

# Capítulo III. Seguridad de la información

## 3.1 Introducción

Hasta hace muy poco, para la mayoría de las organizaciones, la seguridad era cuestión de proteger el acceso a los datos corporativos. Lo importante era impedir que personas no autorizadas tuvieran acceso a información exclusiva o que pudieran provocar algún daño a tal información. A principios de la década de 1980, los sistemas de información evolucionaron de tal manera que se incorporaron a redes en donde la información se podía compartir. Esto trajo consigo una serie de vulnerabilidades ya que, desde el momento que un sistema se encuentra en red, es potencialmente susceptible a ser atacado. Junto con este crecimiento en los sistemas en red surgió también el crecimiento de una nueva industria dedicada a proteger todos esos puntos de acceso vulnerables a ataques. Lo anterior refiere a la industria relacionada con la seguridad de la información.

Una manera de comenzar este tema es definiendo lo que es seguridad. Cardlogix (2004) la define de la siguiente manera: “Seguridad es básicamente la protección de algo que tiene valor para garantizar que no sea robado, perdido o alterado”.

La seguridad en los datos implica aspectos tanto técnicos como sociales. El primero involucra el cómo y qué tanto aplicar seguridad a cierto costo razonable. El aspecto social trata temas como la libertad del individuo, preocupaciones sociales, estándares legales y cómo la necesidad de privacidad las intercepta.

### Seguridad de la Información

“La seguridad de la información es la aplicación de medidas que procuren la seguridad y privacidad de los datos por medio del manejo de su almacenamiento y distribución” (Cardlogix, 2004).

El concepto de seguridad se está volviendo cada vez más sofisticado. En lugar de limitarse a pensar en barreras de seguridad para proteger la información, se empieza a pensar mucho más en los principios subyacentes que se deben aplicar a la información y a los servicios que necesitamos proteger y a los cuales se quiere conceder acceso. Estos principios se han aplicado gracias a los mecanismos de seguridad en los datos que han surgido a raíz de esta problemática.

### ***3.2 Elementos de la seguridad de los datos***

En el proceso de la seguridad de los datos intervienen cuatro elementos importantes que se describen a continuación (Cardlogix, 2001):

1. **Hardware** – Incluye todo lo tangible involucrado en el manejo de la información como servidores, dispositivos de almacenamiento masivo redundantes, líneas y canales de comunicación segura, tarjetas inteligentes y dispositivos remotos que funcionan como interfaces entre el usuario y las computadoras.
2. **Software** – Es todo lo intangible que tiene relación con los datos a proteger. Incluye los sistemas operativos, sistemas de administración de bases de datos, programas de comunicación y de seguridad.
3. **Datos** – Es el elemento que se quiere proteger. Puede incluir desde archivos sencillos hasta bases de datos grandes.
4. **Personal** – Incluye a toda persona que tenga de alguna forma, relación con los datos en cuestión. Esto incluye a los usuarios y generadores de datos, al personal profesional, personal de oficina, personal administrativo y personal técnico.

### **3.3 Mecanismos para la seguridad de los datos**

Entre los servicios o mecanismos que permiten la construcción de una solución segura para el intercambio de información se encuentran los siguientes (Cardlogix, 2001; Nash, Duane, Joseph & Brink, 2002):

- 1. Integridad de Datos** – Este mecanismo responde a la pregunta “¿Están mis datos intactos?”. Por medio de éste, se asegura que los datos no se han perdido o han sido alterados durante su transferencia. Esto se realiza verificando las características del documento y la transacción. Tales características son inspeccionadas y confirman su contenido y correcta autorización. La integridad de los datos se logra por medio de criptografía electrónica la cual asigna una identidad única a los datos, como si fuera una huella digital. Cualquier intento de cambiar esta identidad es revelado y proporciona como resultado que el documento (datos) ha sido alterado.
- 2. Autenticación** – Responde a la pregunta “¿Están los datos correctos y provienen de la entidad correcta?”. Este mecanismo verifica las identidades de los usuarios, servidores, dispositivos y sistemas, para asegurar que son genuinos (Clark, 2003). A diferencia de la identificación, la autenticación no necesariamente requiere unicidad, esto es, sólo se exige que se valide una entidad previamente identificada, conservando así la privacidad, por lo que muchas personas, dispositivos o sistemas, pudieran autenticarse con una misma identidad compartida.
- 3. Identificación** – Responde a la pregunta “¿Quién es o quién está enviando los datos?”. Este proceso consiste en reconocer a un individuo en particular. Esto requiere que la persona o proceso encargado de verificar confronte la información presentada con todas las entidades que conoce, para comprobar con quién se está negociando.

4. **Aceptación** – A este mecanismo también se le conoce como “no repudio”. Asegura la imposibilidad de eludir la responsabilidad en la generación o recepción de una transacción. Esto es, que ninguna de las partes involucradas en una transacción pueda negar el envío o la recepción de información. Este mecanismo utiliza generalmente esquemas basados en firmas digitales.
5. **Autorización y Delegación** – Responde a la pregunta “¿Puedo compartir de manera segura estos datos si así lo deseo?”. El mecanismo permite asignar y administrar privilegios de acceso a usuarios y grupos adicionales. La autorización es el proceso de permitir acceso a datos en específico dentro de un sistema. Delegación es la utilización de un tercero para administrar y certificar cada uno de los usuarios de un sistema (Autoridades de Certificación).
6. **Auditoría y Bitácora** – Responde a la pregunta “¿Puedo verificar que el sistema esté funcionando?”. Este mecanismo provee un monitoreo constante y funciones de asistencia a los sistemas de seguridad. Esta es una examinación y almacenamiento independiente de los registros y actividades para asegurar la conformidad con ciertos controles establecidos, políticas, procedimientos operacionales y recomendar cualquier cambio indicado en estos controles, políticas y procedimientos.
7. **Administración**- Este mecanismo permite la administración del sistema de seguridad. Es la vista general y el diseño de todos los elementos y mecanismos involucrados.
8. **Privacidad y Confiabilidad**- Este mecanismo asegura que sólo los emisores y receptores tienen acceso a los datos. Esto se realiza generalmente empleando una o más técnicas de encriptación para asegurar los datos. Confiabilidad es el uso de encriptación para proteger la información de accesos no autorizados. El texto original se convierte en texto cifrado por medio de un algoritmo para luego ser

descifrado de vuelta al texto original, utilizando el mismo método pero en forma inversa.

