

***Seguridad  
en los  
Sistemas  
Distribuidos***

**Monografía de Adscripción**

**Alumna: Laura V. Domínguez**

**Asignatura: Sistemas Operativos**

**Profesor: Mgter. David L. la Red Martínez**

## Introducción

Desde el *inicio de la era de la computadora moderna* (1945), hasta cerca de 1985, solo se conocía la *computación centralizada*.

A partir de la *mitad de la década de los ochentas* aparecen dos avances tecnológicos fundamentales:

- ✓ Desarrollo de **microprocesadores** poderosos y económicos con arquitecturas de 8, 16, 32 y 64 bits.
- ✓ Desarrollo de **redes de área local (LAN)** de alta velocidad, con posibilidad de conectar cientos de máquinas a velocidades de transferencia de millones de bits por segundo (mb/seg).

Aparecen los **sistemas distribuidos**, en contraste con los *sistemas centralizados*.

- Los sistemas distribuidos necesitan un software distinto al de los sistemas centralizados.
- Los S. O. para sistemas distribuidos han tenido importantes desarrollos pero todavía existe un largo camino por recorrer.
- Los usuarios pueden acceder a una *gran variedad de recursos computacionales*: de hardware y de software.
- Distribuidos entre un gran número de sistemas computacionales conectados.

La evolución de la computación y de las comunicaciones en las últimas décadas:

- Ha hecho más accesibles a los sistemas informáticos.
- Ha incrementado los riesgos vinculados a la seguridad.

La *vulnerabilidad de las comunicaciones de datos* es un aspecto clave de la *seguridad* de los sistemas informáticos; la importancia de este aspecto es cada vez mayor en función de la proliferación de las *redes de computadoras*.

El *nivel de criticidad y de confidencialidad de los datos* administrados por los sistemas informáticos es cada vez mayor:

- Ej.: correo personal, transferencia de fondos, control de manufactura, control de sistemas de armas, control de tráfico aéreo, control de implantes médicos (marcapasos, etc.).

Los sistemas deben funcionar ininterrumpidamente y sin problemas.

- El *sistema operativo*, como *administrador de los recursos* del sistema:
- Cumple una función muy importante en la instrumentación de la seguridad.
- No engloba a todos los aspectos de la seguridad.

- Debe ser complementado con medidas externas al S. O.

La simple *seguridad física resulta insuficiente* ante la posibilidad de acceso mediante equipos remotos conectados.

La *tendencia* es que los sistemas sean *más asequibles y fáciles de usar*, pero la *favorabilidad* hacia el usuario puede implicar un *aumento de la vulnerabilidad*.

Se deben *identificar las amenazas potenciales*, que pueden proceder de fuentes maliciosas o no.

*El nivel de seguridad a proporcionar depende del valor de los recursos que hay que asegurar.*

### **¿Que son los Sistemas Distribuidos?**

**Los Sistemas Distribuidos:** conjunto de computadoras independientes que aparece ante sus usuarios como un sistema consistente y único:

- Se implementa mediante una capa de software que opera sobre el Sistema Operativo: middleware.

Es un sistema de software construido sobre una red: ejemplo WWW: World Wide Web: sistema que ejecuta sobre Internet.

En general se consideran *sistemas distribuidos, en sentido amplio*, a los sistemas en que:

- Existen *varias cpu conectadas* entre sí.
- Las distintas *cpu trabajan de manera conjunta*.

### **Ventajas de los Sistemas Distribuidos con Respecto a los Centralizados:**

\* *Una razón para la tendencia hacia la descentralización es la economía.* Herb Grosch formuló la que se llamaría “Ley de Grosch”:

El poder de cómputo de una cpu es proporcional al cuadrado de su precio:

- ✓ Si se paga el doble se obtiene el cuádruple del desempeño.
- ✓ Fue aplicable en los años setentas y ochentas a la tecnología mainframe.
- ✓ No es aplicable a la tecnología del microprocesador.

La solución más eficaz en cuanto a costo es limitarse a un gran número de cpu baratos reunidos en un mismo sistema.

Los sistemas distribuidos generalmente tienen en potencia una proporción precio / desempeño mucho mejor que la de un único sistema centralizado.

Algunos autores distinguen entre:

- **Sistemas distribuidos:** están diseñados para que *muchos usuarios trabajen en forma conjunta*.
- **Sistemas paralelos:** están diseñados para lograr la *máxima rapidez en un único problema*.

Una *ventaja potencial de un sistema distribuido* es una mayor *confiabilidad*:

- Al distribuir la carga de trabajo en muchas máquinas, la falla de una de ellas no afectara a las demás:
  - La carga de trabajo podría distribuirse.
  - Si una máquina se descompone:
  - Sobrevive el sistema como un todo.

Otra *ventaja importante es la posibilidad del crecimiento incremental o por incrementos*:

- Podrían añadirse procesadores al sistema, permitiendo un desarrollo gradual según las necesidades.
- No son necesarios grandes incrementos de potencia en breves lapsos de tiempo.
- Se puede añadir poder de cómputo en pequeños incrementos.

### REQUISITOS Y AMENAZAS DE SEGURIDAD

Para ser capaz de entender los tipos de amenazas a la seguridad que existen, se necesita efectuar algunas definiciones de los requisitos en seguridad. La seguridad en computadoras y en redes implica tres exigencias:

- **Secreto:** Requiere que la información en un computador sea accesible para lectura solo a los entes autorizados. Este tipo de acceso incluye imprimir, mostrar en pantalla, etc.
- **Integridad:** Requiere que los recursos de un computador sean modificados solamente por entes autorizados. La modificación incluye escribir, cambiar, cambiar de estado, suprimir y crear.
- **Disponibilidad:** Requiere que los recursos de un computador estén disponibles a los entes autorizados.

