Estado del Arte en Criptografía Aplicada a Redes de Telecomunicaciones

Sergio Lillo Morales

Miguel Neira P.

Andrés Tocornal Orostegui

EL55A – Sistemas de Telecomunicaciones

Temario

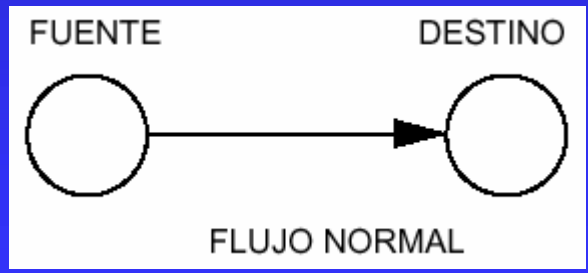
- Introducción y amenazas a la seguridad en transmisión de información.
- Algoritmos Criptográficos Simétricos y Asimétricos.
- PGP y Aplicaciones reales.

Introducción

- ¿Criptografía?
- Según la RAE: Criptografía es el: “Arte de escribir con clave secreta o de un modo enigmático”
- Definición Actual: Conjunto de técnicas que tratan sobre la protección y ocultamiento de la información frente a observadores no autorizados.

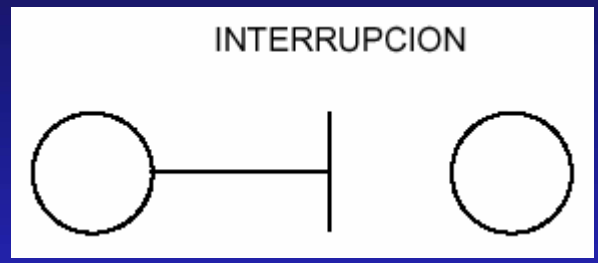
Amenazas a la seguridad

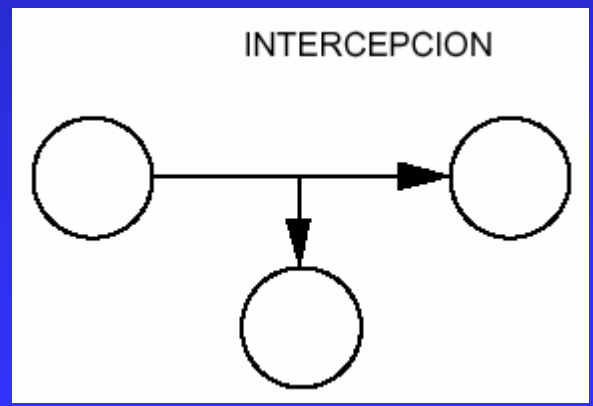
- Redes de comunicaciones actuales permiten la conectividad de un gran número de usuarios.
- Explosión de servicios que necesitan la transmisión de datos por estas redes: necesidad de protección de la información.
- Se puede modelar el sistema como un flujo de información desde una fuente (un fichero o usuario) a un destino (otro fichero o usuario).



Amenazas a la seguridad

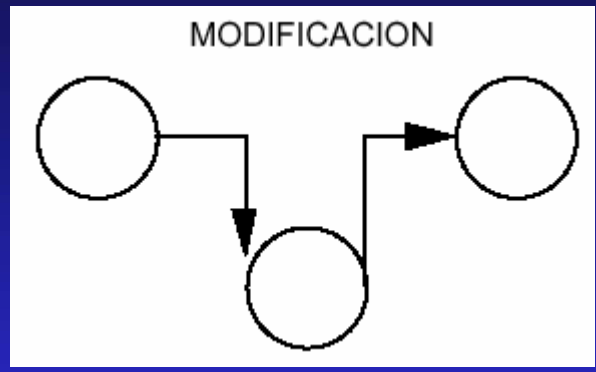
- Interrupción
  - Parte del sistema queda destruida o no disponible.
  - Destrucción hardware, corte de una línea de comunicación.
- Intercepción
  - Una entidad no autorizada accede a parte de la información .
  - Pinchazo línea telefónica, copia ilícita de ficheros, intercepción vía radio comunicaciones móviles.