### **3.4 Criptografía**

Como parte de los mecanismos para brindar seguridad en las transacciones, se encuentra el uso de la criptografía. Esta ciencia parte de la criptología (*criptos* = oculto, *logos* = tratado, ciencia) la cual es el arte de transformar mensajes claros a otros sin sentido alguno. La criptografía significa literalmente “escritura secreta” (Maturana, 2003) y viene del griego *criptos*= oculto, *grafia*= escritura, y aunque se pueden encontrar muchas definiciones de esta palabra, en el campo de la informática, se considera como más comunes las siguientes:

- “La criptografía es el método para convertir datos que están en forma entendible por los humanos a una forma modificada y después devuelta a su forma original, para que su acceso no autorizado sea difícil” (Cardlogix, 2001).
- “Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo sea en absoluto, para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado, sea capaz de entenderlo” (Maturana, 2003).

Los términos “encriptar”, “codificar” y “cifrar” son utilizados indistintamente para referirnos a tales procesos para ocultar información.

Por otra parte, la criptografía se complementa con el criptoanálisis, el cual es la técnica de descifrar textos cifrados sin tener autorización de ellos, es decir, realizar una especie de criptografía inversa para tratar de encontrar las debilidades de los algoritmos y, por consiguiente, aportando a los criptólogos a reforzar sus técnicas de criptografía para hacerlos más seguros. A estos matemáticos e investigadores encargados de romper o encontrar debilidades en los algoritmos se les llama “criptoanalistas”, mientras que a las

personas encargadas de inventar nuevos algoritmos se les llama “criptólogos”. Cuando no se lleva a cabo esta relación criptólogo-criptoanalista se puede tener como consecuencia lo que se conoce como “seguridad en la oscuridad”, lo cual significa que un algoritmo es utilizado sin ser probado previamente por expertos en el área y, por consiguiente, es vulnerable a ser descifrado. Es por esto que, siempre es necesario que un nuevo método de cifrado (algoritmo) se desarrolle a la par de un criptoanálisis para garantizar que nadie lo pueda romper (Nash *et al.*, 2002; Fúster *et al.*, 2001).

### **3.4.1 Tipos de criptografía**

Existen dos tipos de algoritmos criptográficos: simétricos y asimétricos (Nash *et al.*, 2002). En ambos tipos se utilizan llaves criptográficas. Una llave criptográfica es similar a una llave física que se usa para cerrar o abrir una puerta y para cada tipo de cerradura existe una llave con una forma específica que se ajusta a aquella. De igual forma cada algoritmo criptográfico necesita una llave con la extensión correcta (número de bits) y sólo la llave que tenga la longitud y el patrón correcto de bits, podrá permitir que el algoritmo descifre el mensaje.

#### **3.4.1.1 Criptografía simétrica**

Este tipo de criptografía es la más antigua y consiste en tomar el mensaje original como entrada y por medio de una llave generada de manera aleatoria por parte del emisor, se genera un mensaje cifrado. El término “simétrico” se refiere a que esta misma llave la utiliza el receptor para descifrar el mensaje (regresarlo a su forma original). La figura 3.1 muestra el proceso de cifrado y descifrado utilizando criptografía simétrica:

