIMÉTRICA

Ahora, supongamos que Juan quiere contestarle a Ana en secreto. Para cifrar el mensaje, Juan debe tener la clave pública de Ana. Por ello, Ana debe generar su propio par de claves pública/privada y enviar a Juan su clave pública.



3. CIFRADO DE CLAVE ASIMÉTRICA

Juan utiliza la clave pública de Ana para proteger el mensaje y solo Ana podrá leer el mensaje porque es la única persona que conoce la clave privada.



3. CIFRADO DE CLAVE ASIMÉTRICA

Ventajas

- La clave pública se distribuye libremente, por lo que ya no existe el problema del intercambio de la clave que había en los métodos simétricos.
- Solo es necesario un par de claves por interlocutor, con independencia del número de estos, por lo que el espacio de claves es más manejable cuando los interlocutores son muchos.

Inconvenientes

- Requieren mayor tiempo de proceso que el cifrado simétrico.
- Dan lugar a mensajes cifrados de mayor tamaño que los originales.
- Para garantizar la seguridad, requieren claves de mayor tamaño que en el caso de los métodos simétricos.
- Puesto que las claves públicas se distribuyen libremente, hace falta un esquema de confianza que garantice la autenticidad de las claves públicas (que la clave pública sea de quien dice que es, que no ha sido comprometida, etc.).

3. CIFRADO DE CLAVE ASIMÉTRICA: ALGORITMOS DE CIFRADO

- **RSA (Rivest-Shamir-Adelman):** Fue creado en 1977 y es uno de los algoritmos más utilizados. Permite cifrar y firmar digitalmente, aunque es mucho más lento que DES y que otros sistemas de cifrado de clave simétrica. Está basado en la factorización de números primos grandes.
- **DSA (Digital Signature Algorithm):** Algoritmo de firma digital, estándar del Gobierno Federal de Estados Unidos. Para entornos críticos, se ha demostrado que DSA es más seguro que RSA. Permite firmar digitalmente, sin embargo no permite cifrar la información. Una desventaja es que requiere más tiempo de cálculo que el algoritmo RSA.

3. CIFRADO DE CLAVE ASIMÉTRICA: ALGORITMOS DE CIFRADO

- **ElGamal:** Fue escrito por Taher ElGamal en 1984. Algoritmo de uso libre utilizado en software GNU Privacy Guard, en versiones recientes de PGP. Puede ser utilizado para cifrar y firmar digitalmente, con un tiempo de cómputo similar a RSA. Su nivel de seguridad está basado en la dificultad de calcular un logaritmo discreto.
- Realizar la práctica de criptografía de clave asimétrica con el software libre Cryptophane para Windows.

4. ALGORITMO DE CIFRADO HASH

- Una **función hash** es un algoritmo que mapea un conjunto grande de datos de tamaño variable, llamados claves, en pequeños conjuntos de datos de longitud fija.
 - Garantizan la integridad dado que, con cambiar un bit del mensaje original, el resultado obtenido al aplicar la función hash será diferente.
 - Se utilizan en la firma digital de documentos y en mecanismos como el sobre digital.
- **Entrada**

```
graph LR; Zorro[Zorro] --> FuncionHash1[Función Hash]; Zorro1[El zorro rojo corre a través del hielo] --> FuncionHash2[Función Hash]; Zorro2[El zorro rojo camina a través del hielo] --> FuncionHash3[Función Hash]; FuncionHash1 --> DFCD3454[DFCD3454]; FuncionHash2 --> 52ED879E[52ED879E]; FuncionHash3 --> 46042841[46042841]
```

4. ALGORITMO DE CIFRADO HASH

■ Propiedades más importantes de las funciones hash:

- Independientemente del tamaño del mensaje original, al aplicarle la función hash, la huella resultante siempre tendrá el mismo tamaño.
- Con cambiar un único bit del mensaje original, la huella resultante será completamente distinta.
- **Resistencia a la preimagen:** si tenemos el resultado de aplicar una función hash, resulta computacionalmente imposible obtener el mensaje original a partir de este.
 - **Resistencia a la segunda preimagen:** dado un mensaje x , no es posible encontrar otro mensaje x' que produzca el mismo valor hash.
 - **Resistencia a colisiones:** no es posible encontrar 2 entradas que den lugar a un mismo valor hash.

