



UNIVERSIDAD DE CHILE
Facultad de Ciencias Físicas y Matemáticas
Departamento de Ingeniería Industrial
IN73M –Tecnología de la Información I
Prof.: Juan D. Velásquez
Prof. Aux. Pablo Román y Daniel Varela

Control 2 - Pauta
29 de Agosto de 2006

Indicaciones Generales:

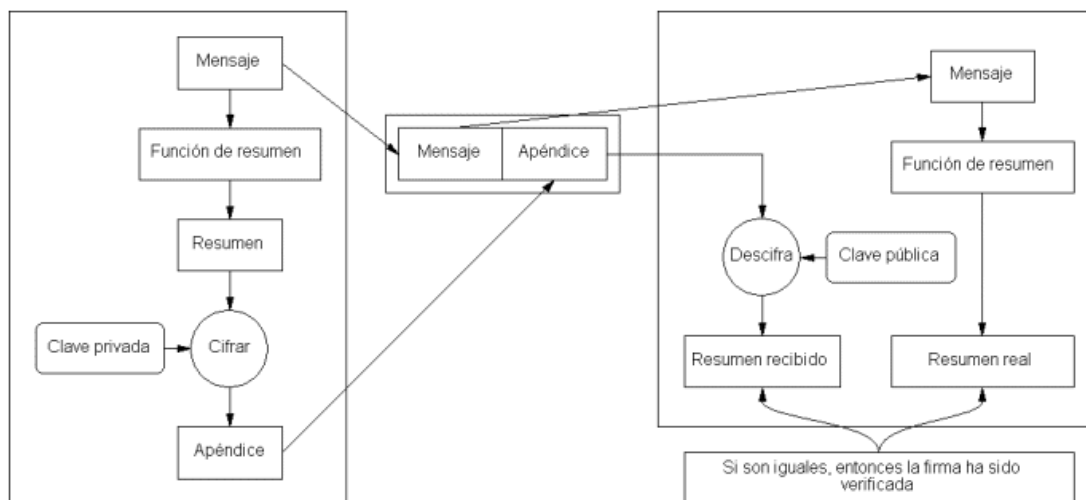
- **Sin Apuntes**
- **Utilice SÓLO las hojas** que se le entreguen para responder cada una de las **partes** del control. No se aceptaran hojas distintas a estas.
- Dispone de 1 hora.

Responda claramente justificando detalladamente sus supuestos cuando corresponda. Note que las preguntas tienen puntajes diferentes.

- a) Explique el funcionamiento la firma digital. Explique tres características de la firma digital **(1 punto)**

R: La firma electrónica es el equivalente digital al concepto legal de la firma en papel, para documentos que se transmiten vía electrónica. Por lo cual la firma electrónica debe cumplir con las siguientes características:

- Autenticación: Ser única tanto para el documento como para el firmante y asegurar que el firmante es el que origino la transmisión.
- No-repudiación: Que el firmante no pueda desdecirse de lo que fue transmitido.
- Integridad: Cambios efectuados mientras se transmite el documento invalidan la firma. Debe tener integridad de datos.



Para ello el diagrama anterior indica el flujo de información necesario para el proceso de acreditación de un documento mediante firma digital, esto funciona mediante un mecanismo de encriptación asimétrica del código hash que constituirá por así decirlo la huella dactilar del documento. La firma digital funciona en base a algoritmos de cifrados, en este esquema existen 3 mecanismos:

1. Un algoritmo de generación de claves
2. Un algoritmo de firmado de documentos
3. Un algoritmo de validación del documento firmado

Los pasos a realizar son los siguientes que se esquematizan en el diagrama anterior son:

1. Generar el resumen del documento (código hash).
2. Encriptar el resumen del documento con la clave privada del emisor.
3. Generar el mensaje que incluye: El resumen encriptado y el documento.
4. Recibir el mensaje extrayendo: El resumen encriptado y el documento.
5. Desencriptar el resumen con la llave publica.
6. Generar el resumen (código hash) con el documento recibido y validar que es el mismo resumen recibido de forma asegurar integridad del mensaje.