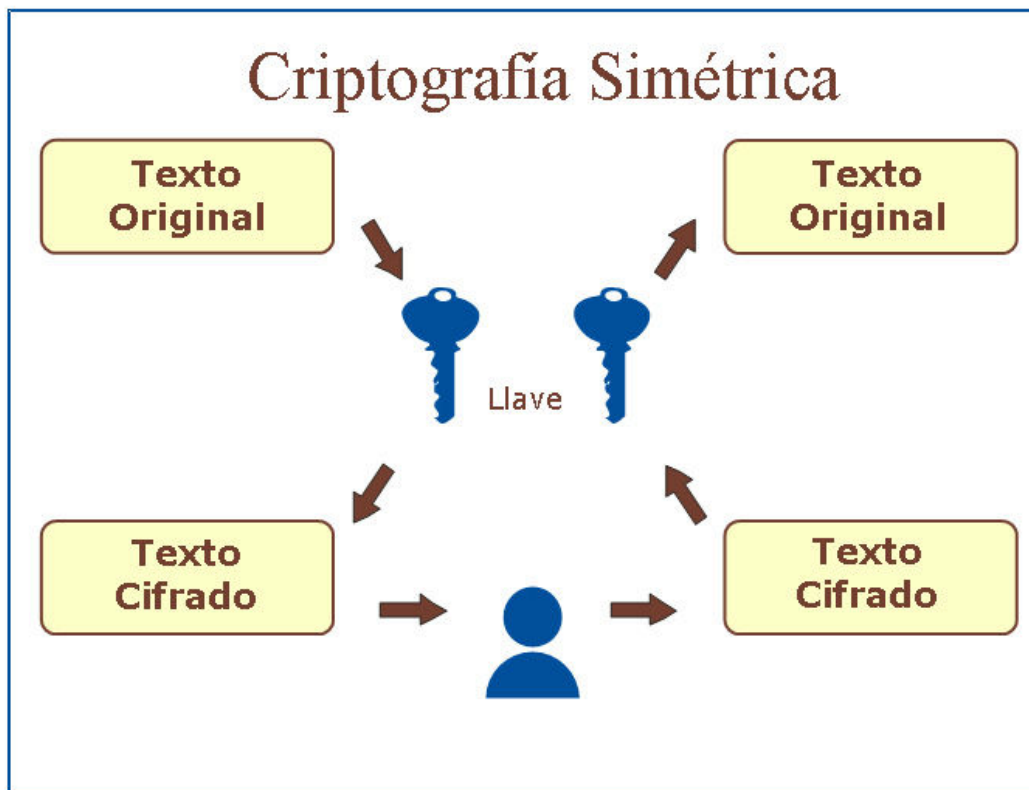


Figura 3.1 Criptografía simétrica

Este tipo de cifrado tiene las ventajas de que es rápido (comparado con el asimétrico) por lo que no impacta mucho en la carga al procesador del algoritmo. El texto cifrado es compacto, ya que generalmente tiene la misma longitud que el texto original y además, es un cifrado seguro. Sin embargo, este tipo de cifrado tiene algunas desventajas, entre ellas que la llave puede ser interceptada por intrusos, debido a que debe enviársele de alguna manera al receptor y esto provocaría que un intruso la capture y pueda descifrar el mensaje. Para cada mensaje que se cifra, se debe generar una nueva llave, dando como consecuencia que el número de llaves que se requiere generar en un ambiente de varios participantes, es aproximadamente el cuadrado del número de participantes, y por lo tanto, no tiene una buena escalabilidad en poblaciones numerosas. Para llevar a cabo esto se requiere una administración compleja de llaves.

### 3.4.1.2 Criptografía asimétrica

La criptografía asimétrica es aquella que emplea algoritmos asimétricos, esto es, que en lugar de usar una sola llave para la realización de la codificación y la decodificación (cifrado y descifrado), se utilizan dos llaves diferentes: una para cifrar, la otra para descifrar. Estas dos llaves son independientes, pero están relacionadas matemáticamente y siempre se generan juntas. El proceso para generarlas es más complejo que en el algoritmo simétrico. El receptor se encarga por anticipado de generar la pareja de llaves, llamadas pública y privada, y se debe encargarse además, de proteger su llave privada. La llave pública la puede conocer todo el mundo ya que por medio de ésta, el emisor genera el mensaje cifrado. Lo importante aquí es que el mensaje no se puede descifrar con la llave pública con la que fue cifrado el mensaje, sino solamente con la llave privada que guarda en secreto el receptor. Dicho en otras palabras, lo que está cifrado con una llave sólo se puede descifrar con la otra. La figura 3.2 muestra el proceso de cifrado y descifrado utilizando criptografía asimétrica.

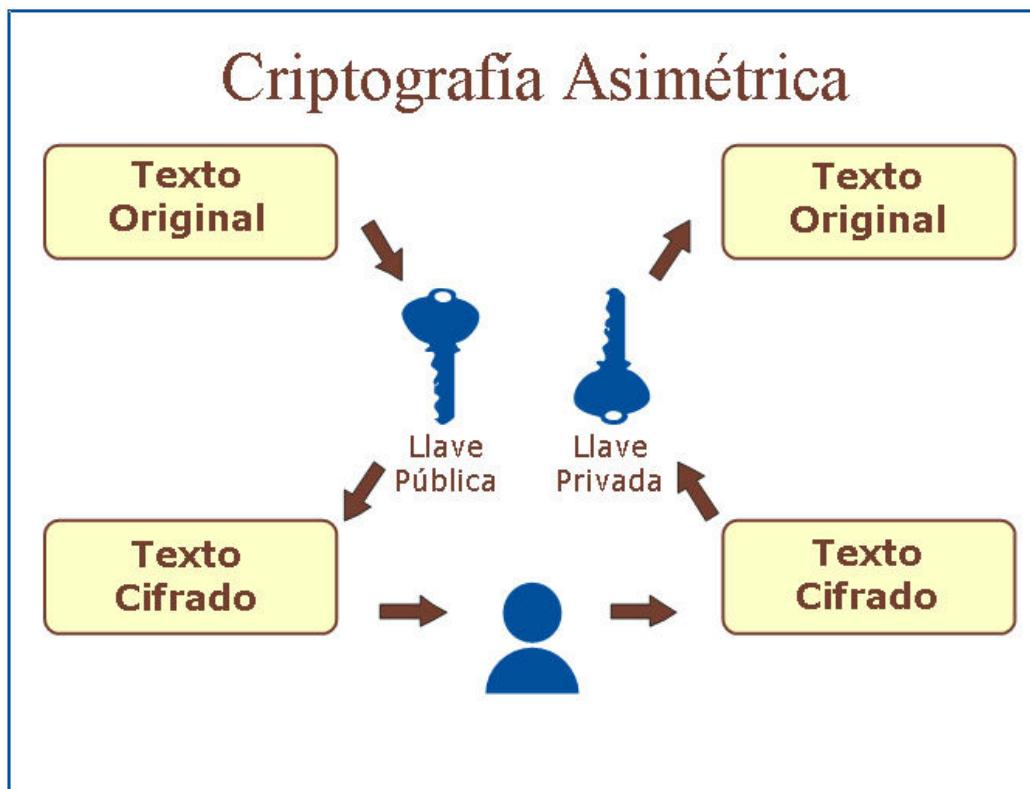


Figura 3.2 Criptografía asimétrica

Este tipo de cifrado es muy seguro y además tiene varias ventajas sobre la criptografía simétrica. Entre estas ventajas están que evita los problemas administrativos de llaves que presenta la criptografía simétrica, ya que cada persona necesita compartir solamente una llave: su llave pública. Además no exige una relación previa entre las partes para hacer el intercambio de documentos cifrados. Por otro lado, dado que no se necesita enviar una llave al receptor (como en el caso de la simétrica), la codificación no sufre por la interceptación de llaves y sólo se puede descifrar el mensaje si se cuenta con la llave privada. Otra ventaja es que soporta firmas digitales y aceptación. Sin embargo, cuenta con algunas desventajas, entre ellas que el cifrado es relativamente lento y además extiende el texto cifrado, requiriendo así más potencia de procesador.

