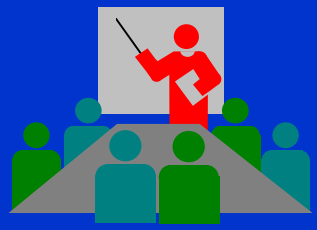
Capítulo 3
Introducción a la Seguridad Informática

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 56 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

¿Cómo definir la seguridad informática?

- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo".
- A partir de estas definiciones no podríamos aceptar que seguridad informática es "la cualidad de un sistema informático exento de peligro", por lo que habrá que buscar una definición más apropiada.
- Algo básico: la seguridad no es un producto, sino un proceso.
- Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:
  - Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico.
- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

http://www.rae.es/

¿Y qué es la criptografía?

La criptografía es aquella rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Un término más genérico es criptología: el compendio de las técnicas de cifra, conocido como criptografía, y aquellas técnicas de ataque conocidas como criptoanálisis.

He aquí una definición menos afortunada de criptografía que podemos encontrar en el diccionario de la Real Academia Española...

Una definición menos afortunada...

La criptografía según la RAE:

"Arte de escribir con clave secreta o de modo enigmático"

Desde el punto de vista de la ingeniería y la informática, es difícil encontrar una definición menos apropiada ☹

- Hoy ya no es un arte sino una ciencia.
- No sólo se escriben documentos, se generan diversos tipos de archivos DOC, DLL, EXE, JPG, etc.
- La clave no es única. Muchos sistemas actuales usan dos claves, una de ellas secreta y la otra pública. En sistemas de navegación segura en Internet se llega a usar 4 claves.
- No hay nada de enigmático ☺ en una cadena de bits.

El término es cifrar no encriptar

Cifra o cifrado:

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreta, no será posible descifrarlo o recuperarlo.

No obstante, la RAE define cifrar como “Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar” ... también muy poco técnica ☹.

En algunos países de Latinoamérica, por influencia del inglés, se usará la palabra encriptar.

Si bien se entiende, esta palabra todavía no existe y podría ser el acto de “introducir a alguien dentro de una cripta”, ... ✝☠✝ ... algo bastante distinto a lo que deseamos expresar... ☺.

Más definiciones y palabras no recogidas

- En el trabajo diario con temas de seguridad informática, nos encontraremos con muchas situaciones parecidas a ésta.
- Por ejemplo, podemos ver en algunos documentos palabras nuevas como securizar y hacker que, a la fecha, no están recogidas en el diccionario de la Real Academia Española.
- Más aún, aunque le parezca increíble no encontrará en ese diccionario palabras tan comunes como factorizar, primalidad, criptólogo, criptógrafo, criptoanalista, etc.
- No obstante sí se recogen criptograma como "Documento cifrado" y además criptoanálisis como "El arte de descifrar criptogramas"... tal vez no muy acertada esta última porque normalmente se habla aquí de criptoanalizar y no descifrar ☹.

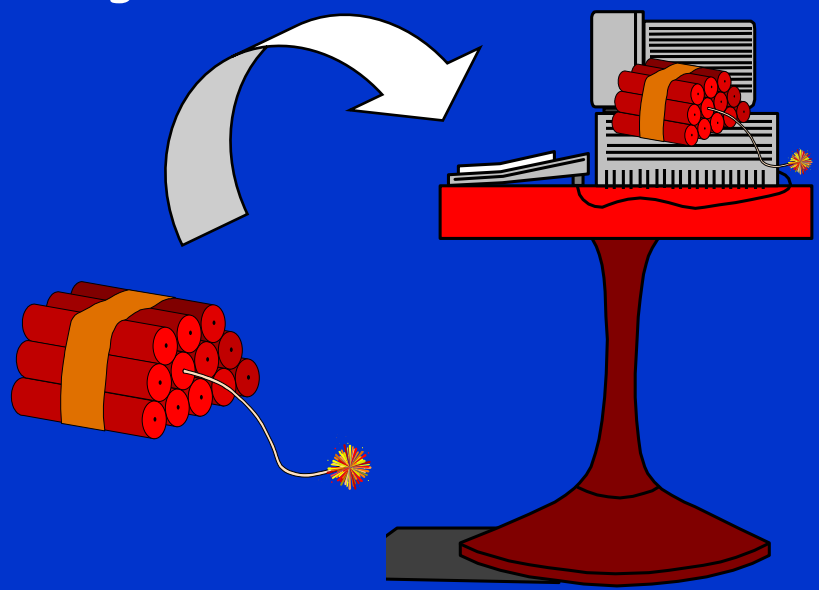
http://www.rae.es/

Unas cuantas definiciones previas

- Criptología: ciencia que estudia e investiga todo aquello relacionado con la criptografía: incluye cifra y criptoanálisis.
- Criptógrafo: máquina o artilugio para cifrar.
- Criptólogo: persona que trabaja de forma legítima para proteger la información creando algoritmos criptográficos.
- Criptoanalista: persona cuya función es romper algoritmos de cifra en busca de debilidades, la clave o del texto en claro.
- Texto en claro: documento original. Se denotará como M.
- Criptograma: documento/texto cifrado. Se denotará como C.
- Claves: datos (llaves) privados/públicos que permiten cifrar un documento y descifrar el correspondiente criptograma.

¿La solución será estar desconectado?

No podemos aceptar esa afirmación simplista que dice que el computador más seguro ...



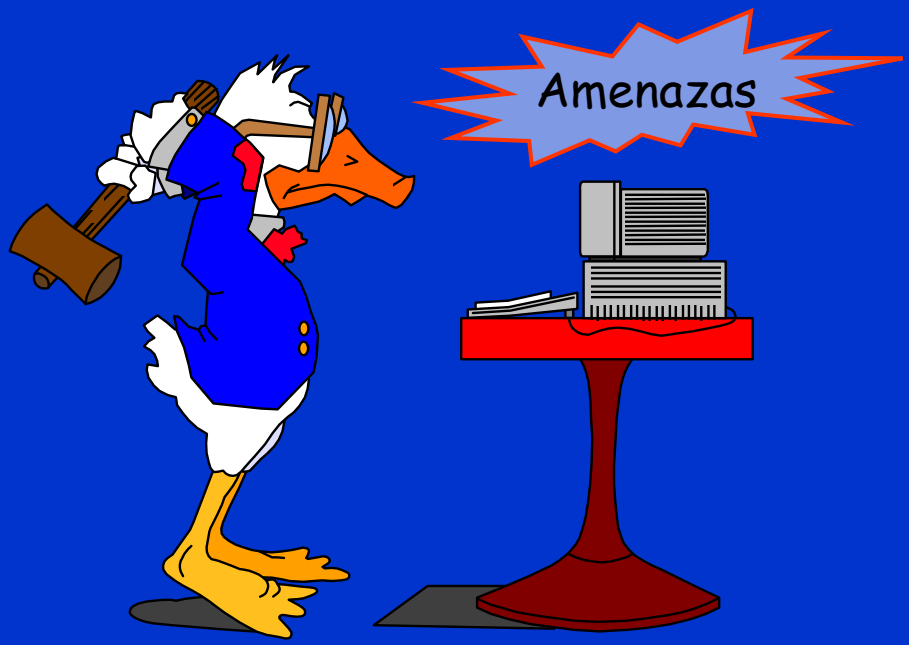
... es aquel que está desconectado y, por lo tanto, libre de todos los peligros que hay en la red.

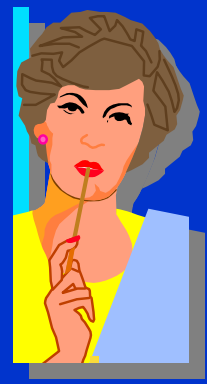
A pesar de todas las amenazas del entorno, que serán muchas y de muy distinto tipo ...

... tendremos que aplicar políticas, metodologías y técnicas de protección de la información porque la conectividad es vital.

¿Tenemos conciencia de las debilidades?

Habrá debilidades tanto internas como externas...





La seguridad informática se convierte en un nuevo motivo de preocupación

A finales del siglo XX e inicios del XII tanto las empresas, organismos e incluso particulares comienzan a tomar verdadera conciencia de su importancia. Hoy en día, tener un sistema que cumpla con los estándares de gestión de la seguridad es sinónimo de calidad de servicio.

Acontecimientos en dos últimas décadas

- A partir de los años 80 el uso del ordenador personal comienza a ser común. Asoma por tanto la preocupación por la integridad de los datos.
- En la década de los años 90 aparecen los virus y gusanos y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.
- Además, comienzan a proliferar ataques a sistemas informáticos. La palabra hacker aparece incluso en prensa.
- Las amenazas se generalizan a finales de los 90; aparecen nuevos gusanos y malware generalizado.
- En los años 00s los acontecimientos fuerzan a que se tome muy en serio la seguridad informática.

¿Qué hay de nuevo en los 00s?