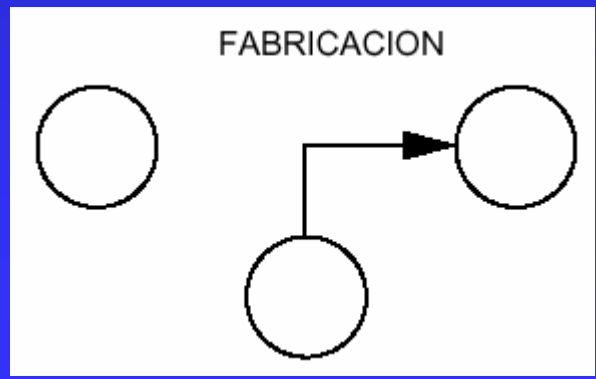




Amenazas a la seguridad

- Modificación
  - Una entidad no autorizada accede a parte de la información y modifica su contenido.
  - Alteración de ficheros de datos, alteración de programas, modificación de mensajes trasmitidos por la red.
- Fabricación
  - Una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo.





Servicios de Seguridad

- Confidencialidad
  - Requiere que la información sea accesible únicamente por las entidades autorizadas (carta lacrada).
- Autenticación
  - Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa (huellas dactilares).
- Integridad
  - Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación , etc… (tinta indeleble).

Servicios de Seguridad

- No repudio
  - Requiere que ni el emisor ni el receptor del mensaje puedan negar la transmisión (correo certificado).
- Control de acceso
  - Requiere que el acceso a la información sea controlado por el sistema destino (llaves y cerrojos).

Mecanismos de Seguridad

- Intercambio de autenticación
  - Corrobora que una entidad, ya sea origen o destino de la información, es la deseada.
- Cifrado
  - Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados.
- Integridad de datos
  - Implica el cifrado de una cadena comprimida de datos a transmitir. Esto se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado de los datos y compara el resultado obtenido con el que le llega, para verificar que no hayan sido modificados.

Mecanismos de Seguridad

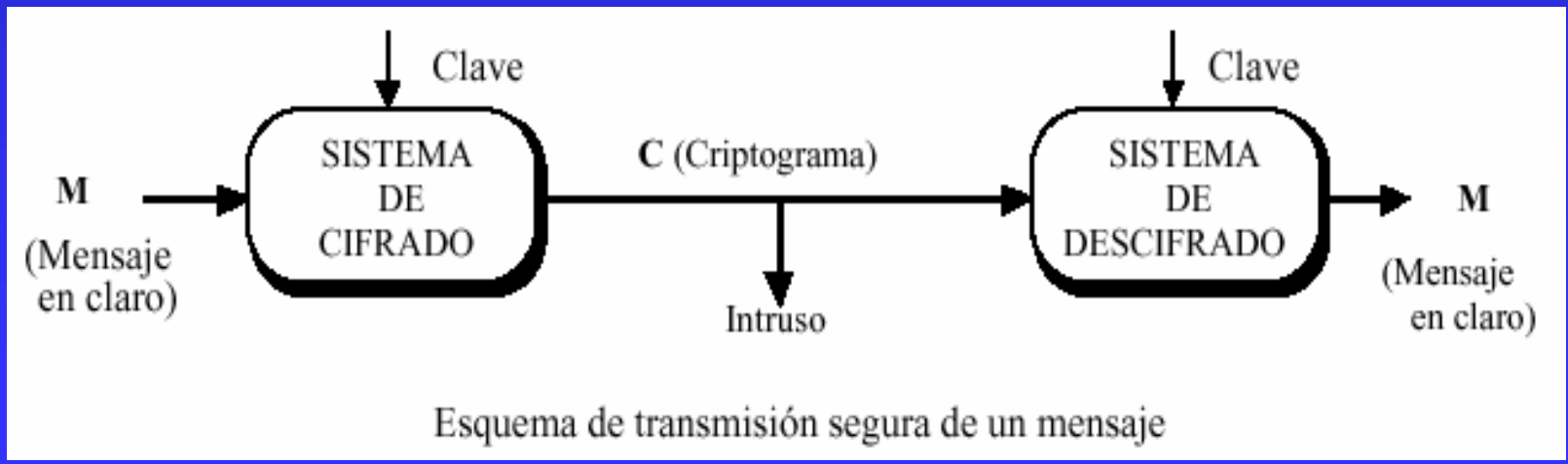
- Firma digital
  - Cifrado, con una clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía al receptor junto con los datos ordinarios. Se procesa en el receptor, para verificar su integridad.
- Control de acceso
  - Sólo aquellos usuarios autorizados acceden a los recursos del sistema o a la red.

