Seguridad en las comunicaciones

Sistemas informáticos en red

Introducción

- Una parte fundamental de la seguridad de los sistemas informáticos es la seguridad en las comunicaciones.
- Los principales objetivos de los sistemas de seguridad en las comunicaciones son:
  - Los accesos a la información, a los sistemas y recursos han de ser **confidenciales**. Es decir, solo se permite el acceso a aquellos usuarios y procesos autorizados.
  - La información y/o recursos han de estar **disponibles** a los usuarios/procesos con permisos.
  - La modificación de información/recursos debe estar limitada a procesos/usuarios **autorizados**.
  - Se debe **garantizar la autenticidad e integridad**. Para ello, se debe poder confirmar la identidad del emisor y receptor, además se debe poder comprobar que el mensaje no ha sido alterado durante su transmisión.

Malware

Introducción

- El malware o software malicioso son programas o archivos diseñados para causar algún tipo de daño a un ordenador, servidor, red o usuario.
- Algunos tipos de malware son:
  - Virus
  - Gusanos
  - Troyanos
  - Spyware

Objetivos del malware

- **Robar información** como datos personales, contraseñas, números de cuenta...
- Crear una red de **ordenadores zombies** o **botnet** para utilizarlos para el envío masivo de spam, phishing o realización de ataques de denegación de servicio.
- **Vender falsas soluciones** de seguridad para solucionar el problema. Por ejemplo nos dicen que tenemos un virus y que hay que pagar una cantidad para conseguir el programa para eliminarlo.
- No dejar arrancar el equipo o **cifrar el contenido de determinados archivos** y solicitar el pago de una cantidad para solucionarlo.

Virus

- Los virus informáticos son programas maliciosos cuyo objetivo es **alterar el funcionamiento** del ordenador sin el permiso del usuario.
- Tienen la facultad de **replicarse al ser ejecutados** infectando así todo el sistema. Es esta característica la que les da su nombre por su similitud con los virus biológicos ya que se propagan como una enfermedad infecciosa.
- Dependiendo del medio que utilicen para infectar el ordenador se clasifican en:
  - Virus residente
  - Virus de arranque
  - Virus de fichero y de macro.

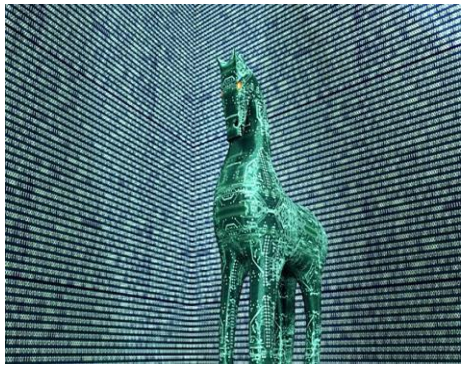
Gusanos

- Los gusanos son parecidos a lo virus, pero a diferencia de estos son capaces de **replicarse sin necesidad de ser ejecutados** por el usuario.
- Muchos gusanos tienen como único objetivo replicarse para **saturar el sistema que infectan**, pudiendo llegar a provocar el colapso del sistema.
- Además de replicarse pueden realizar otras acciones como eliminar archivos, encriptar datos, robo de datos...

Programas espía (spyware)

- Este tipo de malware se instala con el objetivo de **obtener información del usuario** del ordenador infectado.
- A diferencia de los virus no se propagan de un ordenador a otro.
- El adware es un tipo de programa espía que muestra publicidad en ventanas emergentes, barras de herramientas...

