UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACION

ESCUELA DE INGENIERIA DE SISTEMAS

UTILIZACION DE FIRMAS DIGITALES EN EL CORREO ELECTRONICO

TRABAJO DE GRADUACION PREVIO A LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS

AUTORES:
PAUL SEBASTIAN CARRION MARTINEZ
PATRICIO ESTEBAN MONSALVE ESPINOZA

DIRECTOR:
ING. PABLO PINTADO

CUENCA, ECUADOR
2007

DEDICATORIA

La presente monografía esta dedicada ha nuestros padres quienes nos dieron la fuerza y el apoyo constante para cumplir todas nuestras metas que nos hemos planteado desde el inicio de nuestras vidas.

AGRADECIMIENTO

Agradezco a Dios por haberme dado la fe suficiente para llegar hasta esta etapa de mi vida, a mi esposa y mi hija por que han sido mi motor para culminar mis estudios, mis hermanos y mi abuela quienes me dieron sus sabios consejos y se han convertido en mis guías durante toda mi vida.

Patricio Monsalve.

A Dios por haber sido el que me ha permitido este logro, por haberme dado la fuerza necesaria en los momentos de flaqueza, a mis padres por que sin su apoyo incondicional jamás hubiera logrado este triunfo, a mis hermanos, a mis profesores y finalmente a mis compañeros.

Paúl Carrión.

Y un agradecimiento muy especial al Ing. Pablo Pintado quien con su experiencia nos ha sabido guiar y forjar durante el desarrollo de nuestro trabajo.

INDICE

Dedicatoria.....2
Agradecimientos.....3
Índice…….. 4
Resumen.....6
Abstract.....7

Introducción…….....8

Capítulo1: Encriptación……..……..……..….....9

1.1 Introducción…….....9
1.2 Criptología…….……...…….....9
1.3 Criptografía……..…….....13
1.4 Criptografía Híbrida…….……...14
1.5 Criptosistemas……15
1.6 Estructura de un Criptosistema…….....16
1.6.1 Clasificación de los algoritmos de cifrado……...16
1.6.1.1 Según la naturaleza del algoritmo de cifrado…...……16
1.6.1.2 Según la Clave……...19
1.6.1.3 Según el número de símbolos cifrados a la vez.……20
1.7 Encriptación……20
1.8 Data Encryption Standard (DES).....21
1.9 IDEA (Internacional Data Encription Algorithm)……..23
1.9.1 Funcionamiento…….....24
1.10 Sistemas de Clave Pública…….....26
1.11 RSA……...27
1.12 Desencriptación……27
1.13 El Futuro de la Encriptación……28
1.14 Conclusión……..……...29

Capítulo 2: Firmas Digitales….…….....31

2.1 Introducción……31
2.2 Que es la firma digital?.....31
2.3 Como funciona?.....32
2.4 Claves Privadas y Claves Públicas…...……...33
2.5 Que son los Certificados Digitales?…….....35
2.6 Que contiene un certificado Digital?.....38
2.7 Que valor legal tiene una firma Digital?.....39
2.8 Que es una infraestructura de Firma Digital?.....40
2.9 Conclusión……..……..……...41

Capítulo 3: Configuración de las Aplicaciones…….....42

3.1 Introducción……42
3.2 Configuración del Servidor de Correo.....42
3.2.1 Configuración del DNS.....42
3.2.2 Configuración del Named...…….43
3.2.3 Configuración del Sendmail…….46
3.2.4 Configuración del Dovecot……..47
3.2.5 Generación de Certificados Digitales……...47
3.2.6 Configuración del Cliente……53
3.3 Configuración de Servidor de Microsoft Exchange……...55
3.3.1 Creación de una Entidad Emisora de Certificados……...55
3.3.2 Configuración del Administrador del Sistema Exchange……56
3.3.3 Creación de los usuarios…….....58
3.3.4 Creación del Certificado…….....59
3.4 Instalación del Certificado en el Cliente de Correo Microsoft Outlook 2003. …….....…….59
3.5 Conclusión……...62

Capítulo 4: Pruebas……...63
4.1 Introducción……63
4.2 Pruebas del estado de la red……63
4.3 Pruebas de Correo……...64
4.4 Conclusión……..65

Conclusiones…….66
Recomendaciones……..67
Bibliografía…...……68
Glosario...……..69
Anexos……..71