Mecanismos de Seguridad

- Tráfico de relleno
  - Consiste en enviar tráfico redundante junto con los datos válidos para que el enemigo no sepa si se está enviando información, ni qué cantidad de datos útiles se está transfiriendo.
- Control de encaminamiento
  - Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Sistemas Criptográficos

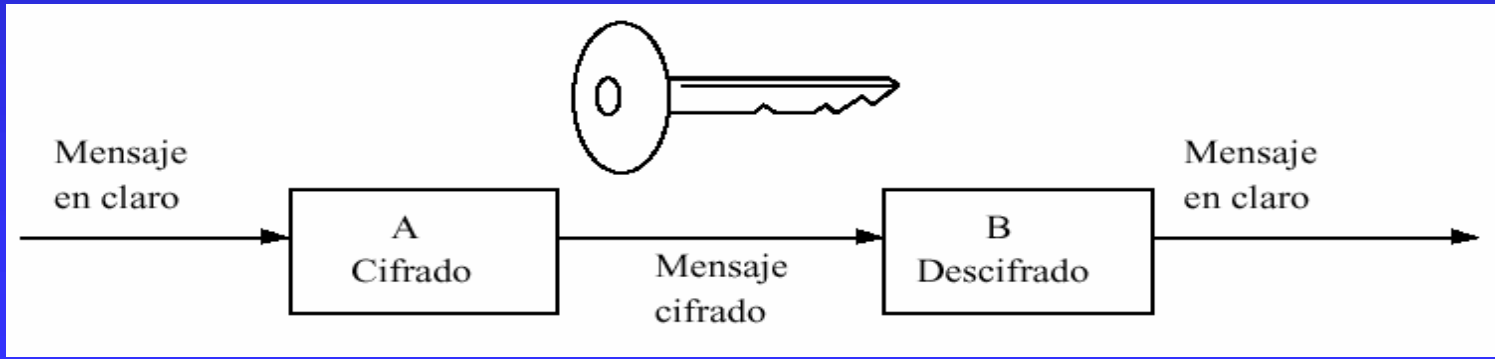
- Función de un sistema criptográfico
  - Es el encargado de calcular el mensaje cifrado C, a partir del mensaje en claro M y de la "clave de cifrado"; y de realizar el proceso inverso, el descifrado, y así determinar M a partir del mensaje cifrado y la "clave de descifrado".
  - Claves iguales: Algoritmos simétricos
  - Claves diferentes: Algoritmos asimétricos



Esquema de transmisión segura de un mensaje

Algoritmos Simétricos

- Son los algoritmos más clásicos de encriptación. Utilizados en redes comerciales desde el principio de los 70.
- Se emplea la misma clave en las transformaciones de cifrado y descifrado.
- Dos sistemas A y B desean comunicarse de forma segura, y mediante un proceso de distribución de claves, ambos compartirán un conjunto de bits que será usado como clave.
- Más significativos: DES, IDEA y AES.