- Principalmente por el uso masivo de Internet, el tema de la protección de la información se ha transformado en una necesidad y con ello se populariza la terminología técnica asociada a la criptología:
  - Cifrado, descifrado, criptoanálisis, firma digital, ...
  - Autoridades de Certificación, comercio electrónico, ...
- Ya no sólo se comentan estos temas en las universidades. Cualquier usuario desea saber, por ejemplo, qué significa firmar un e-mail o qué significa que en una comunicación con su banco aparezca un candado en la barra de tareas de su navegador y le diga que el enlace es SSL con 128 bits.
- El software actual viene con seguridad añadida o embebida.

¿Es atractivo el delito informático?

- Suponiendo que todos entendemos más o menos qué es un delito informático, algo no muy banal dado que muchos países no se ponen de acuerdo, parece ser que es un buen negocio:
  - Objeto pequeño: la información que se ataca está almacenada en contenedores pequeños: no es necesario un camión para robar un banco, llevarse las joyas, el dinero, etc.
  - Contacto físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del propio delincuente.
  - Alto valor: el objeto codiciado tiene un alto valor. Los datos (el contenido a robar) puede valer mucho más que el soporte que los almacena: servidor, computador, disco, CD, etc.
- Aunque no será la única, una de las herramientas de protección de datos más efectiva es el uso de técnicas criptográficas.

Seguridad Física y Seguridad Lógica

- El estudio de la seguridad informática podríamos plantearlo desde dos enfoques distintos aunque complementarios:
  - La Seguridad Física: puede asociarse a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.
  - La Seguridad Lógica: protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía. Este enfoque de las aplicaciones criptográficas, es el que será tratado a lo largo de los capítulos de este libro.
  - La gestión de la seguridad está en medio de la dos: los planes de contingencia, políticas de seguridad, normativas, etc. Aunque muy brevemente, este tema será tratado en un próximo capítulo.
  - ➢ No obstante, tenga en cuenta que esta clasificación en la práctica no es tan rigurosa. En resumidas cuentas, podríamos decir que cada vez está menos claro dónde comienza una y dónde termina la otra.

Principios de la seguridad informática

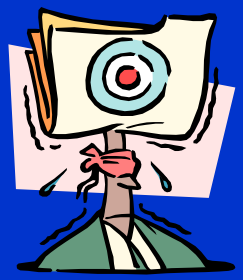
- Veremos a continuación los tres principios básicos de la seguridad informática: el del acceso más fácil, el de la caducidad del secreto y el de la eficiencia de las medidas tomadas.

- Tras los acontecimientos del 11/09/2001 en Nueva York, los del 11/03/2004 en Madrid y los del 07/07/2005 en Londres, que echaron por tierra todos los planes de contingencia, incluso los más paranoicos, comenzamos a tener muy en cuenta las debilidades de los sistemas y valorar en su justa medida el precio de la seguridad.

Es necesario aprender de los errores ☹

http://www.virusprot.com/Opiniones2002.html

1er principio de la seguridad informática



PREGUNTA:

¿Cuáles son los puntos débiles de un sistema informático?

- P1: El intruso al sistema utilizará el artilugio que haga más fácil su acceso y posterior ataque.
- Existirá una diversidad de frentes desde los que puede producirse un ataque, tanto internos como externos. Esto dificultará el análisis de riesgo ya que el delincuente aplicará la filosofía del ataque hacia el punto más débil: el equipo o las personas.

2º principio de la seguridad informática

PREGUNTA:
¿Cuánto tiempo deberá protegerse un dato?

- P2: los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor como tal.
- Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
- Esto nos llevará a la fortaleza del sistema de cifra.

3er principio de la seguridad informática

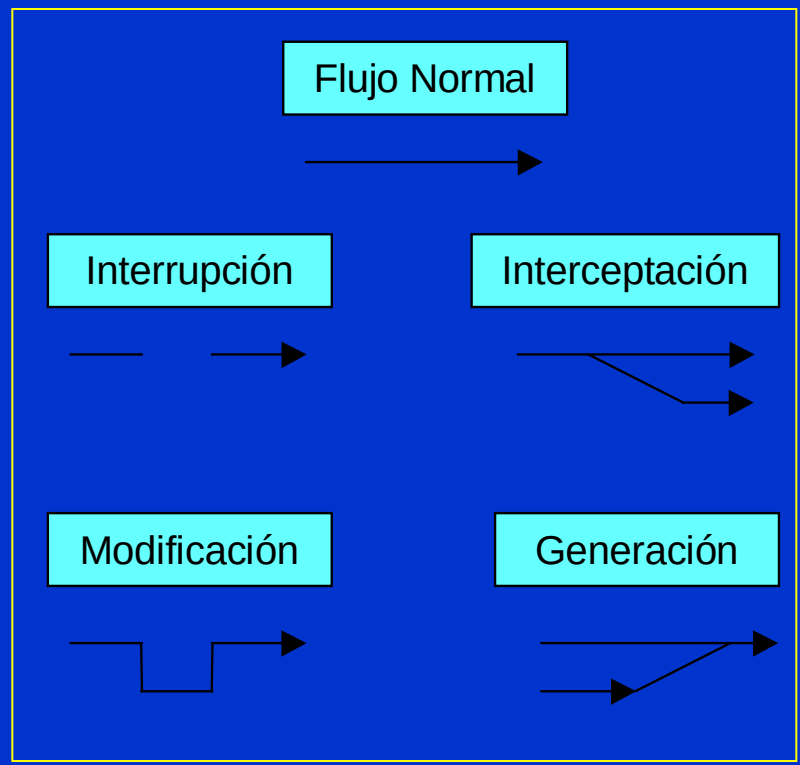
- P3: las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.
  - Efectivo: que funcionen en el momento oportuno.
  - Eficiente: que optimicen los recursos del sistema.
  - Apropiadas: que pasen desapercibidas para el usuario.

Medidas de control

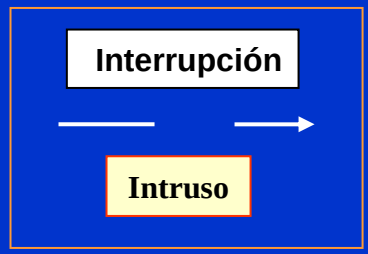
- Y lo más importante: ningún sistema de control resulta efectivo hasta que debemos utilizarlo al surgir la necesidad de aplicarlo. Junto con la concienciación de los usuarios, éste será uno de los grandes problemas de la Gestión de la Seguridad Informática.

Amenazas del sistema

- Las amenazas afectan principalmente al hardware, al software y a los datos. Éstas se deben a fenómenos de:
  - Interrupción
  - Interceptación
  - Modificación
  - Generación



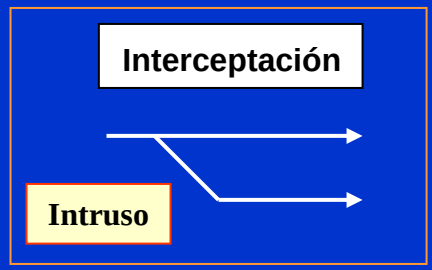
Amenazas de interrupción



- Se daña, pierde o deja de funcionar un punto del sistema.
- Su detección es inmediata.

Ejemplos: Destrucción del hardware.
Borrado de programas, datos.
Fallos en el sistema operativo.

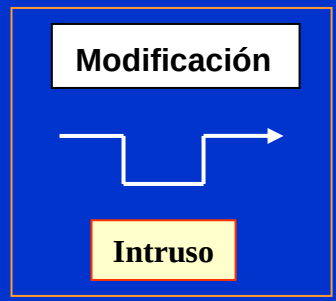
Amenazas de interceptación



- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Su detección es difícil, a veces no deja huellas.

Ejemplos: Copias ilícitas de programas.
Escucha en línea de datos.

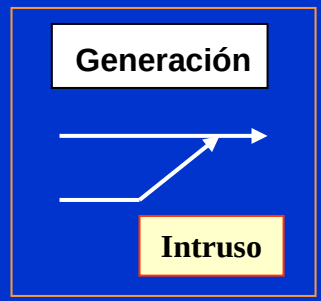
Amenazas de modificación



- Acceso no autorizado que cambia el entorno para su beneficio.
- Su detección es difícil según las circunstancias.

Ejemplos: Modificación de bases de datos.
Modificación de elementos del HW.

Amenazas de generación



- Creación de nuevos objetos dentro del sistema.
- Su detección es difícil: delitos de falsificación.

Ejemplos: Añadir transacciones en red.
Añadir registros en base de datos.

Escenarios de las amenazas del sistema

Interrupción (pérdida)	**Interceptación** (acceso)	**Modificación** (cambio)	**Generación** (alteración)

Datos

Los datos serán la parte más vulnerable del sistema

Ejemplos de amenzas

Hardware

Software

Interrupción (denegar servicio)
Interceptación (robo)

Modificación (falsificación)
Interrupción (borrado)
Interceptación (copia)

Amenazas más características

- Hardware:
  - Agua, fuego, electricidad, polvo, cigarrillos, comida.
- Software:
  - Además de algunos típicos del hardware, borrados accidentales o intencionados, estática, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.
- Datos:
  - Tiene los mismos puntos débiles que el software. Pero hay dos problemas añadidos: no tienen valor intrínseco pero sí su interpretación y, por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público: hay leyes que lo protegen.

