CAPITULO 8

8 Técnicas de Seguridad

8.1 Introducción

Para entender la seguridad en el comercio electrónico es necesario conocer y entender los siguientes básicos:

La Criptología (del griego criptos = oculto y logos = tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias:

- Criptografía
- Criptoanálisis

La Criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial.

El Criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original.

Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su Criptoanálisis correspondiente. [Fúster 98]

La Criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció durante siglos vinculada muy estrechamente a los círculos militares diplomáticos, puesto que eran los únicos que en principio tenían auténtica necesidad de ella.

En la actualidad la situación ha cambiado drásticamente: el desarrollo de las comunicaciones electrónicas, unido al uso masivo y generalizado de las computadoras, hace posible la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger.

Con la introducción del comercio electrónico y sus requerimientos de proteger la información, cuando la Criptografía pasa de ser una exigencia de minorías a convertirse en una necesidad real del hombre común, que ve en esta falta de protección de sus datos privados una amenaza para su propia intimidad.

El esquema fundamental de un proceso criptográfico (cifrado/descifrado) puede resumirse como se muestra en la siguiente figura [Fúster 98]:

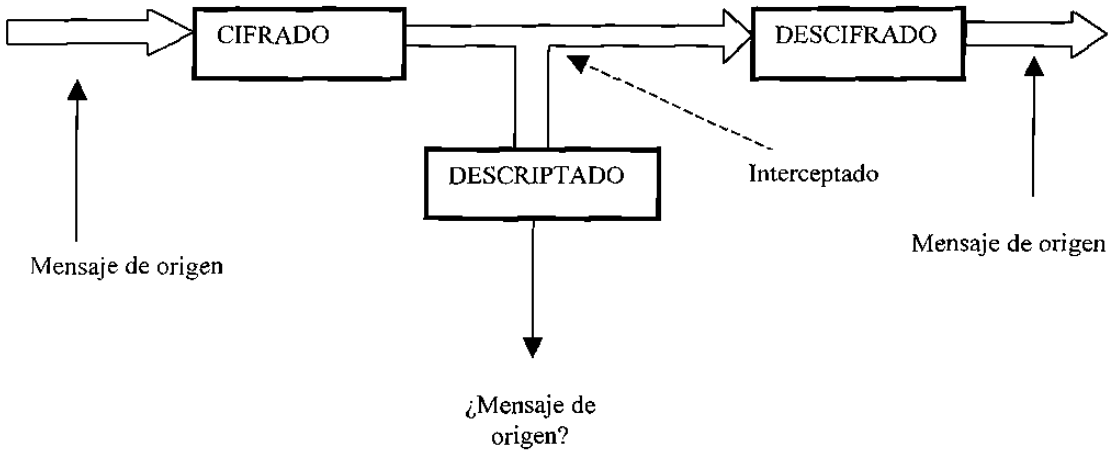


FIGURA 8.1: Proceso general de cifrado/descifrado

A y B son, respectivamente, el emisor y receptor de un determinado mensaje. El emisor A transforma el mensaje original (texto claro o plano), mediante un procedimiento de cifrado controlado por una clave, en un mensaje cifrado (criptograma) que se envía por un canal público.

En recepción B, con conocimiento de la clave transforma ese criptograma en el texto original, recuperando así la información original. Un buen sistema criptográfico será por tanto, aquel que ofrezca un cifrado sencillo pero un descifrado (procedimiento de criptoanálisis) imposible o, en su defecto, muy difícil.

La finalidad de la criptografía es mantener la confidencialidad del mensaje y que la información contenida en el criptograma permanezca secreta. Adicionalmente se garantiza la integridad del mensaje para que este no sea modificado, y la identidad del remitente o destinatario.

Anteriormente la seguridad de la Criptografía clásica era probable pero en la actualidad los procedimientos de la Criptografía moderna han de tener una seguridad matemáticamente demostrable. [Anderson 99]

Los principios básicos utilizados en los primeros criptosistemas fueron la sustitución y permutación de la secuencia de caracteres. Pero esto ha cambiado y actualmente se utilizan algoritmos matemáticos más complejos.

El tipo particular de transformación aplicada al texto claro o las características de las claves o llaves utilizadas marcan la diferencia entre los diversos métodos criptográficos. Teniendo así la siguiente clasificación.

8.2 Métodos Simétricos o Criptografía de Llave Secreta

Este esquema de encripción es llamado simétrico [Rajsbaum 99], [Fúster 98] debido al uso de la misma llave para encriptar y desencriptar un mensaje.

Esto es que el emisor y el receptor tienen una llave secreta compartida conocida por ambos.

El algoritmo más conocido es el DES (Data Encryption Standard) [RSA 99], [DES_FIPS_ 46-1 88]. Inventado por IBM y adoptado como un estándar por el gobierno de los EUA a finales de los 70's. DES es rápido, seguro y confiable. Aunque actualmente la fortaleza de DES con una llave de 56 bits de longitud se ha puesto en tela de juicio, debido al potencial existente de los sistemas distribuidos los cuales trabajan colaborativamente para romper el algoritmo, logrando un tiempo menor a 3 meses para desencriptar el mensaje. Con esto se han propuesto variantes como el Triple – DES. [DES_FIPS_46-3 99]

Debido a estos logros de ruptura del algoritmo DES, se iniciaron esfuerzos para diseñar algoritmos más seguros y libres de las restricciones de exportación. La National Institute of Standards and Technology (NIST) lanzo la convocatoria Advanced Encryption Standard Development Effort [AES 99] con la idea de seleccionar el algoritmo que sustituirá al DES.

El hecho de que el emisor y receptor requieran conocer la llave secreta nos lleva al problema del envío de la llave para poder desencriptar el mensaje enviado por un emisor.

La utilización de medios como el teléfono, fax o correo electrónico son lentos y sujetos de ataques, es por eso que se utilizan algoritmos de llave pública o asimétricos para el envío de la llave y posteriormente se utilizan los algoritmos de llave simétrica como el DES.

8.3 Métodos Asimétricos o Criptografía de Llave Pública

Este esquema de criptografía es el opuesto a la criptografía simétrica, puesto que utilizamos una llave para encriptar y otra diferente para desencriptar.

Anticipadamente se deben crear dos llaves, las cuales están matemáticamente relacionadas de tal forma que cualquier mensaje o texto encriptado con una de las llaves solamente pueda ser desencriptado con la otra y viceversa.

Una de las llaves debe ser designada para ser privada o secreta y la otra para ser pública y dada a conocer a todas las personas interesadas en enviar algún mensaje encriptado. Basado en la premisa de que no es posible derivar la llave secreta a partir de la pública o al revés.

Una de las desventajas de este esquema de encripción es el problema de la lentitud del cálculo ya que un algoritmo asimétrico tarda de 10 a 1000 veces más tiempo de computo que los algoritmos simétricos.

Es de ahí que surja la combinación de ambos métodos. Utilizando los algoritmos asimétricos para enviar la llave única y secreta de los algoritmos simétricos.

Otro conflicto que se genera con los esquemas de criptografía asimétricos es la distribución de las llaves públicas, ya que un impostor puede enviar llaves publicas asumiendo o suplantando la identidad de otra persona y con esto el problema de la autentificación se vuelve a presentar. [Mcclure 98], [PKI 99]

Si el problema de distribución y confianza del origen de la llave público es resuelto, entonces se puede asegurar la identidad del emisor debido a la encripción del mensaje con la llave privada y desencripción con la llave pública correcta. Las autoridades certificadoras realizan el procedimiento de crear los certificados digitales, la administración y envío.

8.4 Firma Digital

El Digital Signature Standard [NIST 92] propuesto por el NIST especifica el Digital Signature Algorithm (DSA) apropiado para las aplicaciones que requieren una firma digital en lugar de escrita. La firma digital DSA es un par de números largos representados en una computadora como cadenas de dígitos binarios. La firma digital es calculada utilizando un conjunto de reglas y un conjunto de parámetros permitiendo la identificación del originador y la integridad de la información.

El DSA incluye la generación de la firma y su verificación. La generación utiliza una llave privada para generar la firma y la verificación de la firma hace uso de la llave pública correspondiente. [Sirbu 97]

Una función hash es utilizada para el proceso de generación de la firma para obtener una versión condensada de los datos y esto es denominado message digest. En el próximo capítulo se explica el funcionamiento del algoritmo MD5, el cual es utilizado para la generación de firmas digitales.

Por lo anterior, una firma digital es un código que es agregado a un mensaje, que puede ser verificado por el receptor para autentificar al creador del mensaje.

Es importante verificar en un sistema de autentificación dos condiciones:

- La firma de un documento de tal forma que la falsificación sea imposible.
- La verificación de que la firma fue realizada por aquel a quien representa.

El temor a los riesgos de seguridad ha creado una demanda de características construidas directamente en los sistemas de comercio electrónico. Los mecanismos y técnicas de seguridad existentes pueden ser combinados para minimizar un gran rango de las amenazas del comercio electrónico. [Baldwin 97]

CAPITULO 9

9 Algoritmos y Protocolos para el Comercio Electrónico

9.1 Introducción

Los algoritmos son procedimientos que detallan un conjunto definido de instrucciones simples que al ser ejecutadas pueden resolver un problema específico. Es importante determinar la cantidad de recursos de tiempo y espacio que requieren los algoritmos para ejecutarse [Weiss 92].

Este análisis de la complejidad de los algoritmos tiene una relación directa con la seguridad que proveen y es otro elemento a considerar en el criptoanálisis. Dado al avance de la tecnología y las ciencias computacionales, algunos algoritmos que antes se creían seguros, ahora ya no lo son y con esto ha quedado al descubierto la vulnerabilidad de los demás algoritmos. Este es el caso específico del algoritmo DES. [DES_CHAL_III 99]

Para resolver estos problemas se están desarrollando algoritmos más seguros, los cuales únicamente puedan ser descifrados mediante la búsqueda exhaustiva o fuerza bruta en un tiempo mayor a la validez de la información que se desea proteger y que inclusive las máquinas actuales y de los próximos años no puedan romper en los períodos necesarios.

Por otra parte, un protocolo es un conjunto de reglas, convenciones o estándares que utilizan dos o más dispositivos para comunicarse.

A continuación se presentan los algoritmos RSA de criptografía de llave pública, DES de criptografía privada DES y MD5 para firmas digitales, de igual forma se presentan los protocolos SET para transacciones electrónicas y el protocolo SSL para comunicación cliente servidor de forma segura bajo el estándar WWW.

9.2. Algoritmo RSA

9.2.1. Introducción

El RSA es el criptosistema de llave pública más popular basado en el modelo de Diffie-Hellman, el cual ofrece encripción y firmas digitales (autenticación). Ron Rivest, Adl Shamir y Leonard Adleman desarrollaron el RSA en 1977, de ahí su nombre formado por la primera letra del apellido de sus inventores. [RSA 99]

La longitud de la llave es variable, la más popular es de 512 bits, pero en la actualidad la llave de 1024 bits es comúnmente utilizada por el Pretty Good Privacy (PGP). [PGP 00],

[YAMAMOTO 96] De igual forma el tamaño de bloques de datos RSA es variable, pero el bloque de texto plano (sin encriptar) debe ser menor que la longitud de la llave. El tamaño del texto cifrado es de la misma longitud que la llave.

RSA es considerablemente más lento que el DES. Es utilizado normalmente para realizar funciones que el DES no puede realizar como la distribución de llaves. El PGP utiliza el algoritmo RSA para distribuir la llave de sesión secreta al destinatario.

9.2.2. Algoritmo RSA

Para generar el par de llaves: privada y pública [Fúster 98].

1. Se eligen dos números primos muy grandes p y q (por ejemplo de 256 bits de longitud)	Seleccionar p,q
2. Hacer n = p * q y guardar en secreto p, q. Es prácticamente imposible obtener los factores de una n tan grande. Se llama modulo a n.	n = p * q
3. Para generar la llave pública, escoja un número e, tal que $1 \leq e < \phi(n)$, o sea menor a n que sea primo relativo a ϕ (n) = (p - 1)(q - 1). Lo que significa que e y theta(n) no tienen factores en común excepto al 1. Por tanto	ϕ (n) = (p - 1)(q - 1)
4. Sea la llave pública {e, n}. E es el exponente publico.	{e, n}
5. Para generar la llave privada, Calcular d que es el inverso multiplicativo (mediante el algoritmo de Euclides extendido) de e mod ϕ (n). De otra forma encontrar otro número d tal que (ed-1) SEA DIVISIBLE por (p-1)(q-1).	e d ≡ 1 (mod ϕ (n))
6. La llave privada es {d, n} D es el exponente privado.	{d, n}
Es necesario mantener secretos los números p,q y ϕ (n)	

TABLA 9.1: Algoritmo RSA

Para encriptar un mensaje m < n para una persona B, únicamente se utiliza la llave pública de B para generar el texto encriptado:

$$c = m^e \bmod n \qquad (9.1.2\text{-a})$$

Unicamente la persona B puede desencriptar el texto cifrado c ya que solo B tiene la llave privada {d, n}:

$$m = c^d \bmod n \qquad (9.1.2\text{-b})$$

Para firmar el mensaje es necesario hacer:

$$s = m^d \bmod n \qquad (9.1.2\text{-c})$$

Para verificar la firma de B se requiere hacer:

$$m = s^e_B \bmod n \qquad (9.1.2\text{-d})$$

donde e es la llave pública de B.

9.2.3. Seguridad del RSA

Algunos ejemplos de ataques serían:

1. El algoritmos RSA se basa en el principio de la dificultad de factorizar un número grande n=p*q donde p y q son números primos grandes.
2. Dada la llave pública {e, n}, es difícil encontrar d el cual es el inverso multiplicativo de e, dado que p y q son desconocidos.
3. Existe un grado alto de dificultad para obtener la llave privada d a partir de la publica (n, e). De cualquier manera si se puede factorizar n en p y q se puede obtener la llave privada d. La seguridad de RSA se basa en el supuesto de la dificultad de la factorización.

Según [RSA 99] existen pocas interpretaciones posibles para romper el algoritmo RSA.

La más peligrosa sería para un atacante el descubrir la llave privada que corresponde a una llave pública dada. Esto permitiría al atacante tanto leer los mensajes encriptados con la llave publica y falsificar las firmas. La manera obvia para realizar este ataque es factorizar el modulo publico n en dos factores primos p y q. A partir de p, q y e, el exponente publico, un atacante puede fácilmente obtener d, el exponente privado. La parte difícil es factorizar n; la seguridad de RSA depende de la dificultad de factorizar. De hecho, la tarea de recuperar la llave privada es equivalente a la tarea de factorizar el modulo: se puede utilizar d para factorizar n, de igual forma el uso de la factorización de n para encontrar d. Las optimizaciones en HW no debilitan el RSA siempre y cuando se utilicen longitudes adecuadas de la llave.

Otra forma de romper el RSA es encontrar una técnica para calcular las raíces e mod n. Dado que $c = m^e \bmod n$, la raíz e de c mod n es el mensaje m. Este ataque permite la recuperación de mensajes encriptados y la falsificación de firmas sin conocer la llave privada. Este ataque es conocido por ser el equivalente de la factorización. No existen métodos actualmente conocidos para romper el algoritmo de esta forma. Pero en casos especiales cuando múltiples mensajes relacionados son encriptados con el mismo exponente pequeño, puede ser posible la recuperación de mensajes.

Estos ataques mencionados son la única forma conocida durante la investigación para romper el algoritmo RSA. Existen métodos para recuperar únicamente mensajes únicos dada una misma llave o recuperaciones parciales de mensajes.

9.3. Algoritmo DES.

9.3.1. Introducción

El algoritmo DES es un acrónimo para Data Encryption Standard y el nombre del Federal Information Processing Standard (FIPS) 46-1 [DES_FIPS_46-1 88], [Mathew DES], [Fúster 98] el cual describe el algoritmo de encripción de datos (DEA – Data Encryption Algorithm). El DEA se encuentra también definido en el estándar ANSI X9.21. Originalmente desarrollado por IBM y conocido como Lucifer, la NSA y la National Bureau of Standards (NBS, ahora el National Institute of Standards and Technology, NIST) jugaron un rol sustancial en las etapas finales del desarrollo.

El DEA, comúnmente llamado DES, ha sido estudiado extensivamente desde su publicación y es el algoritmo simétrico más conocido y utilizado del mundo.

El DEA tiene un tamaño de bloque de 64 bits y utiliza llaves de 56 bits durante la ejecución (8 bits de paridad son eliminados de la llave completa de 64 bits). El DEA es un criptosistema simétrico, específicamente un cifrador Feistel de 16 rondas y fue diseñado originalmente para su implementación en hardware. Cuando es utilizado para comunicación, tanto el emisor como el receptor deben conocer la misma llave secreta, la cual puede ser utilizada para encriptar y desencriptar el mensaje o para generar y verificar un código de autentificación de mensajes (Message authentication code – MAC). El DEA puede ser utilizado para encripción por un único usuario como el almacenamiento de archivos encriptados en el disco duro. Pero en un ambiente multiusuario, la distribución de llaves de forma segura puede ser difícil y la criptografía de llave pública provee una solución ideal a este problema.

El National Institute of Standards and Technology (NIST) ha certificado el DES (FIPS 46- 1) cada cinco años, la última vez fue en 1993 pero no será certificado otra vez. Esto debido a la vulnerabilidad del algoritmo utilizando una llave de 56 bits. Es por ello que el NIST ha iniciado un esfuerzo para desarrollar el Advanced Encryption Standard (AES) [AES 99]. Para especificar un algoritmo de cifrado de bloques simétrico, el cual reemplazará al algoritmo DES.