Troyanos



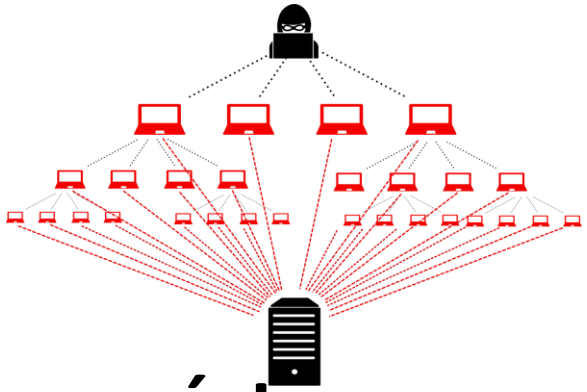
- La característica principal de los troyanos es que se introducen en un ordenador y realizan su función de manera **silenciosa** y aparentemente inocua, sin llamar la atención del usuario.
- Los troyanos toman su nombre del caballo de Troya, táctica que usaron los griegos en la Guerra de Troya según el mito narrado por Homero en su poema épico *Odisea*.
- Un troyano puede tener como objetivo tomar el control del ordenador infectado, realizar ataques **DDoS**, instalar otros virus, lanzar publicidad no deseada...

Ataques comunes

Interceptación

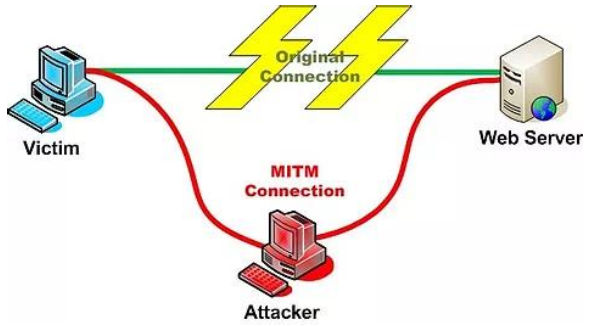
- Cuando una tercera parte, no autorizada, accede al contenido de la información con el objetivo de apropiarse de la misma o con otros objetivos futuros lícitos o no.
- Se observa a la víctima para obtener información, establecer vulnerabilidades y posibles formas de acceso futuras.
- Son **ataques contra la confidencialidad**, el resultado puede ser utilizado en el futuro en otro tipo de ataques.
- Algunos ejemplos concretos son: **sniffing**, **scanning**, **keyloggers**...

Denegación de servicio (DDOS)



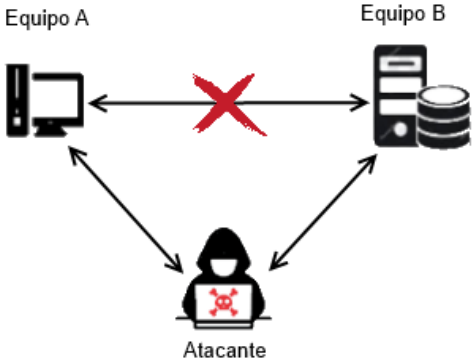
- Consiste en **saturar los recursos del equipo hasta que éste sea incapaz de seguir prestando sus servicios**, mediante consumo de recursos, alteración de configuraciones o alteración de componentes de red.
- Este tipo de ataque suele necesitar la infección previa de un conjunto de ordenadores con algún tipo de **troyano**. Este software malicioso permite tomar el control de la red de ordenadores para realizar ataques coordinados.
- Algunos ejemplos de este tipo de ataque son: **connection flood**, flooding con IP spoofing...

Modificación



- Consiste en que una tercera **parte no autorizada accede** al contenido de la información y la **modifica** de forma que los datos que llegan al receptor de la misma difieren de los originales.
- **Afecta** rincipalmente a la **integridad y disponibilidad**.
- Algunos ejemplos son: **tampering**, data diddling...

Suplantación



- Se busca **suplantar al usuario o sistema** original utilizando distintas técnicas y así tener acceso a la información.
- Generalmente se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña mediante distintos mecanismos.
- **Son ataques contra la autenticación y confidencialidad**, principalmente.
- Algunos ejemplos son: IP splicing-hijacking, browser hijacking, **Man In The Middle**...