La tabla 3.1 muestra la comparación entre estos 2 tipos de cifrados:

<b>Criptografía Simétrica</b>	<b>Criptografía Asimétrica</b>
Utiliza la misma llave para cifrar y descifrar.	Utiliza una llave pública para cifrar y una privada para descifrar.
El cifrado es seguro.	El cifrado es seguro.
El cifrado es rápido.	El cifrado es relativamente lento.
El texto cifrado es compacto.	El texto cifrado se expande.
La llave que genera el emisor para cada proceso de cifrado debe llegar al receptor (está sujeto a interceptación).	No se necesita enviar una llave al receptor por cada proceso de cifrado, por lo que no sufre por la interceptación de llaves.
El número de llaves que se requiere distribuir es aproximadamente el cuadrado del número de participantes.	El número de llaves que se requiere distribuir es el mismo al número de participantes.
Requiere relación previa entre las partes involucradas.	No exige una relación previa entre las partes para el intercambio de llaves.
No se utiliza para firmas digitales ni de aceptación.	Soporta firmas digitales y aceptación

**Tabla 3.1 Comparación entre criptografía simétrica y asimétrica**

### **3.4.1.3 Combinación simétrico / asimétrico**

Como solución a las desventajas que contienen cada uno de los tipos de cifrado mencionados, en muchas aplicaciones se opta por utilizar una combinación de ambos. Este tipo de cifrado utiliza las ventajas de los dos tipos mencionados anteriormente y como resultante se obtiene un nuevo proceso con las características de velocidad, texto compacto, escalabilidad, facilidad de administración de llaves, resistencia a la interpretación y soporte para firma digital y aceptación.

El proceso de cifrado inicia con la generación de una llave simétrica aleatoria que se utiliza para cifrar la información que se desea enviar. Con este tipo de cifrado (simétrico) aseguramos rapidez y además, el resultado es un texto compacto. Luego, en lugar de mandar la llave generada directamente al receptor, lo cual es inseguro por ser vulnerable a interceptaciones, se utiliza el mecanismo de encriptación de llave pública/privada para cifrar la llave generada anteriormente. Esto con la finalidad de que la llave se envíe en forma segura al receptor, quien debe contar con su propia llave privada. A este proceso se le conoce como “operación de llave empaquetada”. Posteriormente se une esta llave empaquetada con el texto cifrado para enviarlo al receptor. A este proceso se le conoce como “sobre digital”. En dado caso de que un intruso interceptara este sobre, no podrá descifrarlo porque para poder tener acceso a la llave simétrica que descifra el texto, primero necesitaría contar con la llave privada que guarda en forma segura el receptor.

Para el proceso de descifrado, se requiere primero descomponer el sobre digital en las dos partes que lo constituyen: el texto cifrado con criptografía simétrica y la llave empaquetada con criptografía asimétrica. Luego, el receptor debe recuperar la llave empaquetada. Para lograr esto, utiliza su llave privada, permitiendo así que solamente esta persona pueda recuperar la llave empaquetada. Con la llave simétrica extraída, se puede entonces descifrar el texto original que contiene el sobre.

Además de clasificar los algoritmos criptográficos en simétricos y asimétricos, se pueden también clasificar de acuerdo a la manera en que operan. Por ejemplo, Menezes, A., Van

Oorschot, P. & Vanstone, S. (2001) define dos tipos de algoritmos criptográficos de acuerdo al tamaño de entrada de los datos:

1. **De Bloque.** Son aquellos que codifican datos en bloques pequeños de longitud fija (por lo común 64 y 128 bits). Este tipo de cifrado se utiliza tanto en algoritmos simétricos, como asimétricos. Entre algunos ejemplos de algoritmos criptográficos de bloque se encuentran IDEA, DES, BLOWFISH, AES, Diffie-Hellman y RSA.
2. **De Flujo (o de Stream).** Son aquellos que operan en bits de datos individuales del mensaje a cifrar. Los algoritmos de este tipo de cifrado son generalmente más rápidos que los de bloque y requieren menos complejidad de hardware. Además, son más apropiados para cuando la capacidad de datos temporales en hardware (buffer) está limitada o cuando se requiere procesar cada bit individualmente conforme se recibe. Al igual que los de bloque, este tipo de cifrado se utiliza tanto en algoritmos simétricos como asimétricos. Entre algunos algoritmos criptográficos de flujo se encuentran ORYX, RC4 y SEAL.

Aunque existe una gran variedad de algoritmos de cifrado, en este trabajo sólo se describe el algoritmo DES (y su variante 3-DES) ya que, como se verá en el capítulo IV, es el algoritmo que utilizan las tarjetas inteligentes empleadas en el sistema propuesto.

### **3.4.2 Algoritmos de cifrado DES y 3-DES**

El algoritmo DES fue desarrollado originalmente por la empresa IBM en 1974, en respuesta a una convocatoria que lanzó el Instituto Nacional de Estándares y Tecnología de los EE.UU. (NIST) para contar con un algoritmo que protegiera información no clasificada. Se requería que no fuera costoso, que fuera muy seguro y que se pudiera utilizar ampliamente. IBM lo presentó con el nombre de “Lucifer”. La Agencia de Seguridad Nacional de los EE.UU. (NSA) lo evaluó y realizó algunas modificaciones

para posteriormente nombrarlo “DES” (Data Encryption Standard) en 1977. Su uso oficial fue reemplazado en 1997 por el algoritmo AES, cuando se demostró que el primero tenía vulnerabilidades, ya que el algoritmo fue quebrado en 1998 utilizando una computadora de \$250,000 dólares, al aplicar ataques de fuerza bruta para adivinar la llave, tomándole 3 días de procesamiento. Sin embargo, se sigue utilizando ampliamente para aplicaciones de servicios financieros y otras industrias en todo el mundo (Tropical Software, 2004; RSA Security, 2004).