9.3.2. Algoritmo DES

El algoritmo DES [Fúster 98], [Mathew DES] trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación inicial fija y, por tanto, sin valor criptográfico. Después se divide el bloque en dos mitades, la derecha y la izquierda. A continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con una transformación g(k1) de la parte derecha, mediante una clave k1. Después se intercambian las partes derecha e izquierda. En la siguiente figura [Fúster 98] se presenta el esquema. En la vuelta número 16 se

omite el intercambio, pero se termina el algoritmo con una permutación final que es la inversa de la inicial.

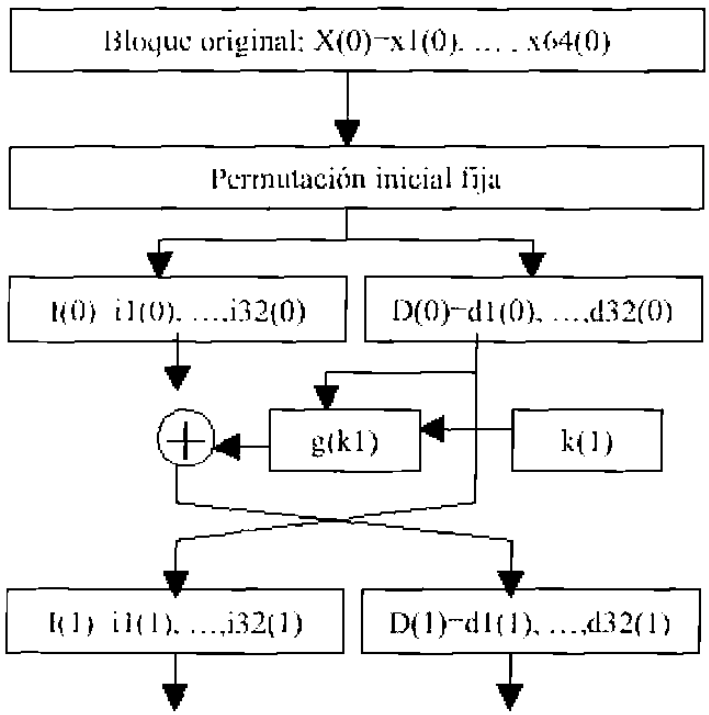


FIGURA. 9.1: Funcionamiento del algoritmo DES.

Para descifrar el algoritmo DES basta con repetir la operación modular, que es una involución; es decir, su aplicación repetida dos veces conduce a los datos originales. En la figura siguiente [Fúster 98] se puede ver el funcionamiento de la involución. No es preciso invertir la transformación g(k1) sino repetirla. Esto permite que dicha transformación sea una función de un solo sentido, empleando operaciones no lineales.

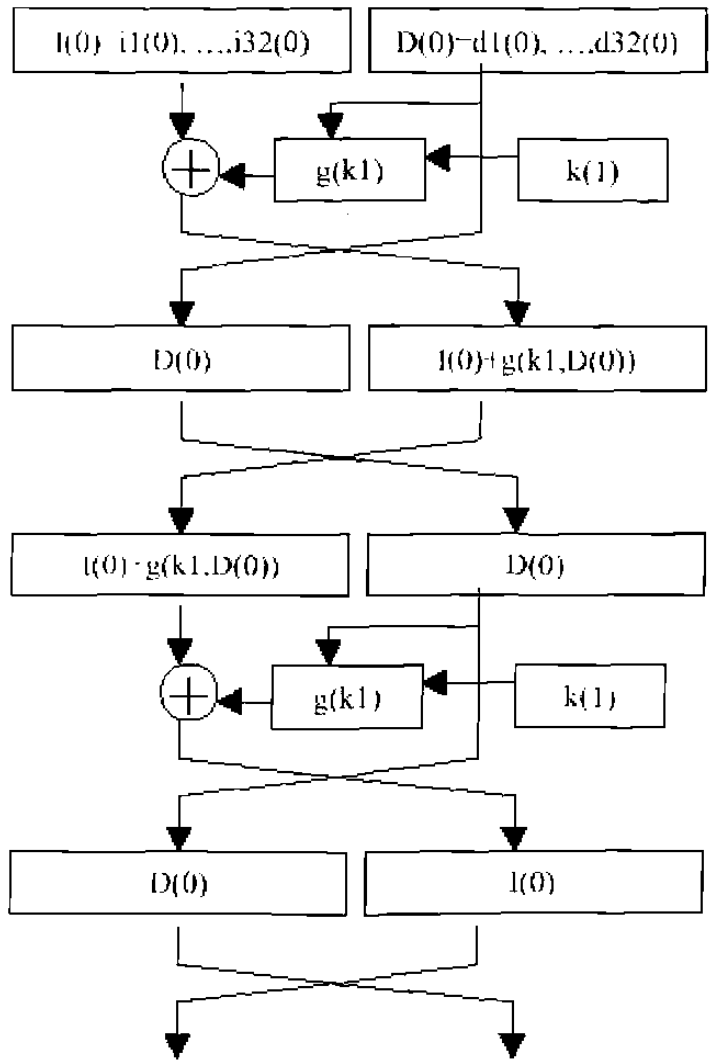


FIGURA. 9.2: Involución en el DES.

Es necesario describir las manipulaciones realizadas en el algoritmo DES. La transformación g(k1) es un conjunto de operaciones que se combinan según se muestra en la siguiente figura [Fúster 98].

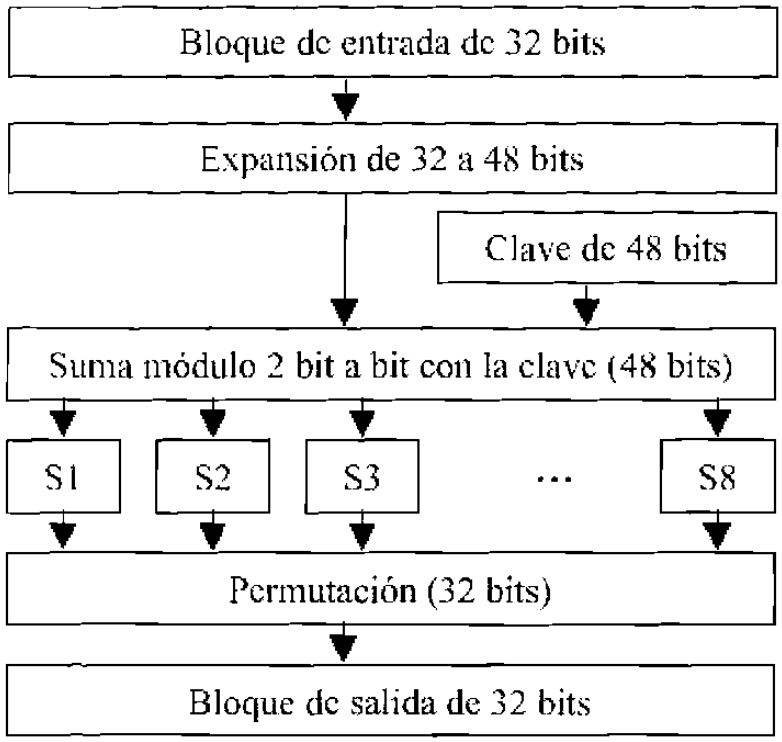


FIGURA. 9.3: Estructura de la transformación g del algoritmo DES.

El algoritmo DES puede ser utilizado para la encripción en varios modos definidos oficialmente [DES_FIPS_81 80] y estos modos tienen una variedad de propiedades:

- El modo Electronic CodeBook (ECB) encripta simplemente bloques de 64 bits de texto plano, uno tras de otro, utilizando la misma llave DES de 56 bits.
- En el modo Cipher Block Chaining (CBC) cada bloque de 64 bits de texto plano se aplica la función OR exclusivo con los bloques previos antes de ser encriptado con la llave DES, con esto la encripción de cada bloque depende de los bloques previos dependiendo del contexto completo del mensaje. Este modo ayuda la protección en contra de ciertos ataques pero no de búsqueda exhaustiva o criptoanálisis diferencial.

- El modo Cipher FeedBack (CFB) permite utilizar el DES con longitudes de bloque menores a 64 bits.
- El modo OFB permite al DES ser utilizado como un flujo de cifrado.

9.3.3. Seguridad del DES

No se han descubierto ataques fáciles al DES, a pesar de los esfuerzos de los investigadores en varios años. El método obvio de ataque es la búsqueda exhaustiva de fuerza bruta para el dominio de llaves, este proceso toma 255 pasos en promedio. Alguna vez se planteó la posibilidad de construir una computadora de propósito especifico capaz de romper el DES por búsqueda exhaustiva en un tiempo razonable. Posteriormente Hellman mostró un cambio en el manejo de memoria que permite mejorar la búsqueda exhaustiva si la cantidad de memoria era abundante. Estas ideas pusieron en tela de juicio la seguridad del algoritmo DES. Los estimados según Wiener son de 35 minutos para realizar la búsqueda exhaustiva con una computadora de un millón de dólares.

El primer ataque al DES que es mejor que la búsqueda exhaustiva en términos de requerimientos computacionales fue la anunciada por Biham y Shamir utilizando una técnica llamada criptoanálisis diferencial. Este ataque requiere la encripción de 247 textos planos escogidos por el atacante. Este ataque no es práctico debido a los requerimientos excesivos de datos y la dificultad en montar un ataque de los textos planos escogidos. Biham y Shamir consideraron seguro al algoritmo DES.

Más recientemente Matsui desarrollo otro ataque conocido como criptoanálisis linear. De acuerdo a este método una llave DES puede ser recuperada por el análisis de 243 textos planos conocidos. Este ataque también resultó impráctico debido al tiempo y poder computacional requerido.

Recientemente se realizó un reto para lograr romper el algoritmo, el objetivo se cumplió en 56 horas mediante el uso del computo distribuido, se puede encontrar más información y detalle en [DISTRIBUTED_NET 99] y en [RSA 99].

El conceso de la comunidad acerca del DES es que todavía no es inseguro, pero pronto lo será, ya que las llaves de 56 bits se están convirtiendo vulnerables a la búsqueda exhaustiva. A partir de noviembre de 1998, el DES no es permitido en el uso del gobierno de los Estados Unidos de Norteamérica. El Triple-DES será utilizado mientras el AES se encuentra listo para ser utilizado como se mencionó anteriormente.

Recomendaciones y consideraciones para utilizar el algoritmo DES.

- Se deben cambiar las llaves DES con frecuencia para prevenir ataques que requieran un análisis sostenido de los datos. En un ambiente de comunicación se debe encontrar una manera segura de comunicar la llave DES entre el emisor y el receptor. Utilizando el RSA o alguna técnica de llave publica para la administración de llaves, resuelve estos dos problemas: el primero es que se genere una llave por cada sesión y la administración segura de la llave DES al encriptarla con la llave publica RSA del receptor.

- Para mayor seguridad se recomienda utilizar la triple encripción con el CBC.
- Las llaves DES pueden ser probadas para que no sean llaves débiles de la siguiente forma.
  1. Existen 4 llaves débiles k para las cuales $E_k(E_k(m))=m$
  2. Existen 12 llaves semi débiles que vienen en pares k1 y k2 tales que $E_{k1}(E_{k2}(m))=m$
  3. Es mejor seleccionar la llave de forma aleatoria de entre 2^{52}

9.4. Algoritmo MD5

9.4.1. Introducción

El algoritmo MD5 o Message Digest toma como entrada un mensaje de longitud arbitraria y regresa como salida una "huella digital" de 128 bits del mensaje (Llamado message-digest, resumen o compendio del mensaje). Se estima que es imposible obtener dos mensajes que produzcan el mismo message-digest. También es imposible producir un mensaje que arroje un message-digest predefinido. Este algoritmo es útil como firma digital de mensajes que serán compactados y encriptados mediante un criptosistema de llave pública.

El MD5 fue desarrollado por Rivest en 1991. Se encuentra optimizado para máquinas de 32 bits. La descripción completa de los algoritmos se puede localizar en [RFC1321 92]. Es básicamente igual a su predecesor MD4 [RFC1320 92] pero con protecciones y un poco más lento pero más seguro. El algoritmo consiste en cuatro rondas distintas. El tamaño del resumen del mensaje así como los requerimientos de padding son iguales que el MD4.

9.4.2. Algoritmo MD5

Empezamos suponiendo que tenemos un mensaje de b-bits como entrada y que se desea encontrar su message-digest. Aquí b es un entero no-negativo arbitrario que puede ser cero y no necesariamente tiene que ser un múltiplo de 8, la longitud también puede ser arbitrariamente grande. El mensaje puede ser representado de la siguiente forma:

m_0 m_1 ... m_{b-1}	(9.3.2-a)

Los siguientes 5 pasos son realizados para calcular el message-digest del mensaje.

Paso 1. Agregado de bits de relleno

El mensaje es "padded" (extendido) para que su longitud en bits sea casi un múltiplo de 512 bits de longitud (congruente a 448, módulo 512). Los 64 bits restantes serán cubiertos con el tamaño del mensaje (expresado en 64 bits).

Paso 2. Agregado de la longitud

Una representación en 64 bits de la longitud b del mensaje es agregada al final del mensaje resultante en el paso previo. Si la longitud del mensaje requiere más de 2^{64} bits entonces se toman únicamente los 64 bits menos significativos.

Como resultado de este paso se obtiene un mensaje de longitud exactamente en múltiplos de 512 bits.

Equivalentemente, este mensaje tiene la longitud exacta de 16 palabras de (32-bits). Sea M[0 ... N-1] que denotan las palabras del mensaje resultante, donde N es un múltiplo de 16.

Paso 3. Inicialización del buffer MD

Un buffer de cuatro palabras (A, B, C, D) es utilizado para calcular el message-digest, donde cada palabra es un registro de 32 bits. Los registros son inicializados a los siguientes valores en hexadecimal con los bytes menos significativos primero.

Palabra A:	01	23	45	67
Palabra B:	89	ab	cd	ef
Palabra C:	fe	dc	ba	98
Palabra D:	76	54	32	10

Paso 4. Procesamiento del mensaje en bloques de 16 palabras

Primero se definen cuatro funciones auxiliares (F,G, H,I) que toman como entrada 3 palabras de 32 bits y producen una palabra de 2 bits.

F(X,Y,Z)=XY. not(X) Z
G(X,Y,Z)=XZ. Y not(Z)
H(X,Y,Z)=X xor Y xor Z
I(X,Y,Z)=Y xor (X. not(Z))

Se define una tabla T[i] de 64 elementos T[1..64] con base a la parte entera de 4294967296 por abs(sin(i)), donde i esta dado en radianes.

Después se ejecuta el siguiente proceso a cada bloque de 16 palabras.

```
For i   0 to N/16-1 do                    /* Copiar el bloque i en X */
        For j   0 to 15 do
                Set X[j] to M[i*16+j].
        end /* del ciclo en j */
        AA   A , BB   B, CC = C,  DD = D
        Round 1
        Round 2
        Round 3
        Round 4
        *Ejecutar las sig. sumas. (Incrementar c/u de los 4 reg. por el valor anterior al inicio del bloque*/
        A   A + AA
        B   B + BB
        C   C + CC
        D   D + DD
End /* del ciclo en i */
```

Round 1. Sea [abcd k s i] la siguiente operación a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 0 7 1]	[DABC 1 12 2]	[CDAB 2 17 3]	[BCDA 3 22 4]
[ABCD 4 7 5]	[DABC 5 12 6]	[CDAB 6 17 7]	[BCDA 7 22 8]
[ABCD 8 7 9]	[DABC 9 12 10]	[CDAB 10 17 11]	[BCDA 11 22 12]
[ABCD 12 7 13]	[DABC 13 12 14]	[CDAB 14 17 15]	[BCDA 15 22 16]
Round 2. Sea [abcd k s i] la siguiente operación a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 1 5 17]	[DABC 6 9 18]	[CDAB 11 14 19]	[BCDA 0 20 20]
[ABCD 5 5 21]	[DABC 10 9 22]	[CDAB 15 14 23]	[BCDA 4 20 24]
[ABCD 9 5 25]	[DABC 14 9 26]	[CDAB 3 14 27]	[BCDA 8 20 28]
[ABCD 13 5 29]	[DABC 2 9 30]	[CDAB 7 14 31]	[BCDA 12 20 32]
Round 3. Sea [abcd k s t] la siguiente operación a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 5 4 33]	[DABC 8 11 34]	[CDAB 11 16 35]	[BCDA 14 23 36]
[ABCD 1 4 37]	[DABC 4 11 38]	[CDAB 7 16 39]	[BCDA 10 23 40]
[ABCD 13 4 41]	[DABC 0 11 42]	[CDAB 3 16 43]	[BCDA 6 23 44]
[ABCD 9 4 45]	[DABC 12 11 46]	[CDAB 15 16 47]	[BCDA 2 23 48]
Round 4. Sea [abcd k s t] la siguiente operación a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 0 6 49]	[DABC 7 10 50]	[CDAB 14 15 51]	[BCDA 5 21 52]
[ABCD 12 6 53]	[DABC 3 10 54]	[CDAB 10 15 55]	[BCDA 1 21 56]
[ABCD 8 6 57]	[DABC 15 10 58]	[CDAB 6 15 59]	[BCDA 13 21 60]
[ABCD 4 6 61]	[DABC 11 10 62]	[CDAB 2 15 63]	[BCDA 9 21 64]

FIGURA. 9.4: Procedimiento para el cálculo del algoritmo RSA

Paso 5. Salida

El message-digest producido como salida es A, B, C y D. Esto es empezando con el menos significativo como A y el más significativo como D.

