Criptografía

Por. Daniel Vazart P.

Think Linux

Que es ?

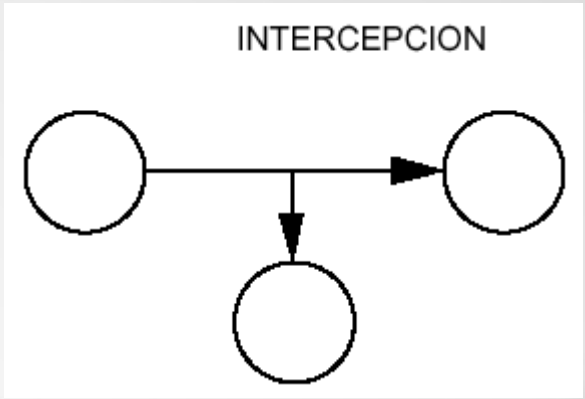
La finalidad de la criptografía es, en primer lugar, **garantizar el secreto en la comunicación entre dos entidades** (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: **que el remitente sea realmente quien dice ser y que el contenido** del mensaje enviado, habitualmente denominado criptograma, **no haya sido modificado en su tránsito.**

Think Linux

Amenazas

- Intercepción

• Una entidad no autorizada accede a parte de la información .
• Intercepción de una línea de comunicación.
• Copia ilícita de archivos, intercepción vía comunicaciones móviles.

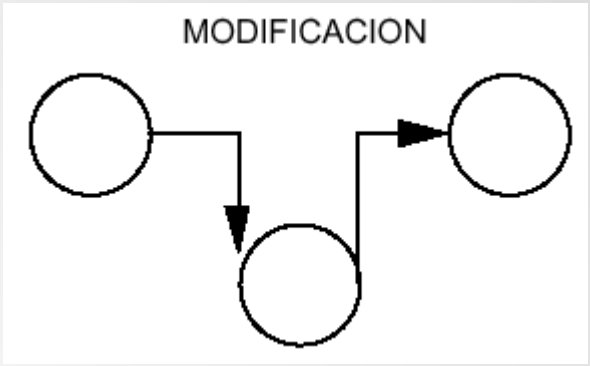


Think Linux

Amenazas

- Modificación

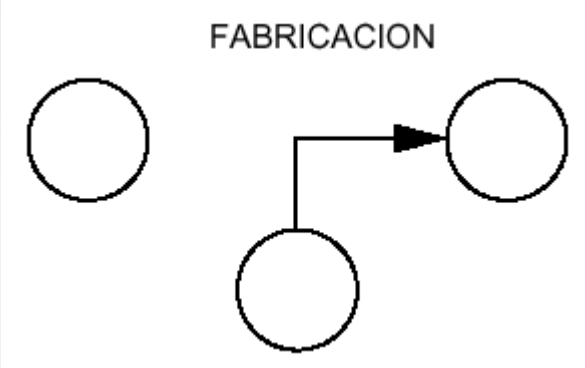
• Una entidad no autorizada accede a parte de la información y modifica su contenido.
• Alteración de archivos, alteración de programas, modificación de mensajes trasmitidos por la red.



Think Linux

Amenazas

- Fabricación
  - Una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo.



Métodos Criptogáficos

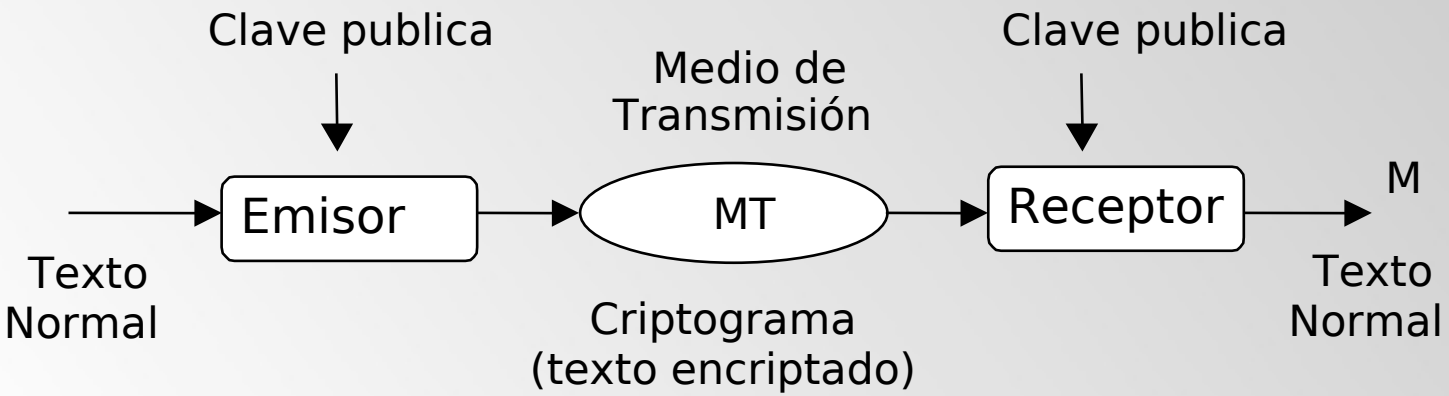
Criptografía Simétrica

- Utiliza una clave única para encriptar y desencriptar la información.
- Tanto el transmisor como el receptor deben conocer la misma clave.
- La clave es el algoritmo de encripción (no viaja con el paquete).