Los tipos de agresión a la seguridad de un sistema de computadoras o de redes se caracterizan mejor viendo la función del sistema como proveedor de información. Existen cuatro categorías generales de agresión:

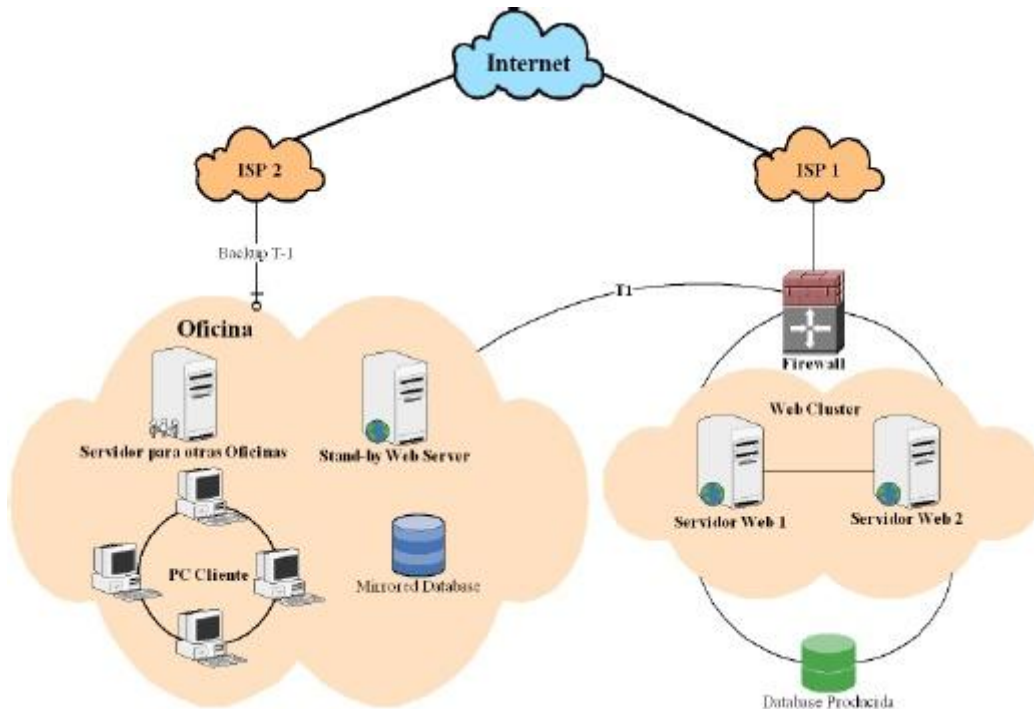
- ✓ **Interrupción:** Un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Esta es una agresión de disponibilidad. Ejemplo de esto es la destrucción de un elemento hardware.
- ✓ **Intercepción:** un ente no autorizado consigue acceder a un recurso. Esta es una agresión a la confidencialidad. Ejemplos de agresiones a la confidencialidad son las intervenciones de las líneas para calcular datos.
- ✓ **Modificación:** un ente no autorizado gana acceso y deteriora el recurso. Esta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos.
- ✓ **Fabricación:** Una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad. Algunos ejemplos son la inclusión de mensajes falsos en una red.

### **¿QUE SE QUIERE PROTEGER ?**

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos.

- ✓ **Hardware:** Entendemos por hardware al conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, discos externos. . .) o tarjetas de red.
- ✓ **Software:** Entendemos por software al conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.
- ✓ **Datos:** Entendemos por dato al conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Generalmente tienen que existir los tres aspectos descritos para que haya seguridad: por ejemplo, en un sistema Unix se puede conseguir confidencialidad para un determinado fichero haciendo que ningún usuario (ni siquiera el root) pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.



Dependiendo del entorno en que un sistema Unix trabaje, a sus responsables les interesara dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondría la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde un disco de back-up) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios no autorizados. En cambio, en un servidor NFS de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: Es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

### Ataques pasivos

Las agresiones pasivas son del tipo de las escuchas o monitorizaciones ocultas de las transmisiones. Existen dos tipos de agresiones: divulgación del contenido de un mensaje o análisis del tráfico.

La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico, un fichero transferido puede contener información sensible o confidencial.

El segundo tipo de agresión pasiva es el análisis del tráfico que es más sutil.

Un medio de enmascarar el contenido de los mensajes es el encriptado. Pero si se tiene protección de encriptado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de las computadoras que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados.

Las agresiones pasivas son muy difíciles de detectar ya que no implican la alteración de los datos.

### **Ataques activos**

Estas agresiones suponen la modificación de los datos o la creación de datos falsos y se subdividen en cuatro categorías: enmascaramiento, repetición, modificación de mensajes y denegación de un servicio.

Un enmascaramiento tiene lugar cuando una entidad pretende ser otra entidad diferente.

Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa.

La repetición supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

La modificación de mensajes significa que alguna porción de algún mensaje legítimo se altere, o que el mensaje se retrase o se reordene para producir un efecto no autorizado.

La denegación de servicio ocurre cuando se produce intencionalmente una saturación de requerimientos falsos sobre, por ejemplo, un servidor, para impedir que el mismo disponga de tiempo para atender adecuadamente a los requerimientos auténticos.

## La necesidad de las políticas de seguridad

Las políticas de alto nivel son pautas sobre la seguridad de la información.

Sin políticas es imposible la creación de sistemas seguros.

Una política de seguridad se divide en los estados de un sistema autorizado y no autorizado.

La institución de políticas de seguridad incluye las leyes, normas y prácticas que regulan cómo una institución gestiona y protege los recursos.

Los sistemas informáticos de la institución deben hacer cumplir estas políticas que se ven reflejadas en sus mecanismos (ej.: el modelo de capas).

✓ **Sistemas Abiertos / Cerrados:**

- En un sistema cerrado, nada es accesible al menos que se autorice expresamente.
- En un sistema abierto todo es accesible a menos que esté explícitamente denegado.

✓ **Menos privilegio (lo que necesita conocer):**

- Deben ser autorizadas sólo para tener acceso a los recursos que necesitan.

✓ **Maximizar el intercambio:**

- Hacer a la información lo más accesible posible.

✓ **Autorización:**

- Las normas explícitas deben definir quién puede utilizar qué recursos y cómo.

✓ **Obligación:**

- Estas políticas definen qué debe o no debe realizarse.

✓ **Separación de los derechos:**

- Las funciones críticas deben ser asignadas a más de una persona o sistema.

✓ **Auditoria:**

- Debe llevar un registro de lo que se hizo y en qué momento.

✓ **Control Centralizado / Descentralizado:**

- En un sistema descentralizado sus divisiones tienen autoridad para definir sus propias políticas.
- ✓ **Propiedad y administración:**
  - Una política administrativa separa la administración de los datos de su uso.
  - La propiedad puede violar la separación de los derechos cuando el usuario de la información también es su administrador.
- ✓ **Rendición de cuentas individuales:**
  - Deben ser identificados y sus actuaciones grabadas y revisadas.
- ✓ **Roles:**
  - Un grupo de derechos que se le da a los usuarios de acuerdo a sus funciones.
- ✓ **Nombre o número dependiendo de su control de acceso:**
  - El acceso de control está designado por su número.
- ✓ **Contenido- dependiendo del control de acceso-:**
  - El acceso a los datos depende de los requerimientos de los archivos específicos.

## **Aplicación - Políticas Específicas**

### **Políticas de confidencialidad:**

- **Clasificación de documentos:** Los documentos son clasificados en función de la sensibilidad de su información.
- **Categorías:** Definen particiones verticales de los niveles.
- **Originator controlled (ORCON):** Un documento sólo se libera a las personas o unidades que estén en una lista específica hecha por el inventor.
- **Acceso a lo total:** Los usuarios están autorizados a leer sólo los valores de los datos agregados.