9.4.3. Seguridad del MD5

El único ataque conocido es la búsqueda exhaustiva, aunque se han detectado pseudo colisiones para el MD5.

9.5. Protocolo Secure Socket Layer (SSL) Versión 3.0

9.5.1. Introducción

El SSL es un protocolo de seguridad que provee privacidad en las comunicaciones a través de Internet. El protocolo permite a las aplicaciones cliente/servidor comunicarse de tal forma, de acuerdo al diseño, para prevenir la escucha (eavesdropping), intromisiones (tampering) o falsificación de mensajes (message forgery) evitando así la creación ilegal de mensajes, como si fueran oficiales.

Las metas del protocolo SSL V3.0 [SSL 96] en orden de prioridad son:

- Seguridad criptográfica: SSL debe ser utilizado para establecer una conexión segura entre dos entidades.
- Interoperabilidad: Las diversas aplicaciones SSL V3.0 deber ser capaces de intercambiar con éxito los parámetros criptográficos sin conocer el código de la otra aplicación.
- Extensibilidad: SSL busca proveer un marco de trabajo en el cual se puedan incluir nuevos métodos de encripción sin la necesidad de crear un nuevo protocolo y evitar la necesidad de implementar una nueva y completa librería de seguridad.
- Eficiencia relativa: Las operaciones criptográficas tienden a utilizar intensivamente el CPU sobre todo en operaciones de llave pública. Por esta razón el protocolo SSL ha incorporado un esquema opcional de cache para sesiones con el objeto de reducir el número de conexiones que deben ser establecidas a partir de cero.

La meta principal del protocolo SSL es proveer privacidad y confiabilidad entre dos aplicaciones que se encuentran comunicando. El protocolo esta compuesto de dos capas. En el nivel más bajo, encima de algún protocolo confiable de transporte (ej. TCP) se encuentra el protocolo de registro SSL (SSL Record Protocol). Este es utilizado para la encapsulación de varios protocolos de más alto nivel. Uno de esos protocolos encapsulados, el protocolo de iniciación de SSL (Handshake Protocol), permite al servidor y cliente la autentificación mutua, así como la negociación del algoritmo de encripción y las llaves criptográficas antes de que el protocolo de aplicación transmita o reciba el primer byte de datos. Otra ventaja del SSL es la independencia del protocolo de aplicación y se puede utilizar un protocolo de mas alto nivel de forma transparente.

El protocolo SSL provee seguridad en la conexión con 3 propiedades básicas:

- La conexión es privada. Se utiliza encripción después de haber realizado el proceso de iniciación y haber negociado una llave secreta. La criptografía simétrica es utilizada para la encripción de datos. Ejemplo: DES, RC4.
- La identidad de las entidades puede ser autentificada utilizando la criptografía asimétrica o de llave publica. Ejemplo: RSA, DSS.
- La conexión es confiable. El transporte de mensajes incluye una verificación de la integridad de los mensajes utilizando un código de autentificación de mensaje (MAC – Message Authentication Code) basado en una llave. Para los cálculos MAC son utilizadas funciones hash seguras (ej. SHA, MD5).

Las cuatro operaciones criptográficas utilizadas son: el firmado digital, encripción cifrada en flujo, encripción cifrada en bloque y encripción de llave pública.

- En el firmado digital, funciones hash de una vía son utilizadas como entrada para el algoritmo de firmado. En el caso de firmado de RSA una estructura de 36 bytes de dos funciones hash (una SHA y otra MD5) es firmada (encriptada con la llave privada). En DSS, los 20 bytes del hash SHA son ejecutados directamente a través del algoritmo de firmado digital sin un hashing adicional.
- En la encripción cifrada en flujo, el texto plano es pasado por una función Or exclusiva con la misma cantidad de salida generada por un generador pseudo aleatorio de números seguro.
- En la encripción cifrada en bloques, cada bloque de texto plano se encripta usualmente en bloques de 64 bits.
- En la encripción de llave pública, funciones de una vía con trampas (trapdoors - rutinas que permiten ingresar al sistema sin que la identidad sea autentificada) secretas, son utilizadas para encriptar los datos de salida. Los cuales pueden ser únicamente desencriptados con la llave privada y viceversa.

9.5.2. Protocolo SSL

El protocolo SSL es un protocolo de capas. En cada una, los mensajes pueden incluir campos para longitud, descripción y contenido. SSL toma los mensajes para ser transmitidos, fragmenta los datos en bloques manejables, opcionalmente compacta los datos, aplica el MAC, encripta y transmite el resultado. Los datos recibidos son desencriptados, verificados, descomprimidos y ensamblados de nueva cuenta para ser entregados a los clientes de más alto nivel.

la iniciación es completada, las dos entidades tiene secretos compartidos los cuales son utilizados para encriptar registros y calcular los MAC en sus contenidos. El MAC es calculado antes de la encripción.

Protocolos Adicionales

Es posible modificar la estrategia de cifrado mediante el cambio de especificaciones de cifrado como son las llaves o el algoritmo utilizado. De igual forma existe un protocolo de alerta que permite anunciar la descripción y severidad de diversos mensajes como los errores o la finalización de la conexión para evitar el ataque por truncamiento.

Protocolo de iniciación (handshake)

Los parámetros criptográficos del estado de sesión son producidos por el protocolo de iniciación, que opera en la parte superior de la capa de registro. Cuando un cliente y servidor SSL inician por primera vez la comunicación, existe un acuerdo sobre la versión del protocolo, la selección de algoritmos criptográficos, la autentificación mutua y las técnicas de encripción de llave pública para generar los secretos compartidos.

Protocolo de datos de la aplicación

En el protocolo de datos de aplicación, los mensajes de datos de aplicación son llevados por la capa de registro y son fragmentados, compactados y encriptados según el estado de conexión actual. Los mensajes son tratados como datos transparentes a la capa de registro.

Criptografía

El intercambio de llaves, autentificación, encripción y algoritmos MAC son determinados por el servidor.

- Cálculos de criptografía asimétrica. Los algoritmos asimétricos son utilizados en el protocolo de iniciación para autentificar a las partes y para generar las llaves y secretos compartidos. Se utilizan los siguientes algoritmos: Diffie Hellman, RSA, Fortezza.
- Cálculos de criptografía simétrica. Esta técnica es utilizada para encriptar y verificar la integridad de los registros SSL y es especificada por el CipherSpec actual. Un ejemplo típico es encriptar los datos con el DES y generar los códigos de autentificación con el MD5. Antes de que la encripción segura y la verificación de integridad puedan ser realizadas en los registros, el cliente y el servidor requieren generar información secreta y compartida solo conocida por ellos. Este valor es de 48 bytes y es denominado el secreto maestro. El cual se utiliza para generar llaves y secretos para cálculos de encripción y MAC.

Los elementos mencionados previamente son parte del protocolo SSL y pueden ser representados de forma gráfica aunque parcialmente, como se muestra en el diagrama del apéndice A.

9.5.3. Análisis del protocolo SSL

El protocolo SSL requiere para su implementación seguir las siguientes recomendaciones:

- Las restricciones de exportación de US limitan las llaves RSA para encripción a 512 bits pero no establece límites en la longitud de las

llaves RSA para las operaciones de firma. Los certificados deber de ser mayores a 512 bits de longitud, dado que las llaves RSA de 512 bits no son seguras para operaciones que requieran gran seguridad. Por tanto las llaves deben de ser cambiadas diariamente o cada 500 transacciones, por ejemplo.

- SSL requiere un generador de números pseudo aleatorios criptográficamente seguro (pseudorandom number generator PRNG). Los PRNG basados en operaciones hash seguras como el MD5 y SHA son aceptables pero no proveen mayor seguridad que el tamaño del estado del generador de números aleatorios. Por ejemplo los PRNG basados en MD5 usualmente proveen 128 bits de estado.
- Las implementaciones son responsables de verificar la integridad de los certificados y debe generalmente soportar mensajes de revocación de certificados. Los certificados deben ser verificados siempre para asegurar el firmado apropiado por una autoridad certificadora confiable (CA).

De acuerdo al análisis [Wagner 96] el protocolo SSL presenta imperfecciones menores que pueden ser fácilmente corregidas sin modificar la estructura básica del protocolo. En general el protocolo SSL 3.0 provee una seguridad excelente contra la escucha y los ataques pasivos. Aunque se han revelado algunos ataques pasivos, por lo que es necesario modificar la especificación para detectar ataques como cambio del algoritmo de cifrado y el engaño de algoritmo de intercambio de llaves. Otro problema mayor es la comunicación entre SSL 3.0 y 2.0 o la intrusión para hacer creer que la otra parte utiliza la versión 2.0 del protocolo, ya esta versión tiene un gran número de problemas de seguridad que pueden ser aprovechadas. El protocolo SSL de iniciación tiene varias vulnerabilidades. Una imperfección en el protocolo no necesariamente produce una implementación vulnerable. No obstante es

necesario que la especificación prevenga explícitamente de una ataque o permita la prevención directa.

El estudio [Mitchell 97] utiliza una herramienta de análisis denominada Murφ para analizar el protocolo de inicialización de la especificación SSL 3.0. El enfoque de trabajo fue utilizar modelos escalables los cuales permiten ir incrementado las variables o condiciones y por ello el nivel de seguridad. Al ser aplicado al SSL 3.0 la herramienta no detecto problemas o riesgos de la seguridad del protocolo.

9.6. Protocolo SET

9.6.1. Introducción

Debido a las predicciones sobre el incremento de la industria del comercio electrónico, las instituciones financieras o los emisores de tarjetas de crédito o débito requieren establecer medios seguros para ofrecer a sus clientes la conveniencia y seguridad de los pagos en línea. [Brands 95] El protocolo Secure Electronic Transaction (SET) [SET 99], [Varadharajan 96] fue desarrollado en 1995 en conjunto por Visa y Martercard como un método para transacciones seguras de pago con tarjeta a través de redes abiertas. SET es publicado como una especificación abierta para la industria.

Adicionalmente a las dos empresas mencionadas se tuvo asistencia en el desarrollo de la especificación por parte de GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa y VeriSign. [Visa 97]

El protocolo SET permite satisfacer la demanda del mercado para el procesamiento de transacciones en línea, con una relación costo – beneficio aceptable y de forma segura.

Los sistemas de pagos y las instituciones financieras deben proveer servicios para transmisión confidencial, autentificación de entidades involucradas, aseguramiento de la integridad de instrucciones de pago en las ordenes de compra de bienes y servicios y autentificar la identidad del poseedor de la tarjeta de crédito o débito y el comerciante o proveedor.

Para cumplir los requerimientos mencionados anteriormente, el protocolo SET utiliza la criptografía para provee confidencialidad a la información, asegurar la integridad de los pagos y autentificar tanto al comerciante como al poseedor de la tarjeta.

Con base a lo anterior, SET define los algoritmos y protocolos necesarios para ofrecer los servicios requeridos de seguridad. La especificación denota las siguientes características:

- Confidencialidad de la información. SET utiliza la encripción de mensajes para asegurar la confidencialidad de la información.
- Integridad de los datos. SET provee las firmas digitales que aseguran la integridad de la información de pago.
- Autentificación de la cuenta del poseedor de la tarjeta. SET utiliza las firmas digitales y los certificados del poseedor de la tarjeta para asegurar la autentificación de la cuenta del poseedor de la tarjeta.
- Autentificación del comerciante. SET provee el uso de firmas digitales y certificados del comerciante para asegurar la autentificación del comerciante.
- Inter operabilidad. SET utiliza protocolos y formatos de mensaje previamente definidos para asegurar la interoperabilidad.
- El alcance de la especificación incluye la aplicación de los algoritmos criptográficos (como el RSA y DES), los formatos de mensajes de certificados, compra, autorización, captura y de los objetos en cuestión, así como los mensajes entre los participantes.

9.6.2 Protocolo SET

SET utiliza la criptografía de llave privada y de llave pública para asegurar la confidencialidad. La integridad y autentificación son aseguradas mediante el uso de firmas digitales.

Combinada con los message digest, la encripción utilizando la llave privada permite a los usuarios firmar digitalmente los mensajes. Un message digest es un valor generado por un mensaje que es único a ese mensaje. SET utiliza un par de llaves públicas y privadas para la encripción y decripción de los mensajes y otro par para la creación y verificación de las firmas digitales.

Para garantizar la autentificación es necesario una tercero de confianza para autentificar la llave pública y es denominada Autoridad Certificadora (AC) como se mencionó en la sección 8.1.1.

El diagrama del Apéndice A muestra un esquema parcial del proceso de encripción.

9.6.3. Análisis del protocolo SET

No se encontró evidencia de análisis de la seguridad del protocolo que muestren problemas. Sin embargo los comentarios son con relación a la eficiencia del algoritmo o al marcado uso a los pagos electrónicos sin proporcionar un marco completo del flujo de las operaciones del comercio electrónico.

9.7. X.509

9.7.1. Introducción

La recomendación o norma internacional X.509 [X.509 93] define un marco para ofrecer servicios de autentificación por el directorio a sus usuarios. Describe dos niveles de autentificación: simple mediante el uso de una contraseña como verificación de una identidad pretendida y fuerte, que implica credenciales formadas usando técnicas criptográficas.

Esta norma fue elaborada para facilitar la interconexión de sistemas de procesamiento de información con el fin de proporcionar servicios de directorios. El conjunto de todos estos sistemas, junto con la información contenida por el directorio pueden ser considerados como un todo integrado, llamado directorio. La información contenida por el directorio, denominada colectivamente base de información de directorio (DIB), se utiliza típicamente para facilitar la comunicación entre, con o sobre objetos tales como entidades de aplicación OSI, personas, terminales y listas de distribución.

Adicionalmente la norma define un marco para el suministro de servicios de autentificación por el directorio a sus usuarios. Estos usuarios incluyen el propio directorio, así como otras aplicaciones y servicios. El directorio puede emplearse para satisfacer las necesidades de autentificación y otros servicios de seguridad. Es el lugar natural para obtener la información de autentificación de cada una de las demás partes.

El método de autenticación fuerte especificado en esta especificación de directorio se basa en los criptosistemas de claves públicas. Es una gran ventaja de esos sistemas el que los certificados de usuario pueden estar contenidos en el directorio como atributos, y ser comunicados libremente dentro del sistema del directorio y obtenidos por los usuarios del directorio del mismo modo que

otra información de directorio. Se supone que los certificados de usuario están formados por medios «fuera de línea», y que son introducidos en el directorio por su creador. La generación certificados de usuario la efectúa cierta autoridad de certificación «fuera de línea» que está completamente separada de los DSA en el directorio. En particular, no se imponen requisitos especiales a los suministradores del directorio para almacenar o comunicar certificados de usuario en una manera segura.

El marco de autentificación fuerte no obliga a utilizar un criptosistema en particular. Se pretende que el marco sea aplicable a cualquier criptosistema de llave pública adecuado, y soportará por consiguiente cambios en los métodos usados como un resultado de futuros avances en criptografía, técnicas matemáticas o capacidades de computación. Sin embargo, dos usuarios que desean autentificar tienen que soportar el mismo algoritmos criptográfico para que la autentificación se realice de forma correcta.

El procedimiento para obtener una llave pública de un usuario es el siguiente: Para que un usuario confíe en el procedimiento de autentificación, tiene que obtener la llave pública del otro usuario desde una fuente en la cual confía. Dicha fuente, llamada autoridad decertificación (CA), usa el algoritmo de llave pública para certificar la clave pública, produciendo un certificado. El certificado, cuya forma se especifica en esta cláusula, tiene las siguientes propiedades:

- Cualquier usuario con acceso a la llave pública de la autoridad de certificación puede extraer la llave pública que fue certificada.
- Ninguna parte que no sea la autoridad de certificación puede modificar el certificado sin que esto sea detectado (los certificados son infalsificables).

Como los certificados son infalsificables, pueden publicarse insertándolos en el directorio, sin que éste tenga que tomar disposiciones especiales para protegerlos.

Una autoridad de certificación produce el certificado de un usuario firmando una colección de informaciones, incluidos el nombre distinguido y la llave pública del usuario, así como un identificador único opcional con información adicional sobre el usuario. No se especifica aquí la forma exacta del contenido del identificador único, que se deja a la autoridad de certificación y podría ser, por ejemplo, un identificador de objeto, un certificado, una fecha u otra forma de certificación sobre la validez del nombre distinguido.

El siguiente tipo de datos ASN.1 puede usarse para representar certificados:

```
Certificate ::=                 SIGNED { SEQUENCE {
version                         [0] Version DEFAULT v1,
serialNumber                                CertificateSerialNumber,
signature                                   AlgorithmIdentifier,
issuer                                  Name,
validity                                Validity,
subject                                 Name,
subjectPublicKeyInfo                        SubjectPublicKeyInfo,
issuerUniqueIdentifier          [1] IMPLICIT UniqueIdentifier OPTIONAL,
subjectUniqueIdentifier         [2] IMPLICIT UniqueIdentifier OPTIONAL
```

9.8. Resumen y Conclusiones de los Algoritmos y Protocolos para el Comercio Electrónico

La siguiente tabla muestra los mecanismos proporcionados por los algoritmos y protocolos de comercio electrónico:

	RSA	DES	MD5	SSL	SET	X.509
Autentificación	X		X	X	X	X
Confidencialidad	X	X		X	X	
Integridad			X	X	X	
No - Repudiación	X			X	X	X

TABLA 9.2: Resumen de algoritmos y protocolos

La autentificación y no-repudiación pueden ser verificados únicamente cuando la creación, almacenamiento y distribución de llaves sean confiables, solo así la identidad puede ser garantizada, como se mencionó anteriormente, la participación de una autoridad certificadora permitirá facilitar el proceso de autentificación.