DES es un algoritmo de cifrado simétrico que utiliza bloques de 64 bits de datos. La llave de cifrado y descifrado consiste de 64 dígitos binarios, de los cuales se utilizan solamente 56 que son generados de manera aleatoria. Los 8 bits restantes no se utilizan en el proceso de cifrado, se utilizan para detección de errores utilizando la comprobación por paridad par.

Al inicio del proceso se realiza una permutación de los datos por cada bloque, posteriormente se realiza un proceso de cómputo complejo que consiste de 16 iteraciones el cual es dependiente de la llave utilizada (básicamente consiste en repetir el proceso 16 veces). Al final se realiza una permutación inversa a la inicial (Daley, W. & Kammer, 1999).

Triple-DES, o también conocido como 3-DES, es una variante del algoritmo DES, el cual básicamente ejecuta tres veces el algoritmo DES sobre el mensaje a cifrar. Esto lo hace utilizando tres llaves de 64 bits cada una, formando un total de 192 bits (24 caracteres). Al igual que el algoritmo DES, cada una de estas llaves utiliza solamente 56 bits y los 8 restantes son para comprobación de paridad, por lo que la llave resultante que se utiliza es de 168 bits. El modo en que opera es que los datos se cifran con la primera llave, luego se descifran con la segunda y finalmente se cifran de nuevo con la tercera llave. Esto lo hace 3 veces más lento que DES, pero miles de millones de veces más seguro si se usa apropiadamente (Tropical Software, 2004).

### **3.4.3 Uso de la criptografía en el proceso de autenticación**

En la sección 3.3 se menciona a la autenticación como uno de los mecanismos para brindar seguridad en la información. La mayoría de los mecanismos de autenticación, si no es que todos, involucra el compartir un secreto entre todos los participantes involucrados en la transacción. Dos de estos mecanismos incluyen distintas formas de cifrado y descifrado de información. La primera utiliza algoritmos de criptografía simétrica, mientras que el segundo utiliza algoritmos de criptografía asimétrica (Jurgensen & Guthery, 2002). Algunas tarjetas inteligentes utilizan criptografía para realizar el proceso de autenticación, tal como se describe a continuación.

#### **3.4.3.1 Proceso de autenticación de tarjetas inteligentes usando criptografía simétrica**

Con este mecanismo, cada tarjeta requerirá almacenar dos llaves: una que usará para que se autentique la aplicación de la terminal con la tarjeta y otra que se usará para que la tarjeta se autentique con la aplicación. La aplicación de la terminal requerirá tener almacenado un gran número de llaves, esto es, una por cada tarjeta que tendrá acceso al sistema, además de la que utilice para autenticarse con las tarjetas.

Este esquema presenta algunos riesgos de seguridad. Por ejemplo, como la llave que almacena cada una de las tarjetas también debe estar almacenada en la aplicación de la terminal, se pudiera poner en riesgo la identidad de la tarjeta, si por alguna razón las llaves que se almacenan en el servidor son extraídas por personas no autorizadas. Como consecuencia, estas personas pudieran clonar tarjetas usando estas llaves y tener acceso al sistema. Por otro lado, la llave que utiliza la aplicación para autenticarse con las tarjetas se encuentra almacenada en cada una de las tarjetas. Si esta llave se logra extraer de cualquier tarjeta, pudiera utilizarse en otra aplicación, simulando ser la aplicación original.

En la figura 3.3 se muestra cómo se lleva a cabo el proceso de autenticación entre la tarjeta y la terminal. El proceso implica la autenticación de ambas partes, esto es, tanto de la tarjeta como de la terminal. En la figura sólo se muestra la parte donde la tarjeta se autentica con la terminal.

Para realizar este proceso, ambas partes deben tener almacenada la misma llave y mantenerla en privado. La tarjeta, para autenticarse con la terminal, le envía un comando solicitando este proceso. La terminal, en respuesta, cifra un texto arbitrario para enviárselo a la tarjeta y ver si ésta puede descifrarlo. La única manera en que pueda ser descifrado por la tarjeta es si contiene la misma llave con la que fue cifrado por la terminal. Una vez que la tarjeta lo descifra, lo envía de regreso a la terminal y ésta lo valida comparándolo con el original. Si ambos textos son idénticos, significa que la tarjeta posee la misma llave, dando inicio a que establezca una identidad de confianza.