INDICE FIGURAS

Figura 1 Ejemplo de Criptografía…….14
Figura 2 Ejemplo de Criptosistema……...16
Figura 3 Data Encryption Standard (DES)……23
Figura 4 Funcionamiento de las Firmas digitales……33

RESUMEN

En la presente monografía trataremos diversos temas, uno de ellos es la Encriptación, en el que se tocaran temas como la historia, donde encontramos conceptos como la criptología y criptografía que son los primeros sistemas de ocultamiento de información que existieron, con el avance de la informática también permitieron que los diferentes algoritmos de cifrado fueran resueltos de forma mas rápida por la gran velocidad de procesamiento del computador, ya que tienen formulas matemáticas demasiado complejas.

En las comunicaciones digitales a nivel global y mas específicamente en el correo electrónico el elemento mas importante es la seguridad, tanto las firmas digitales como los certificados digitales generan confianza en los usuarios al momento de depositar la información en la red, no sea alterada por usuarios no autorizados.

Hablaremos mas ampliamente del tema de las firmas digitales y los certificados digitales, detallando su concepto y uso que se tiene a nivel mundial, los elementos que conforman los certificados digitales, y su valor legal.

Y como punto final dejamos la parte de configuraciones donde se explicara paso a paso la configuración del Servidor de Correo electrónico (Microsoft Exchange de Windows Server 2003) y la configuración para la parte correspondiente al Cliente (Microsoft Outlook), para lograr la aplicación de la Firma Digital.

ABSTRACT

In the actual document we will talk about divers subjects, one of the them is Encriptation, here we also will talk about the history of it, where we will found concepts like cryptology and cryptography which are the first information hiding systems to exist, informatics evolve and as a consequence the computers allow a great variety of algorithms to calculate faster since the processors speed quickly rise, since this algorithms have complex mathematic formulas.

Digital communications at global level and especially email the most important element is security, Digital Signature and Digital Certificate bring security to the users to send information trough the web and this information stay protected and not being manipulated by hackers.

Here we will describe the subject of Digital Signature and Digital Certificate, specifying the concept and the powerful and practice use of these tools, the elements of the Digital Certificates, and their legal value.

In the end we will talk about configuration where we explain step by step how to set up the configuration for a Mail Server (Microsoft Exchange of Windows Server 2003) and also the client section (Microsoft Outlook), to achieve the application of the Digital Signature.

INTRODUCCION

Desde hace miles de años atrás el hombre se esforzó por la búsqueda del conocimiento viendo el poder que tenía, este lucho por proteger esta sabiduría de sus enemigos, y así nacieron los primeros sistemas de codificación.

En la actualidad la información es uno de los recursos más preciados que existen para una empresa, y siendo nosotros concientes de esto hemos decido realizar esta monografía con la finalidad de conocer y aplicar diferentes métodos y tecnologías para proteger la información y a las personas que utilizan esta en sus labores diarias.

En esta monografía hablaremos sobre los procedimientos utilizados hoy en día para dar seguridad a la comunicación de datos a través del Internet, es decir metodologías como la Encriptación, y tecnologías como las Firmas Digitales y Certificados Digitales.

En la siguiente investigación desplegaremos los temas antes mencionados en un documento teórico dividido en dos capítulos y además dos capítulos más donde hablaremos sobre aspectos prácticos sobre el uso de las firmas y certificados digitales y las configuraciones respectivas sobre el servidor de correo Mail Exchange de Windows Server 2003 y el cliente de correo electrónico Microsoft Outlook.

CAPITULO I ENCRIPTACION

1.1 Introducción.

En el presente capitulo se dará a conocer cómo se llego a la Encriptación, basado en los estudios de ramas que fueron las predecesoras de la misma, y también tratando temas como la clasificación de los diferentes tipos de algoritmos de cifrado que existen en la actualidad.

1.2 Criptología.

La *criptología* es el estudio de los criptosistemas, sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado (o nadie) pueda descifrarlo. Sus áreas principales de interés son la criptografía y el criptoanálisis, pero también se incluye la esteganografía como parte de esta ciencia aplicada. En tiempos recientes, el interés por la criptología se ha extendido también a otras aplicaciones aparte de la comunicación segura de información y, actualmente, una de las aplicaciones más extendidas de las técnicas y métodos estudiados por la criptología es la autenticación de información digital.