Debilidades del sistema informático (1)

HARDWARE - SOFTWARE - DATOS
MEMORIA - USUARIOS

Los tres primeros puntos conforman el llamado Triángulo de Debilidades del Sistema:

- Hardware: pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- Software: puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- Datos: puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

Debilidades del sistema informático (2)

- Memoria: puede producirse la introducción de un virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- Usuarios: puede producirse la suplantación de identidad, el acceso no autorizado, visualización de datos confidenciales, etc.

- Es muy difícil diseñar un plan que contemple minimizar de forma eficiente todas estas amenazas, y que además se entienda y pase desapercibido por los usuarios.
- Debido al principio de acceso más fácil, el responsable de seguridad informática no se deberá descuidar ninguno de los cinco elementos susceptibles de ataque al sistema.

Confidencialidad, integridad y disponibilidad

Estos son los tres elementos básicos de la seguridad informática:

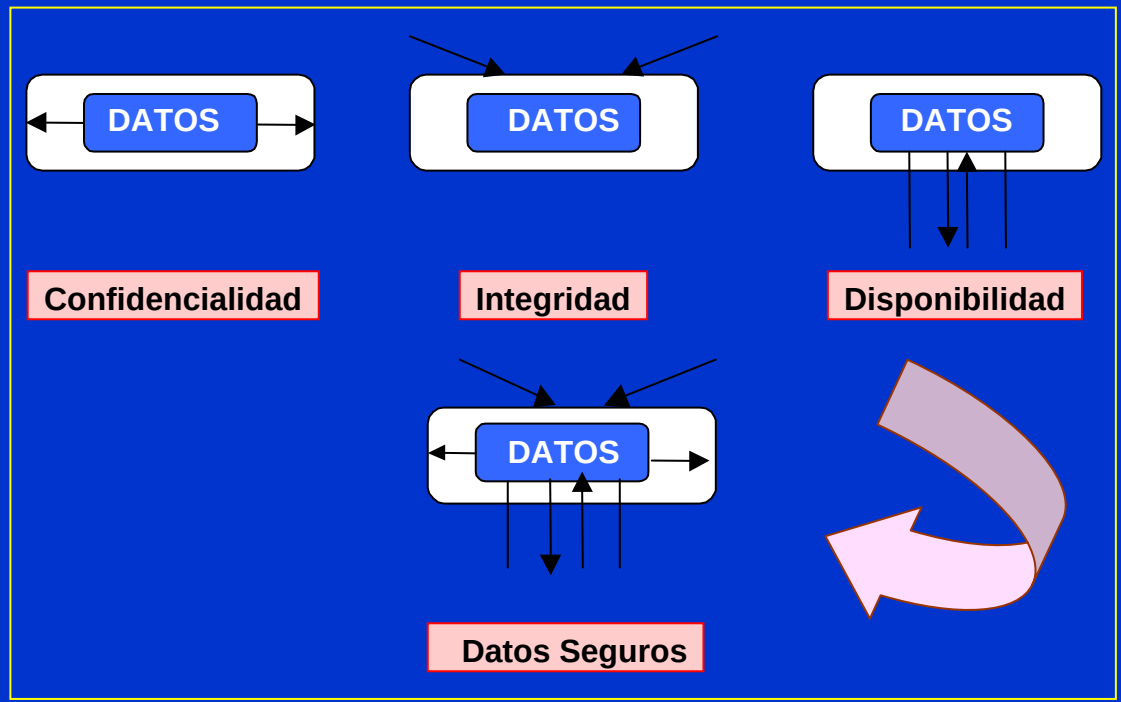
- Confidencialidad
  - Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.
- Integridad
  - Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.
- Disponibilidad
  - Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

No repudio de origen y destino

- No Repudio
  - Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático.
  - Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación.
  - Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.

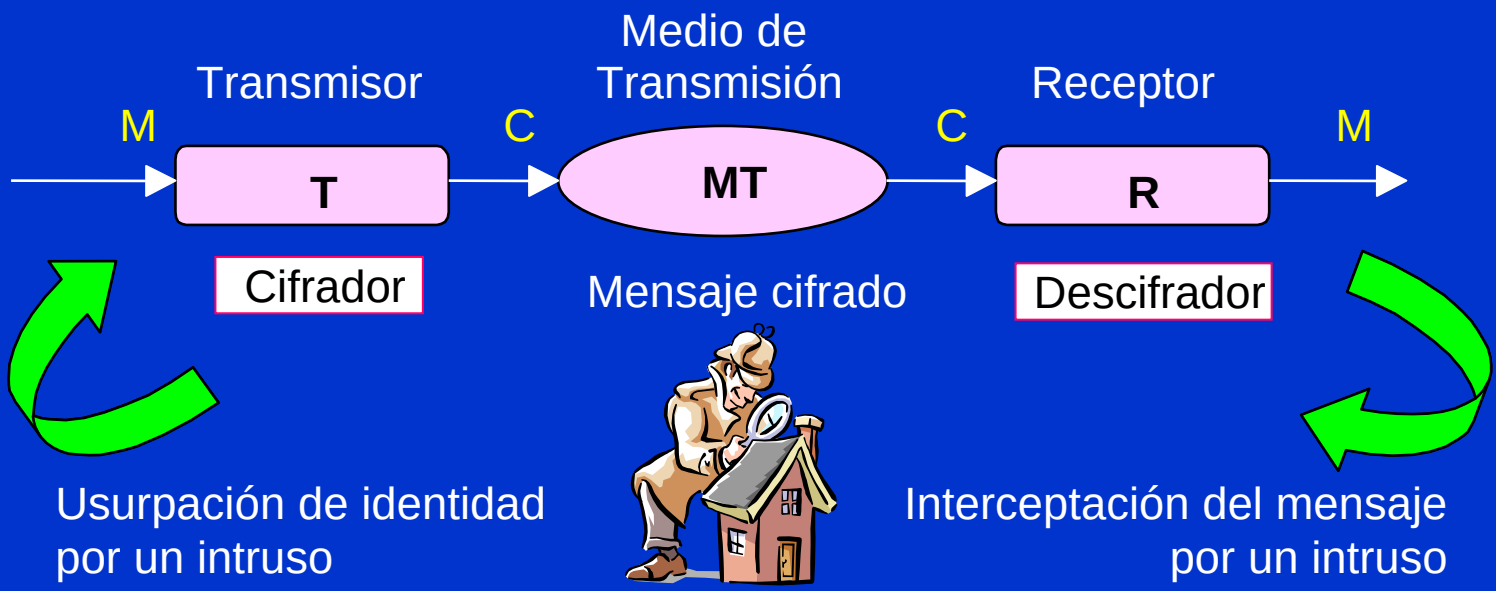
El concepto de datos seguros

Si se cumplen los principios vistos anteriormente, diremos en general que los datos están protegidos y seguros.



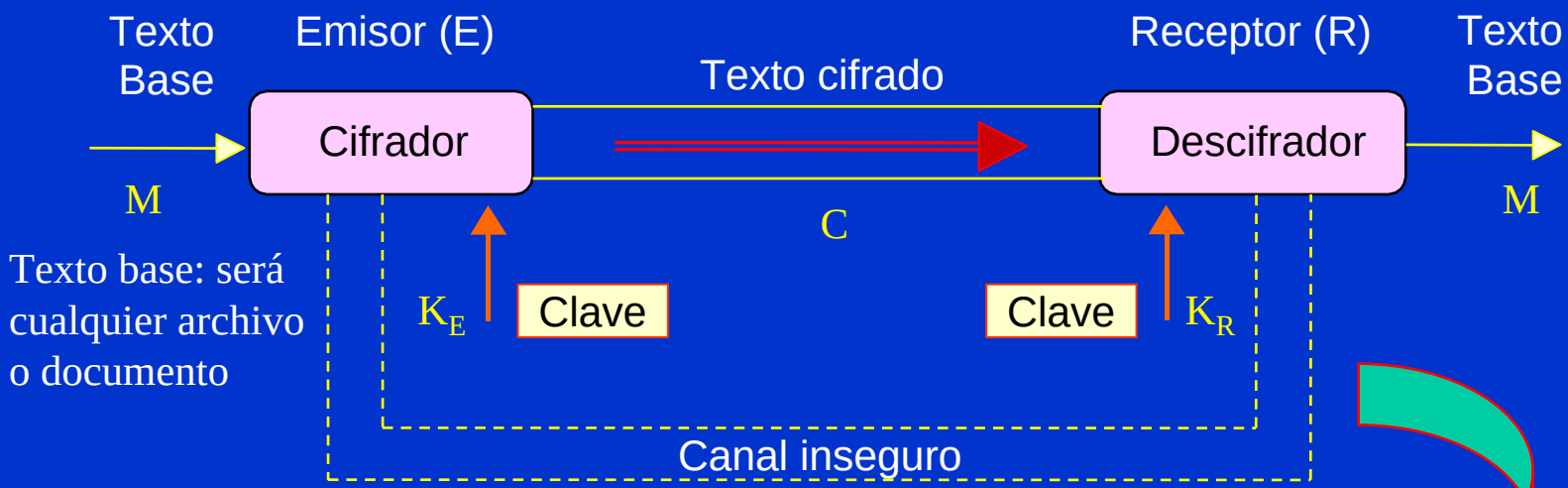
Esto se entiende en el siguiente sentido: los datos sólo pueden ser conocidos por aquellos usuarios que tienen privilegios sobre ellos, sólo usuarios autorizados los podrán crear o bien modificar, y tales datos deberán estar siempre disponibles.