Este mecanismo adicionalmente se mejora con:

1. Encriptación/desencriptación del documento vía clave privada/pública en el paso 3-4. Para mejorar los aspectos de seguridad y confidencialidad.
2. Validación por terceras partes de la firma incluida en el mensaje. Es el llamado notario electrónico.
3. Uso de pares de claves distintas para uso de firma y de cifrado del documento.
4. Caducación de las firmas.

b) ¿Qué es y para que sirve un gestor de claves? **(0.5 punto)**

La logística de los procesos de encriptación/desencriptación de mensajes requiere de la administración eficiente y libre de errores de un volumen cada vez mayor de claves. Como es sabido, estas no son simples password de 4 dígitos como uno está acostumbrado a tener, sino que son claves más bien generadas al azar y que caducan el tiempo. Para ello se requiere de un sistema eficiente y automático que efectúe la gestión de los procesos que involucren la seguridad de los cifrados y firmas digitales. Este sistema debe ofrecer las siguientes funcionalidades:

- Administrar la generación de claves.
- Almacenar el histórico de claves generadas.
- Gestionar la caducidad de las claves.
- Distribución de claves. En caso de encontrarse en un ambiente empresarial la distribución de claves es un tema complejo por lo variado de roles y permisos variables en el tiempo.
- Asegurar que las claves se encuentren seguras. Si un tercero logra acceder a este sistema de claves se quiebra la seguridad.

c) Analice la siguiente afirmación. “Para aumentar la seguridad de nuestro sistema de comercio electrónico, aumentaremos de 64 a 128 la cantidad de bits de la clave de encriptación”. ¿Está de acuerdo con esa medida? **(0.5 punto)**

Consideremos los siguientes aspectos:

- **Volumen del problema:** En el comercio electrónico es fácil tener del orden de decenas de miles de solicitudes de transacción por minuto. Las cuales tienen una duración de unos pocos milisegundos en ejecutarse.
- **Mercado Objetivo:** Los usuarios de los sistemas de comercio electrónico son estadísticamente sensibles al tiempo de respuesta del sistema.
- **Costo de Infraestructura:** Mejorar la eficiencia de los sistemas en línea, puede ser resuelta con el uso de servidores mas poderosos y funcionando en paralelo. Sin embargo el costo de esta solución es exponencialmente más costosa a medida que se requiere mayor eficiencia.
- **Costos de Seguridad:** El costo de encriptación de los mensajes a medida que el tamaño de la clave crece es también exponencial. Por lo cual puede llevar a que lo que demora encriptar el mensaje sea mayor a lo que demora en procesarse la transacción.

La disyuntiva entonces esta en balancear el equilibrio entre estas 4 fuerzas. Por ejemplo los bancos que gastan del orden del 10% de sus utilidades brutas en TI y tienen un gran incentivo por securizar las transacciones de sus clientes, efectúan un gran gasto en equipos para poder llevar a cabo todos los procesos de encriptación y de transacciones necesarias. Por otro lado empresas de retail menores dejan este tema a un tercero como es webpay para las transacciones criticas y las menores las mantienen con un bajo grado de encriptación. Esta claro que es más difícil romper las claves mientras mas grande es la llave de encriptación, sin embargo con una política de renovación de clave adecuada se obtiene un grado de seguridad suficiente para fines pedidos.

d) ¿Qué es y para que sirve un Sistema Administrador de Bases de Datos Relacionales?
(0.5 punto)

Un Sistema Administrador de Base de Datos Relacionales (SABDR) es un software diseñado para los siguientes propósitos:

- La administración de datos acumulados en un repositorio persistente.
- Ejecución de consultas sobre esos datos de numerosos clientes.
- Los datos almacenados cumplen con las restricciones de un modelo relacional.
- Ejecución de operaciones transaccionales sobre los datos y su estructura.
- Seguridad de datos.
- Las consultas posibles se canalizan a través del lenguaje SQL, el cual esta diseñado de acuerdo al modelo relacional.
- Integridad y consistencia de datos.
- Tiene capacidades de computar operaciones (filtrado, ordenamiento, etc.) entre conjuntos de datos.
- Controlar el acceso a los datos de acuerdo a diferentes perfiles y administrar la seguridad de las claves de acceso a ellos.