Think Linux

Métodos Criptogáficos

Criptografía Simétrica



- **Problema:** ¿Que medio seguro utilizar para decirle la clave publica al receptor?

Think Linux

Métodos Criptogáficos

Algoritmos de cifrado Simétricos: DES

- El estándar americano DES es el criptosistema simétrico que mayor popularidad ha alcanzado.
- Se eligió uno presentado por IBM y tras una serie de revisiones públicas, fue adoptado como estándar en 1977.
- Emplea una clave de 56 bits y opera con bloques de datos de 64 bits.
- Con la tecnología de esa época hubieran tardado 2200 años en probar todas las posibles claves.

Think Linux

Métodos Criptogáficos

Algoritmos de cifrado Simétricos: IDEA

- Tuvo su aparición en 1992.
- Considerado por muchos el mejor y más seguro algoritmo simétrico disponible en la actualidad.
- Trabaja con bloques de 64 bits de longitud, igual que el DES, pero emplea una clave de 128 bits.
- Se usa el mismo algoritmo tanto para cifrar como para descifrar

Think Linux

Métodos Criptogáficos

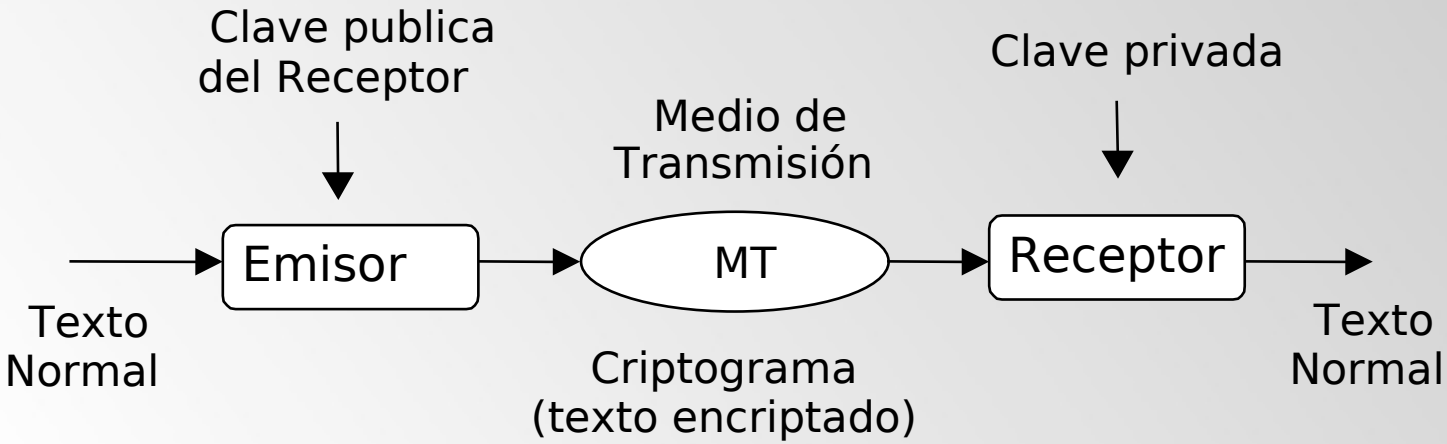
Criptografía Asimétrica

- Utiliza una clave publica y una privada tanto en el emisor como en el receptor.
- El emisor encripta el mensaje utilizando la clave publica del receptor.
- El receptor desencripta el mensaje utilizando su clave privada.

Think Linux

Métodos Criptogáficos

Criptografía Asimétrica



Think Linux

Métodos Criptográficos

Algoritmos de cifrado Asimétricos: RSA

- Es el algoritmo asimétrico más sencillo de comprender e implementar.
- Desde su nacimiento nadie ha conseguido probar o rebatir su seguridad, pero se le tiene como uno de los algoritmos asimétricos más seguros.
- Algoritmo utilizado en el SSH (Secure Shell Client).
- El principal inconveniente es la lentitud.

Think Linux

Métodos Criptográficos

Algoritmos de cifrado Asimétricos: PGP

- PGP surgió a principios de los años 90 para mejorar las características de los algoritmos anteriores.
- PGP cifra primero el mensaje empleando un algoritmo simétrico, ya que éstos son más rápidos que los asimétricos. Para ello usa una clave generada aleatoriamente y posteriormente codifica la clave mediante un algoritmo asimétrico haciendo uso de la clave pública del destinatario.
- Gran parte de la seguridad de PGP reside en la calidad del generador aleatorio que se emplea para generar claves de sesión.
- Cada clave aleatoria solo sirve para una sesión, ya que a la siguiente sesión se usará otra. Así conseguimos que si un intruso consigue descifrar una clave, no pueda descifrar los mensajes transferidos en sesiones posteriores.