Sistema de cifra



Sea cual sea el medio de transmisión o almacenamiento (enlace, red telefónica, red de datos, disco magnético, disco óptico, etc.), éste será siempre y por definición un medio inseguro. Por lo tanto, habrá que adaptarse a este medio usando el cifrado. Tal vez esto deje de ser cierto en los futuros sistemas con criptografía cuántica.

Esquema de un criptosistema



Hablaremos entonces de:

- Un espacio de textos en claro M
- Un espacio de textos cifrados C
- Un espacio de claves K
- Unas transformaciones de cifrado $E_{KE}(M)$
- Unas transformaciones de descifrado $D_{KR}(C)$

Funciones y operaciones de cifra

- C = E(M)
- M = D(C)
- M = D(E(M))

Si se usa una clave k:

- C = E(k,M) o $E_k(M)$
- M = D(k, E(k,M))
- M = D(k_R, E(k_E,M))

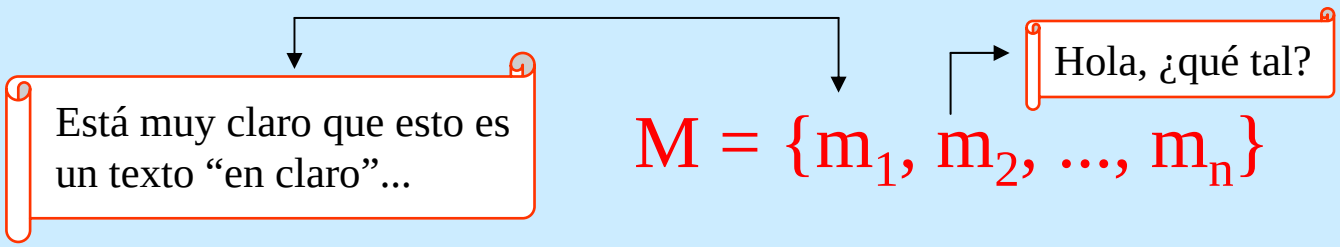
E(M): Cifrado del mensaje M

D(C): Descifrado del criptograma C

Las operaciones D y E son inversas o bien lo son las claves que intervienen. Esto último es lo normal, usando inversos dentro de un cuerpo finito. Por tanto, se recupera así el mensaje en claro.

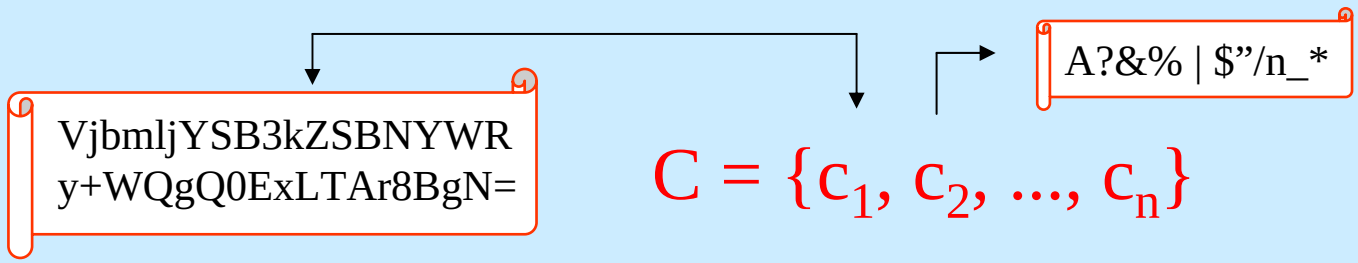
Es el caso típico de los sistemas modernos: los algoritmos E y D son iguales y la clave k_R es la usada en el extremo receptor y la clave k_E en extremo emisor.

El espacio de mensajes M



- Componentes de un mensaje inteligible (bits, bytes, pixels, signos, caracteres, etc.) que provienen de un alfabeto previamente establecido como en el ejemplo.
- El lenguaje tiene unas reglas sintácticas y semánticas.
- En algunos casos y para los sistemas de cifra clásicos la longitud del alfabeto indicará el módulo en el cual se trabaja. En los modernos, no guarda relación.
- Habrá mensajes con sentido y mensajes sin sentido.

El espacio de textos cifrados C



- Normalmente el alfabeto es el mismo que el utilizado para crear el mensaje en claro.
- Supondremos que el espacio de los textos cifrados C y el espacio de los mensaje M (con y sin sentido) tienen igual magnitud.
- En este caso, a diferencia del espacio de mensajes M, serán válidos todo tipo de criptogramas, con y sin sentido, como es lógico.

El espacio de claves K

$$K = \{k_1, k_2, ..., k_n\}$$

- Se supone que es un conjunto altamente aleatorio de caracteres, palabras, bits, bytes, etc., en función del sistema de cifra. Al menos una de las claves en un criptosistema se guardará en secreto.
- Si el espacio de claves K fuera tan grande como el de los mensajes M, se puede lograr un criptosistema con secreto perfecto.

Transformaciones de cifrado E_k

$$E_k: M \rightarrow C \qquad k \in K$$

- E_k es una aplicación con una clave k, que está en el espacio de claves K, sobre el mensaje M y que lo transforma en el criptograma C.
- Es el algoritmo de cifra. Sólo en algunos sistemas clásicos el algoritmo es secreto. Por lo general el algoritmo de cifra será de dominio público y además su código fuente está disponible en Internet.

Transformaciones de descifrado D_k

$$D_k: C \rightarrow M \qquad k \in K$$

- D_k es una aplicación con una clave k, que está en el espacio de claves K, sobre el criptograma C y que lo transforma en el texto en claro M.
- Se usa el concepto de inverso. D_k será la operación inversa de E_k o bien -que es lo más común- se usa la misma transformación E_k para descifrar pero con una clave k' que es la inversa de k dentro de un cuerpo.

Requisitos de seguridad de un sistema

- El algoritmo de cifrado y descifrado deberá ser rápido y fiable.
- Debe ser posible transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado.
- La seguridad del sistema deberá residir solamente en el secreto de una clave y no en las funciones de cifra.
- La fortaleza del sistema se entenderá como la imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable) de romper la cifra o encontrar una clave secreta a partir de otros datos de carácter público.

Recomendaciones de Bacon

- Filósofo y estadista inglés del siglo XVI
  - Dado un texto en claro M y un algoritmo de cifra E_k, el cálculo de $E_k(M)$ y su inversa debe ser sencillo.
  - Será imposible encontrar el texto en claro M a partir del criptograma C si se desconoce la función de descifrado D_k.
  - El criptograma deberá contener caracteres distribuidos para que su apariencia sea inocente y no dé pistas a un intruso.

Teniendo en cuenta los siglos trascurridos desde estas afirmaciones, éstas siguen siendo válidas hoy en día.

http://www.sirbacon.org/links.html

Recomendaciones de Kerckhoffs

Profesor holandés en París en el siglo XIX

- K_1 El sistema debe ser en la práctica imposible de criptoanalizar.
- K_2 Las limitaciones del sistema no deben plantear dificultades a sus usuarios.
- K_3 El método de elección de claves debe ser fácil de recordar.
- K_4 La transmisión del texto cifrado se hará por telégrafo.
- K_5 El criptógrafo (equipo o máquina de cifrar) debe ser portable.
- K_6 No debe existir una larga lista de reglas de uso.

Al igual que en el caso anterior, estas recomendaciones siguen siendo válidas si las adaptamos a nuestra época y tecnología.

http://en.wikipedia.org/wiki/Kerckhoffs%27_law

Fortaleza de la cifra: tipos de ataques

Conociendo el algoritmo de cifra, el criptoanalista intentará romper la cifra en uno de estos escenarios:

1. Contando únicamente con el criptograma.
2. Contando con texto en claro conocido.
3. Eligiendo un texto en claro.
4. A partir de texto cifrado elegido.