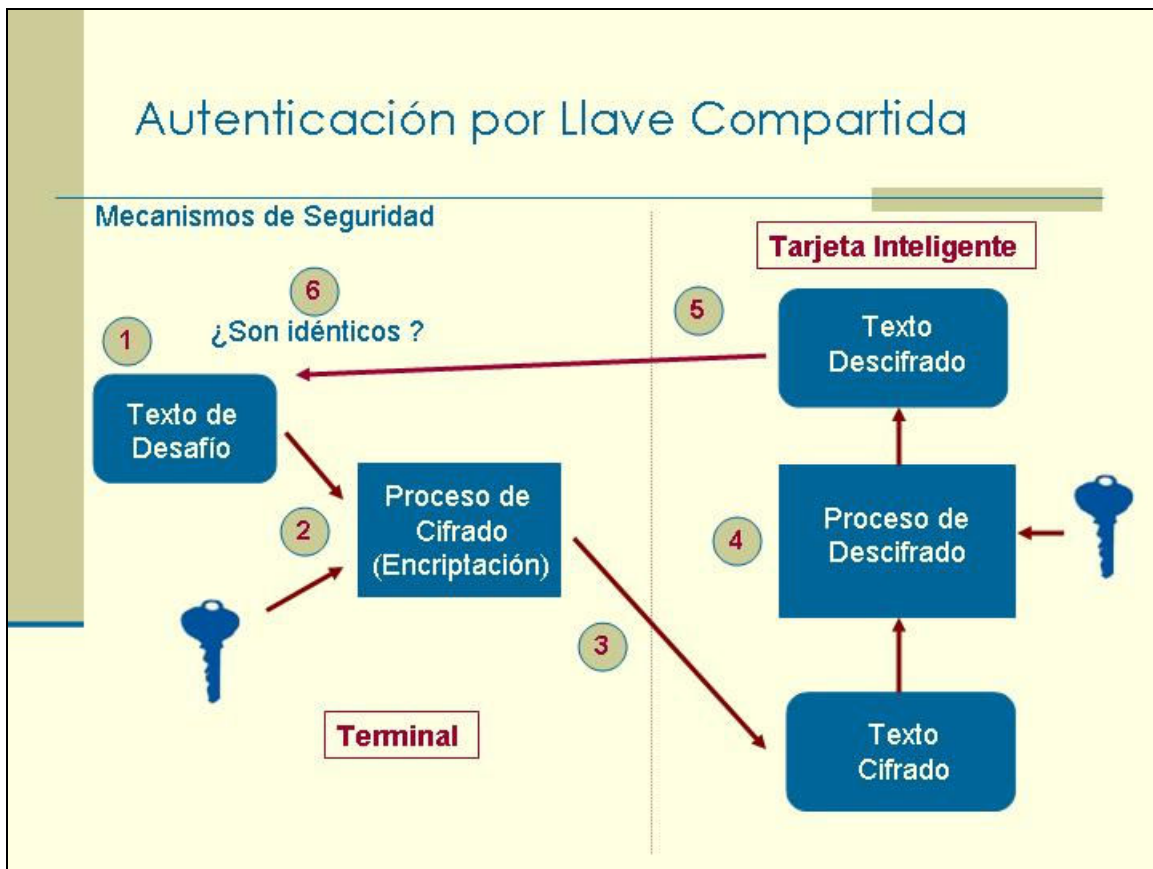


Figura 3.3 – Autenticación de tarjetas inteligentes por medio de llave compartida

Un mecanismo que se utiliza comúnmente para reforzar la seguridad en el uso de tarjetas inteligentes para autenticarse a un sistema, es el de clave secreta (PIN). Este mecanismo utiliza una clave secreta que se almacena en la tarjeta y que sólo el dueño de la tarjeta conoce. Al momento de iniciar una transacción con una aplicación, el dueño de la tarjeta debe introducir esta clave, la cual es comprobada por la aplicación, asegurando así que el usuario se identifique antes de proceder con la transacción.

### **3.4.3.2 Proceso de autenticación de tarjetas inteligentes usando criptografía asimétrica**

Como se mencionó anteriormente, este mecanismo utiliza dos llaves independientes pero relacionadas matemáticamente. Una llave se distribuye públicamente y la otra se mantiene en privado. Algunas tarjetas inteligentes utilizan este mecanismo para autenticación. El proceso se lleva a cabo para ambas partes, esto es, para autenticar la tarjeta con la aplicación de la terminal y viceversa. En la figura 3.4 se muestra cómo se presenta este mecanismo cuando la aplicación requiere autenticarse con la tarjeta. En este caso, la tarjeta requiere saber si la aplicación comparte el mismo secreto que ella. Para lograr esto, la aplicación de la terminal debe mantener oculta su llave privada, esto es, que nadie tenga acceso a ella, sino solamente la misma aplicación, porque esta llave representa su identidad. La llave pública que corresponda a la llave privada puede ser distribuida libremente, por lo tanto, se puede almacenar en toda aquella tarjeta inteligente que requiera acceder a la aplicación. En el ejemplo de la figura 3.4 se muestra que, para que la aplicación de la terminal se autentique con la tarjeta, primero debe solicitarlo. En respuesta a esto, la tarjeta genera un texto arbitrario que usará como reto al cifrarlo con la llave pública que obtuvo anteriormente de la aplicación de la terminal. Este texto cifrado es enviado a la terminal y ésta lo descifra con la llave privada que almacena. Si la aplicación de la terminal logra descifrarlo a su forma original, significa entonces que esa llave privada está relacionada con la llave pública que contiene la tarjeta. Por lo tanto, la tarjeta procede a aceptar la negociación al autenticar la aplicación. Obviamente, el procedimiento inverso permitirá que la tarjeta se autentique con la aplicación de la terminal.



Figura 3.4 – Autenticación de tarjetas inteligentes por medio de llave pública

### 3.5 Algoritmos hash y firmas digitales

El algoritmo hash es aquel que se utiliza para asegurar que los datos no han sido alterados durante su envío. A grandes rasgos, el algoritmo consiste en comprimir los datos de tal manera que se genera un valor numérico único conocido como “valor hash”. Si los datos originales son alterados, se produce un valor hash distinto al producido por los datos originales. El emisor genera un valor hash con los datos originales y envía tanto los datos, como el valor hash al receptor. Cuando éste recibe los datos, vuelve a generar un valor hash digital utilizando el mismo algoritmo y posteriormente compara ambos valores (el generado por el emisor y el generado por el receptor). Si son idénticos, significa que el mensaje no ha sido alterado. Pero si son distintos, significa que en alguna parte del envío los datos fueron alterados (Nash *et al.*, 2002).

Un buen algoritmo hash debe detectar cualquier cambio en los datos, por más mínimo que este sea. Además, estos algoritmos tienen la propiedad de que no se puede poner a funcionar el algoritmo hacia atrás y recuperar el texto original. Además, el valor hash resultante no dirá nada sobre el texto original. Entre los más conocidos se encuentran MD2 (de DSA), MD5 y SHA-1.