La técnica de transformación de datos que permite hacerlos inútiles frente a intrusos se le denomina “criptografía”, al arte de desbaratar estas técnicas se le llama “criptoanálisis” y conjuntamente se les conoce como “criptología”. Aunque el término "criptología" no está recogido todavía en el Diccionario de la Real Academia (siendo una traducción directa de la palabra inglesa Cryptology) la verdad es que se ha convertido en una palabra de uso común entre los expertos en seguridad de comunicaciones.

Vulgarmente, se consideran los términos encriptar y cifrar como sinónimos, al igual que sus respectivas contrapartes, desencriptar y descifrar, pero no ocurre lo mismo con el término codificar. No obstante, se debe utilizar el término cifrar en vez de encriptar, ya éste aún no está contemplado por la Real Academia Española, se trata de un anglicismo de los términos ingleses encrypt y decrypt. Por definición codificar significa expresar un mensaje utilizando algún código, pero no necesariamente de forma oculta, secreta o in entendible; escribir en idioma español implica el uso de un código, que será comprensible para los hispanos pero no tanto para quienes no dominan el idioma; la matemática y la lógica tienen sus propios códigos, y en general existen tantos códigos como ideas.

El procedimiento utilizado para cifrar datos se realiza por medio de un algoritmo al cual se le puede considerar como una función matemática. Por lo tanto, un algoritmo de cifrado es una fórmula para desordenar una información de manera que ésta se transforme en incomprensible, usando un código o clave en ocasiones, más de una. Los mensajes que se tienen que proteger, denominados texto en claro, se transforman mediante esta función, y a la salida del proceso de puesta en clave se obtiene el texto cifrado, o cifrograma. En muchos casos, existe un algoritmo de descifrado encargado de reordenar la información y volverla entendible, pero no siempre es así. Cuando existen ambas funciones, una para cifrar y otra para descifrar, se dice que el sistema criptográfico es de dos vías o reversible a partir de un mensaje en claro se puede obtener uno cifrado y a partir de éste se puede obtener el mensaje original, mientras que cuando no existe una función para descifrar se dice que el sistema es de una sola vía a partir de un mensaje cifrado no es posible obtener el mensaje en claro que lo generó; la aplicación de esto es, por ejemplo, para el almacenamiento de contraseñas.

La transformación de datos provee una posible solución a dos de los problemas de la seguridad en el manejo de datos. El problema de la privacidad y el de la autenticación, es evitar que personas no autorizadas puedan extraer información del canal de comunicación o modificar estos mensajes.

Desde el punto de vista histórico los métodos de cifrado se han dividido en dos categorías: cifradores de sustitución y cifradores de transposición. En un cifrador de sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para disfrazarlas. Los cifradores de sustitución preservan el orden de los símbolos del texto en claro, pero los disfrazan. El cifrador de sustitución más antiguo que se conoce es el cifrador de César, atribuido a Julio César. En este método, A se representa por D, B por E, C por F, y así cada letra se sustituye por la que se encuentra tres lugares delante de ella, considerando que luego de la Z vuelve a comenzar por la A. Una variante del cifrador de César es permitir que el alfabeto cifrado se pueda desplazar k letras (no sólo 3), convirtiéndose k en la clave.

Una mejora al cifrador de César es la de relacionar a cada letra del alfabeto con un carácter. En este sistema, llamado sustitución monoalfabética, la clave consistirá en la cadena completa de caracteres del alfabeto. El ataque a estos anteriores sistemas es aprovechar las propiedades estadísticas de los lenguajes. Sabiendo el idioma del texto en claro y calculando el porcentaje de ocurrencias de letras y de combinaciones de dos y tres letras se puede adivinar una palabra y así deducir la clave.

Una forma de fortalecer el cifrador de César se logra utilizando múltiples sistemas de César aplicados periódicamente. Este sistema se conoce como cifrado polialfabético, un

ejemplo es el sistema criptográfico de Vigenére. Consiste en una matriz cuadrada la cual contiene 26 alfabetos de César. Ahora la clave estaría constituida por una palabra simple más la matriz de 26 x 26.

Este sistema resultó bastante seguro por algún tiempo, debido principalmente a la imposibilidad de determinar el largo de la clave. Una vez encontrado el largo de la clave es posible encontrar las sustituciones simples agrupando las letras. En 1863 F. W. Kasiski resolvió el problema de encontrar el largo de la clave a través de la técnica llamada: La incidencia de las coincidencias.