### **Políticas de integridad:**

- **La integridad de los documentos:** Un documento no puede ser modificado o sólo se puede registrar las modificaciones.

- Cambio limitado: Los datos sólo se pueden modificar en la forma prescripta.

### **Grupo de políticas:**

- Acciones autorizadas: Las personas sólo pueden realizar acciones para las que fueron autorizadas.
- Rotación de los derechos: Una tarea no debe ser realizada siempre por la misma persona.
- Operación de la secuenciación: Los pasos de algunas tareas deben llevarse a cabo en un orden específico.

### **Políticas de conflicto de intereses:**

- Política de Muralla: La información se agrupa en clases de “conflicto de intereses”.
- Conflicto de roles: Un usuario no puede tener dos funciones que pueden implicar un conflicto de intereses.

### **Modelos de seguridad**

- Los modelos de seguridad son más precisos y detallados que la expresión de las políticas.
- Pueden describirse de manera formal o semi-formal.
- Pueden ser obligatorios o discrecionales.
- Una clasificación divide a los modelos:
  - ✓ La matriz de acceso.
  - ✓ Acceso basado en funciones de Control.
  - ✓ Los modelos multinivel.

### **La matriz de acceso**

Es un modelo de seguridad que se puede aplicar a cualquier sistema.

- El modelo define:
  - Un conjunto de sujetos S.
  - Un conjunto de objetos protegidos O.
  - Un conjunto de tipos de acceso T.
- Una combinación (sujeto, objeto protegido, tipo de acceso) o (s, o, t) es una norma de autorización.

- Un amplio modelo de acceso: la autorización de la regla tiene la forma (s, o, t, p, c, f). (sujeto, objeto protegido, tipo de acceso, predicado ,comprobación de derecho, copia de bandera )
- Los sistemas de bases de datos generalmente utilizan un subconjunto (s, o, t, p). (sujeto, objeto protegido, tipo de acceso, predicado)

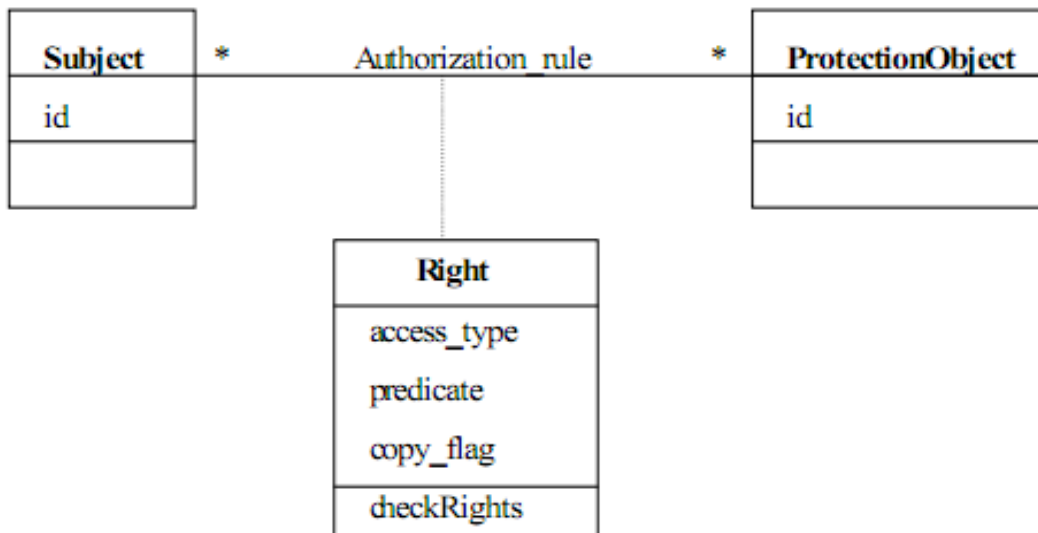


Figura 1.1: The authorization pattern.

- La matriz original de Lampson, tenía el concepto de propietario.
- La matriz de Lampson y su extensión, incluyen las operaciones de modificar la matriz y permiten la propagación de los derechos.
- Harrison, Ruzzo y Uhlman ampliaron y formalizaron este modelo.
- La principal diferencia es la forma en que la matriz es cambiada.

### **Control de Acceso basado en funciones-RBAC (Role-Based Access Control)**

- Puede considerarse como una variación de la matriz de acceso, donde los sujetos sólo pueden ser funciones.
- Los derechos se asignan a las funciones, no a los individuos.
- RBAC convenientemente puede aplicar las políticas de mínimos privilegios, y la separación de funciones.
- También utiliza el concepto de período de sesiones.
- Una manera de hacer cumplir la política de mínimos privilegios es asignar derechos a las funciones de casos de uso.

- Los casos de uso se utilizan para definir un sistema con todos los accesos necesarios para sus funciones.

### **Los modelos multinivel**

- Los datos se clasifican en niveles de sensibilidad y los usuarios tienen acceso de acuerdo con sus autorizaciones.
- Estos modelos se han formalizado en tres formas diferentes:
  - ❖ **El modelo de La Bell-Padula:** *destinado a controlar las fugas de información entre los niveles.*
  - ❖ **El modelo de Biba:** *que controla la integridad de los datos.*
  - ❖ **El modelo de celosía:** *generaliza los niveles parcialmente ordenados de los modelos anteriores utilizando el concepto de matemática de celosías.*

### **Modelo de confidencialidad La Bell-Padula**

- Clasifica los temas y datos en niveles de sensibilidad.
- La clasificación,  $C$ , de los objetos de datos define su sensibilidad.
- En cada nivel superior de acceso de la matriz se va refinando el control de acceso.
- Un nivel de seguridad se define como un par (nivel de clasificación, conjunto de categorías).
- Un nivel de seguridad domina otro si y sólo si su nivel es mayor o igual que las otras categorías y su nivel incluye las otras categorías.
- Dos propiedades, conocidas como “no leer” y “no escribir”, definen un flujo seguro de información:
  - **Propiedad de seguridad simple (ss):** *Un sujeto  $S$  puede leer un objeto  $O$  sólo si su clasificación domina la clasificación del objeto, es decir,  $C(s) \Rightarrow C(o)$ .*
  - **\* Propiedad:** *Un sujeto  $S$  que puede leer un objeto  $o$  se le permite escribir sobre un objeto  $p$  sólo si la clasificación de  $p$  domina la clasificación de la  $o$ , por ejemplo,  $C(p) \Rightarrow C(o)$ .*
    - Este modelo también incluye sujetos de confianza.
    - Son necesarios para el desempeño de las funciones administrativas.
    - Este modelo se complementa con el modelo de integridad Biba.