Data Encryption Standard (DES)

- El estándar americano DES es el criptosistema simétrico que mayor popularidad ha alcanzado.
- Nació como petición del gobierno de los EEUU al “National Bureau of Standards” en 1973 para poder mantener comunicaciones seguras.
- Se eligió uno presentado por IBM y tras una serie de revisiones públicas, fue adoptado como estándar en 1977.
- El algoritmo se basa en permutaciones, substituciones y sumas módulo 2.
- 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. Hoy en dia sólo se tarda 3 días!!!!

International Data Encryption Algorithm (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.
- Se basa en los conceptos de confusión y difusión, utilizando puertas XOR.

A.E.S.

- Publicado el 2 de Octubre de 2000 por el NIST como ganador de la convocatoria AES (estándar de cifrado avanzado).
- Se intuye que substituirá al actual D.E.S.
- El tamaño de clave debe ser de, al menos, 128, 192 y 256 bits (debe admitir los tres), y el tamaño de bloque de cifrado debe ser de 128 bits.
- Buena combinación de seguridad, velocidad, eficiencia (en memoria y puertas lógicas), sencillez y flexibilidad.

A.E.S.

- Los productos que incorporen AES podrán ser exportados fuera de EE.UU., lo que incrementará la seguridad y la interoperatividad de los productos con tecnología criptográfica.

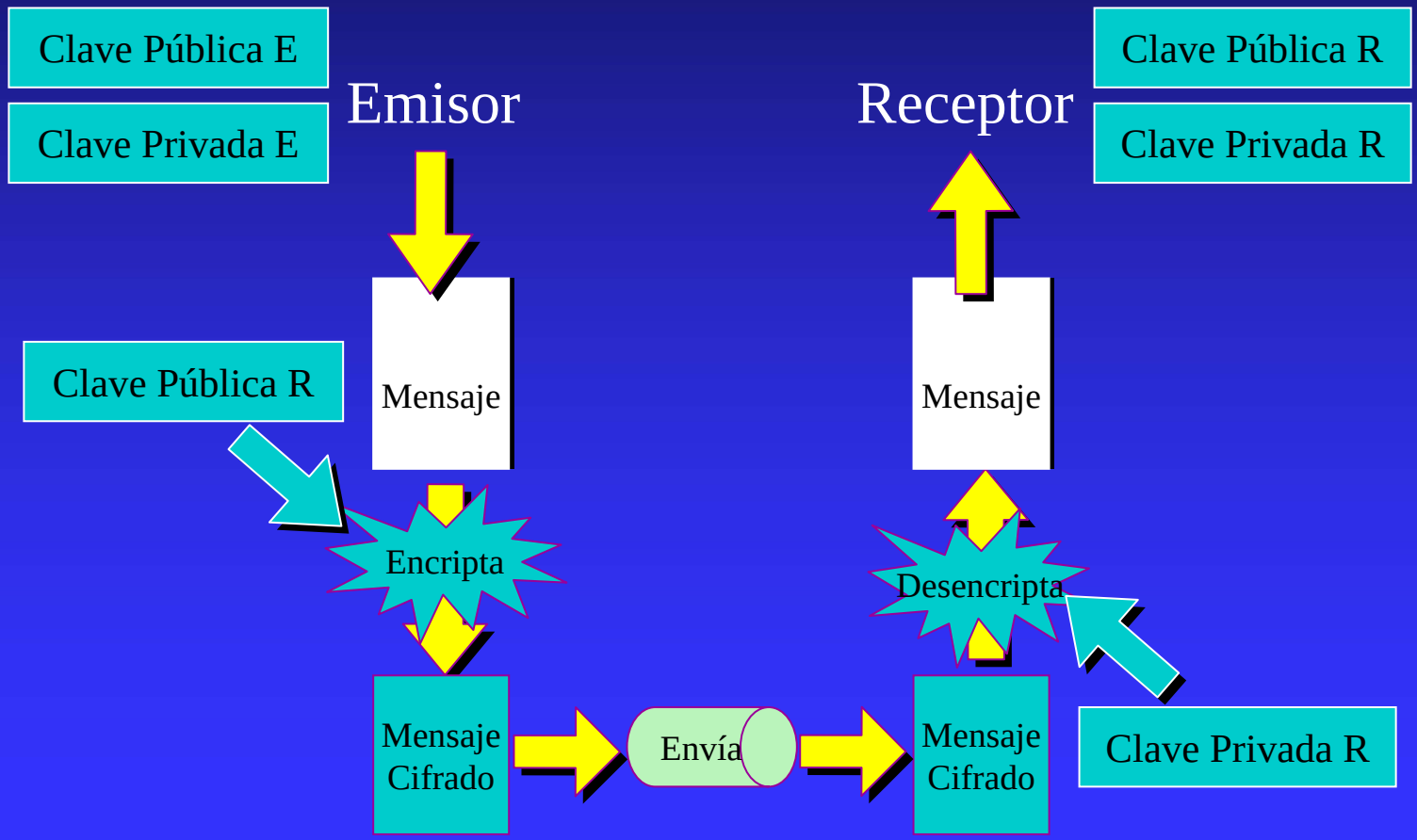
- Consta de crear una subclave de la clave original y a partir de ella ir haciendo rondas sucesivas de transformaciones.