No solo los algoritmos de encripción y las técnicas criptográficas requieren una revisión sobre la seguridad que proveen. Los protocolos de autentificación y de comercio electrónico también así lo requieren.

Debido a la demanda de acceso seguro para realizar compras por parte de los consumidores, los protocolos de comercio electrónico requieren de métodos formales para verificar su diseño e implementación. Es por ello que actualmente hay estudios como el [Bolignano 97] que realizan propuestas para verificar estos protocolos y así evitar amenazas a la seguridad en su utilización para el comercio electrónico.

Finalmente, la selección de los algoritmos y protocolos de comercio electrónico depende del proyecto que se requiera implementar. Para proyectos de comercio electrónico entre Persona a negocio se recomienda el uso de SSL versión 3, pero para un proyecto de negocio a negocio, el protocolo SET y el lenguaje XML son una opción que cada vez se utiliza más.

Con relación a los algoritmos, el RSA sigue siendo seguro por lo tanto se recomienda continuar con su uso. Para el caso del algoritmo DES, la situación es diferente, ya que aunque se recomienda utilizar el Triple DES, es necesario dar seguimiento al avance del es fuerzo para sustituir el algoritmo DES por parte de la NIST, ya que se encuentra en las rondas finales para liberar la especificación del nuevo algoritmo de encripción simétrica o llave privada.

El uso de firmas digitales se recomienda utilizar el MD5 ya que su seguridad es suficiente para la mayoría de los proyectos.

A continuación se presentan los proyectos que se realizaron como soporte a la base teórica, los algoritmos utilizados fueron el DES, RSA y MD5 para realizar una implementación simple del procedimiento de transferencia de información segura del protocolo SET.

CAPITULO 10

10 Proyecto de Comercio Electrónico Desarrollado

10.1 Proyecto de desarrollo de un Site de Comercio Electrónico de una Empresa Maquiladora de Ejes y Frenos para Camiones

10.1.1 Antecedentes

Con el progreso de la humanidad, el hombre a buscado la manera de hacer mas fácil la forma en que realiza su vida cotidiana, y con el desarrollo de nuevas técnicas y procedimientos de realizar las cosas lo a logrado, por este motivo desarrolla día a día nuevas herramientas, formas y procedimientos, las cuales las a llevado e implementado para con ello tratar de llevar una vida mas vida practica. Una de estas técnicas que actualmente esta teniendo un enorme auge es la de realizar transacciones comerciales con las empresas de una manera mas rápida y segura, dado que la complejidad y aunado a esto la confianza que se tiene actualmente de este tipo de procedimientos por su seguridad y eficacia, las empresas están llevando acabo inversiones en este punto para poder desarrollar sus herramientas propias para realizar dichos negocios.

Una de estas Empresa en la cual se me permitió participar de manera plena en el desarrollo e implementación de un Site del tipo comercial fue la Empresa DIRONA S.A. de C.V., en la cual tratando de competir de manera mas plena y de la manera mas eficiente, visualizo como objetivo a corto plazo el poner a funcionar un departamento que se encargara de este proyecto, en el cual se llevo acabo la tarea de buscar una manera segura, rápida y eficiente de llevar acabo las mismas. Dado que actualmente nuestro país esta sufriendo una acelerado crecimiento en su factor tecnológico y aunado a esto la competencia mas amplia de no solo en el ramo nacional, sino también en plano internacional se creo esta herramienta que trataremos de explicar más detalladamente más adelante.

DIRONA S.A. de C.V., para dar solución a este problema se creo la división llamada SUDISA, la cual se encuentra ubicada en la ciudad de Guadalajara Jalisco, y dicha división tiene como objetivo: llevar acabo el total control y manejo de todas las ventas, manejo y seguimiento de las transacciones comerciales realizadas por la empresa a través del E-commerce.

10.1.2 Descripción del proyecto

Para la realización de este objetivo se trato de visualizar todos y cada unos de los puntos requeridos por parte de la empresa y sus clientes directos e indirectos. Se crea un portal de negocios, en el cual cualquier persona que cubra con cierto perfil para ser considerado cliente de negocios, en el cual se llevara acabo la consulta, la verificación de precios, cantidad de material en existencia, la solicitud en línea del mismo y su compre, y el seguimiento correspondiente a dicha nota de compra. El portal de transacciones comerciales permitió desarrollar un agente virtual de ventas, el cual muestra sugerencias sobre las diferentes piezas que se manufacturan en la empresa así como su existencia física y su tiempo de entrega. Esto se logro mediante la inclusión de un motor de PROLOG desarrollado en el lenguaje JAVA. Este motor permite realizar inferencias sobre una pequeña base de datos la cual lleva la relación y

orden de los inventarios reales y a su vez tratar de llevar un completo orden de la producción de la empresa. La interfaz gráfica permite capturar el modelo, tipo, el destino, el costo y el tipo de pago de las notas de venta. El proyecto fue delimitado para aceptar un rango mínimo de valores y opciones de ventas, además de tener una base de conocimientos muy limitada, esto con el objeto de presentar un programa ligero para ser utilizado en un ambiente como Internet, y dado que algunos clientes no cuentan todavía con una infraestructura más poderosa para realizar sus transacciones por este medio más rápido.

10.2 Tecnologías a utilizar

El tipo de herramientas a utilizar para la realización de este proyecto, es envase al tipo de aplicaciones de uso común actualmente en la industria de las telecomunicaciones e informática y normas y reglamentos que rigen este tipos de negocios, actualmente en nuestro país y a nivel mundial. Para lo cual se considero la normativa del tipo de trafico (o flujo) de datos que circulan a través de Internet actualmente, además tomando en cuenta el echo de que aun en estos días, algunas empresas se niegan a estar invirtiendo constantemente en nuevos equipos y materiales de telecomunicaciones, se trato de utilizar un sistema complejo el cual permitiera en pocos segundos el llevar acabo cierto tipo de operaciones en el menor tiempo posible. Para lo cual se utilizaron las herramientas como son Java el cual permite el desarrollo de aplicaciones cliente - servidor que se ejecutan en un navegador de Internet. Adicionalmente se utilizó una implementación de CORBA denominada Orbacus CORBA, permitiendo así el diseño de una aplicación distribuida para el procesamiento de transacciones, también se utilizo la Herramienta de seguridad de logi.crypto, las cuales son una implementación de los principales algoritmos de seguridad como son: DES, RSA, MD5, etc. Estas librerías permitieron realizar la implementación del esquema de seguridad según el protocolo SET., Lenguaje C++ por ser un complemento de para la puesta en marcha de dichas herramientas, Xml por ser un lenguaje de programación de paginas electrónicas

de alta complejidad, Remote Method Invocation (RMI) de Java el cual sirve para manejar y manipular bases de datos en tiempo real no importando la ubicación del usuario que la manipule, de los navegadores de Internet Nestcape y Explorer sus librerías de seguridad en su condigo fuente, así como el plug-in de VRML (Cosmoplayer) por ser un medio complejo y de baja cantidad de requerimientos para manipulación de base de daos lo cual es muy satisfactorio ya dado que la gran mayoría de los usuarios en la actualidad no cuentan con la infraestructura tan actualizada en sus sistemas de comunicaciones.

Considerando el flujo de capital que se lleva acabo en este tipo de giros comerciales, se tienen que utilizar las mejores herramientas tanto humanas como del tipo electrónico.

Teniendo como antecedente lo anterior, también se procedió a la implantación de un sistema de control de flujo de usuarios para interactuar con los servidores en los que se colocaría la información, se colocaron candados de protección llamados Proxy´s que funcionan como escudos y filtran la información que pasa por ellos.

10.3 Proceso de Operación

El proceso de manejo de este Site por parte de los usuarios o clientes a manejar nuestra información vital, se manejo de la siguiente manera:

Dar de alta un cada uno de los usuarios, para esto se le asigno un Login y un Password único de identificación, el cual no puede ser alterado ni modificado en línea, para mayor seguridad y confianza de parte de un cliente.

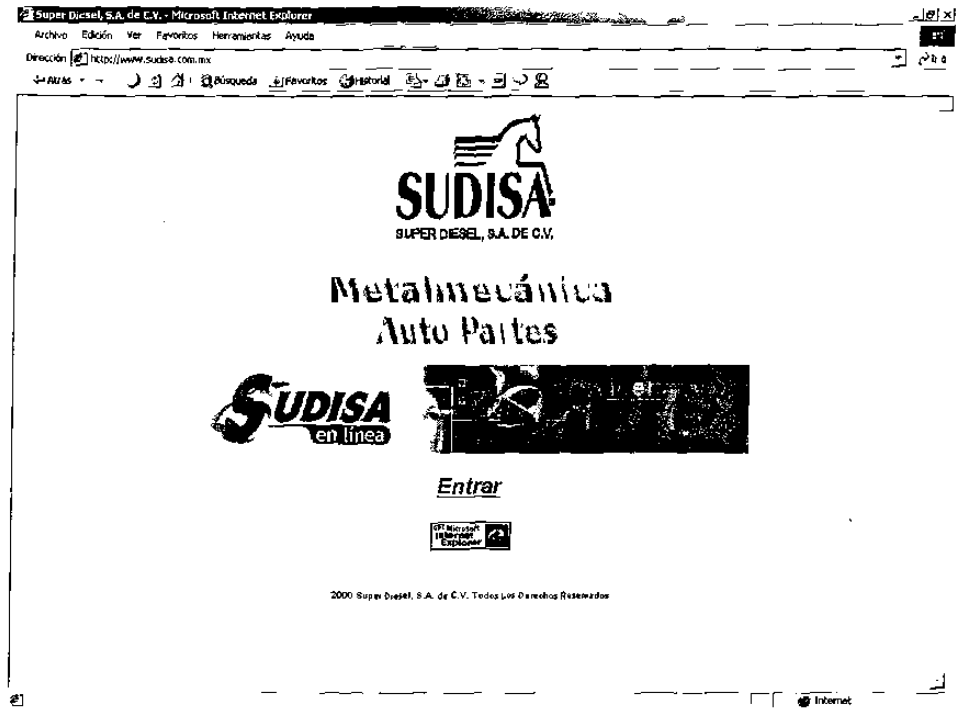


FIGURA 10.1: Pagina de presentación de nuestro proyecto.

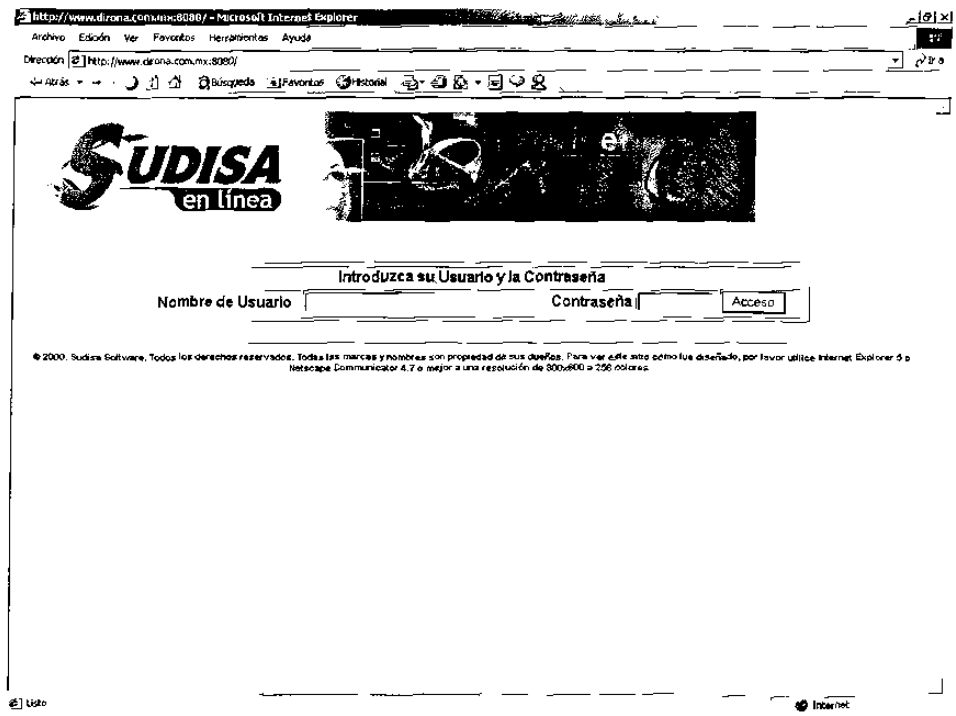


FIGURA 10.2: Pagina de identificación de Usuarios.

En dado caso de que el usuario no sea reconocido por el sistema, el usuario es ubicado en un sistema básico de consulta simple de datos.

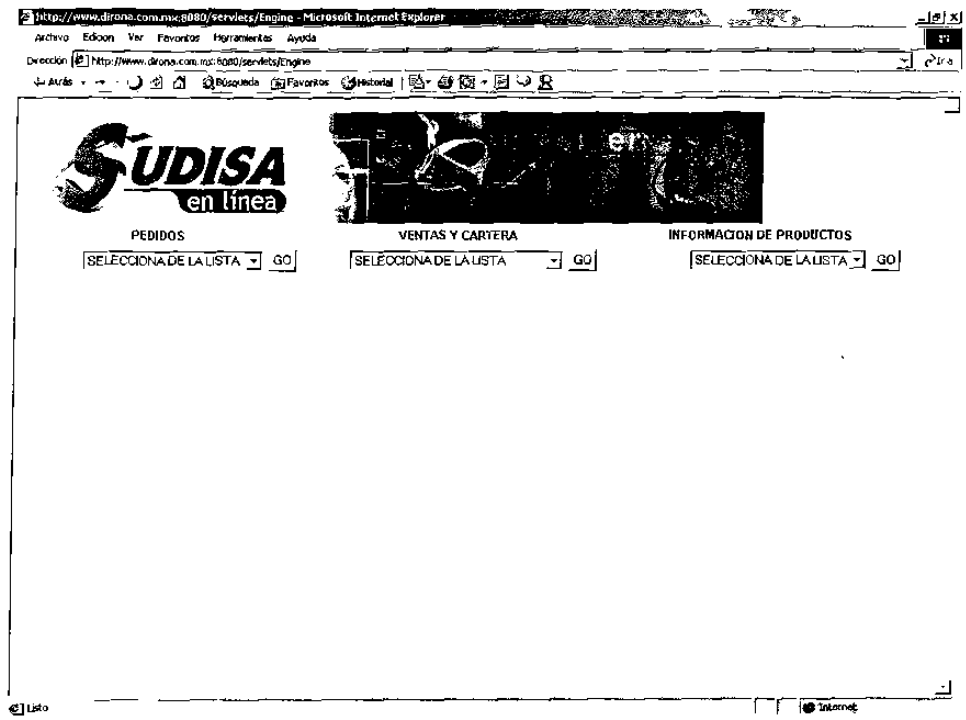


FIGURA 10.3: Despliegue de pagina de consulta simple.

Si del caso contrario su identificación es adecuada en el sistema, se le despliega la misma pantalla, pero mostrando un pequeño cambio el cual consiste en dar una bienvenida.

En la siguiente serie de figura se muestran los primeros 3 menús con operaciones básicas de consulta de pedidos, captura del mismo, manejo de estados de cuenta, y existencias de los mismos entre otras cosas.

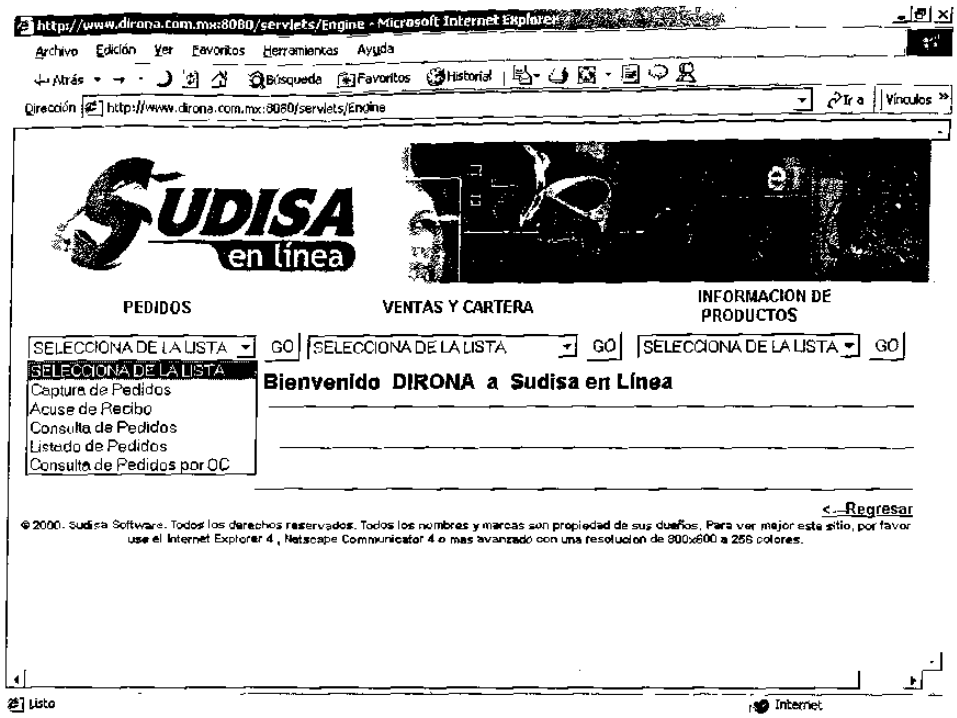


FIGURA 10.4: Despliegue del primer menú.