Que utilizar ?

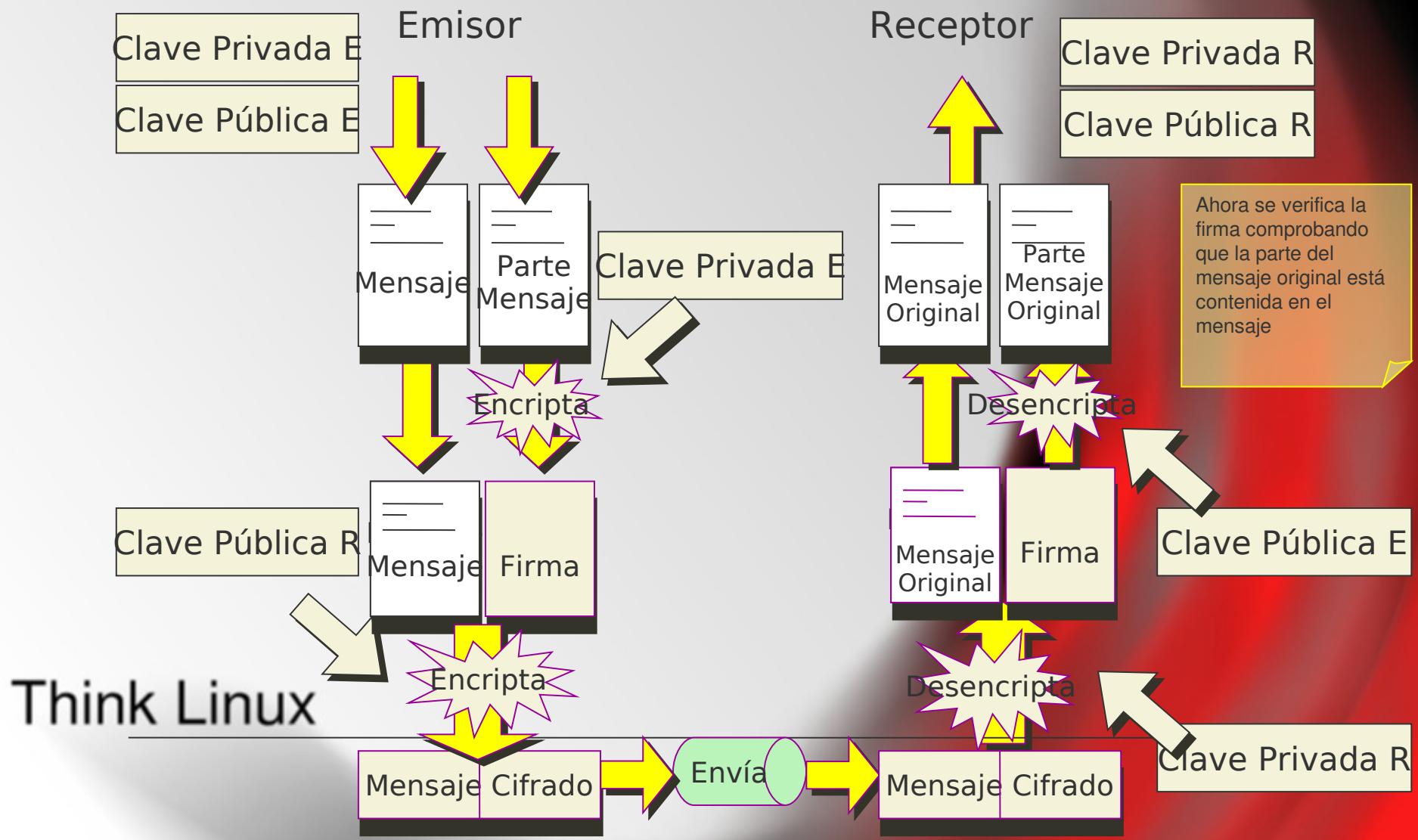
- Los sistemas de clave pública son más rápidos, aunque como hemos visto es posible que no sean tan seguros. Hay algunos tipos de ataques que les pueden afectar.
- Los sistemas de clave privada son más lentos, aunque son más seguros, los algoritmos son más complejos y es más difícil su traducción por otros sujetos que los no autorizados.

Think Linux

Firmas Digitales

• El concepto de la firma digital se basa en la verificación de la autoría de un mensaje.
• El Receptor confirma que el Emisor es quien dice ser.
• El Receptor confirma si el mensaje fue modificado o alterado.
• La firma digital se genera a partir del mensaje y de la clave privada de

Firmas Digitales



Think Linux