Algoritmos Asimétricos

- Son aquellos que emplean una doble clave, és decir, una clave denominada pública y otra clave privada.
- La clave privada sólo la posee el receptor y la utiliza para desencriptar.
- La clave pública la posee el receptor, pero se la pasa al emisor para que la utilice a la hora de encriptar su mensaje.
- Son más seguros, ya que aunque un intruso consiga la clave pública, no será capaz de encontrar la clave privada a través de la clave pública para poder desencriptar el mensaje.
- El principal inconveniente es que resulta computacionalmente muy costoso su implementación.
- A la hora de encriptar, son mucho más lentos que los algoritmos simétricos.

Algoritmos Asimétricos

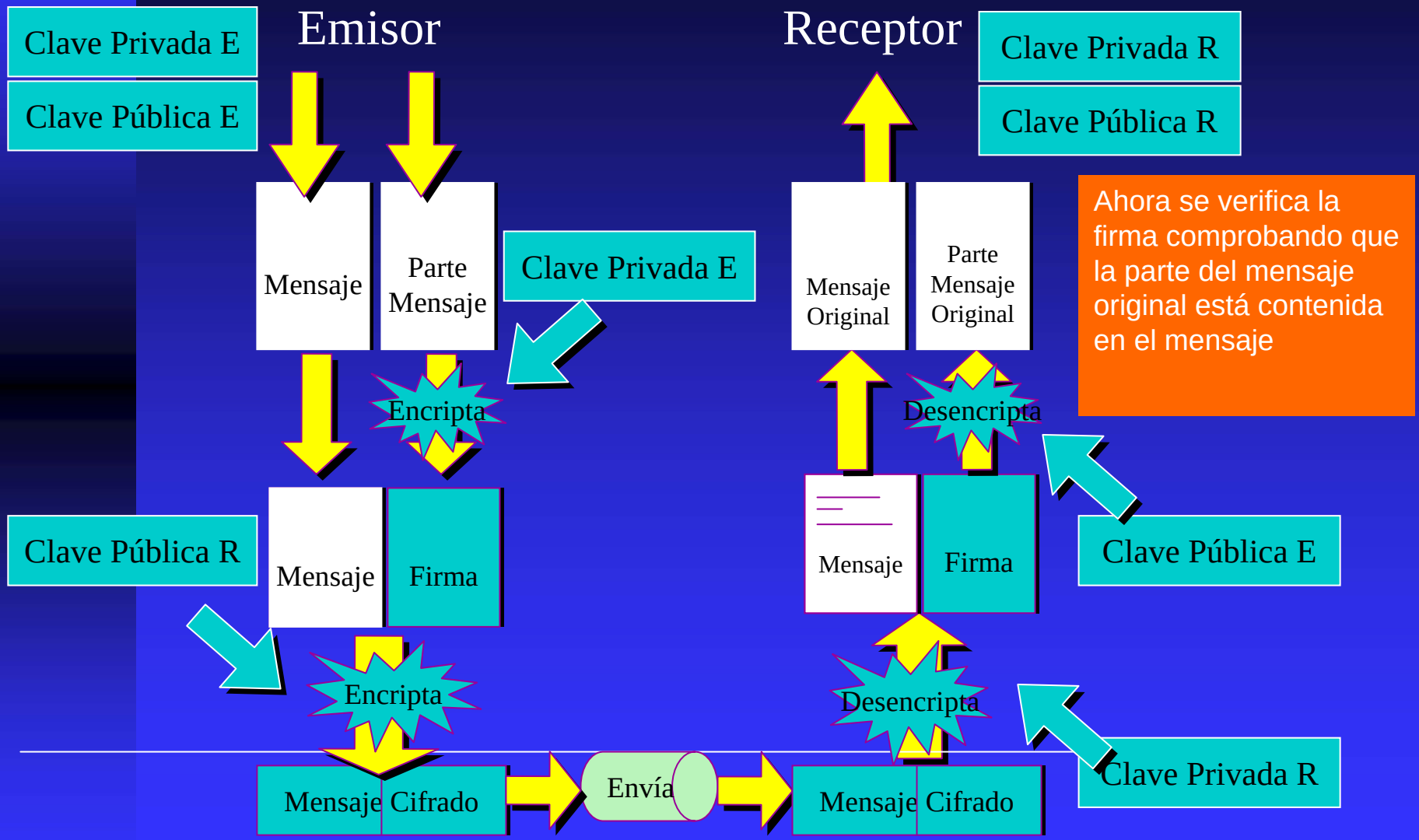
Transmisión de mensajes mediante el uso de algoritmos de encriptación asimétricos, como el RSA.



RSA

- Es el algoritmo asimétrico más sencillo de comprender e implementar.
- Su nombre proviene de sus tres inventores: Rivest, Shamir y Adleman.
- Desde su nacimiento nadie ha conseguido probar o rebatir su seguridad, pero se le tiene como uno de los algoritmos asimétricos más seguros.
- Se basa en la dificultad para factorizar números grandes, así pues, las claves se calculan a partir de un número que se obtiene como producto de dos números primos grandes.