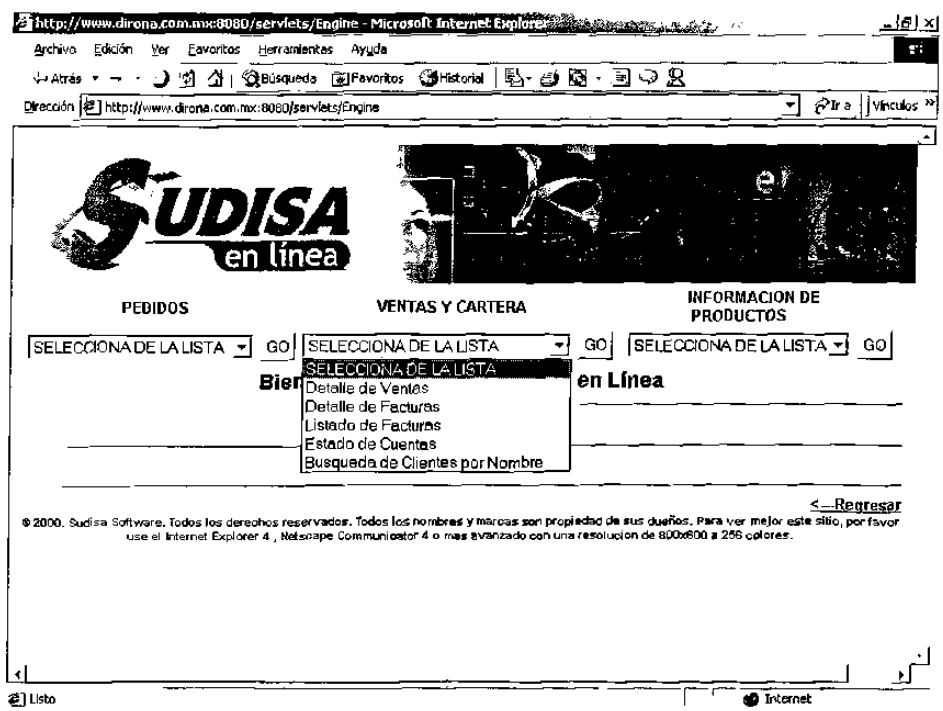


FIGURA 10.5: Despliegue del segundo menú.

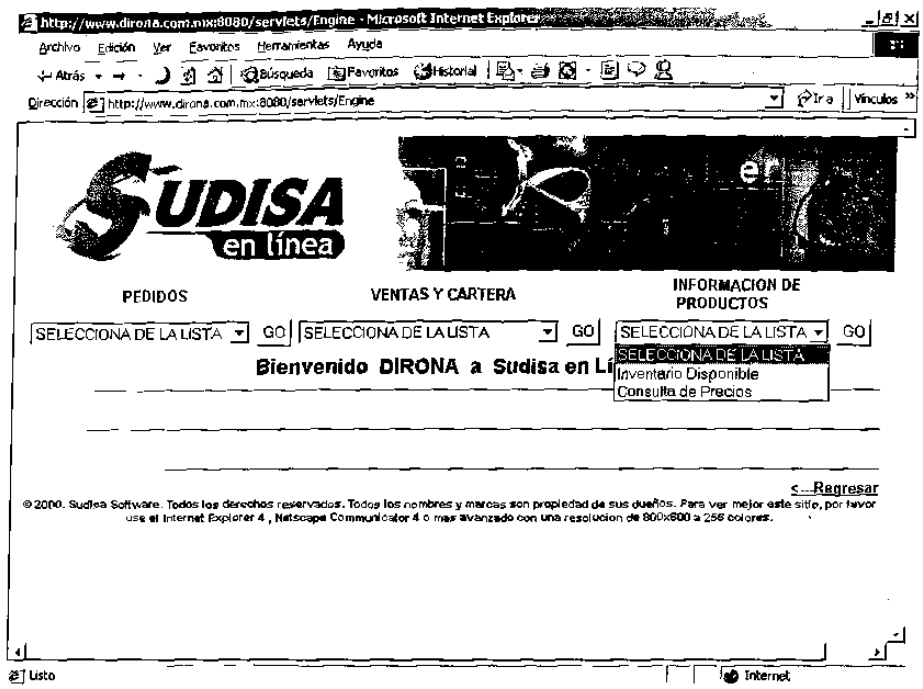


FIGURA 10.6: Despliegue del tercer menú.

En la pantalla siguiente se muestra la forma de llenado de una forma para la captura y levantamiento de una orden de pedido de piezas.

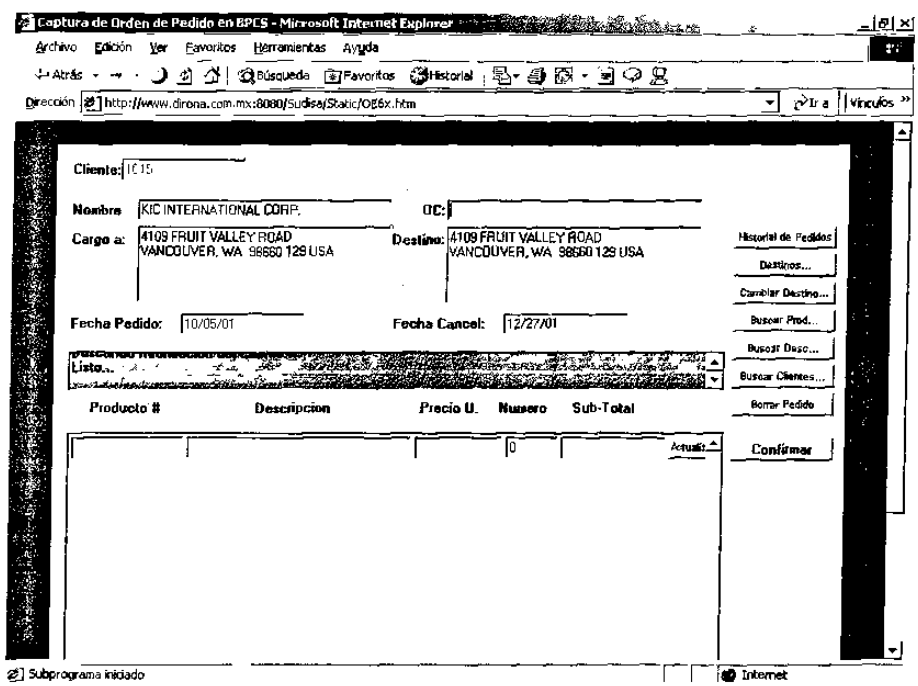


FIGURA 10.7: Despliegue la forma de solicitud de pedido.

En la que se puede apreciar como datos primarios en nombre del cliente, su dirección fiscal del mismo y el lugar donde se proceda a depositar la carga, además de anexar información referente a la fecha de solicitud del mismo y fecha máxima para la cancelación del mismo, y en la parte inferior una descripción detallada de cada una de las piezas a adquirir por parte del cliente, a la derecha se puede apreciar una serie de botones que dan paso a cada una de las operaciones de llenado de la forma descrita.

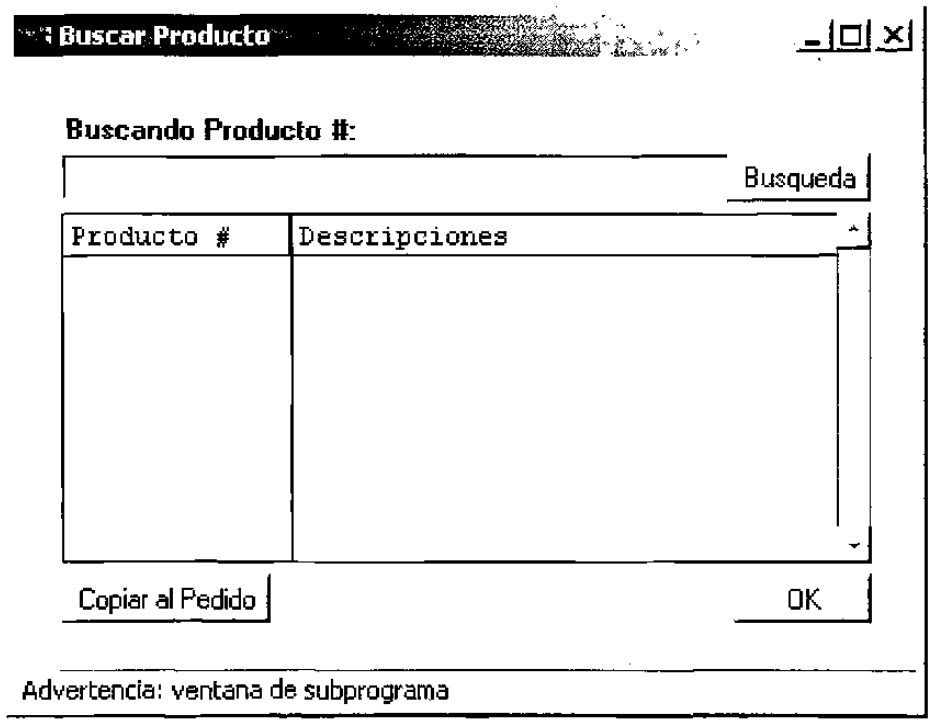


FIGURA 10.8 Menú búsqueda de productos.

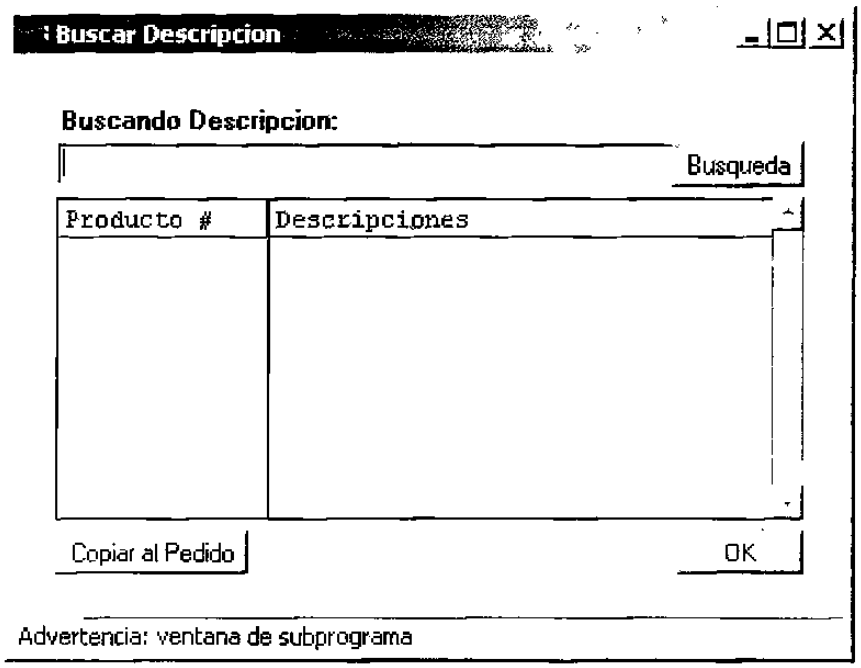


FIGURA 10.9 Menú búsqueda de articulo por numero de parte.

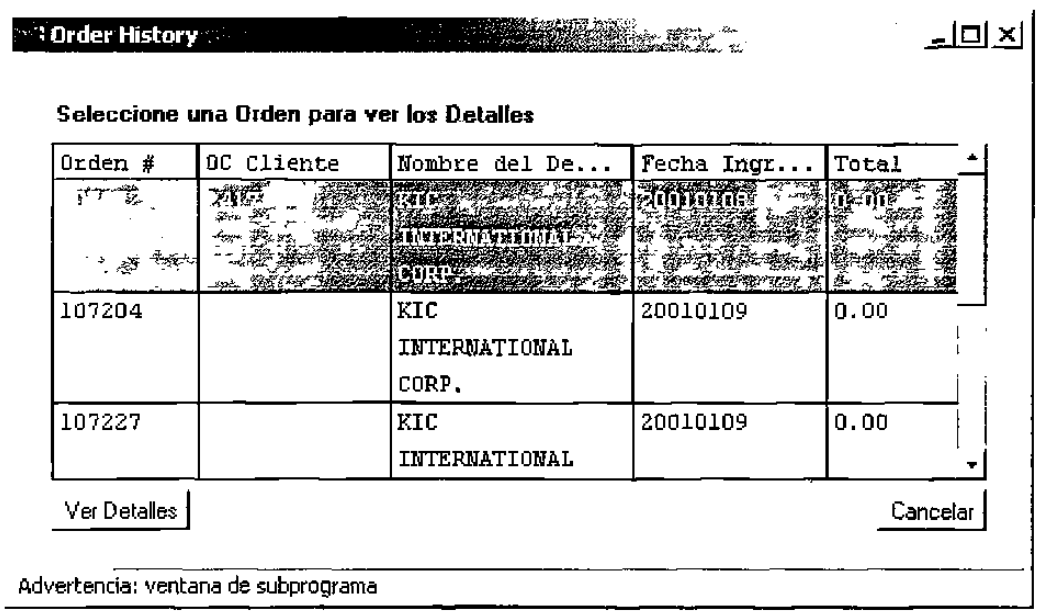


FIGURA 10.10 Menú detallando cada uno de los pedidos del cliente.

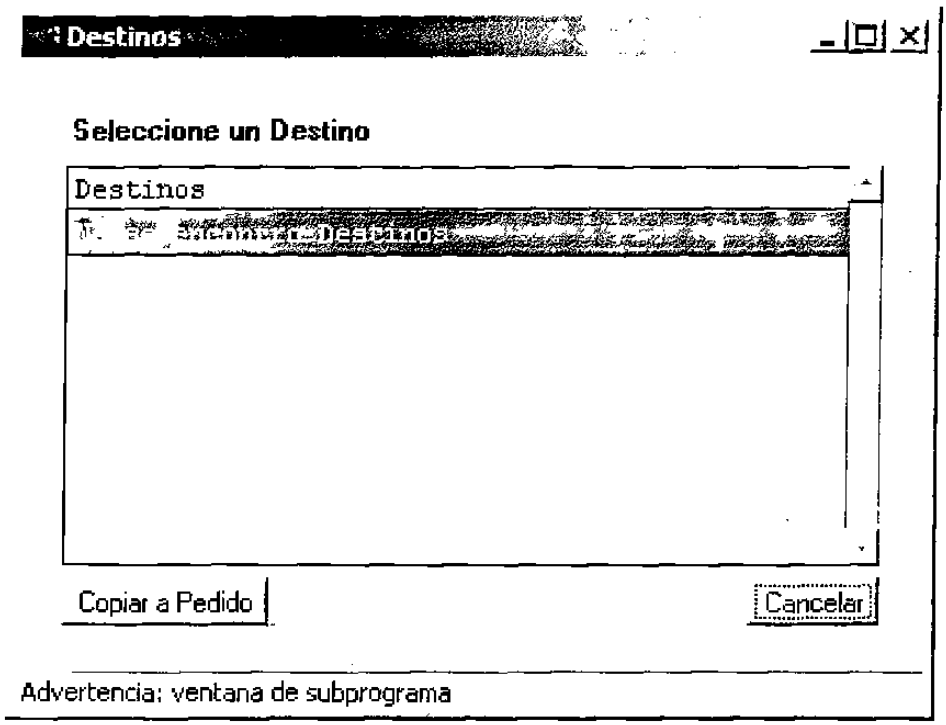


FIGURA 10.11 Menú de verificación de destino.

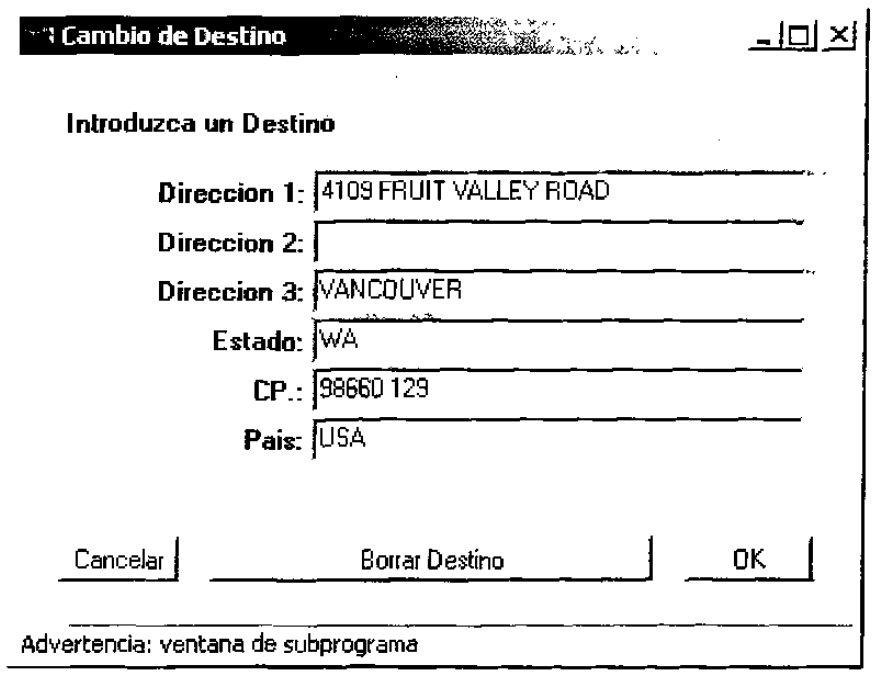


FIGURA 10.12: Menú de modificación del destino.