4. ALGORITMO DE CIFRADO HASH

- ¿En qué situaciones se utilizan funciones hash?

- En la protección de contraseñas.
- Como parte de algunos de los pasos de los algoritmos de cifrado simétrico y asimétrico.
- En el mecanismo de firma digital.
 - En un flujo de datos, en el que se garantice la integridad, como por ejemplo el software que nos descargamos, en el que podemos comprobar que el software se ha descargado sin errores mediante la huella hash.



Gato.jpg

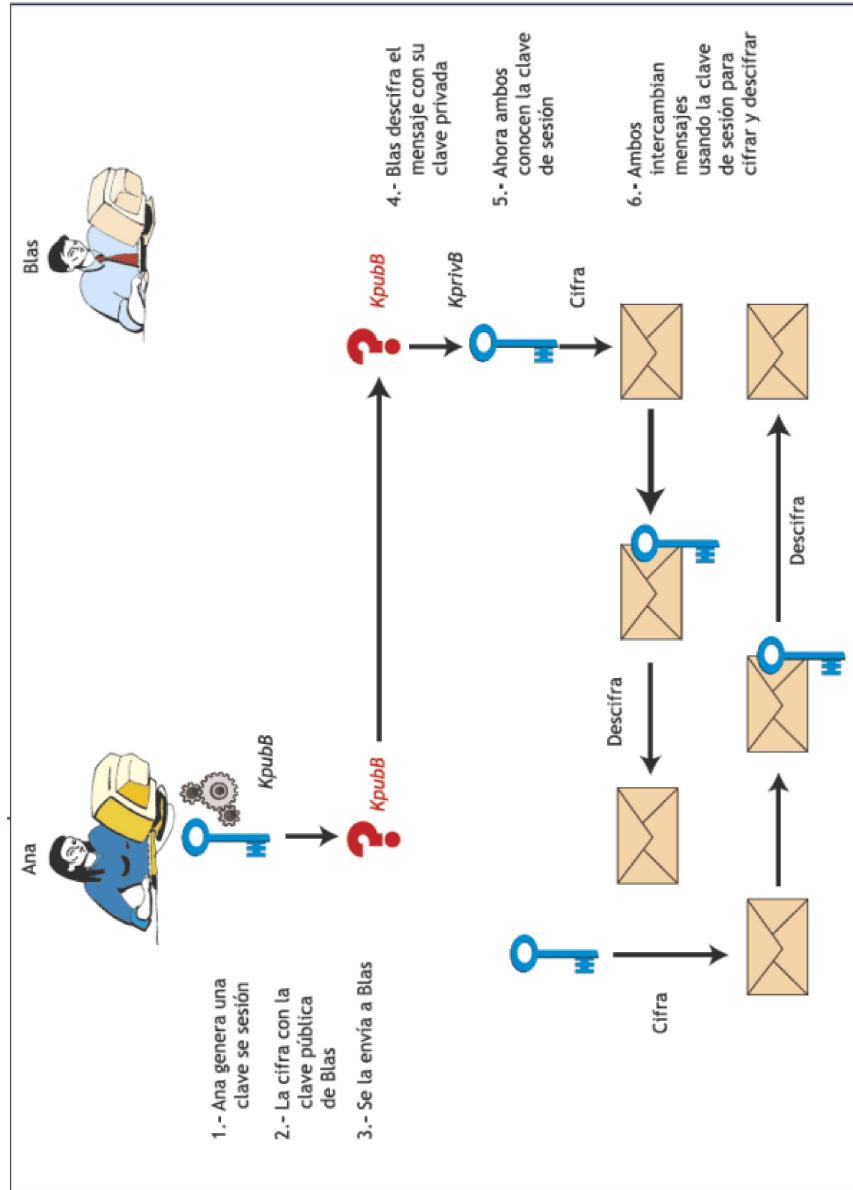
Algoritmos hash destacados:
SHA, SHA-1, MD5 y RIPE-MD.