Medidas de seguridad

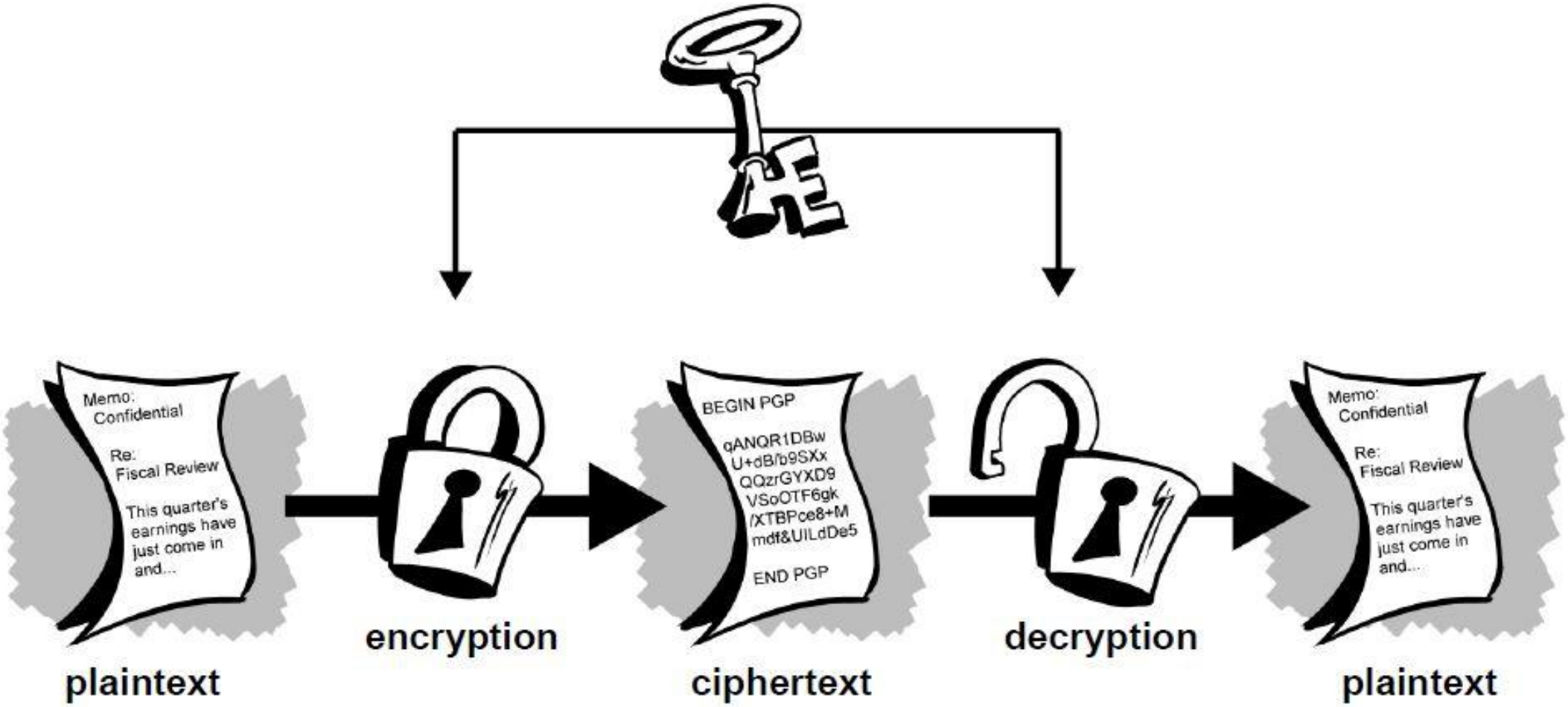
Criptografía

- La criptografía consiste en un conjunto de técnicas que permiten codificar una información de forma que sea **ininteligible** para receptores no autorizados.
- En el mundo de la informática se aplica con varios objetivos:
  - Seguridad en las comunicaciones.
  - Identificación y autenticación.
  - Certificación.
- Cuando navegamos por internet utilizando el protocolo *https* todos los datos transmitidos entre el navegador y el servidor son cifrados criptográficamente.
- Veamos este vídeo para saber más.