ATAQUE POR FUERZA BRUTA

5. Buscando todas combinaciones posibles de claves.

Un algoritmo de cifra será fuerte si, conociendo su funcionamiento o código, conociendo el texto cifrado y conociendo el texto en claro, el ataque a la clave de cifra secreta es computacionalmente muy difícil.

Clasificación de los criptosistemas

- Sistemas de cifra: clásicos versus modernos
  - Clasificación histórica y cultural (no técnica).
- Sistemas de cifra: en bloque versus en flujo
  - Clasificación de acuerdo a cómo se produce la cifra.

- Sistemas con clave: secreta versus pública
  - Clasificación de acuerdo al uso de una única clave secreta (sistemas simétricos) o bien dos claves, una de ellas pública y la otra privada (sistemas asimétricos).

Cifrado en bloque y cifrado en flujo

- CIFRADO EN BLOQUE:
  - El mismo algoritmo de cifra se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave. El bloque de texto o información a cifrar normalmente será de 64 ó 128 bits.
- CIFRADO EN FLUJO:
  - El algoritmo de cifra se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y de mayor longitud que el mensaje. La cifra se hace carácter a carácter o bit a bit.

Comparativa de cifra: bloque vs flujo

CIFRADO EN BLOQUE

Ventajas:

* Alta difusión de los elementos en el criptograma.
* Inmune: imposible introducir bloques extraños sin detectarlo.

Desventajas:

* Baja velocidad de cifrado al tener que leer antes el bloque completo.
* Propenso a errores de cifra. Un error se propagará a todo el bloque.

CIFRADO EN FLUJO

Ventajas:

* Alta velocidad de cifra al no tener en cuenta otros elementos.
* Resistente a errores. La cifra es independiente en cada elemento.

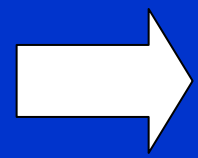
Desventajas:

* Baja difusión de elementos en el criptograma.
* Vulnerable. Pueden alterarse los elementos por separado.

Confidencialidad versus integridad

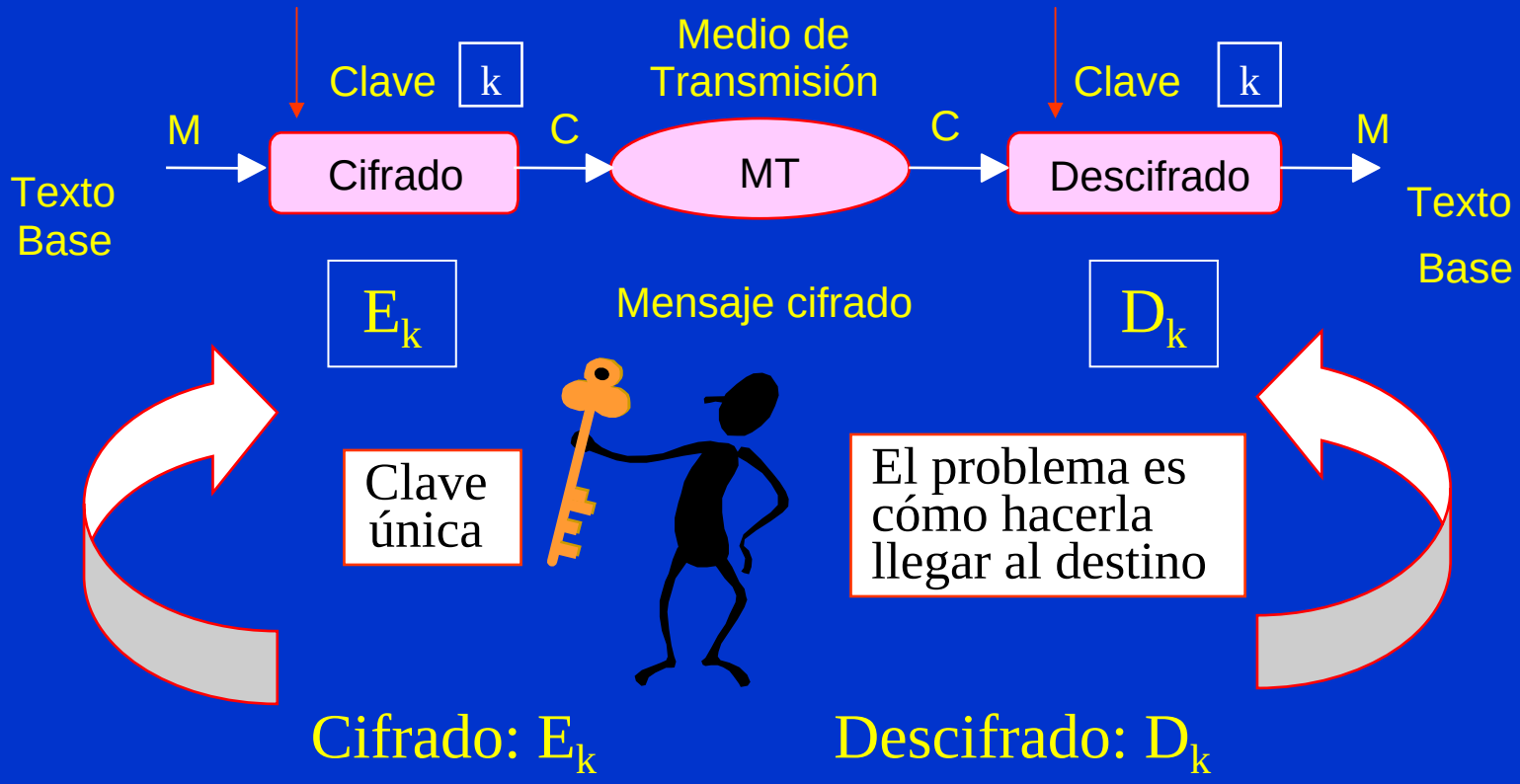
- Vamos a ver cómo se obtienen en cada uno de estos sistemas de cifra (cifrado con clave secreta o sistemas simétricos y cifrado con clave pública o sistemas asimétricos) los dos aspectos más relevantes de la seguridad informática:

La confidencialidad y la integridad de la información

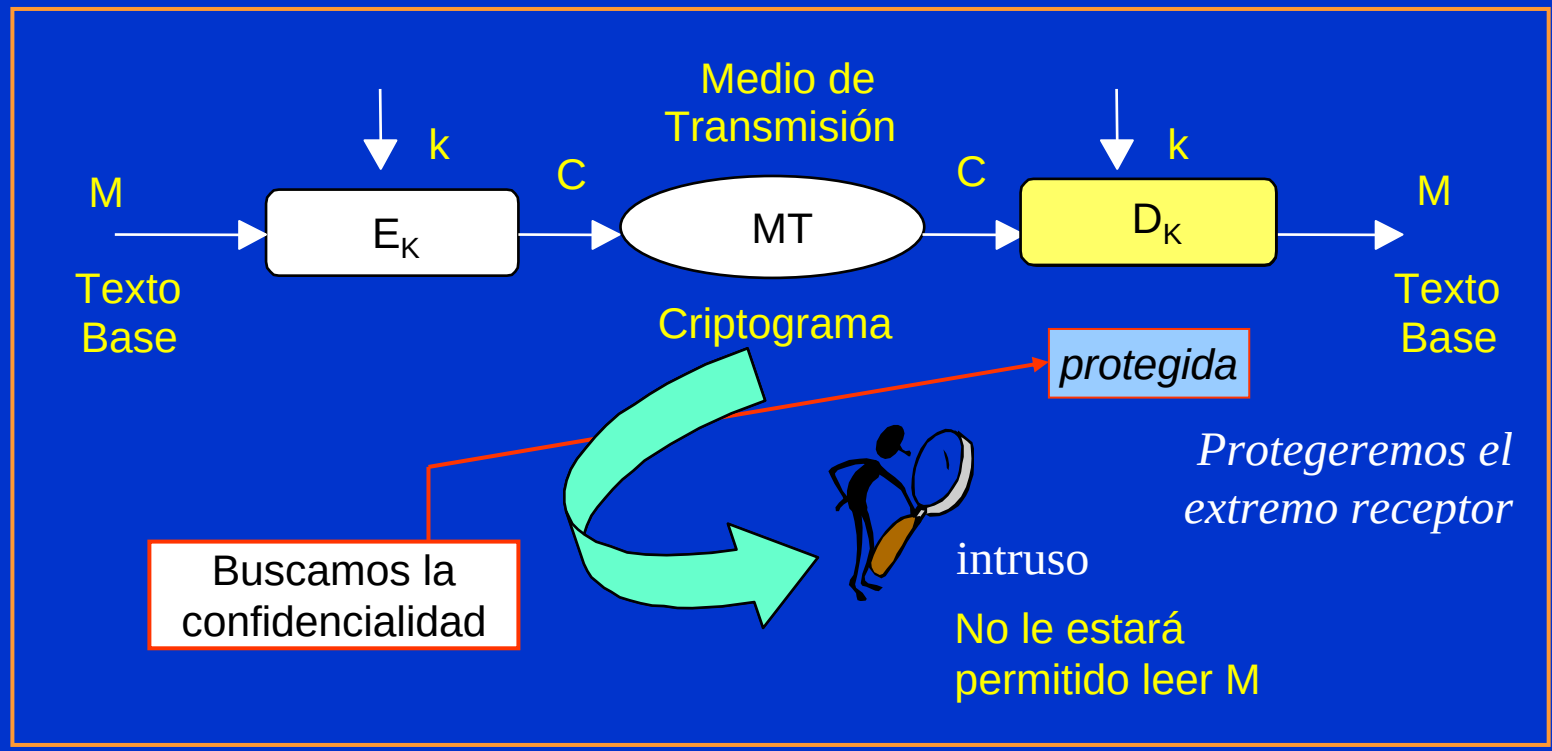


Llegaremos a un concepto de mucha utilidad en criptografía al analizar el sistema con clave pública...