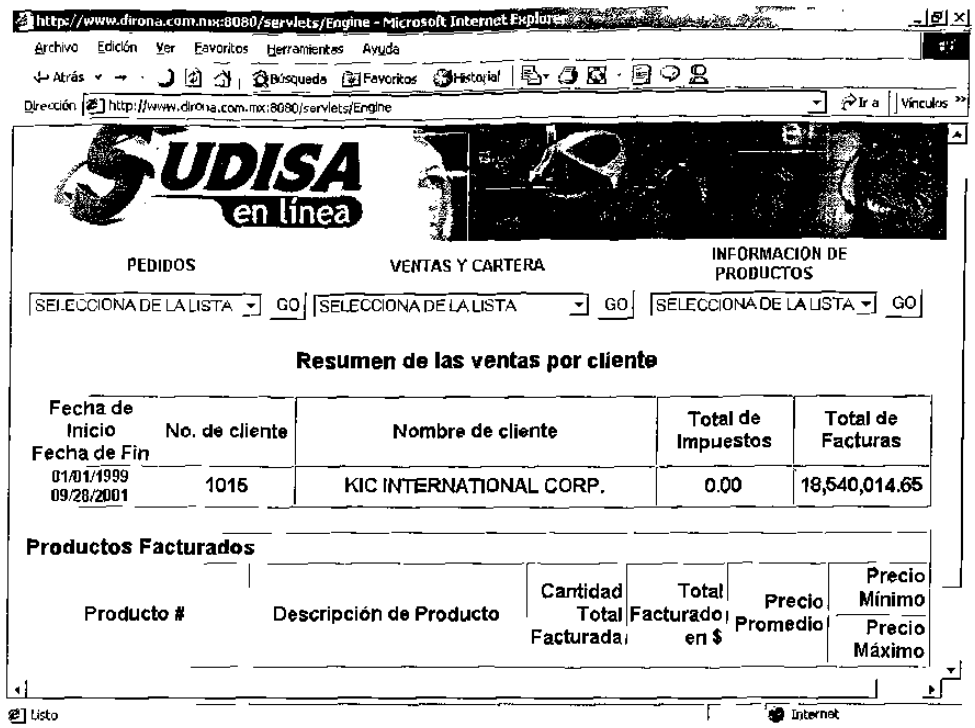


FIGURA 10.13: Resumen de ventas realizadas.

10.4 Conclusiones

La puesta en marcha de este tipo de proyectos deja muchas buenas expectativas a todos las personas que quieren poder cubrir más ampliamente las inquietudes, su poder de crecimiento y bajos costos de operación dado que siempre se puede mantener un contacto directo entre el proveedor y su cliente.

Para las personas que deseen o quieran desarrollar un campo de trabajo, este nueva forma de trabajo es altamente satisfactorio, dado que su potencial de crecimiento es muy elevado.

Como nota final se tienen que considerar los siguientes puntos para una correcta puesta en marcha de un proyecto parecido.

Problema Detectado	Solución o trabajo a futuro
Autentificación mutua entre el cliente y el servidor	Utilización de encripción asimétrica, lo cual a su vez generó el siguiente problema
Administración y distribución de las llaves públicas utilizadas para autentificar	Es necesario realizar una investigación para dar solución a este problema y se deja como un trabajo a futuro la distribución, almacenamiento y administración de llaves públicas o certificados. Lo anterior quedó fuera del alcance de este proyecto
Excesivo el tiempo de envío del servidor al cliente de la librería de CORBA	Las librerías de CORBA deben de ser incluidas en los navegadores. Aunque se encuentran algunas versiones incompletas del estándar en el Netscape
Falta de análisis de los algoritmos utilizados en la implementación y específicamente en las librerías utilizadas para evitar problemas de seguridad como puertas traseras o caballos de Troya.	Es necesario incluir en la metodología de desarrollo de sistemas de comercio electrónico una etapa durante la cual se realice un análisis de las librerías de seguridad que serán utilizadas en el proyecto

TABLA 10.1 Problemas y Soluciones a Futuro.

CAPÍTULO 11

11 Conclusiones y Recomendaciones

11.1 Conclusiones

El trabajo de investigación realizado en el desarrollo de la tesis permitió identificar los cambios y requerimientos necesarios para incursionar en el comercio electrónico, el cual tendrá un gran crecimiento en el número de usuarios del Internet, que es actualmente de más de 200 millones en todo el mundo. Queda claro el potencial para el intercambio de productos, servicios o información por medio de este nuevo medio de venta y distribución.

Existe una gran cantidad y diversidad de sitios en Internet que ofrecen productos, servicios o información bajo el esquema de negocio a persona y negocio a negocio.

Actualmente en México se requiere avanzar en temas y aspectos legales, económicos, sociales y políticos para aprovechar la ventaja competitiva que ofrece el comercio electrónico, con la consecuente reducción de costos de operación. La generación de nuevos productos y servicios, y la necesidad de recursos humanos especializados. Debido al retraso en México del comercio digital, existen múltiples oportunidades que pueden ser aprovechadas por emprendedores, así como la generación de proyectos de investigación y vinculación del área académica y empresarial. Derivado de los anterior, es

posible crear las empresas denominadas "Internet Startups", las cuales presentan un gran riesgo pero también una gran oportunidad.

La tecnología se encuentra lista para enfrentar los requerimientos de infraestructura de comunicaciones, hardware, software y seguridad que requieren las aplicaciones de transacciones electrónicas. A pesar de ello es necesario realizar un análisis de riesgo que permita identificar y cuantificar los riesgos al realizar un proyecto de comercio electrónico.

Durante el desarrollo del proyecto de implementación del protocolo SET, el cual se basó en el esquema básico de seguridad presentado en el Apéndice A permitió detectar algunos problemas como fueron: la administración y distribución de llaves, validación de la seguridad en las librerías de código, el uso e implementación de algoritmos más seguros, entre otros.

El uso de certificados por parte de las empresas debe de ser extendido a los usuarios finales, así como la creación de autoridades certificadores y la legislación correspondiente. Por otra parte es necesario definir nuevos protocolos de comercio electrónico que complementen la capacidad de pagos electrónicos del SET. Para ello el uso del XML debe permitir un mayor intercambio de información de forma transparente entre las empresas.

La hipótesis presentada en la tesis fue que es posible minimizar los riesgos de la seguridad del comercio electrónico a través de Internet siempre y cuando se utilicen los mecanismos, técnicas, algoritmos y protocolos adecuados, los cuales deben de ser analizados de forma continua, ya que pueden ser atacados en cualquier momento poniendo al descubierto su vulnerabilidad.

Por tanto, la correcta selección e implementación de los mecanismos, técnicas, algoritmos y protocolos para el comercio electrónico permite garantizar

con un alto porcentaje la seguridad en las transacciones electrónicas a través de Internet.

Por lo anterior, la realización de un proyecto de comercio electrónico presenta retos que van desde la base teórica del comercio electrónico y la estrategia hasta la selección de los mecanismos, técnicas, algoritmos y protocolos de comercio digital. La investigación y el desarrollo de la clínica empresarial logró cumplir el objetivo de presentar una confrontación de la teoría con un proyecto real, el cual identificó la complejidad de los proyectos de comercio electrónico.

Finalmente en el Apéndice A se incluyó una guía del documento que pretende unificar los conceptos presentados en este documento de forma gráfica, permitiendo identificar los temas relevantes para el desarrollo de un proyecto de comercio electrónico tanto para el modelo de negocio a persona como el modelo de negocio a negocio, el cual incluye el modelo de intra-negocio.

11.2 Recomendaciones

El desarrollo del presente trabajo de tesis sobre el comercio electrónico y la seguridad inherente a cualquier sistema distribuido, deja algunas incógnitas que deberán ser aclaradas y detalladas en diversos trabajos en un futuro.

Es necesario desarrollar proyectos de comercio electrónico utilizando el estándar XML y SSL, con el objetivo de evaluar de forma práctica las ventajas y desventajas de ambas tecnologías, además de identificar situaciones o problemas distintos a los presentados en esta tesis en la implementación de un proyecto de comercio electrónico.

Un proyecto que involucra ambas tecnologías es un "digital marketplace", el cual permite a un grupo de empresas realizar las operaciones de compra y venta mediante el apoyo de un sistema capaz de extender dichas operaciones a un tercero.

Adicionalmente es necesario desarrollar una guía de seguridad que permita definir un procedimiento de verificación de la autentificación, confidencialidad, integridad y no - repudiación.

Además de incluir un estudio profundo sobre la seguridad bajo el enfoque matemático. Es importante incluir lineamientos base para la definición de una estrategia de comercio digital y profundizar en los aspectos económicos, de negocios, sociales y legales requeridos para una incursión en esta nueva forma de realizar negocios de forma electrónica.

BIBLIOGRAFIA

1. Advanced Encryption Standard [AES 99], NIST, http://csrc.nist.gov/encryption/aes/, Año de Consulta 2001

2. Alberts Robert J. [Alberts 98], Townsend Anthony M., Whitman Michael E., The Threat of Long-Arm Jurisdiction to Electronic Commerce, Communications of the ACM, Diciembre 1998, Vol 41. No 12.

3. Comité Editorial AMECE [AMECE1 99], La Factura Electrónica: un documento que las empresas ya están esperando, http://www.amece.com.mx/f_bole22.html, Noviembre 2000

4. GILCE [AMECE2 99] y la legislación del Comercio Electrónico, http://www.amece.com.mx/f_bole24.html, Diciembre 2000

5. Anderson Ross J. [Anderson 99], Why Cryptosystems Fail, Communications of the ACM, Noviembre 2000 Vol. 37 No. 11, pg. 32-40

6. Applegate [Applegate 96], L.M., Holsapple, C.W., Kalakota, R., Radermacher, F.J., y Whinston, A.B., Electronic commerce: building blocks of new business oportunity. J. Organiz. Comput. Electr. Comm. 6. 1 (1997), pg. 1-10

7. Baldwin Robert W. [Baldwin 97], Chang C. Victor, Locking the e-safe, IEEE, Febrero 1997, pg. 40-46.

8. Banamex [Bnx_edi 99], EDI, http://www.banamex.com/portal/banamex/bdigital/edi.htm, Año de Consulta 2001

9. Bolignano Dominique [Bolignano 97], Dyade GIE, Towards the Formal Verification of Electronic Commerce Protocols, IEEE, 1997, pg. 133-146.

10. [Bosak 99] Bosak Jon, Bray Tim, XML and the Second-Generation WEB, Scientific American, Mayo 1998.

11. BOTTS Steve [Botts 96], The Internet as a Key Element of your EDI Strategy, Premenos Corp., 1996,, http://www.commerce.net/events/conference/1996/edi/index.htm

12. Brands Stefan [Brands 95], Electronic Cash on the Internet, IEEE, 1997, pg. 64-84

13. [Burrows 90] BURROWS MICHAEL, ABADI MARTIN, ROGER NEEDHAM, A Logic of Authentication, ACM Transactions on Computer Systems, Vol 8, No. 1, Febrero 1999, Páginas 18-36.

14. Camp L. Jean [Camp 97], Sirbu Marvin, Critical Issues in Internet Commerce, IEEE Communications Magazine, Mayo 1998, pg. 58-62.

15. [Carter 98] Carter Glyn, A matter of trust, IEEE , 1999

16. [Clarke 98] CLARKE, Roger, Electronic Data Intechange (EDI): An Introduction, Xmax Consultancy Pty Ltd, Australian National University, Diciembre 1999, http://www.anu.edu.au/people/Roger.Clarke/EC/EDIIntro.html

17. CORNELLA [Cornella 99], Alfonso, Ciclo de Vida y Cadena de Valor en Información, EXTRA!-NET, El impacto de la información online en las organizaciones, Mensaje 162, ESADE Barcelona, 1999. http://www.extra-net.net/articulos/en961009.htm

18. Courouris G. [Coulouris 94], Dollimore J., Kindberg T., Distributed Systems: Concepts and Design, Addison – Wesley, Febrero 1996.

19. http://orgwis.gmd.de/focus.html#SWB, http://www.dml.cs.ucf.edu/cybrary/fyi_cscw.html, Año de Consulta 2001

20. Cudi – Corporación Universitaria para el Desarrollo de Internet, Antecedentes, WWW, http://www.internet2.edu.mx/antece.htm, Año de Consulta 1999

21. Cudi [CUDI_MX2 99]– Corporación Universitaria para el Desarrollo de Internet, Miembros, WWW, http://www.cudi.edu.mx/membre.htm, Año de Consulta 2001

22. Chew Suan-Suan, Kok-Leong Ng, Chye-Lin Chee, Iauth: An Authentication System for Internet Applications, IEEE, 1997, pg. 654-659

23. http://www.nist.gov/ [DES_FIPS_46-1 88] Fecha de Publicación 22 de enero de 1988

24. http://csrc.ncsl.nist.gov/cryptval/des/fr990115.htm, Publicación 15 de enero de 2000

25. DES Modes of Operation [DES_FIPS_81 80], Publicación en diciembre 2 de 1980

26. DES Challenge [DES_CHAL_III 99] III http://www.rsa.com/rsalabs/des3/des3_qa.html, Año de Consulta 1999.

27. Deswarte Yves [Deswarte 97], Internet Security Despite Untrustworthy Agents and Components, IEEE, 1997, pg. 218 –219

28. Distributed net [DISTRIBUTED_NET 99], http://distributed.net, Año de Consulta 2001

29. DTD [DTD 00], http://www.w3.org/XML/1998/06/xmlspec-report/ 19980910.htm, Año de Consulta 2000

30. Enterprise Java Beans (EJB) [EJB 00] , Año de Consulta 2000, http://java.sun.com/products/ejb/index.html, http://java.sun.com/products/ejb/newspec.html, http://java.sun.com/products/ejb/docs.html,

31. ENIAC Page [Eniac 98], Qué es EDI?, 1998, http://www.eniac.com/edihtm.htm

32. EURO PAPERS [EURO 00], http://europa.eu.int/euro/html/rubrique-defaut5.html?rubrique=133&lang=5, Año de Consulta 2000

33. Fúster Amparo [Fúster 98], Martínez Dolores de la Guía, Hernández Luis, Montoya Fausto, Muñoz Jaime, Técnicas Criptográficas de protección de datos, Alfaomega, 1998

34. Garcés Rosas José [Garcés 98], Moreno Ledezma Gabriel, La Oferta de Servicios Internet en México, Tendencias Generales 1997-2002, Select - IDC, 1998.

35. XML Reality Check [Gartner 99], GartnerGroup, Conference presentation, 1999

36. Gleick James, The End of Cash, http://www.around.com/money.html,[Gross 99] Gross Neil, Building Global Communities, Business Week, Marzo 22 1999, pg. EB22– EB23.

37. Hamm Steve [Hamm 99], Stepanek Marcia et al., Electronic Business a Survival Guide, Business Week, Marzo 22 2000, pg. EB6 – EB27.

38. [Hsiao 79] Hsiao David K. [Hsiao 79], Kerr Douglas S., Madnick Stuart E., Computer Security, Academic Press ACM Monograph Series, 1989

39. Hsu Yung-Kao [Hsu 98], Seymour Stephen P., AN INTRANET SECURITY FRAMEWORK BASED ON SHORT-LIVED CERTIFICATES, IEEE, Marzo – Abril 1998.

40. HTML [HTML 00], Año de Consulta 2000 http://www.w3.org/TR/html4/, http://www.ietf.org/rfc/rfc1866.txt,

41. IBM Application Framework for e-business [IBM1 00], Año de Consulta 2000, http://www-4.ibm.com/software/ebusiness/AppServices.html

42. Arquitectura Tecnológica (IBM) [IBM2 00], Año de Consulta 2000, http://www-4.ibm.com/software/ebusiness/e-comServices.html, http://www-4.ibm.com/software/ebusiness/paper-arch_overview.html.

43. INEGI [INEGI1 00], Estructura Poblacional de México, WWW, http://www.inegi.gob.mx/poblacion/espanol/estrupob/pob_01.html, Año de Consulta 2000

44. Mission de Internet 2 [InternetII_A 00], WWW, Año de Consulta 2000 http://www.internet2.edu/html/mission.html#,

45. http://www.internet2.org [InternetII_B 00], Año de Consulta 2000

46. Comisión Europea [Ispo_cec 99], Electronic Commerce - An Introduction, Julio 1999, http://www.ispo.cec.be/ecommerce/answers/introduction.html

47. Jayaram N.D. [Jayaram 98], Morse P L R, NETWORK SECURITY - A TAXONOMIC VIEW, IEEE, Año de Consulta 1998

48. Java Database Connectivity (JDBC) [JDBC 00], Año de Consulta 2000, http://java.sun.com/products/jdbc/index.html, http://java.sun.com/products/jdbc/datasheet.html, http://java.sun.com/products/jdbc/features.html, http://java.sun.com/products/jdk/1.3/docs/guide/jdbc/index.html

49. Java Server Pages (JSP) [JSP 00], Año de Consulta 2000, http://java.sun.com/products/jsp/index.html

50. Kalakota Ravi [Kalakota 96], B. Whinston Andrew, FRONTIERS OF ELECTRONIC COMMERCE, 1996.

51. Kalakota Ravi[Kalakota 97], B. Whinston Andrew, ELECTRONIC COMMERCE A Manager's Guide, 1998

52. Kapidzic Nada, Davidson Alan, A Certificate Management System: Structure, Functions and Protocols, IEEE, 1995, pg. 153-160.