Función Hash
SHA-256

Hash
47e283abc01852a6
750fca9bdcc30e7a7
993a21800202c72f
5aa54a0b274e5253

5. SISTEMAS HÍBRIDOS

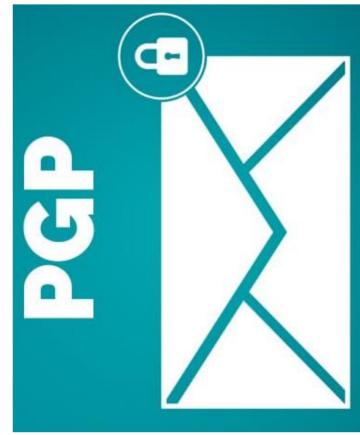
- Los criptosistemas híbridos tratan de aprovechar lo mejor de cada uno de los sistemas de cifrado de clave simétrica y asimétrica, tratando de obtener un criptosistema rápido y eficiente que permita el intercambio de contraseñas en canales de comunicación inseguros.



4.7. Esquema de la transmisión de mensajes mediante sistemas de criptografía híbrida.

5. SISTEMAS HÍBRIDOS

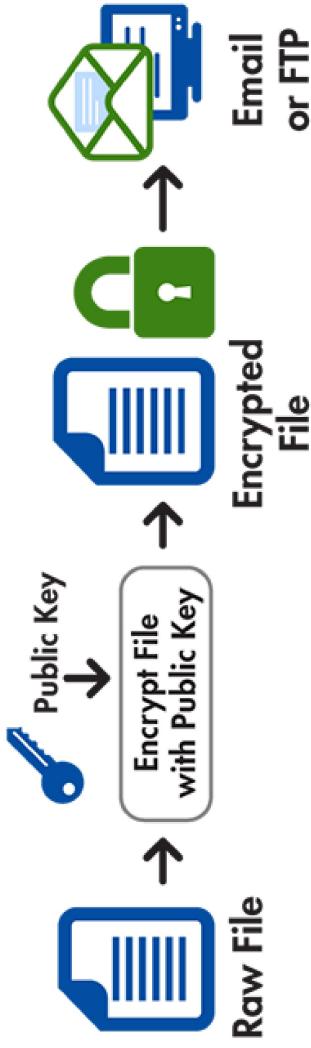
- **PGP:** herramienta que permite el cifrado de datos, archivos y mensajes mediante la utilización y codificación asimétrica junto con la simétrica.
- **Objetivo:** proteger la información utilizando la criptografía de clave pública y facilitar la autenticación de documentos mediante las firmas digitales.
- Utiliza claves asimétricas que son almacenadas en el disco duro en ficheros llamados **llaveros**. Existe un llavero para las claves públicas utilizadas y otro para las claves privadas.
- PGP se utiliza en:
 - Cifrado de ficheros, documentos y discos (PGPDisk).
 - Firma digital y cifrado de correos electrónicos (PGPmail).
 - Comunicaciones seguras (PGPNet).