Criptosistemas de clave secreta

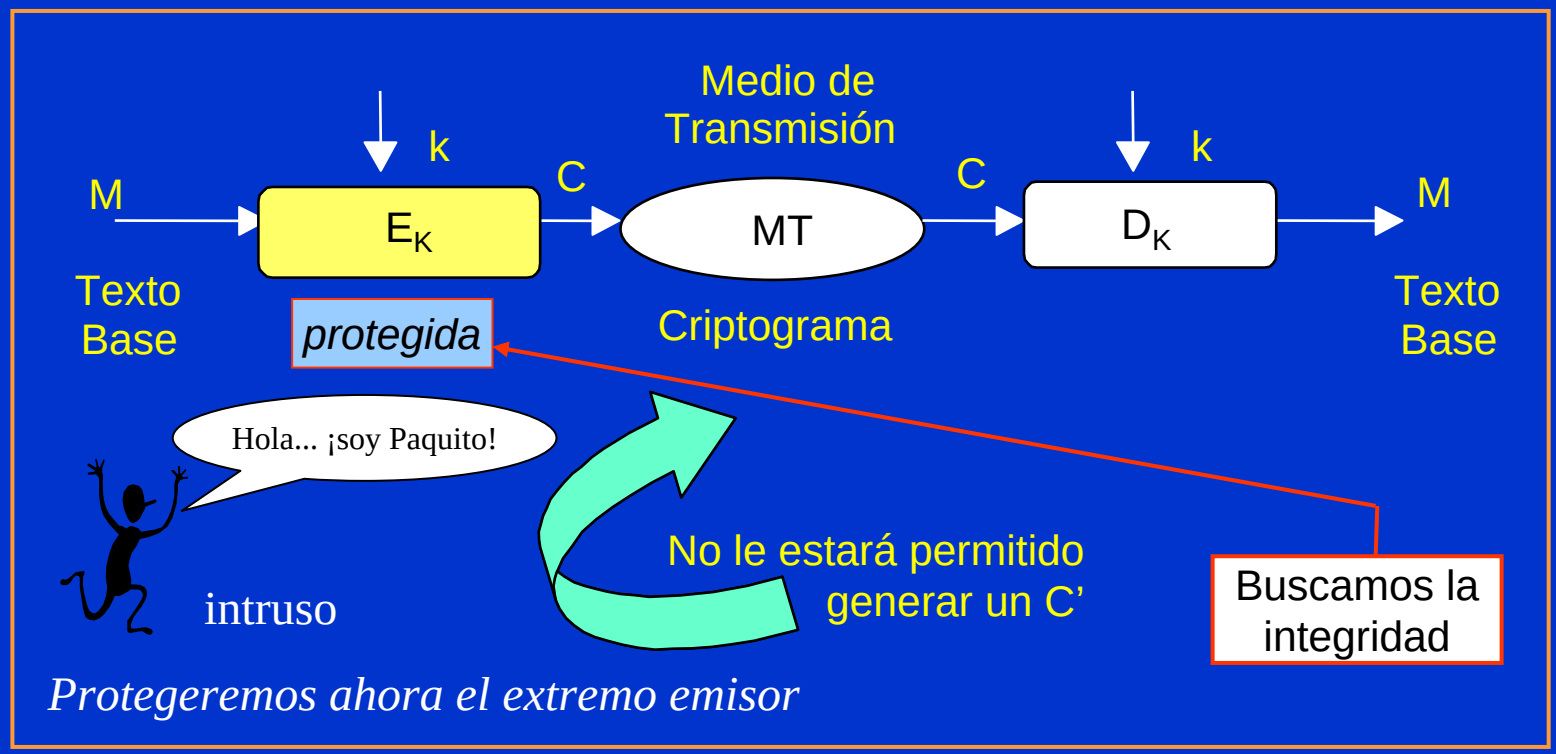


Confidencialidad con clave secreta



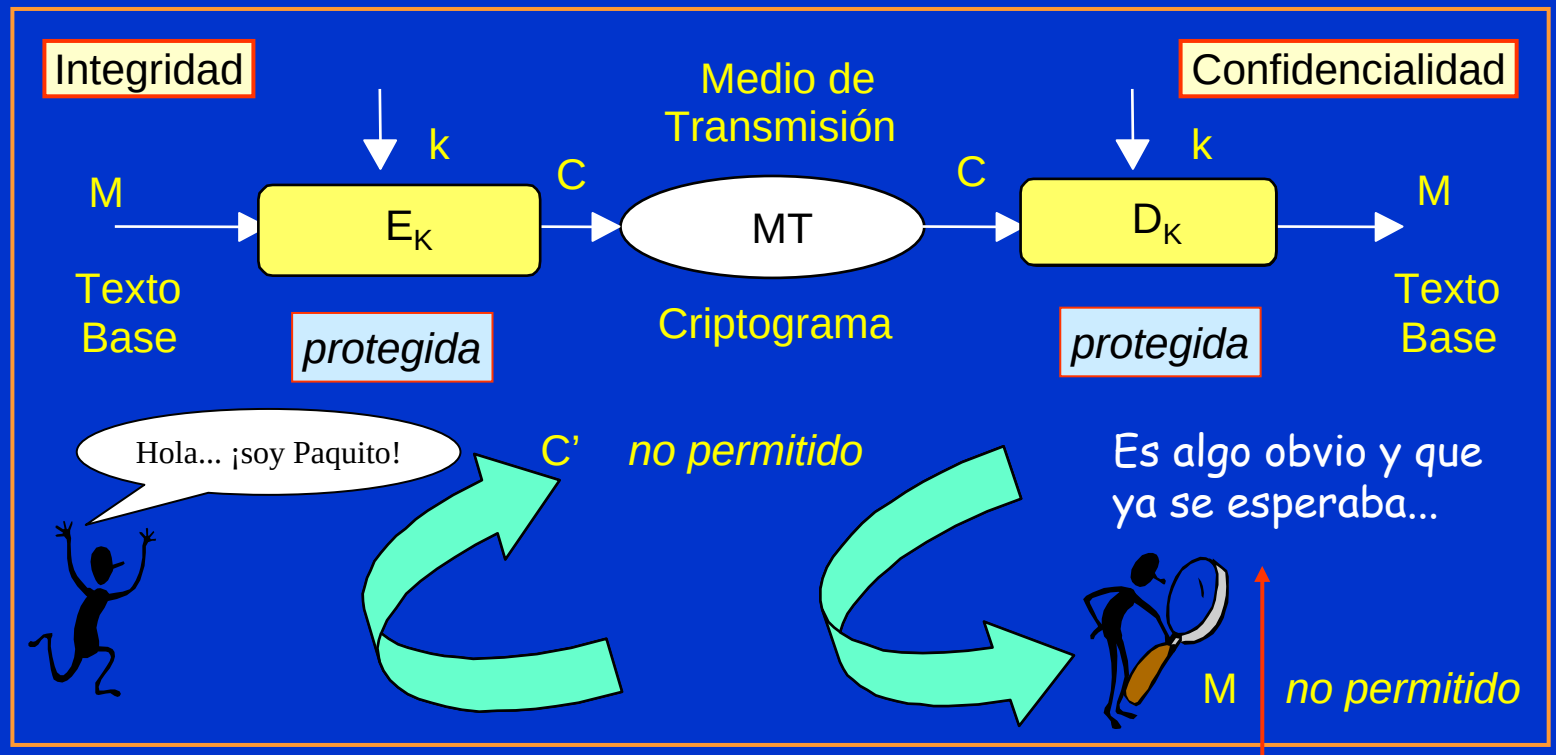
El criptoanalista no podrá descifrar el criptograma C o cualquier otro texto cifrado bajo la transformación E_K.