Encriptación con clave simétrica

- Son los algoritmos de cifrado que utilizan la misma clave para encriptar y desencriptar la información.
- La ventaja principal es que son bastante rápidos.
- El principal problema es que es necesario distribuir la clave de encriptación, pudiendo ser interceptada.
- Algunos de los algoritmos de clave simétrica más utilizados son:
  - AES
  - CTC
  - CBC

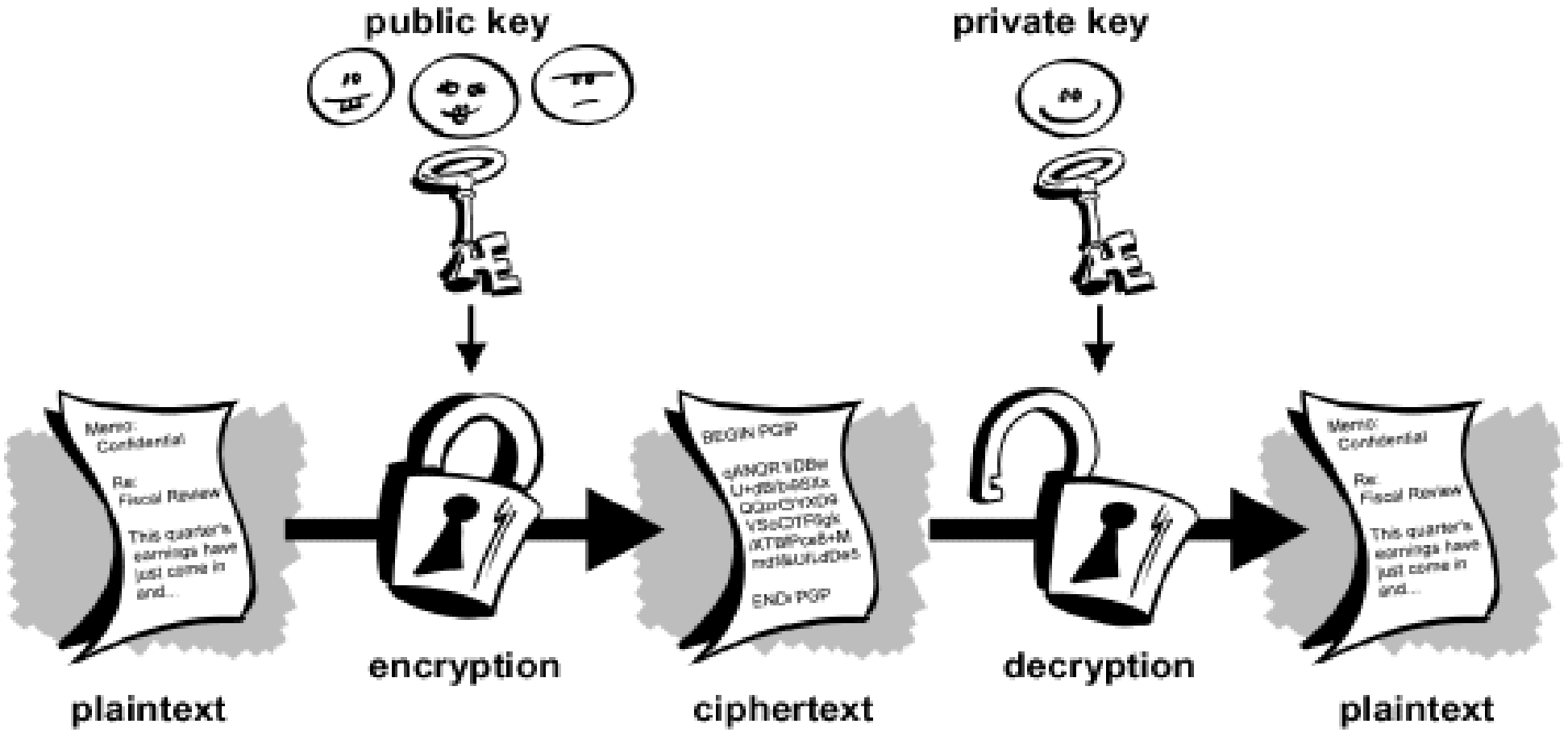
Encriptación con clave simétrica



Encriptación con clave asimétrica

- Son los algoritmos de cifrado que utilizan **dos claves**: una **pública** para encriptar y una **privada** para desencriptar.
- La clave pública se calcula a partir de la privada, pero no es computacionalmente viable realizar el proceso inverso.
- Para realizar una comunicación entre dos partes se siguen estos pasos:
  - El receptor publica su clave pública.
  - El emisor encripta el mensaje utilizando la clave anterior.
  - Se envía el mensaje al receptor
  - El receptor desencripta el mensaje utilizando su clave privada (solo él la conoce)

Encriptación con clave simétrica



Encriptación con clave asimétrica

- La principal ventaja de esta familia de algoritmos es que **no hay que distribuir la clave privada** y, por tanto, no puede ser interceptada.
- La desventaja estos algoritmos son **más lentos** que los simétricos.
- El algoritmo de clave asimétrica más utilizado es **RSA**.