### El modelo de integridad Biba

- ✓ Clasifica los datos en los niveles de integridad.
- ✓ Incluye las propiedades:
  1. **Propiedad de seguridad simple:** *Un sujeto  $S$  puede modificar un objeto  $o$  sólo si  $(s) > = I(o)$ .*
  2. **Integridad \*- propiedad:** *Si un sujeto  $s$  tiene acceso para leer un objetos  $o$  con el nivel de integridad  $I(o)$ ,  $s$  puede escribir en el objeto sólo si  $p(o) > = I(p)$ .*

### El modelo de celosía

- Una celosía es una estructura matemática que consta de elementos parcialmente ordenados.
- Cada par de elementos tiene un límite superior mínimo y un máximo límite inferior.
- Las celosías no son estrictamente de orden jerárquico.
- Son más difíciles de aplicar que las jerarquías simples.
- Por todo ello, se utilizan con poca frecuencia en la práctica.

## Criptografía

**La criptografía:** es el arte o la ciencia de escribir en “cifra” o “código”; deriva del griego: kryptos: escondido, oculto; graphos: grafía, escritura.

Es un conjunto de técnicas que permiten tornar incomprensible un mensaje riginalmente escrito con claridad, de tal forma que normalmente solo su destinatario pueda descifrarlo y comprenderlo.

El “desciframiento” requiere el conocimiento de una “llave” o “clave” que es una información secreta conocida por el destinatario.

**El criptoanálisis:** deriva del griego: kryptos: escondido, oculto; analysis: descomposición. Es el arte o la ciencia de determinar la “clave” o de descifrar mensajes sin conocerla.

**La criptología:** deriva del griego: kryptos: escondido, oculto; logos: estudio, ciencia. Es la ciencia que reúne a la criptografía y el criptoanálisis.

### La esteganografía:

- ✓ Trata de ocultar información sensible, a simple vista, contenida en otro tipo de información.

✓ Ejemplo:

- En un archivo gráfico, utilizar el bit menos significativo del color de todos y cada uno de los puntos de la imagen para transmitir cierta información.
- Alguien que vea la imagen no se dará cuenta de nada ya que el cambio que se produce en la imagen no es significativo.

Texto plano:

- ✓ Es el texto que queremos proteger mediante el uso de técnicas criptográficas.
- ✓ El conjunto de todos estos textos se denota como “**m**”.

Criptograma:

- ✓ Es el texto una vez que ha sido transformado mediante alguna técnica criptográfica.
- ✓ Este texto resulta ilegible a no ser que se conozca la clave para volver a recuperar el “texto plano” original. El conjunto de todos estos textos se denota como “**c**”.

**Encriptación:**

- es el proceso que transforma un texto plano en un criptograma.

**Desencriptación:**

- es el proceso que recupera el texto plano de un criptograma.

**Conjunto de claves:**

- es el conjunto de claves que se pueden utilizar para encriptar mensajes empleando un determinado sistema criptográfico.
- se denota como “**k**”.

**Dispositivo de encriptación:**

- es cualquier dispositivo que transforme un elemento de **m** en un elemento de **c**.
- se denota como “**e**”.

**Dispositivo de desencriptación:**

- es cualquier dispositivo que transforme un elemento de **c** en un elemento de **m**.
- se denota como “**d**”.

**Criptosistema, sistema criptográfico o sistema de cifrado:** es el conjunto (**m, c, k, e, d**).

### Alfabeto:

- Es el conjunto de símbolos utilizados en los textos planos o en los criptogramas.
- Los símbolos utilizados en los textos planos y en los criptogramas no tienen que ser los mismos.
- Se denota como:
  - $\Sigma_m$  al alfabeto utilizado en los textos planos.
  - $\Sigma_c$  al alfabeto utilizado en los criptogramas.

### Proceso de encriptación:

Para un criptosistema cualquiera  $(m, c, k, e, d)$ , es un dispositivo de encriptación que será, desde el punto de vista matemático, una *función*:

$$E : M \times K \longrightarrow C \times K \\ (m, k) \longrightarrow (c_k, k)$$

Dado un texto plano y una clave genera un criptograma.

### Proceso de desencriptación:

Para un criptosistema cualquiera  $(m, c, k, e, d)$ , es un dispositivo de desencriptación que será, desde el punto de vista matemático, una *función*:

$$D : C \times K \longrightarrow M \times K \\ (c_k, k) \longrightarrow (m, k)$$

Dado un criptograma y una clave recuperamos el texto plano.

Si se *encripta* un mensaje y luego se lo *desencripta* se debe obtener el texto plano original:

$$D(E(m, k)) = (m, k)$$

➤ Las *claves débiles* ( $k$ ):

- dejan el criptograma igual ó muy parecido al texto plano, ya sea al encriptar una o  $n$  veces consecutivas el texto plano:

$$\exists k \in K \quad E(m, k) = (m, k)$$

$$E^{(k)}(m, k) = (m, k)$$

## Las principales formas de ataques

Las principales *formas de ataques* a un sistema criptográfico son las siguientes:

- Por fuerza bruta.
- Por texto plano escogido.
- A partir de texto plano.
- Análisis por frecuencias

### ✓ **Ataque por fuerza bruta:**

- Si se tiene un criptograma, mediante este método se probarán todas las claves posibles para obtener el texto plano.
- Si el conjunto de posibles claves es alto, este sistema es inviable.
- Normalmente no se lo considera como una forma de criptoanálisis:
  - No busca puntos débiles del sistema criptográfico.
  - Únicamente utiliza todas las claves posibles.

### ✓ **Ataque por texto plano escogido:**

- Consiste en elegir varios textos planos y obtener sus criptogramas asociados.
- Esto implica tener acceso al dispositivo de encriptación, pero no a la clave de encriptación.

### ✓ **Ataque a partir de texto plano:**

- El atacante tiene acceso a textos planos y a sus correspondientes criptogramas.

### ✓ **Análisis por frecuencias:**

- Este tipo de ataque es utilizado para romper sistemas criptográficos simétricos.
- Se basa en:
  - Estudiar la frecuencia con la que aparecen los distintos símbolos en un lenguaje determinado.

- Luego estudiar la frecuencia con la que aparecen en los criptogramas.
- De esta manera establecer una relación y obtener el texto plano.

### **Algoritmos de Criptografía de Datos**

La *criptografía computacional* se usa para garantizar:

- ✓ sigilo de la información.
- ✓ integridad de la información.
- ✓ autenticación del usuario.
- ✓ autenticación de los remitentes.
- ✓ autenticación de los destinatarios.
- ✓ autenticación de actualidad.

#### ✓ **Sigilo de la información:**

- Significa que solamente los usuarios autorizados (personas o procesos):
  - tendrán acceso a la información.
  - podrán tornarla inteligible.