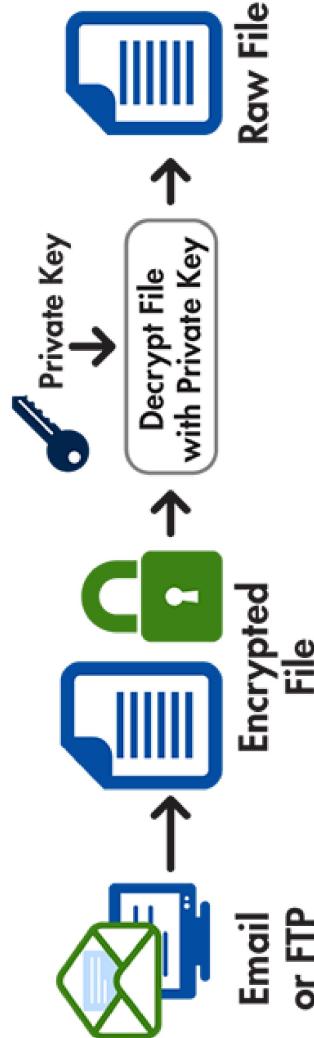
5. SISTEMAS HÍBRIDOS

- **Proceso de cifrado:** consiste en que la clave pública del receptor cifra la clave simétrica o clave de sesión con la que se cifra el mensaje a enviar.
- **Proceso de descifrado:** el receptor utiliza su clave privada para descifrar la clave de sesión secreta, la cual, a su vez, se utiliza para descifrar los datos comprimidos.

Encryption Process

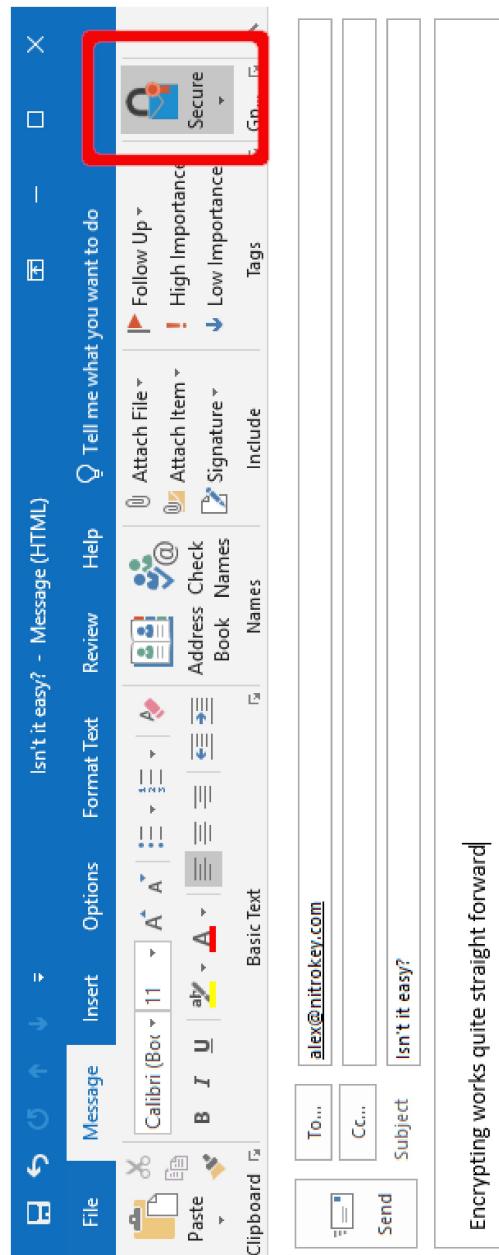


Decryption Process



5. SISTEMAS HÍBRIDOS

- **OpenPGP:** protocolo de encriptación de correo electrónico libre basado en criptografía de clave asimétrica.
 - Define formatos estándar para crear mensajes encriptados, firmas, certificados e intercambio de claves privadas.



Encrypting works quite straight forward|

5. SISTEMAS HÍBRIDOS

- **GnuPG:** herramienta de software libre y de código bajo licencia GPL utilizada para el **cifrado y firmas digitales**. Añade mejoras de seguridad y nuevas funcionalidades respecto a PGP.
 - Utiliza algoritmos como ElGamal, CAST5, TripleDES, AES y Blowfish.
 - Se utiliza en algunos SO como FreeBSD, OpenBSD, GNU/Linux, MAC OS X o Windows y también en clientes de correo electrónico y en gestores de información personal.