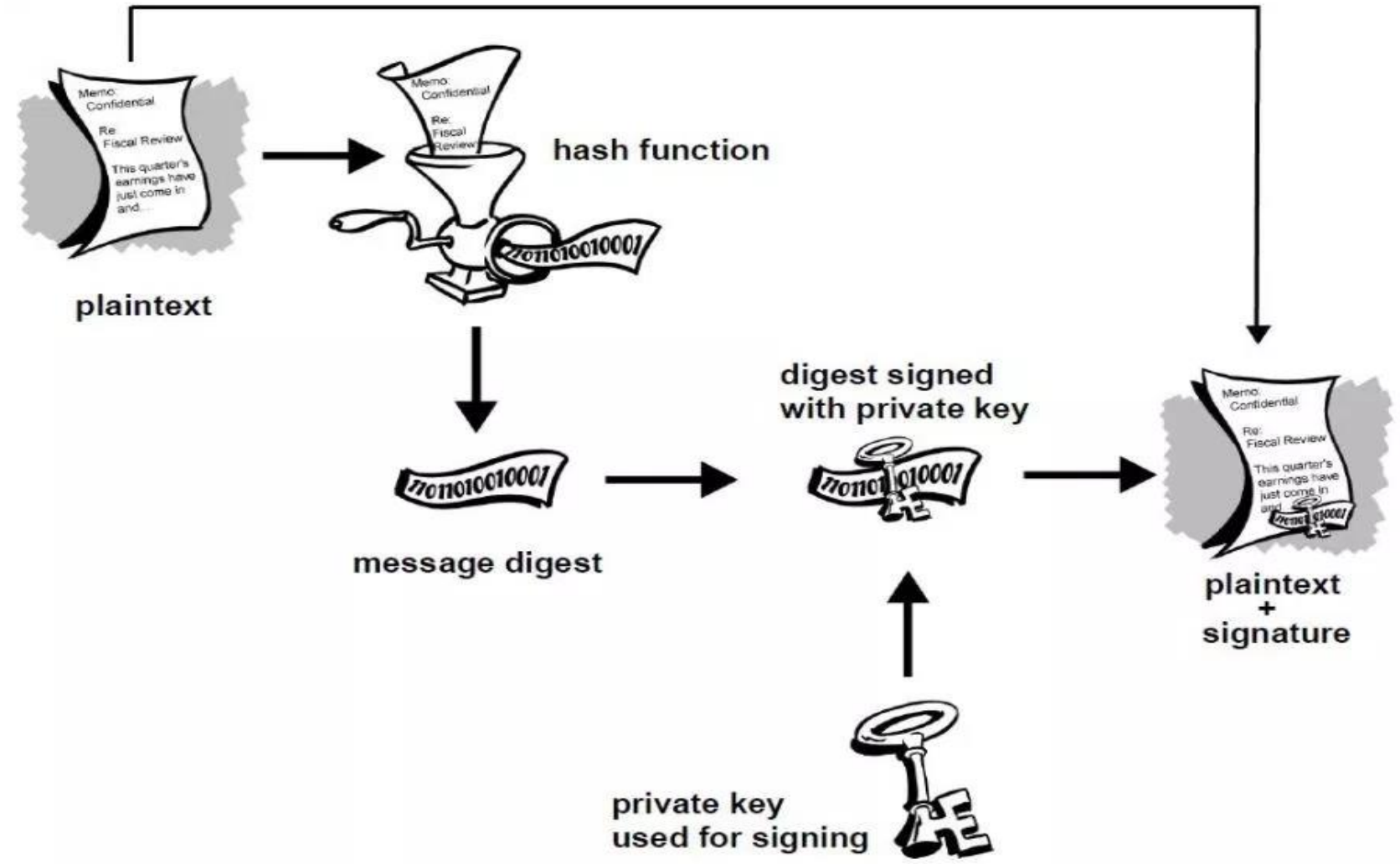
Firma digital

- Es una técnica que permite **comprobar la identidad del emisor** de un mensaje, a través de la firma del mismo.
- También permita **asegurar la integridad del mensaje**, es decir, que no ha sido modificado durante la transmisión.
- Está basado en el uso de **algoritmos de clave asimétrica.**
- El algoritmo más usado es **DSA**.

Proceso de firma digital

- El **emisor publica su clave pública**.
- Se **calcula el hash del mensaje** a enviar.
- Se **encripta el hash** utilizando la clave privada del emisor.
- Añade el hash encriptado al mensaje y **lo envía al receptor**.
- El **receptor desencripta el hash** con la clave pública del emisor.
- El receptor **comprueba que el hash es correcto**. De no ser correcto, significa que el emisor no es quien dice ser o que el mensaje ha sido alterado durante la transmisión.

Firma digital



Políticas de seguridad

- Son un **conjunto de reglas y configuraciones** que establecen medidas de seguridad encaminadas a proteger determinados recursos informáticos.
- Periódicamente, se debe realizar un análisis de riesgos donde se establecen los puntos débiles del sistema y se implementan medidas para mitigarlos.