#### ✓ **Integridad de la información:**

- Significa garantizar al usuario que los datos correctos originales no fueron alterados:
  - intencionalmente.
  - accidentalmente.

#### ✓ **Autenticación del usuario:**

- Es el proceso que permite al sistema verificar si una persona o proceso con el que se está comunicando es realmente quien alega ser:
  - persona.
  - proceso.

#### ✓ **Autenticación de los remitentes:**

- Es el proceso que permite a un usuario asegurarse de que el mensaje (datos) recibido fue realmente enviado por el remitente.

✓ **Autenticación de los destinatarios:**

- Consiste en tener una prueba de que un mensaje (datos) enviado fue recibido correctamente por los destinatarios.

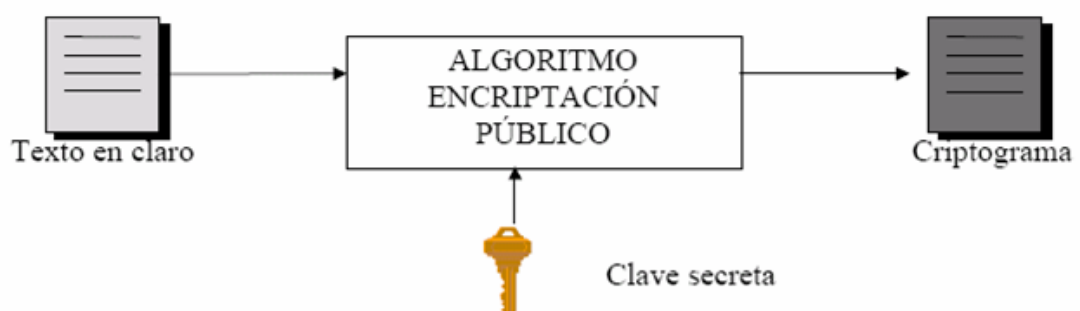
✓ **Autenticación de actualidad:**

- Consiste en probar que un mensaje es actual y no un mensaje antiguo reenviado.

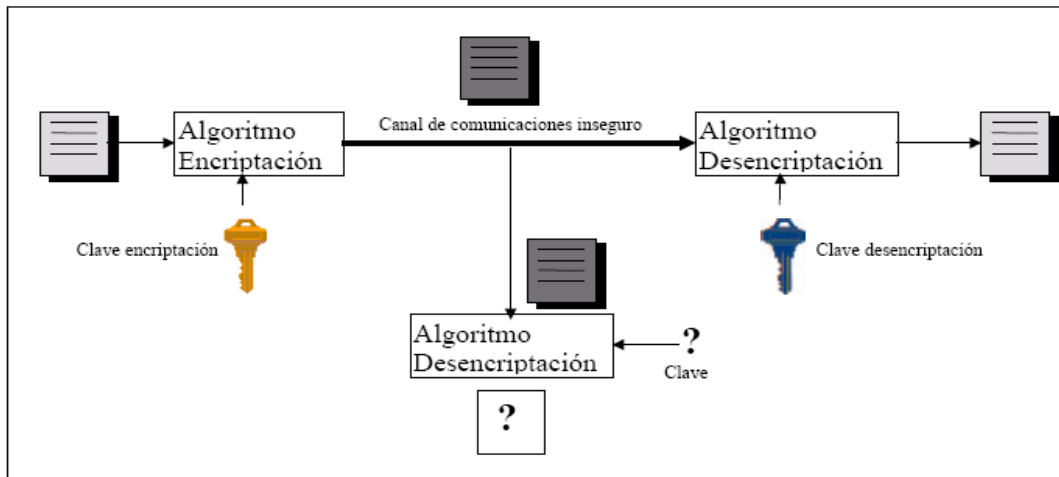
Algoritmo de Encriptación *Secreto*



Algoritmo de Encriptación Público:



Los Algoritmos Públicos son inservibles sin las claves.



### Algunos algoritmos de criptografía de datos

#### *Sustitución monoalfabética:*

- Consiste en cambiar un carácter por otro conforme a una tabla dada.
- La tabla es la “clave de ciframiento”.
- Para campos alfabéticos hay  $26! \cong 4 * 1026$  llaves de ciframiento diferentes.
- La encriptación de cada símbolo es independiente del mensaje.
- Es relativamente fácil de descifrar mediante análisis estadísticos de frecuencias.

Un ejemplo de tabla de sustitución es el siguiente

texto original	texto cifrado	texto original	texto cifrado
a	i	n	a
b	s	o	g
c	n	p	u
d	l	q	y
e	b	r	k
f	q	s	o
g	c	t	x
h	r	u	j
i	d	v	w
j	t	w	h
k	p	x	m
l	e	y	v
m	z	z	f

texto original: centro de computos.

texto cifrado: nbaxkg lb ngzujxgo.

Sustitución monoalfabética de César:

- ✓ Fue utilizada por Julio César para comunicarse con sus generales.
- ✓ Cada letra del texto es sustituida por otra que está tres letras adelante en orden alfabético.
- ✓ La llave de ciframiento es 3, pero se podría usar otra entre 1 y 26.
- ✓ Es fácil de descifrar.
- ✓ Un ejemplo con tabla de sustitución llave 3 es:
  - Texto original: centro de computos siglo xxi.
  - Texto cifrado: fhqwur gh frpsxwrv vljor aal

Sustituciones polialfabéticas:

- La encriptación de cada símbolo del alfabeto depende del mensaje y no resulta siempre en el mismo símbolo encriptado.
- *Sustitución de Vigenere:*
  - Se utiliza una tabla de conversión numérica.
  - Existe una clave como paso intermedio.
  - La tabla es la siguiente:

a	0	j	9	s	18
b	1	k	10	t	19
c	2	l	11	u	20
d	3	m	12	v	21
e	4	n	13	w	22
f	5	o	14	x	23
g	6	p	15	y	24
h	7	q	16	z	25
i	8	r	17		

- la llave podría ser:

m	a	c	k
12	0	2	10

Sustitución “on time pad”:

- ✓ Es una sustitución de Vigenere en la que la clave es tan grande como el texto.

- ✓ Si las letras de la clave se eligen aleatoriamente, la distribución de letras en el texto cifrado es *uniforme*.

### **Funciones unidireccionales**

Son aquellas que satisfacen las siguientes propiedades:

- ✓ Es barato (en tiempo, espacio y dinero) calcular el valor  $f(x)$  de la función en un punto  $x$  dado.
- ✓ Es caro (en tiempo, espacio y dinero), dado  $v$  determinar un  $x$  tal que  $f(x) = v$ .

Una función es *unidireccional* si es:

- ✓ Computacionalmente viable computarla.
- ✓ Computacionalmente inviable computar su inversa.