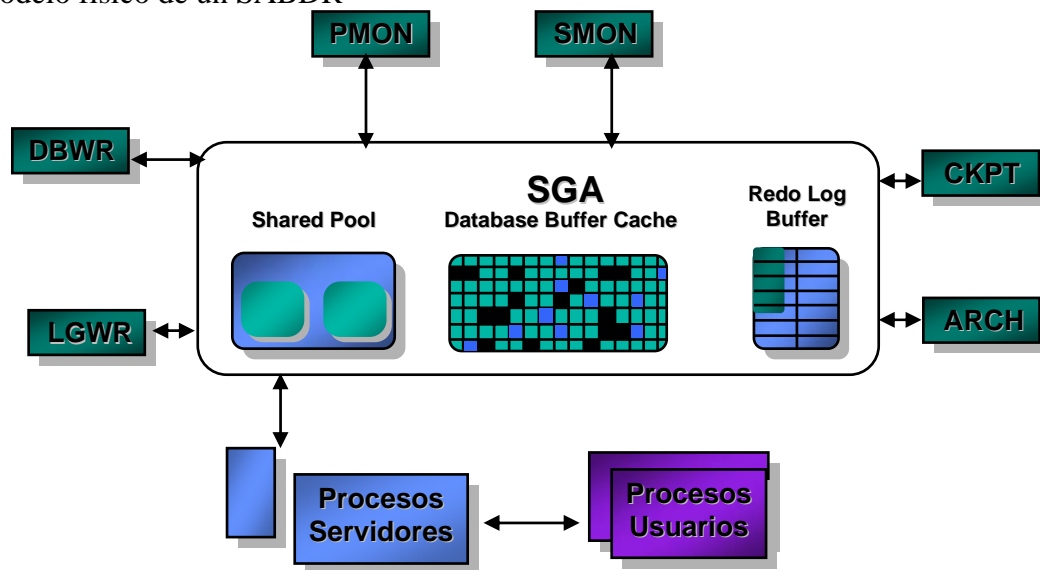
El modelo relacional se aplica en este contexto considerando tablas de datos (pueden considerarse un símil a tablas excel) que se consideran entidades cuyas columnas representan sus atributos, las cuales tienen relaciones entre ellas las cuales son subconjunto

del producto cartesiano entre ellas. Este conjunto de entidades y relaciones se mapea en las bases de datos relacionales manteniendo las relaciones entre ellas como restricciones de consistencia de los datos y las entidades como tablas de datos.

Se ha visto que si trabaja con los datos bajo este esquema entonces se obtienen las siguientes ventajas:

- Es relativamente fácil de entender para la contraparte técnica o para un cliente, en comparación con las antiguas formas de modelamiento de datos.
- Elimina la redundancia de los datos.
- Cualquier consulta que por sobre los datos se realice, es posible de ser contestada.
- Ya está estandarizado y los desarrolladores lo entienden fácilmente.
- Permite dimensionar los requerimientos de hardware para la base de datos.

El modelo físico de un SABDR



e) ¿Qué se entiende por “tercera parte de la confianza”? ¿Cómo se implementa? (0.5 punto)

Consiste en la implementación de la firma digital avanzada, en cuanto a disponer de un tercero (autoridad certificadora) que tiene la facultad de confirmar si el certificado emitido es válido. Esta entidad certificadora constituye lo que se denomina un “notario electrónico”, que al igual que su homólogo responde por las firmas emitidas bajo su jurisdicción. En principio esta autoridad deberá además bloquear un certificado en el caso que se pruebe que contiene información falsa o reciba una orden de bloqueo. En resumen este mecanismo permite:

- Que las partes que negocian se identifiquen.
- La confidencialidad y la integridad de los contenidos de sus envíos.
- El no repudio de los compromisos adquiridos por vía electrónica

Los certificados pueden ser de 3 tipos: para personas, para organizaciones, para servidores. Un certificado consta de los siguientes elementos:

- La llave pública que se está firmando.
- Un nombre de quien lo emite (persona, organización o servidor)

- Periodo de validez.
- La ubicación del emisor (URL, dirección, país, ...)
- La Firma digital del certificado (todo lo anterior), que fue emitida por la autoridad certificadora (notario digital) con su llave privada propia.