Integridad con clave secreta



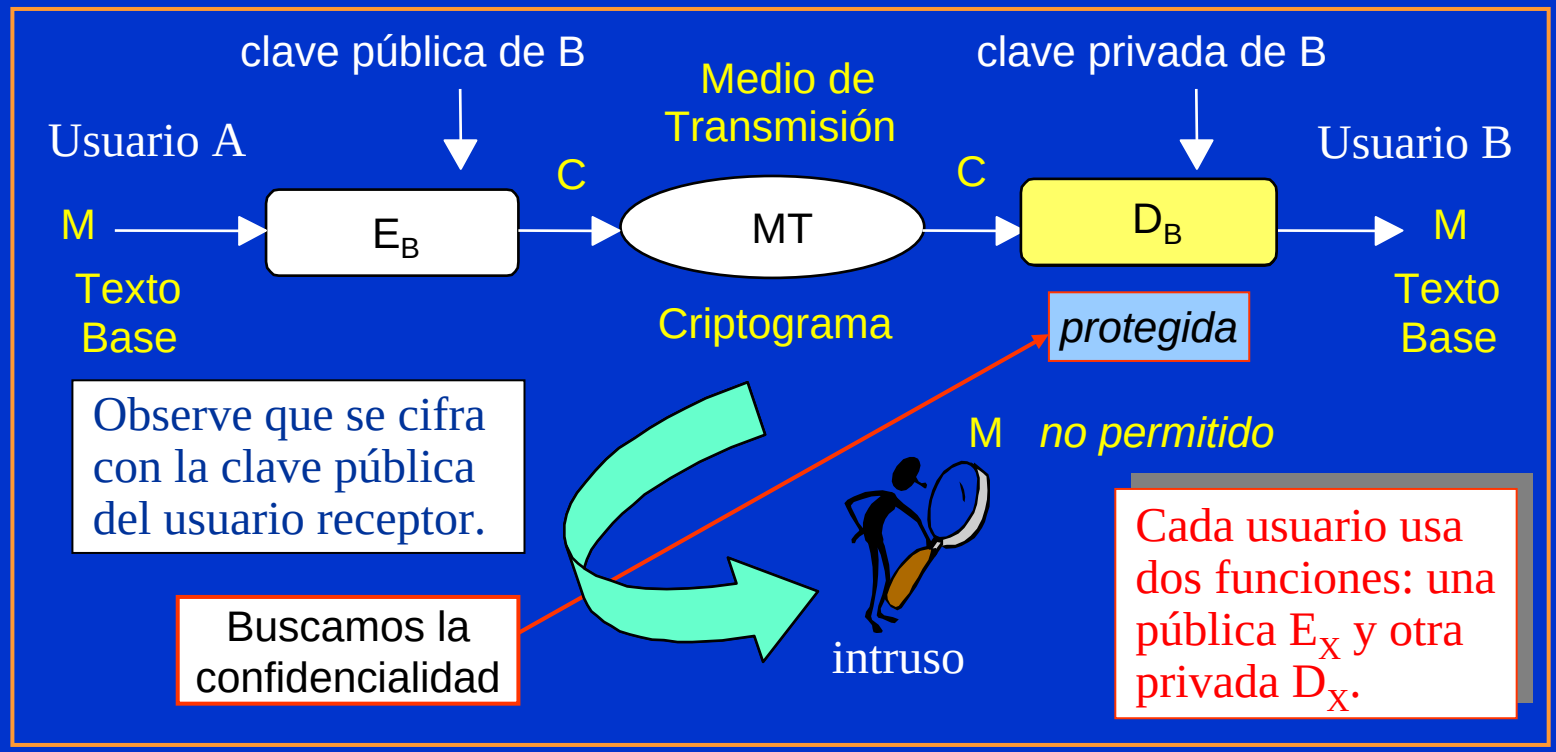
El criptoanalista no podrá cifrar un texto en claro M' y enviarlo al destinatario como $C' = E_K(M')$.

Resumen para sistemas de clave secreta



La confidencialidad y la integridad se lograrán simultáneamente si se protege la clave secreta.