Una función unidireccional puede ser:

- ✓ *Con secreto*: existe una información (secreto) que torna la computación de su inversa viable.
- ✓ *Sin secreto*: no existe una información (secreto) que torna la computación de su inversa viable.

Para seleccionar una función unidireccional como función de ciframiento, el analista debe suponer que:

- ✓ El algoritmo de ciframiento es de dominio público.
- ✓ Alguien podría tener acceso al texto cifrado.

### **Sistemas criptográficos simétricos o de “llave privada”. El caso del DES**

Un sistema criptográfico es *simétrico de llave secreta* si:

- ✓ La llave de desciframiento es igual a la llave de ciframiento, o.
- ✓ La llave de desciframiento es una función computacionalmente viable de la llave de ciframiento.

La llave sólo debería ser conocida por el remitente y el destinatario de los datos.

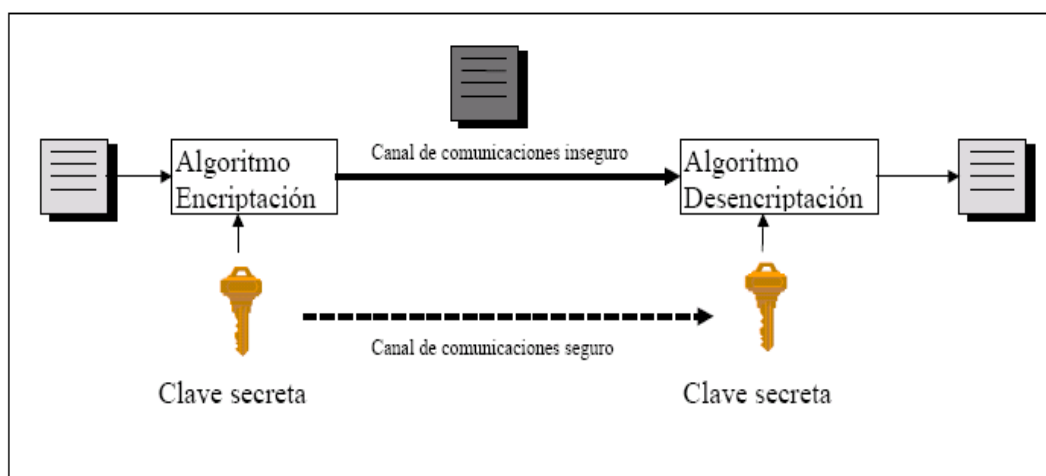
La llave de ciframiento no precisa ser secreta si la función que la relaciona con la llave de desciframiento es computacionalmente inviable.

Las principales *ventajas* son:

- ✓ Los algoritmos son relativamente “fáciles” de implementar.
- ✓ Requieren relativamente “poco” tiempo de cómputo.

La principal *desventaja* es:

- ✓ Las claves han de transmitirse por un canal seguro, algo que puede ser difícil de realizar.



**D.E.S.:** *Data Encryption Standard: Estándar de Ecriptación de Datos:*

- Es un sistema criptográfico simétrico.
- Es uno de los sistemas utilizados por las agencias del gobierno de EE. UU. No relacionadas con la seguridad nacional.
- Fue creado por IBM partiendo del proyecto Lucifer y propuesto al NBS (National Bureau of Standards), hoy NIST (National Institute of Standards and Technology), que lo adoptó en 1977 al igual que el ANSI (American National Standards Institute).
- Está disponible en “chips” pero su exportación está controlada por el Departamento de Estado de EE. UU.
- Cifra bloques de 64 bits en bloques de 64 bits.

Utiliza una clave de 64 bits (8 de paridad, el último bit de cada byte):

- Modificación del NBS, inicialmente eran 128.

Divide los datos o mensajes en bloques de 64 bits y los cifra por separado.

Utiliza un “dispositivo” denominado SBB (Standard Building Block o Constructor Estándar de Bloques):

- ✓ Requiere como entrada un bloque de 64 bits y una clave de 48 bits.
- ✓ Produce una salida de 64 bits.
- ✓ Requiere 16 dispositivos SBB.

Descifrarlo mediante la prueba completa de las claves posibles exigiría  $256 \cong 7 * 1016$  ciframientos.

Considerando que un ciframiento pueda probarse en un microsegundo, que un año tiene  $\approx 3 * 1013 \mu s$  y que las pruebas se hagan *sin paralelismo*: tardaríamos cerca de 2.333 años en determinar una llave con texto conocido.

*Otros criptosistemas simétricos:*

- Australia: Loki, Loki91.
- EE. UU.: RC2, RC4, RC5, Blowfish, Akelarre, Skipjack.
- Rusia: Gost.
- Canadá: Cast.
- Suiza: Idea.
- Bélgica: Rijndael.

## **SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS. EL CASO DEL RSA**

La criptografía *asimétrica* surge para solucionar el problema que tiene la criptografía simétrica:

- ✓ La distribución de la clave: se tenía que hacer mediante un canal seguro, algo difícil de realizar.

Una solución a esto la dieron *Diffie* y *Hellman* en 1976:

- ✓ Su solución proponía utilizar *funciones de un sentido* en canales abiertos.

*Funciones de un sentido*

Supongamos que  $f(x)$  es una función de un sentido, entonces:

- Es fácil el cálculo  $y = f(x)$ , conocido  $x$ .
- Conocido  $y$  es computacionalmente imposible el cálculo de  $x = f^{-1}(y)$ .
- Ej.: *exponenciación modular*:

$$y \equiv g^x \pmod{p}$$

Donde  $g, x \in \mathbb{Z}$  y  $p$  es un número primo con más de 200 dígitos.

La complejidad computacional es  $O(\log p)$ .

La *función inversa* es:

$$x \equiv \log_g y \pmod{p}$$

Su complejidad computacional es de tipo exponencial:

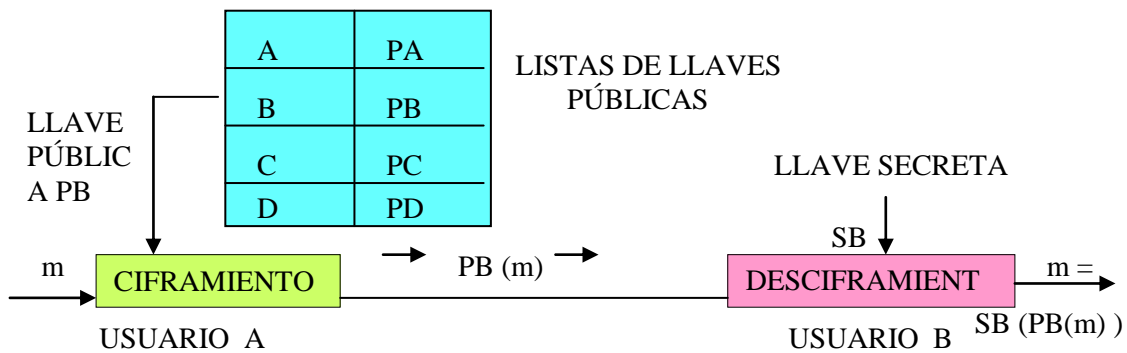
$$O(e^{\sqrt{\log p \log \log p}})$$

Cuando  $p$  tiene un tamaño de más de 200 dígitos es prácticamente imposible el cálculo de esta función.