- Algoritmo utilizado en el SSH (Secure Shell Client)

RSA Usando Firmas Digitales



PGP *(Pretty Good Privacy)*

- 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.

PGP *(Pretty Good Privacy)*

Implementaciones típicas:

- Codificación de mensajes: encriptación simétrica con clave aleatoria, recodificada con clave de usuario.
- Firma digital: con el fin de garantizar la autenticidad de un mensaje.
- Armadura ASCII: generar salidas binarias con código imprimible para poder almacenar salidas de archivos.

Criptografía en Chile

Laboratorio de Criptografía Aplicada y Seguridad

- Iniciativa del Centro de modelamiento matemático en conjunto con el DCC, ambos de la Universidad de Chile.
- Desarrollar experiencia local en los temas de seguridad que son necesarios para el desarrollo del país.
- Facilitar el desarrollo de masa crítica de investigadores nacionales en áreas tecnológicas (informática y matemática aplicada).
- Promover el uso de Internet y de sistemas abiertos fortaleciendo la confianza de la comunidad en ellos haciendo más confiable y seguro su utilización.

CASLab

LABORATORIO DE CRIPTOGRAFÍA APLICADA Y SEGURIDAD

Aplicaciones Comerciales de Criptografía

- www.acepta.com
- Realiza:
  - Certificado de Firma
  - Certificado Sitio Web
  - Carpeta Web
  - Dispositivos Criptográficos: Token USB