Confidencialidad con clave pública

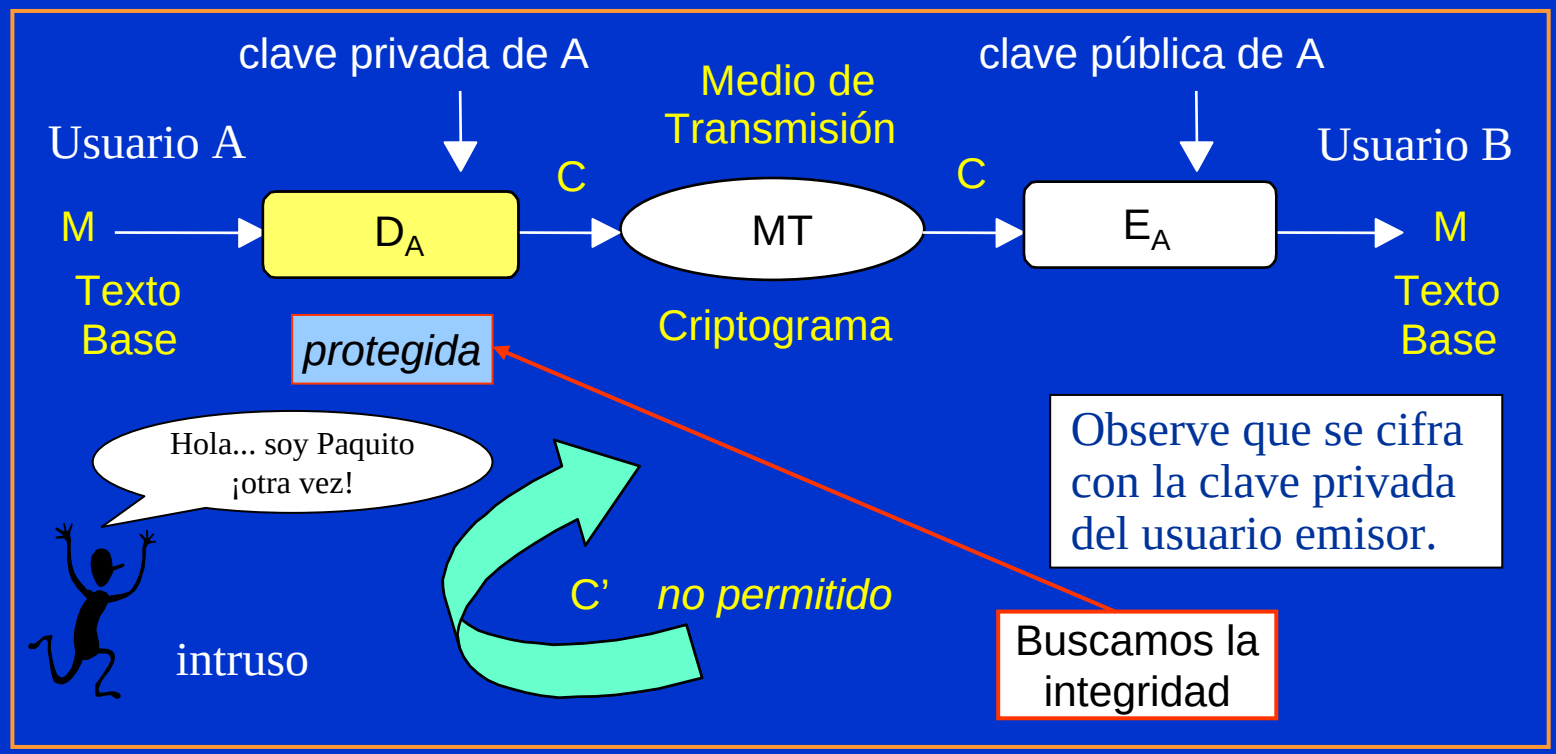


$$C = E_B(M)$$

$$M = D_B(C) = D_B(E_B(M))$$

E_B y D_B son operaciones inversas dentro de un cuerpo

Integridad con clave pública

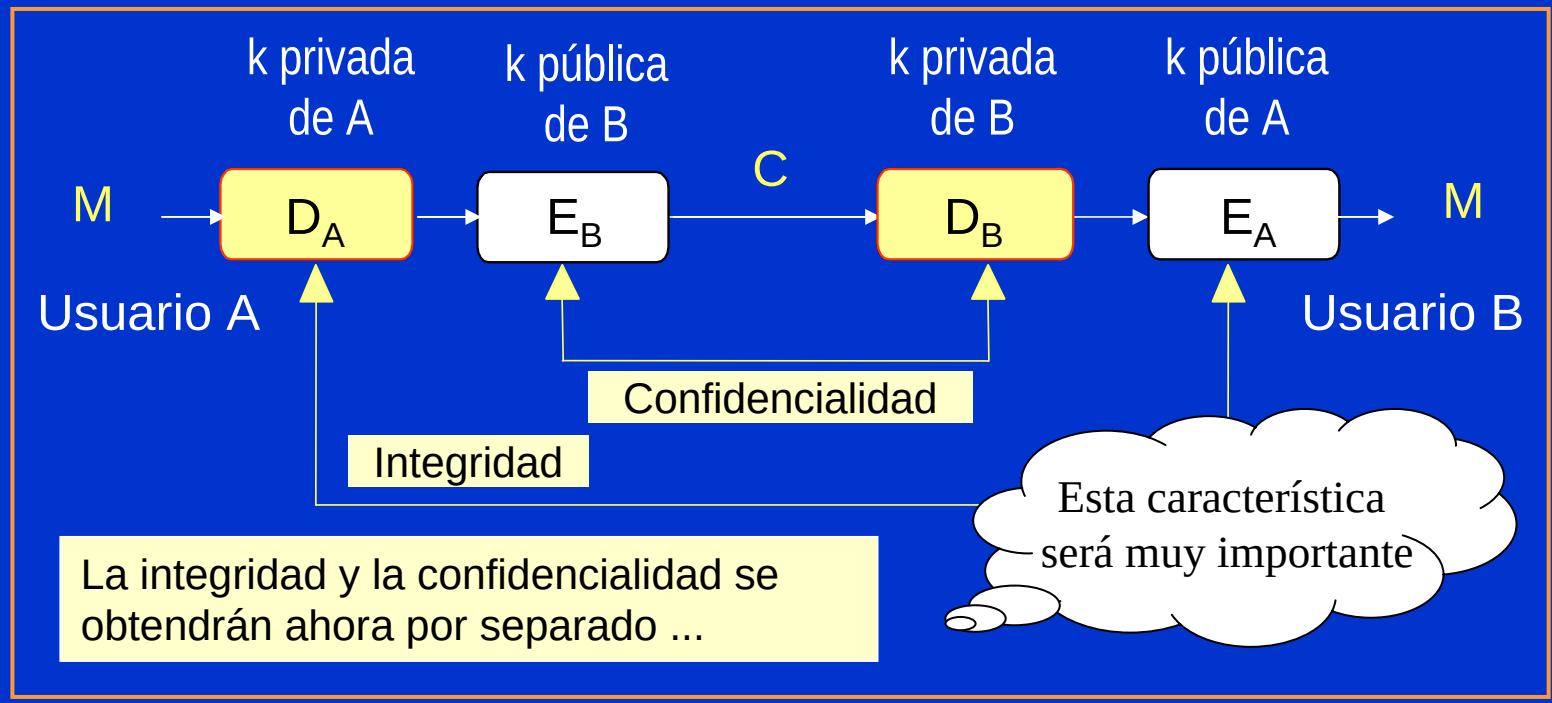


$$C = D_A(M)$$

$$M = E_A(C) = E_A(D_A(M))$$

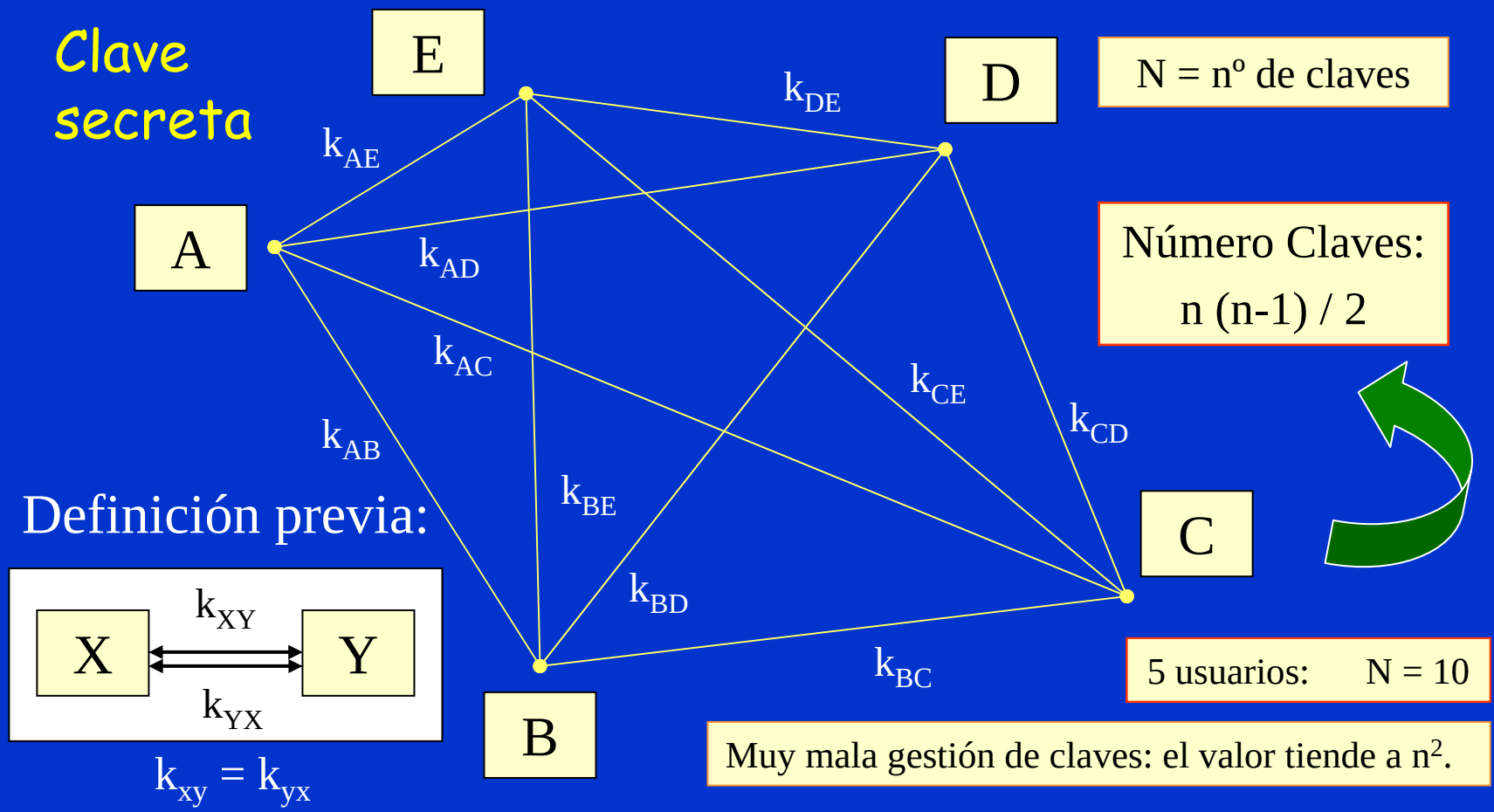
D_A y E_A son operaciones inversas dentro de un cuerpo

Resumen para sistemas con clave pública



$C = E_B(D_A(M))$	Cifrado del mensaje con firma digital
$M = E_A(D_B(C))$	Descifrado y comprobación de firma

Gestión de claves en sistemas simétricos



La solución híbrida

¿Es entonces la clave pública la solución a todos nuestros problemas?

¡ NO !

- Tendrá como inconveniente principal (debido a las funciones de cifra empleadas) una tasa o velocidad de cifra mucho más baja que la de los criptosistemas de clave secreta.

¿Solución?

Sistemas de cifra híbridos
Los esquemas actuales de protocolos seguros en Internet, redes y entornos de cómputo personal (PC) funcionan así.

Fin del capítulo

Cuestiones y ejercicios (1 de 2)

1. Un empleado poco satisfecho ha robado varios discos duros de muy alta calidad con datos de la empresa. ¿Qué importa más, el costo de esos discos o el valor de los datos? Justifique su respuesta.
2. En una empresa se comienza a planificar estrategias de acceso a las dependencias, políticas de backup, de protección de los equipos ante el fuego, agua, etc. ¿Eso es seguridad física o lógica? ¿Por qué?
3. En nuestra empresa alguien usa software pirata. ¿Es una amenaza de interrupción, interceptación, modificación o de generación?
4. Una clave de sesión en Internet para proteger una operación de cifra dura 45 segundos. Si alguien intercepta el criptograma, ¿debemos preocuparnos si sabemos que la próxima vez la clave será otra?
5. Si se prueban todas las combinaciones posibles de una clave para romper un criptograma, ¿qué tipo de ataque estamos realizando?

Cuestiones y ejercicios (2 de 2)

6. Si protegemos una clave en el extremo emisor, ¿qué buscamos, la confidencialidad o la integridad? ¿Y si es en el extremo receptor?
7. ¿Por qué en un sistema simétrico se obtienen la confidencialidad y la integridad al mismo tiempo protegiendo sólo la clave?
8. Explique qué significa que en un sistema de cifra asimétrica se obtengan la confidencialidad y la integridad por separado.
9. Si se cifra un mensaje con la clave privada del emisor, ¿qué se obtiene? ¿Y si el emisor cifra con la clave pública del receptor?
10. ¿Tiene sentido que el emisor cifre de forma asimétrica con su clave pública? ¿Qué logramos con ello? ¿Para qué serviría?
11. Queremos comunicarnos 10 usuarios con un sistema de cifra de clave secreta única entre cada dos miembros. ¿Cuántas claves serán necesarias? ¿Es eficiente el sistema? ¿Y si hay un usuario más?