Se la conoce como *logaritmo discreto* y es de gran importancia en la criptografía asimétrica.

Un sistema criptográfico es *asimétrico* o de *llave pública* si:

- ✓ La llave de desciframiento es distinta de la llave de ciframiento.
- ✓ La llave de desciframiento es una función computacionalmente intratable de la llave de ciframiento.
- ✓ Cada usuario posee:
  - Una llave de ciframiento pública.
  - Una llave de desciframiento secreta.



*Intercambio de Diffie-Hellman*

- ✓ Utiliza la función de exponenciación modular en canales abiertos.
- ✓ Se tienen datos públicos, que conoce todo el mundo, y datos privados, que únicamente conocen aquellos que los han generado.
- ✓ Ambos datos, tanto públicos como privados, se utilizan para generar una clave secreta común que puede ser utilizada en cualquier criptosistema simétrico.
- ✓ Sean **A** y **B** dos personas que desean comunicarse:
  - **A** y **B** eligen un  $n^\circ$  primo  $p$  con más de 200 dígitos.
  - Se elige:

$$g \in \mathbb{Z}/p \text{ tal que } \langle g \rangle = \mathbb{Z}/p$$

- Los valores  $p$  y  $g$  son públicos.
- Tanto **A** como **B** eligen sendos valores aleatorios, privados,  $x_A$  y  $x_B$  tales que:

$$x_A, x_B \in \mathbb{Z}/p$$

- **A** envía a **B**:

$$y_A \equiv g^{x_A} \pmod{p}.$$

- **B** envía a **A**:

$$y_B \equiv g^{x_B} \pmod{p}$$

- Se calcula la clave secreta de encriptación:

$$z_{AB} = z_{BA}$$

- **A** la calcula:

$$z_{BA} \equiv y_B^{x_A} \equiv g^{x_B \cdot x_A} \pmod{p}$$

- **B** la calcula:

$$z_{AB} \equiv y_A^{x_B} \equiv g^{x_A \cdot x_B} \pmod{p}$$

En este esquema los datos públicos son  $p$ ,  $g$ ,  $y_A$ ,  $y_B$ .

En el caso de que alguien quisiera conocer la clave secreta a partir de los datos públicos:

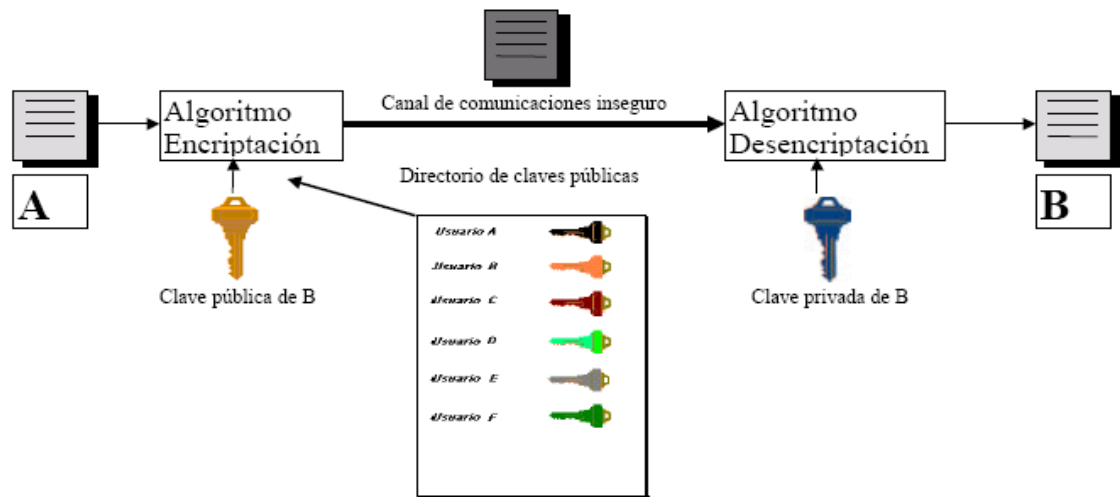
- Tendrá que conocer  $x_A$  o  $x_B$  para generar la clave secreta  $z_{AB}$ :

Lo que equivale a resolver una de estas dos ecuaciones:

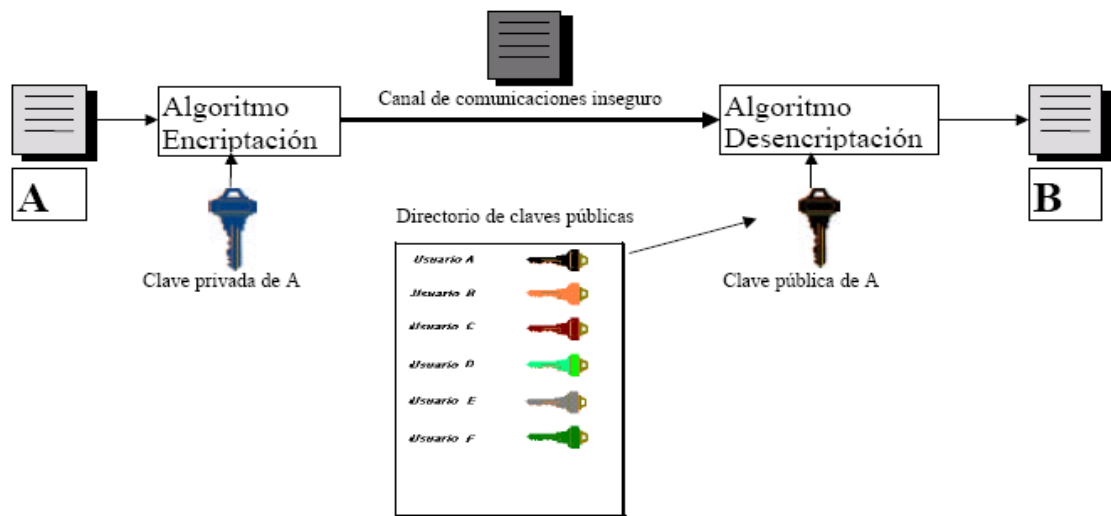
$$x_A \equiv \log_g y_A \pmod{p}$$

$$x_B \equiv \log_g y_B \pmod{p}$$

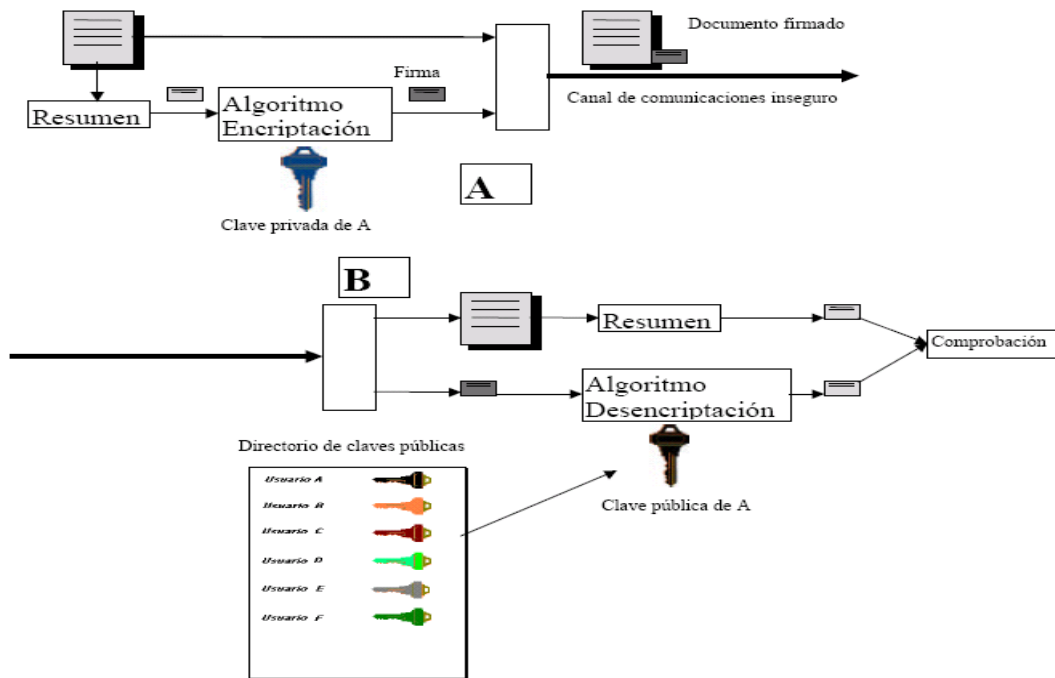
Significa resolver un problema con complejidad computacional exponencial, y dado que  $p$  posee 200 o más dígitos, no es computacionalmente posible.



### Encriptación para **autenticación**



## Encriptación para **firma digital**



## EL ALGORITMO RSA

Este algoritmo es de *clave pública (asimétrico)* y debe su nombre a sus tres inventores:

- **Rivest, Ron.**
- **Shamir, Adi.**
- **Adleman, Leonard.**

Se considera que es el algoritmo público más utilizado y seguramente el más sencillo tanto para su comprensión, como para su implementación.

Este algoritmo basa su *seguridad* en la intratabilidad de la *factorización de números primos grandes (10200)*.

## Descripción del RSA

Un usuario elige dos números primos  $p$  y  $q$  de 200 dígitos aproximadamente, siendo  $n = p \cdot q$ .

Buscamos  $e$  tal que sea primo con:  $\phi(n) = (p - 1) \cdot (q - 1)$ .

Como  $e$  y  $\phi(n)$  son primos entre sí, entonces existe  $d$  tal que:

$$e \cdot d \equiv 1 \pmod{\phi(n) = n + 1 - p - q}$$

$d$  se puede calcular mediante el *algoritmo de Euclides*.

Clave pública:  $(e, n)$ .

Clave privada:  $(d, n)$ .

Los datos que han de mantenerse privados son:

- $p$  y  $q$ ;  $\phi(n)$ ;  $d$ .

Cualquiera que conozca estos datos podrá descifrar los mensajes del propietario de la clave.

Además de estos datos hemos de fijar la longitud de bloque:

- ✓ Longitud del bloque que vamos a cifrar.
- ✓ Longitud del bloque cifrado.

Para romper este criptosistema se pueden intentar varias formas:

- ✓ A fuerza bruta.
- ✓ Mediante un ataque de intermediario.
- ✓ Intentando resolver cualquiera de los dos logaritmos discretos anteriores
- ...

Resolviendo:

- $e \cdot d \equiv 1 \pmod{\phi(46927)}$ .
- Equivale a conocer  $\phi(46927)$ , que a su vez equivale a conocer la factorización en números primos de 46927:

- Es un problema con el mismo grado de complejidad que el logaritmo discreto (problema de tipo exponencial) para números lo suficientemente grandes . . .

*Otros criptosistemas asimétricos:*

- Elgamal, Rabin.

## **Conclusión**

Podemos concluir que en los últimos años el tema de la seguridad en los sistemas se ha tornado en un asunto de primera importancia dado el incremento de prestaciones de los mismos, así como la imparable ola de ataques o violaciones a las barreras de acceso a los sistemas implementados en aquellos. Los "incidentes de seguridad" reportados continúan creciendo cada vez a un ritmo más acelerado, a la par de la masificación de la Internet y de la complejidad del software desarrollado. Teniendo presente que no existe un sistema seguro pero que sí se puede proteger a los sistemas, es que existen métodos para proteger los datos de un sistema y recomendaciones para el uso de dichos sistemas.

Los sistemas seguros deben ser capaces de detectar y responder a esta agresión mientras ocurre y reaccionar ante la misma.

Es importante destacar que no existe un control de seguridad único, sino que las empresas deben contar con diversas capas de seguridad en todos los niveles de su estructura de información, para poder así detectar el problema de seguridad en algunos de estos puntos antes de que el ataque llegue a la información crucial.

## ***Bibliografía***

Cano; Heimy J. Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Universidad de los Andes, Colombia, 1998.

Fernandez Eduardo B, Curso Postgrado Seguridad en Sistemas Distribuidos Florida Atlantic University, Chapter 2, USA 2004.

Fernandez Eduardo B, Curso Postgrado Seguridad en Sistemas Distribuidos Florida Atlantic University, Chapter 8, USA 2004.

Fernandez E.B ; C.Wood; and R.C. Summers. Data base security: requirements, policies, and models. IBM Systems Journal, vol. 19, No 2,229-252,1980.

La Red Martínez David L, Diseño y Administración de Datos ( material de la asignatura Diseño y Administración de Datos).

La Red Martínez David L., Sistemas Operativos, Corrientes 2001.

R. Sandhu et al. Role-Based Access Control models. Computer, vol. 29, No2,38-47, February 1996.

<http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SOF.htm>

<http://www.cs.columbia.edu/~fernando/papers/memoria.pdf>.