Una aplicación muy común de este tipo de algoritmo son las firmas digitales. Orlin, (1997-2000) define una firma digital como “una forma matemática precisa de adjuntar la identidad de una persona a un mensaje, son mucho más difíciles de falsificar que las firmas escritas y el mensaje firmado no puede ser modificado sin invalidar la firma”. Las firmas digitales tienen la característica de permitir verificar la autenticidad del documento o contrato firmado (mensaje), además de permitir verificar la identidad del firmante. Esto es, que hace posible que el destinatario se asegure de que el mensaje que recibe, es enviado por quien dice ser el remitente. Además, deben ser fáciles de crear, fáciles de verificar, pero difíciles de falsificar.

Si durante el proceso de envío se llegara a alterar, aunque sea una letra de un documento firmado, ya no se podría verificar la firma de tal documento. Para llevar a cabo esto, las firmas digitales hacen uso de los algoritmos hash mencionados anteriormente. La capacidad que tienen estos algoritmos para detectar el más pequeño de los cambios en un texto, es lo que les da su utilidad para verificar la integridad del mensaje.

Las firmas digitales se basan en la criptografía asimétrica, donde se utiliza una llave pública que puede conocer todo el mundo, como si fuera un número telefónico, y una llave privada, que la debe conocer solo la persona que firma el documento.

### ***3.6 Protocolo de Capa de Socket Segura (SSL)***

En las últimas dos décadas, universidades, empresas, agencias de gobiernos y personas en general, han sacado provecho de las ventajas que brindan los avances en las tecnologías de redes de datos. Cada vez más se desarrollan aplicaciones que utilizan la red Internet

para cubrir las necesidades de transferencia de información. Sin embargo, la seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada a Internet. Es por esto que se deben utilizar mecanismos para protección de los recursos de las redes privadas, incluyendo el evitar accesos no autorizados y protección de la integridad y privacidad de la información. Una solución segura para proteger enlaces de datos a través de Internet es el Protocolo de Capa de Socket Segura (SSL).

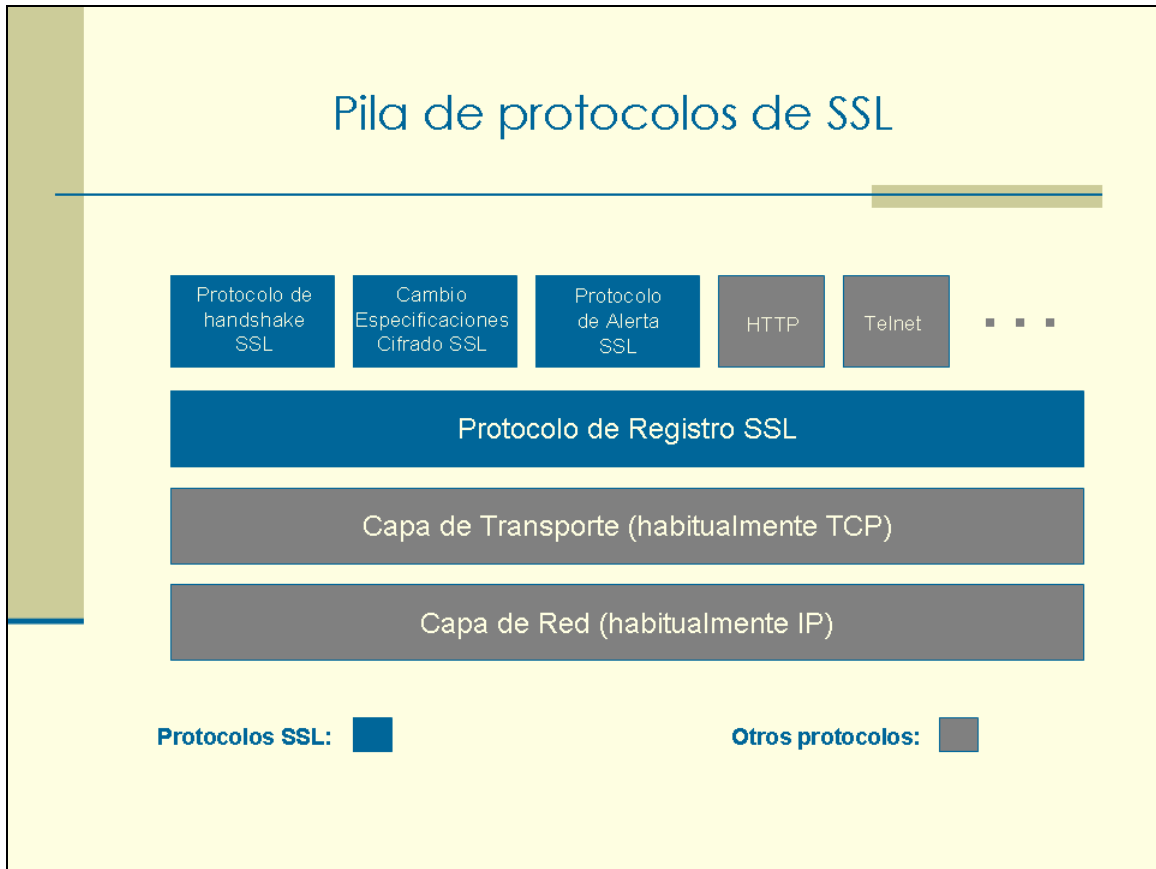
SSL, al cual se le conoce hoy como *Transport Layer Security* (TLS), fue desarrollado originalmente por la empresa Netscape Corporation en 1994 y se propuso como un estándar diseñado para brindar un enlace seguro entre navegadores y servidores de Internet. Esta tecnología permite asegurar un sitio de Internet por medio del cifrado de la información y la autenticación (Coulouris, Dollimore, & Kindberg, 2001). Aunque SSL es el sistema de cifrado de datos más utilizado en Internet, no sólo se utiliza para conexiones Web seguras, sino también para todo tipo de aplicaciones de red que necesitan cifrado en conexiones de punto a punto (Johnson, Gossels & Davis, 2004).