53. G.W. Keen Peter [Keen 97], Balance Craigg, ON – LINE PROFITS A MANAGER'S GUIDE TO ELECTRONIC COMMERCE. Harvard Business School Press Boston, Massachusetts, 1997.

54. Krause Micki [Krause 99], Tipton Harold F., Handbook of Information Security Management, 1999, editorial Auerbach.

55. Lobel Mark [Lobel 99], The Case for Strong User Authentication, Security Dynamics, http://www.securid.com/products/whitepapers/casestrong-wp.html, Año de Consulta 1999

56. LOTUS NOTES [LOTUS_NOTES 00], Año de Consulta 2000 http://www.lotus.com/home.nsf/welcome/notes, http://www.lotus.com/home.nsf/welcome/domino, http://www.lotus.com/products/r5web.nsf/webfamilypi/Family+of+Servers?opendocument, http://www.lotus.com/home.nsf/welcome/learnspace,

57. Lu W.P. [Lu 92], Sundareshan M.K., Enhanced Protocols for Hierarchical Encryption Key Management for Secure Communication in Internet Environments, IEEE Transactions on Communications, Vol 40 No 4, Abril 1992, pg. 658 – 660

58. Machover Carl [Machover 97], Internet Business Opportunities, IEEE, 1997, pg. 138-143.

59. Marín Erasmo [Marín 99], Comentarios a la Modificación del Artículo 211 del Capítulo II del Código Penal "Acceso Ilícito a Sistemas y Equipos de Informática", Revista Soluciones Avanzadas, Volumen 7, No. 71, Julio 1999, pg. 23-24.

60. Fischer Mathew [Mathew 00], How to implement the Data Encryption Standard, Eurocrypt informations, http://www.satswiss.com/twinpics/des-how-to.html, Año de Consulta 2001

61. McClure Stuart [Mcclure 98], PKI tames network security. (developing a public key infrastructure), InfoWorld, Septiembre 14 1998 v20 n37 pg65.

62. McChesney Michael C. [mcchesney 97], Banking in cyberspace: an investment in itself, IEEE SPECTRUM, Febrero 1997, pg. 54-49.

63. Mitchell John C. [Mitchell 97], Shmatikov Vitaly, Stern Ulrich, Finite-State Analysis of SSL 3.0 and Related Protocols, Stanford University, Agosto 1997.

64. http://www.intel.com/intel/museum/25anniv/hof/moore.htm, Año de consulta 2000

65. NIST [Nist 92], The Digital Signature Standard, Communications of the ACM, Julio 1999 Vol. 35, No. 7, pg. 36 – 40

66. [NUA1 00] Nua Internet Surveys, How Many Online, WWW, http://www.nua.ie/surveys/analysis/graphs_charts/comparisons/how_many_online.html,, Año de Consulta 2000

67. Nua Internet Surveys [NUA2 00], Ecommerce US, WWW, http://www.nua.ie/surveys/analysis/graphs_charts/comparisons/ecommerce_us.html, Año de Consulta 2000

68. Nua Internet Surveys [NUA3 00], América Latina, WWW, http://www.nua.ie/surveys/how_many_online/s_america.html, Año de Consulta 2000

69. Oppliger Rol f[Oppliger 95], Internet security enters the Middle Ages, IEEE, Octubre 1998, pg. 100-101

70. http://www.intel.com/PentiumIII/ [Pentium_III 00], Año de Consulta 2000

71. Pretyy Good Privacy [PGP 00], Año de Consulta 2000, http://www.pgpi.org, http://www.pgpi.org/doc/pgpintro/,

72. Understanding Public Key Infrastructure (PKI) The Key Management Problem [PKI 99], Security Dynamics, Año de Consulta 1999, http://www.securid.com/products/whitepapers/pki/index.html

73. Project Management Institute [PMBOK1 99], A Guide to the Project Management Body of Knowledge, 1996, PMI Publishing Division, WWW, Año de Consulta 1999, http://www.pmi.org/publictn/pmboktoc.htm

74. Ponce Bob [Ponce 99], The Impact of MP3 and the Future of Digial Enterteinment Products, IEEE Communications Magazine, Septiembre 1999.

75. Pulido Karla [Pulido 99], EDI y XML en el comercio electrónico entre empresas, Trabajo de Tesis, ITESM - CCM, 1999.

76. Rajsbaum Sergio [Ra0jsbaum 99], Panorama General de Criptografía y seguridad, Parte II, Soluciones Avanzadas, Año 7 #71, Julio 99, pg. 38-48

77. RDF [RDF 00], Año de Consulta 2000, http://www.w3.org/RDF/

78. R. Rivest [RFC1320 92], RFC 1320, The MD4 Message-Digest Algorithm, http://andrew2.andrew.cmu.edu/rfc/rfc1320.html, Abril 1992.

79. R. Rivest [RFC1321 92], RFC 1321, The MD5 Message-Digest Algorithm, http://andrew2.andrew.cmu.edu/rfc/rfc1321.html, Abril 1992.

80. Rheingold Howard [Rheingold 99], The Internet and the Future of Money, Tomorrow Column, http://www.transaction.net/press/tomorrow.html, Año de Consulta 1997

81. Riggins Frederick J. [Riggins 98], Rhee Hyeun-Suk (Sue), Toward a unified view of Electronic Commerce, Communications of the ACM, Octubre 1998 Vol. 41 No. 10, pg. 88 – 95.

82. RSA Laboratories [RSA 99] , FAQ About Today's Cryptography v4.0 http://www.rsa.com, Año de Consulta 1999

83. Russ Mundy [Russ 97], Chair, Panel On Security Of The Internet Infraestructure, IEEE,1997, pg. 72

84. Universidad Virtual [RUV 99], ITESM, http://www.ruv.itesm.mx, Año de Consulta 2000

85. Saha Avi [Saha 99], Application Framwork for e-business:Portals, IBM Software Strategy, November 1999, http://www-4.ibm.com/software/developer/library/portals/index.html

86. SDH Pocket Guide [SDH 00], Año de Consulta http://www.wg.com/techlibrary/articles/sdh_guide1.html

87. The Role of Strong Authentication in Securing Business Over the Internet [securitydynamics WP], Whitepaper Security Dynamics.

88. Java Servlets [Servlets 00], Año de consulta 2000, http://java.sun.com/products/servlet/index.html, http://java.sun.com/products/servlet/2.2/, http://java.sun.com/products/servlet/2.2/javadoc/index.html.

89. SET [SET 99], Año de Consulta 1999, http://www.setco.org/, http://www.setco.org/set_specifications.html

90. Sheperd Simon J [Sheperd 96], LESSONS LEARNED FROM SECURITY WEAKNESSES IN THE NETSCAPE WORLD WIDE WEB BROWSER, IEEE, 1996

91. Sirbu Marvin A. [Sirbu 97], Credits and debits on the Internet, IEEE SPECTRUM, Febrero 1997, pg. 23-29.

92. Social Web Research Program [Social_web 00], http://orgwis.gmd.de/projects/SocialWeb/, Año de Consulta 00

93. SONET Telecommunications Standard Primer [SONET 00], http://www.tek.com/Measurement/App_Notes/SONET/, Año de Consulta 2000

94. Freier Alan O. [SSL 96], Karlton Philip, Kocher Paul C., The SSL Protocol Version 3.0, Internet Draft, Netscape Communications Corporation, Marzo 1999

95. Internet Startups [Startups 00], http://www.internetnews.com/bus-news/article/0,1087,3_314701,00.html, Año de Consulta 2000

96. Steinauer Dennis D. [Steinnauer 97], Wakid Shukri A., Rasberry Stanley, Trust and Traceability in Electronic Commerce, Standard View Vol 5. No 3, Septiembr 1997, pg. 118-124.

97. Stockel Anna [Stockel 95], Securing Data and Financial Transactions, IEEE, 1998, pg. 397- 401.

98. Tidwell Doug [Tidwell 99], Tutorial: Introduction to XML, XML developerWorks Team, Julio 1999, http://www.ibm.com/developerWorks

99. Recomendación UIT – T X.509 [X.509 93], diciembre de 1993. Servicios de Directorio. Autenticación.

100. Margherio, ET. AL. [USDC 99], The emerging digital economy, U.S. Department of Commerce, Año de consulta 1999

101. U.S Government Working Group on Electronic Commerce [USGWGEC 98], First Annual Report, Noviembre 1999

102. Varadharajan Vijay [Varadharajan 96], Mu Yi, On the Design of Secure Electronic Payment Schemes for Internet, IEEE, 1996, pg. 78-87.

103. SET Secure Electronic Transaction Specification Book 1: Business Description, Visa – Mastercard [Visa 97], Mayo 31 de 1999.

104. Visa México [Visa_mx 99], http://www.visa.com.mx/s3_tec_com3.html, Año de Consulta 2001

105. Wagner David [Wagner 96], Schneier Bruce, Analysis of the SSL 3.0 protocol, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, Noviembre 1996, pp. 29-40. http://www.counterpane.com/ssl.html

106. Weiss Mark Allen [Weiss 92], Data Structures and Algorithm Analysis, Benajamin Cummings, 1998

107. Welch Brian [Welch 99], Electronic banking and treasury security, CRC Press NatWest, 1999

108. Winslett Marianne [Winslett 99], Ching Neil, Jones Vicki, Slepchin Igor, Assuring Security and Privacy for Digital Library Transactions on the Web: Client and Server Security Policies, IEEE, pg. 140-151, Año de Consulta 1999

109. Xlink [XLINK 00], Año de consulta 2000, http://www.w3.org/TR/xlink/

110. Recomendación W3 XML [XML 00], Año de Consulta 2000, http://www.w3.org/XML/, http://www.w3.org/TR/1998/REC-xml-19980210

111. XSL [XSL 00], Año de Consulta 2000, http://www.w3.org/Style/XSL/Overview.html, http://www.w3.org/TR/xsl/, http://www.w3.org/TR/xslt,

112. Yahya Y. Al-Salqan [Yahya 97], Future Trends In Internet Security,IEEE,1997, pg. 216- 217.

113. YAMAMOTO Kazuhiko [Yamamoto 96], An Integration of PGP and MIME, IEEE, 1996, pg. 17-24.

114. Yan Gloria [Yan 97], C. Paradi Joseph And Suneel Bhargava, BANKING ON THE INTERNET AND ITS APPLICATION, IEEE, 1997, pg. 275-284

Listado de Tablas de Referencia

Listado de Figuras de Referencia

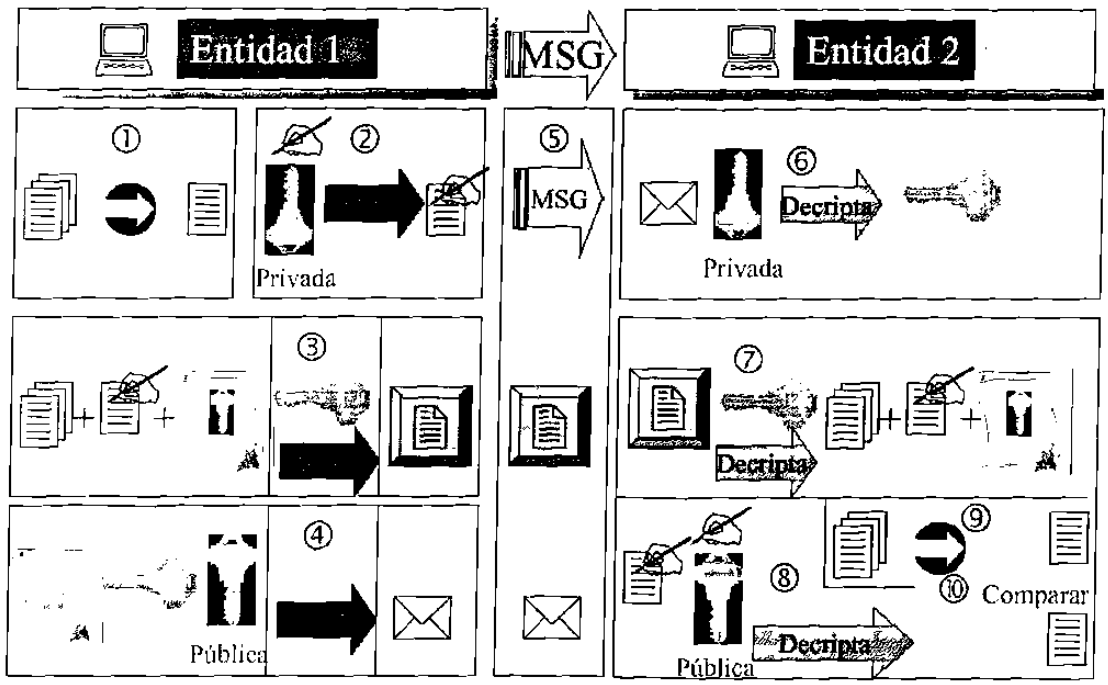
APENDICE A

DIAGRAMA DEL PROTOCOLO SET

GUIA DE REFERENCIA

DIAGRAMA DEL PROTOCOLO SSL

DIAGRAMA DEL PROTOCOLO SET



1. Crear el Message Digest
2. Crear la firma digital
3. Generar una llave simétrica aleatoria
4. Encriptar la llave simétrica
5. Envío de mensaje
6. Desencriptar la llave simétrica
7. Desencriptar la información
8. Desencriptar el Message Digest
9. Crear el Message Digest
10. Comparar los Message Digest