La implementación de este mecanismo se hace de la siguiente manera en el caso de una interacción de un sitio seguro vía SSL:

1. Cada servidor que utilice SSL debe tener un certificado de servidor.
2. Cuando un browser se conecta a un servidor web, mediante protocolo SSL, el servidor le envía su llave pública dentro de un certificado (el nombre actual del formato del certificado se llama X.509v3).
3. El certificado permite autenticar el servidor, para distribuir su llave pública la que se usará para enviar la información inicial que el cliente envía al servidor.
4. El browser revisa varios campos de los certificados del servidor. Si un campo no corresponde a lo que se espera, puede no permitir la conexión.
5. Por ejemplo, se valida si el certificado tiene una fecha de duración válida.
6. También se valida la dirección del servidor (se valida un campo del certificado con el nombre DNS de la computadora en la que se ejecuta el servidor, comprobando que ese campo sea igual al nombre de la computadora a la que se ha conectado).

f) Mencione y explique dos problemas en el proceso de extracción de información a partir de los datos **(0.5 punto)**

- Desafíos técnicos de integrar datos de fuentes heterogéneas. En la industria es común encontrar en empresas de larga trayectoria, sistemas de diferentes etapas tecnológicas. Es por lo tanto muy común encontrar fuentes de datos de las muy variadas especies: archivos planos, bases de datos muy variadas, bases de datos propietarias, datos distribuidos en la red pertenecientes a terceros, archivos office, etc. El desafío es consolidar toda esta heterogeneidad en un solo repositorio.
- Desafío de consolidar los datos: Elección de un tiempo y de un algoritmo. Debemos centrarnos en transformar los datos en información en cierto hito en el tiempo de consolidación de datos.
- Acceso simultáneo a datos operacionales entorpece la producción.
- Procesamiento de los datos es un proceso lento y la ventana de tiempo disponible es corta.

g) Explique tres características que permitan diferenciar a un sistema operacional de un sistema de información. **(0.5 punto)**

- El sistema operacional (SO) esta orientado a una clase de usuario relacionada con ingreso y modificación de datos operacionales. El sistema de información (SI) esta orientado a la información (ya de carácter más agregado) para la toma de decisiones sobre ellos.
- SO esta orientado a las transacciones, SI esta orientado al análisis.
- SO tiene un uso constante y estable en el tiempo, SI tiene un uso por periodo de intenso uso.

- SO acceso a pocos registros, SI acceso a muchos registros.
- En tiempos de respuestas SO deben ser de segundos y los SI de mas de varios minutos.
- SO tiene muchos usuarios concurrentes, SI tiene pocos usuarios concurrentes.

h) ¿Qué es OLAP? ¿Cuál es su utilidad práctica? **(0.5 punto)**

OLAP: On Line Analytical Processing. Esta orientado a proveer de una respuesta en un tiempo razonable para preguntas que requieren de un análisis sobre el comportamiento del negocio. Estas consultas son de carácter complejo y variado ya que están sujetas a los vaivenes del negocio. Por este motivo las consultas se realizadas son de un carácter dimensional, en el sentido que cataloga los datos en diferentes dimensiones las cuales cruzan de acuerdo al objetivo que se encuentra buscando. OLAP toma una fotografía consistente de los datos operacionales para consolidarlos en un cubo OLAP, el cual básicamente dispone de los registros acumulados y resumidos en una tabla de “fact” en la cual se cruzan con variadas tablas de dimensiones que sirven para agrupar los elementos de la tabla “fact”. Con esta arquitectura se obtiene una fuente de información agregada condicionada a condicionamientos en las diferentes dimensiones.

OLAP soporta:

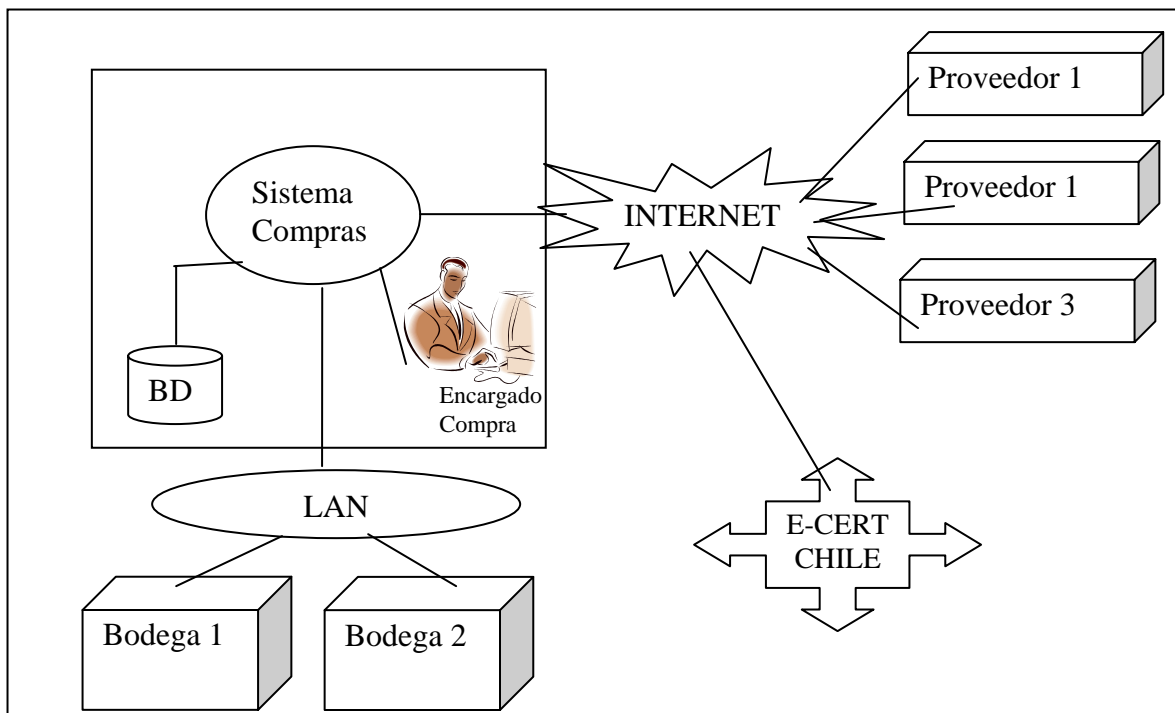
- Vista conceptual multidimensional.
- Transparencia
- Accesibilidad
- Rendimiento consistente para la generación de informes.
- Dimensionalidad genérica.
- Soporte para múltiples usuarios.
- Operaciones sin restricciones entre dimensiones.
- Manipulación intuitiva de los datos.
- Generación de informes flexible.
- Cantidad no acotada de dimensiones y niveles de acumulación

La utilidad práctica es de ser la base para el análisis de estudios de alto nivel como son los estudios de mercado y comportamiento de la organización. Cuyos resultados son claves a la hora de tomar decisiones estratégicas.

i) ACME Inc. es una empresa de retail desea establecer una relación B2B con sus proveedores, para lo cual está buscando un método que les permita implementar un sistema de ordenes de compra seguro. En la actualizada, el proceso de compra de insumos se inicia con la creación de un documento de inventario, el cual posee una lista de todos los productos que están bajo cierto stock. Luego la planilla es dividida de acuerdo a los productos que cada proveedor posee, generándose un documento por proveedor u orden de compra por proveedor. Finalmente, es el encargado de compra de cada línea de producto en ACME es quien firma la respectiva orden de compra, escribe su rut, y se la envía al proveedor, quién ya conoce y mantiene un registro de cada firma del personal autorizado para compra de sus clientes.

Para esta situación, explique cómo se podría automatizar el proceso de compra, brindando seguridad, no repudiación de la orden y autenticación de las partes involucradas (1.5 punto)

Se diseña el sistema de órdenes de compra en base a las operaciones actuales que incluye además la incorporación de un mecanismo de firma digital avanzada para la autenticación y no-repudiación de las órdenes de compra.



El sistema funcionaría de la siguiente manera:

- Las bodegas actualizarían día a día la base de datos de inventario de ACME.
- Periódicamente el encargado de ventas revisa el reporte “Documento de Inventario” el cual muestra los niveles críticos de productos en inventario. El encargado de compra tiene un acceso al sistema restringido bajo un mecanismo de autenticación que puede ser una tarjeta inteligente o sensor biométrico.
- Según sea la política, a través del sistema de compras genera una orden de compra por proveedor de productos. Esta orden lleva incorporada el certificado digital de ACME con el cual se firma el documento “Orden de Compra”. Posteriormente se encripta con clave pública de forma de tener un grado de seguridad en el proceso.
- Debido a que es un negocio electrónico B2B cada proveedor recibe como parte de la funcionalidad de sus sistemas el documento firmado con el certificado digital de ACME y validado en línea por E-CERT quien es la tercera parte de la confianza en este proceso. E-CERT valida este proceso debido a que se encuentra así provisto en la legislación vigente.

El proceso así definido dispone de no-repudiación y autenticación de las OC.