- Basándose en los riesgos detectados, se definen **planes de contingencia y seguridad**. Estos planes están centrados en conseguir fortalecer los pilares de la seguridad en las comunicaciones: **confidencialidad**, **disponibilidad**, **integridad** y **autenticidad**.

Políticas de seguridad comunes

- Política de contraseñas
- Política de actualizaciones
- Política de uso del correo electrónico
- Política de aplicaciones permitidas
- Políticas de uso de conexiones externas
- Políticas de almacenamiento y copias de seguridad
- Políticas de uso de equipos corporativos
- Políticas de dispositivos personales

Mecanismos de seguridad

- **Filtros** de contenido
- Redes privadas virtuales o **VPN**: Consiste en la extensión de una red local a través de una red pública (como Internet), de tal manera que se pueda establecer una conexión virtual segura punto a punto.
- Cortafuegos o **firewall**: son herramientas que controla el tráfico entrante y saliente. Permiten establecer reglas que restringen el tráfico de datos por la red. El objetivo es evitar accesos no autorizados y malos usos de la red.

Mecanismos de seguridad

- **Software antimalware**: nos sirve para evitar que programas maliciosos (virus, gusanos, troyanos...) infecten el sistema.
- Herramientas de **cifrado**: nos permiten encriptar las comunicaciones para conseguir confidencialidad en las comunicaciones.
- **Protocolos seguros**:
  - SSL/TLS
  - HTTPS
  - SFTP
  - OpenSSL