GUIA DE REFERENCIA

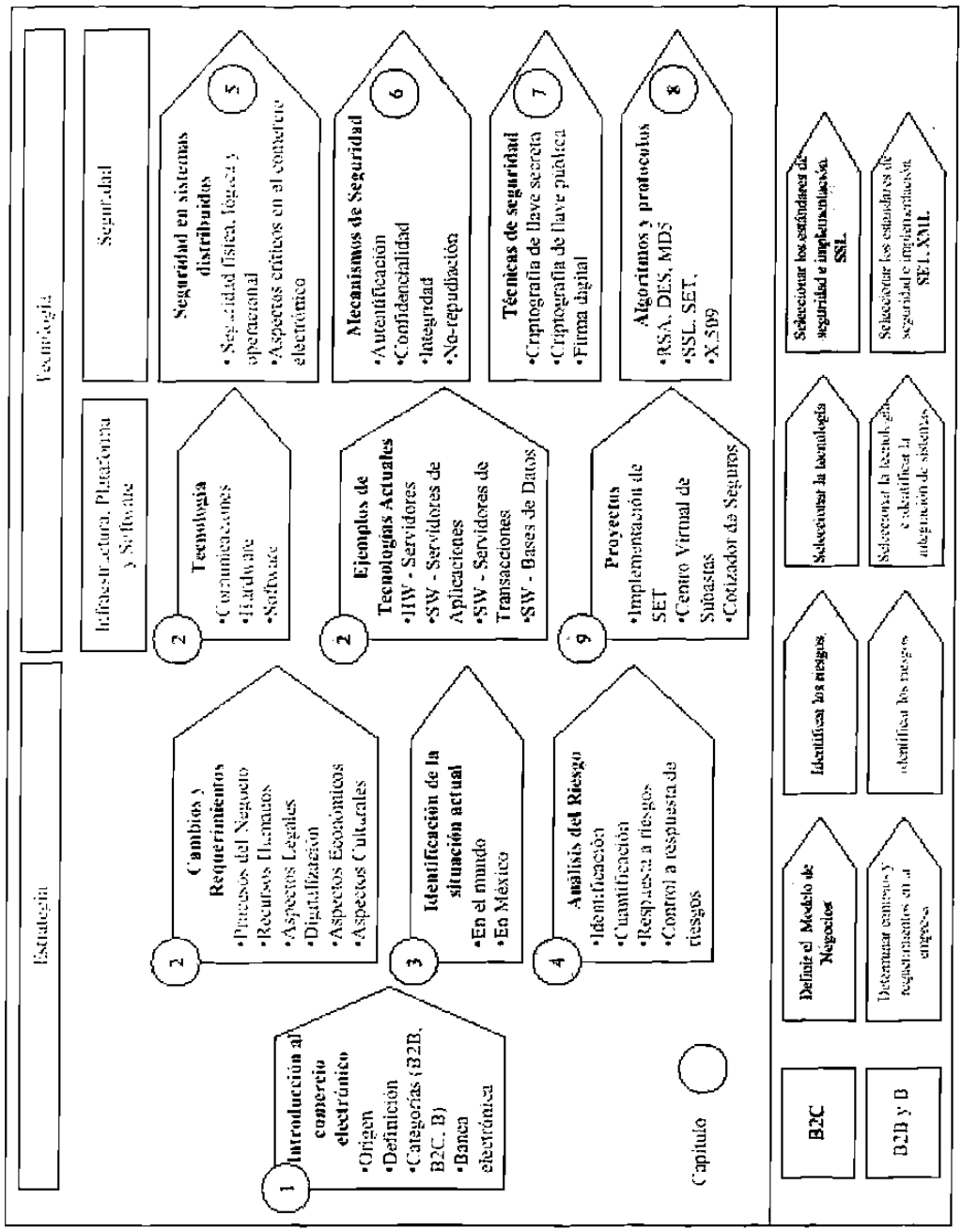
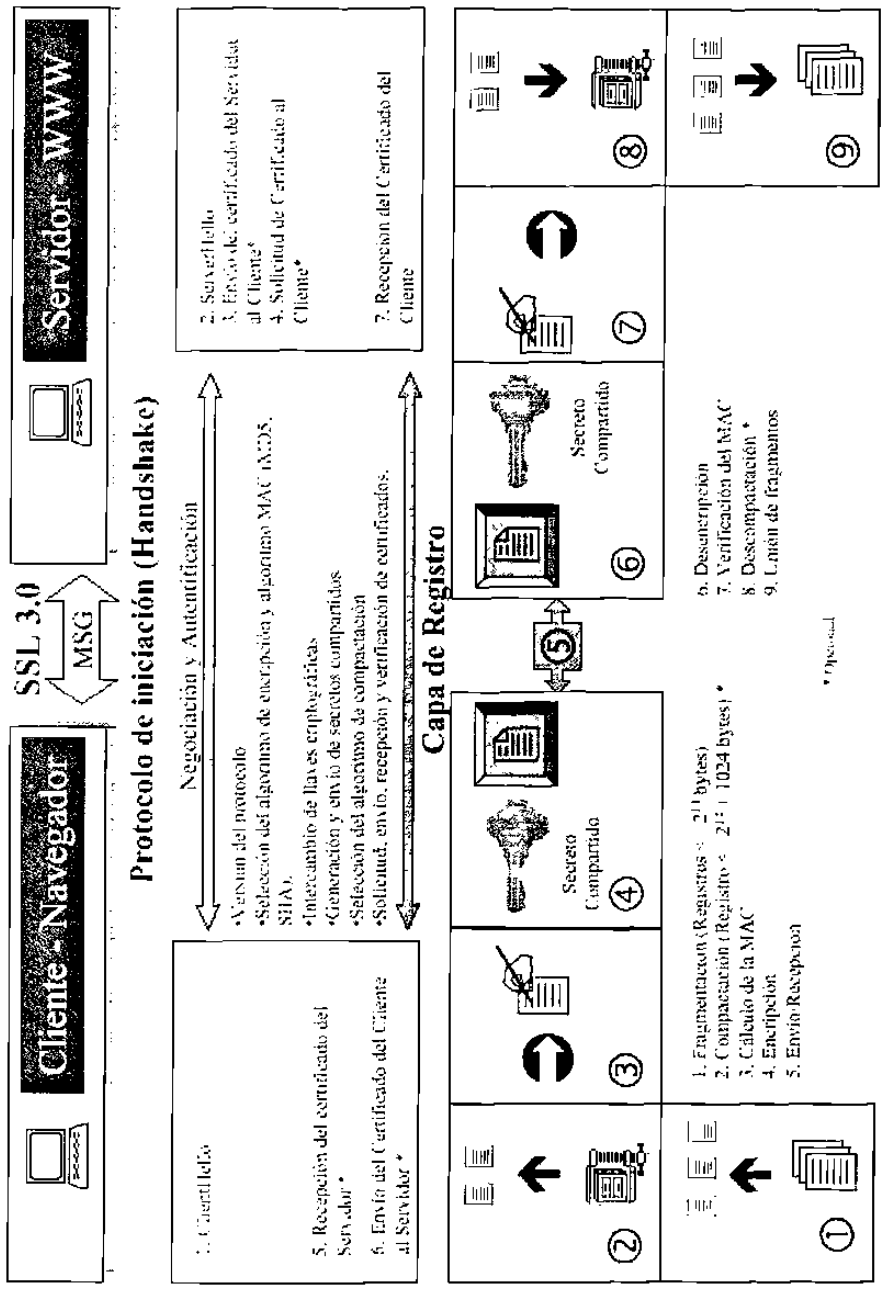


DIAGRAMA DEL PROTOCOLO SSL



APENDICE B

ANEXO A. Introducción al XML

ANEXO A. Introducción al XML

El eXtensible Markup Language (XML) [XML 00] es una nueva tecnología para aplicaciones WEB que se prevé sustituya el HyperText Markup Language (HTML) en los próximos años. XML es el estándar del World Wide Web Consortium (W3C) completado en 1998 que permite crear etiquetas personalizadas y auto descriptibles, a diferencia del HTML. [HTML 00]

La respuesta entusiasta hacia el XML es impulsada debido a la esperanza de resolver uno de los problemas más grandes del WEB y es el la gran cantidad de información disponible y la dificultad para encontrar de forma precisa la información requerida. Estos problemas se deben a la naturaleza del HTML, lenguaje principal de WEB. A pesar de ser el lenguaje más exitoso de publicación electrónico, este es superficial y únicamente expresa como se debe ver el texto, imágenes y botones en una página. La utilización de etiquetas enmarcadas los símbolos (<,>) muestran como se debe ver la información en el browser.

En 1986 surgió un estándar de la International Standards Organization (ISO) llamado Standard Generalized Markup Language (SGML), el cual es un metalenguaje que ha probado su utilidad en aplicaciones de publicación. Por cierto el HTML fue definido utilizando el SGML. El único problema con el SGML es, que es demasiado general.

A partir del SGML el grupo de W3C se dio a la tarea de eliminar los problemas del SGML y desarrollo el XML, el cual consiste en una serie de reglas para crear un metalenguaje a partir de la nada. Estas reglas aseguran que un solo programa compacto llamado parser pueda procesar estos nuevos lenguajes.

A diferencia de la mayoría de los formatos de datos, el XML también hace sentido al ser humano, debido a que consiste en texto ordinario. El poder de XML radica: que las etiquetas siempre vienen en pares como los paréntesis y que pueden ser anidados, uno dentro de otro en múltiples niveles. Esta regla de anidamiento automáticamente obliga a una cierta simplicidad en cada documento XML, el cual toma la estructura conocida como árbol y con ello, las relaciones no son ambiguas Por último otra fortaleza del XML es la utilización del sistema de codificación de caracteres llamado Unicode. Permitiendo así la generación de texto en la mayoría de los lenguajes en el mundo.

Estas características han permitido generar etiquetas específicas para cada industria haciendo más fácil y precisa la búsqueda de información. Como parte del proyecto XML se ha creado un estándar complementario para los metadatos. El Resource Description Framework (RDF) [RDF WWW]el cual hace para los datos WEB lo que las tarjetas de un catálogo en una librería, hace por los libros. Con esto la recuperación de información será más rápida y precisa.

Otra estándar XML denominado Xlink [XLINK 00] permitirá escoger dentro de una lista de múltiples direcciones para realizar las funciones de ligas o hypertexto en el HTML. A diferencia presenta la ventaja de tener ligas indirectas almacenadas en una base de datos. El proceso de actualización se realiza en la base de datos.

Las características anteriores permitirán un procesamiento eficiente, búsquedas más precisas y enlaces más flexibles, con lo cual se revolucionará la

estructura del WEB, haciendo posible nuevas formas de acceso a la información.

Al definir un nuevo lenguaje XML los diseñadores deben acordar por lo menos tres cosas: las etiquetas que serán permitidas, el esquema de anidamiento y como se deben procesar las etiquetas. Los dos primeros dos, el vocabulario y la estructura son típicamente codificados en un Document Type Definition (DTD) [DTD 00], aunque su uso no es imperativo. Aunque su uso hace más fácil la escritura de software.

En cuanto al estilo el XML permite "escribir una vez y publicar en cualquier parte". El XML permite etiquetar el contenido y aplicar reglas para dar formato mediante plantillas (Stylesheets) utilizando el eXtensible StyleSheet Languaje (XSL) [XSL 00].

Con esta nueva forma de incluir el formato y contenido se puede realizar el intercambio de documentos estandarizados como actualmente se realiza en el mundo de los negocios mediante el uso de ordenes de compra, facturas, recibos, etc. Los documentos funcionan ya que no es necesario conocer los procedimientos internos de las partes involucradas y únicamente se expone la información necesaria. Con ello los negocios en línea podrán utilizar esta nueva forma de intercambiar documentos. [Bosak 99]

Las aplicaciones XML proveen ventajas debido a la habilidad para el intercambio de datos. Las diversas organizaciones o las diferentes partes de una organización difícilmente estandarizan un conjunto de herramientas, y por lo tanto, la comunicación entre dos grupos toma una gran cantidad de tiempo. XML hace fácil el envío de datos estructurados a través del WEB sin pérdida de información en la transferencia. [Tidwell 99]

XML simplifica las transacciones negocio a negocio en el WEB y el intercambio de información entre negocios (B2B) se realiza mediante el seguimiento a las reglas de un documento definido en el DTD.

La importancia de XML viene de sus implicaciones y aplicación potencial para el comercio electrónico basado en el WWW, la administración del contenido de una organización, búsqueda de información, descripciones técnicas, integración de aplicaciones y comunicación entre aplicaciones y entre servidores. [Gartner 99]

El XML y el Internet han reducido las barreras del comercio electrónico con relación al costo y a la complejidad. El XML no reemplaza el EDI (Electronic Data Interchange) sino por el contrario lo extienda permitiendo a las pequeñas y medianas compañías realizar comercio electrónico. El EDI es una tecnología probada por más de 20 años con más de 300,000 empresas en todo el mundo, pero tiene la desventaja de utilizar pequeños mensajes con códigos que representan valores completos y el alto costo de implementación. Es ahí donde el XML combina los metadatos con datos permitiendo la fácil lectura de mensajes para el ser humano y las computadoras.

El uso de XML para aplicaciones de comercio electrónico requiere la inclusión de un esquema de seguridad que permita garantizar la autentificación, confidencialidad, integridad y no-repudiación. Esto puede complementarse con el uso del protocolo SSL y el uso de certificados en los navegadores de Internet que estarán disponibles en poco tiempo.

GLOSARIO

AES	Advanced Encription Standard (encriptación Avanzada del tipo estandar)
ATM	Automatic Teller Machine. (Cajero Automático)
B Business.	Categoría de comercio electrónico que considera a los procesos Internos del negocio
B2B Business to Business.	Categoría de comercio electrónico que considera el comercio electrónico entre empresas
B2C Business to Consumer.	Categoría de comercio electrónico que considera el comercio electrónico entre una empresa y un consumidor final
BACS	Banker's Automated Clearing System (Sistema Bancario Automatizados)
CD ROM	Compact Disk Read Only Memory (disco compacto)
Certificado Digital	Archivo que contiene información sobre la identidad de una persona, empresa o sistema
Ciberespacio	Conjunto de seres humanos interconectados a través de computadoras y redes de telecomunicaciones sin importar la geografía física Clientes Máquinas o computadoras que realizan la función de solicitar información a un servidor bajo la relación cliente/servidor

Clusters	Grupo de terminales o computadoras conectadas a una unidad de control en común o servidor que comparten la carga de trabajo y brindan apoyo en caso de que algún nodo falle
CORBA	Common Object Request Broker Architecture (Arquitectura y especificación para la creación, distribución y administración de programas u objetos distribuidos en una red)
CRM	Customer Relation Management (Término de la industria de tecnologías de información para las metodologías, software y capacidades en Internet que ayudan en la forma en que se relacionan las empresas con sus clientes)
Checksum	Conteo de número de bits en una unidad de transmisión utilizada para verificar que el número de bits recibidos sea el mismo que el número de bits enviados
DES	Data Encription Standard (Estándar de encripción de criptografía de llave privada)
DSS	Digital Signature Standard
DVD	Digital Versatile Disk (Tecnología de discos ópticos que remplazarán al CDROM)
Eavesdropping	Escuchas
EDI	Electronic Data Interchange (Intercambio electronico de Datos)
EFT	Electronic Funds Transfer (fundamentos de Transferencia Electronica)
EFTPOS	Electronic Funds Transfer Point Of Sales Enterprise Java Beans (Arquitectura desarrollada por SUN para la administración de componentes desarrollados en el lenguaje de programación JAVA)

Extranet	Red privada que utiliza los protocolos de Internet y los sistemas de telecomunicaciones públicos para compartir de forma segura, información de negocios y operaciones entre diversas empresas
FTP	File Transfer Protocol (Protocolo de transferencia de archivos entre computadoras a través de Internet)
Groupware	Programas que ayudan a las personas a trabajar de forma colaborativa y de forma colectiva sin importar su ubicación física Hash Función unaria que es utilizada para mapear un argumento a un resultado de un tamaño predeterminado.
HTML	HyperText Markup Language (Conjunto de símbolos y marcas que permiten consultar información en el WWW a través de un navegador como Netscape o Internet Explorer Internet Sistema de computadoras conectadas en red pública en todo el mundo Internet II Proyecto de universidades y empresas de EU para el desarrollo de redes y aplicaciones avanzadas para la enseñanza e investigación)
Intranet	Red privada basada en las tecnologías y protocolos de Internet IRC
Java	Lenguaje de programación diseñado para ambientes distribuidos en Internet
Java Server Pages	Tecnología utilizada para el control del contenido y apariencia de páginas WWW
JDBC	Especificación de Interface de programación de aplicaciones para conectar al lenguaje de programación Java con base de datos
Kerberos	Método seguro para la autentificación de solicitudes a servicios

KM	Knowledge Management (Tecnología de Información para la administración del conocimiento que permite adquirir, almacenar y transferir el conocimiento entre personas mediante el uso de un sistema)
Llave privada	Llave mantenida en secreto y otorgada por una autoridad certificadora que permite junto con la llave pública realizar operaciones de encripción y decripción
Llave pública	Llave otorgada por una autoridad certificadora la cual se distribuye a la personas que requieran enviar un mensaje, que permite junto con la llave privada realizar operaciones de encripción y decripción
MAC	Message Authentication Code (mensaje Automatizado)
Message forgery	Falsificación de mensajes
MIPS	Míllions of instructions per second (Unidad para definir la capacidad de procesamiento de una computadora)
MP3	MPEG-1 Audio Layer-3 (Formato para la compresión de secuencias de sonido y audio)
Newsgroups	Grupos de noticias (Discusión de temas específicos a través de comentarios escritos a un servidor de Internet centra)l
NIST	National Institute of Standards and Technology
PGP	Pretty Good Privacy (Programa utilizado para encriptar y decriptar información generalmente correo electrónico)
Portales	Sitio WEB de inicio y punto de entrada hacia otros sitios en Internet
POS	Point Of Sales (puntos de venta)
RFP	Request For Proposal (Búsqueda avanzadas)

RMI	Remote Method Invocation (Librerías de programación en Java para ejecutar métodos en un equipo remoto)
SDH	Synchronus Digital Hierarchy (Estándar para transmisión síncrona de datos)
Servlets	Tecnología Java que permite ejecutar programas en un servidor
SET	Secure Electronic Transaction (tranzaciones electronicas de alta seguridad)
SONET	Estándar para transmisión de datos sincronos en medios ópticos
SSL	Socket Secure Layer
SWIFT	Society for Worldwide Interbank FundsTransfer Tampering Intromisiones (Sociedad reguladora)
VAN	Value Added Network (Red de compartición de servicios de banda ancha)
VPN	Virtual Private Network (Red privada de datos que utiliza la infraestructura de las redes publicas de datos de forma segura mediante procedimientos de seguridad)
VRML	Virtual Reality Modeling Language (Lenguaje para la descripción de imágenes en 3 dimensiones e interacciones con el usuario)
WWW	World Wide Web
XML	Extensible Markup Language (Lenguaje que permite integrar además de formato a las páginas WWW, un significado y descripción de la información contenida en el documento)

AUTOBIOGRAFIA

Candidato para el Grado de Master en Ciencias de la Administración con especialidad en Relaciones Industriales.

Tema de Tesis: "La Seguridad en el Comercio Electrónico como Solución a una nueva forma de llevar acabo Transacciones Comerciales de las Empresas"

Nació en la ciudad de Poza Rica de Hgo. Veracruz, el 27 de Julio de 1976, Hijo del Sr. Francisco Cabrera Martínez y de Sra. Maria de la luz Taque Cabrera, Hermano de Sr. Ernesto C. Cabrera Taque, Srita. Gloria Cabrera Taque y Jorge Cabrera Taque.

Egresado de la Facultad de Ingeniería Mecánica y Eléctrica de Universidad Autónoma de Nuevo León, Obteniendo el grado de Ingeniero en Electrónica y Comunicaciones, en Diciembre de 1998.

Contando también con el Titulo de Técnico en Electromecánica, del C.B.T.i.s. No. 78, de la Ciudad de Poza Rica de Hgo. Veracruz, egresado en Junio de 1994.

Contando con la Experiencia Profesional en el área de la investigación, implementación y desarrollo de nuevas Tecnologías, y en las áreas de la

Informática y las Telecomunicaciones, Habiendo participado en el desarrollo e implementación del Site de Comercio de la Compañía Dirona S.A. de C.V., además de Participar y colaborar en el Departamento de Electrónica y Comunicaciones de la Facultad de Ingeniería Mecánica y Eléctrica de la Universidad Autónoma de Nuevo León.