Para que se pueda crear una conexión segura usando tecnología SSL, se requiere que el servidor Web tenga un certificado SSL. Tal certificado contiene, entre otros elementos, la identidad del sitio y la compañía a la que pertenece. Además, el servidor crea dos llaves, una pública y otra privada. La llave pública se utiliza para cifrar información mientras que la llave privada se utiliza para descifrarla. La llave pública no necesita ser secreta, sino que se incluye en un archivo de datos que contiene los detalles del sitio Web (llamado Solicitud de Firma de Certificado o CSR) el cual es validado por una Autoridad de Certificación (*Certification Authority* o CA) y esta se encarga de expedir el certificado SSL conteniendo los detalles del sitio para permitir realizar conexiones SSL. Cuando un navegador Web se conecta a un dominio seguro, se lleva a cabo una negociación (*handshake*) de SSL que autentica el servidor y el cliente estableciendo un método de cifrado y una llave única de sesión. A partir de aquí, se establece una sesión segura que garantiza privacidad e integridad en los mensajes. Cada certificado SSL se crea para un servidor en particular de cierto dominio para una entidad de negocio verificado (SSL.com, 2005).

Entre los datos que contiene el certificado SSL, se encuentran el nombre del dominio, el nombre de la compañía, dirección, ciudad, estado y país. También se incluye la fecha de expiración del certificado, así como los detalles de la Autoridad de Certificación responsable de la expedición de tal certificado. Cuando un navegador Web se conecta a un servidor que utiliza SSL, obtiene el certificado SSL y verifica que no ha expirado, que ha sido expedido por una Autoridad de Certificación en la cual el navegador Web confía y verifica también que está siendo utilizado por el sitio de Internet que lo ha proporcionado. Si una de estas verificaciones falla, el navegador Web despliega una advertencia informándole al usuario que está accediendo a un sitio no seguro por SSL (SSL.com, 2005).

El protocolo SSL consta de dos capas implementadas en bibliotecas de software en el nivel de aplicación tanto en el navegador Web como en el servidor. La primera capa es la que implementa un canal seguro, cifrando y autenticando mensajes transmitidos a través de cualquier protocolo orientado a conexión. A esta capa se le conoce como Capa de Protocolo de Registro SSL (ver figura 3.5). La segunda capa se encarga de llevar a cabo el *handshake* entre el navegador Web y el servidor para establecer y mantener una sesión SSL (un canal seguro) entre ambos. Para cada sesión segura se le da un identificador y cada uno de los participantes puede almacenarlos en una memoria tipo caché para uso posterior, evitando así volver al proceso de crear una nueva sesión.

Debido a que la intención de SSL es añadir comunicación segura a los protocolos de nivel de aplicación existentes, se diseñó para encontrarse en el modelo de capas OSI, entre los niveles de protocolos de transporte (por ejemplo TCP) y los protocolos de aplicación y presentación como pudieran ser HTTP, FTP, SMTP, Telnet, etc.



**Figura 3.5 - Pila de protocolos de SSL**

Como SSL soporta varias opciones criptográficas, al comenzar el *handshake*, el servidor le muestra al cliente una lista de los catálogos de cifrado disponibles, así como de métodos de compresión, en caso de que se utilice. El cliente responde seleccionando uno de ellos o indicando error si no tiene disponible ninguno de los cifrados o tipos de compresión, que el servidor muestra. Además, ambas partes pueden intercambiar certificados de llave pública, utilizando el formato estándar X.509. Para más información de este estándar, consulte Coulouris, Dollimore & Kindberg (2001) en la sección 7.4.4 que habla sobre estándares de certificación y autoridades de certificación.

Para cada sesión SSL, el servidor tiene que autenticarse con el cliente. Esto se hace con la finalidad de evitar que la respuesta que recibe el cliente sea de otro servidor o que la información sea interceptada. Con el proceso de autenticación, el servidor le asegura al cliente su identidad. En el caso de la versión 3.0 de SSL, el cliente también se autentica

con el servidor, llevando a cabo un proceso de autenticación mutua. SSL utiliza criptografía tanto simétrica como asimétrica. La criptografía asimétrica (o criptografía de llave pública) se utiliza para el proceso de autenticación, mientras que la criptografía simétrica (o de llave privada) se utiliza para cifrar los datos que se transmiten asegurando así, la privacidad e integridad del mensaje (Johnson, Gossels & Davis, 2004).

### **3.7 Conclusiones**

En este capítulo presenté una idea general de lo que es la seguridad de la información y algunos mecanismos que se utilizan para llevarla a cabo. Se mostró también la manera en que se lleva a cabo el proceso de autenticación entre tarjetas inteligentes y las aplicaciones con las que operan, utilizando criptografía como herramienta esencial para tal función. Durante la investigación se observó que el tema de la seguridad de la información es muy amplio y dinámico, ya que conforme evolucionan los sistemas informáticos, también evolucionan los mecanismos para protegerlos. Por lo tanto, se puede inferir que cuando se requiere brindar seguridad de la información a un sistema, se debe considerar como algo primordial, su grado de complejidad y a su vez, identificar aquellos puntos de acceso vulnerables a ataques por personas ajenas al mismo. Cualquiera de estos puntos de acceso que permita proporcionar información a personas no autorizadas o externas al sistema, representa un riesgo para la totalidad de dicho sistema. Coulouris, Dellimore & Kindberg (2001), al hablar de seguridad señalan que “El diseño de los sistemas seguros parte de un listado de premisas de ataque y un conjunto de peores casos posibles”. Es por esto que se debe tener conocimiento a detalle sobre los aspectos de seguridad que involucra un sistema y revisar cada una de las etapas por las que exista transferencia o administración de la información, incluyendo no sólo a los equipos y sistemas informáticos, sino también al personal que tiene acceso a ella. Además es de suma importancia definir y asegurar que se cumplan con reglamentos de seguridad en todos los niveles del sistema.