El cifrado Vernam es un caso particular del Vigenere con una clave de igual largo que el texto a codificar. Eligiendo la clave en forma aleatoria el sistema es incondicionalmente seguro pero tiene el inconveniente que ambos transmisor y receptor deben saber la clave y esta se debe comunicar por otro canal que sea seguro.

A diferencia de los cifradores de sustitución, los cifradores de transposición, reordenan las letras pero no las disfrazan. Consiste en una tabla con determinado número de columnas, este número de columnas estará dado por la cantidad de caracteres de la clave que a su vez no tendrá ningún carácter repetido. La clave tiene el propósito de numerar las columnas correspondiendo a la primera letra en orden alfabético el número 1. El texto en claro se escribe en las filas de la tabla de arriba hacia abajo, el texto codificado será leído verticalmente comenzando por la columna 1, luego la 2, etc.

En una computadora el procedimiento de codificación se puede realizar por software o por hardware. La codificación por software puede ser específica de una aplicación. La codificación independiente de la aplicación se puede hacer por hardware o a

partir de un programa que funcione casi al mismo nivel que un sistema operativo, por ejemplo, assembler.

1.3 Criptografía.

La criptografía del griego *kryptos*, "ocultar", y *grafos*, "escribir", literalmente "escritura oculta" es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en secreto, esta técnica no se considera criptografía, sino esteganografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en

blanco usados para justificar un texto. La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles espías. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

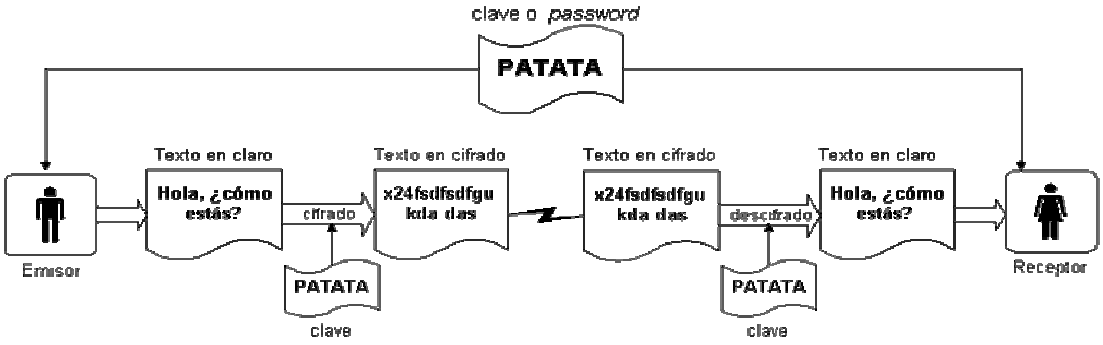


Figura 1 Ejemplo de Criptografía

1.4 Criptografía híbrida.

Es un método criptográfico que usa tanto para cifrado simétrico como asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión.

1.5 Criptosistemas.

Matemáticamente, podemos definir un criptosistema como una cuaterna de elementos, formada por:

- Un conjunto finito llamado alfabeto, a partir del cual, y utilizando ciertas normas sintácticas y semánticas, podremos emitir un mensaje en claro u obtener el texto en claro correspondiente a un mensaje cifrado. Frecuentemente, este alfabeto es el conjunto de los enteros módulo que, donde que es el número de elementos que tiene el alfabeto.
- Otro conjunto finito denominado espacio de claves, formado por todas las posibles claves, tanto de cifrado como de descifrado, del criptosistema.
- Una familia de aplicaciones del alfabeto en sí mismo, llamadas transformaciones de cifrado. El proceso de cifrado se suele representar como

$$\mathbf{(k, a) = c}$$

- Otra familia de aplicaciones del alfabeto en sí mismo, llamadas transformaciones de descifrado.

Muchos autores dividen a su vez un miembro de esta cuaterna, el alfabeto, en dos espacios diferentes: el espacio de mensajes, formado por los textos en claro que se pueden formar con el alfabeto, y el espacio de cifrados, formado por todos los posibles criptogramas que el cifrador es capaz de producir. Sin embargo, tanto el texto en claro como el cifrado han de pertenecer al alfabeto, por lo que hemos preferido no hacer

distinciones entre uno y otro, agrupándolos en el conjunto para simplificar los conceptos que presentamos. Así, un criptosistema presenta la estructura mostrada en la figura.

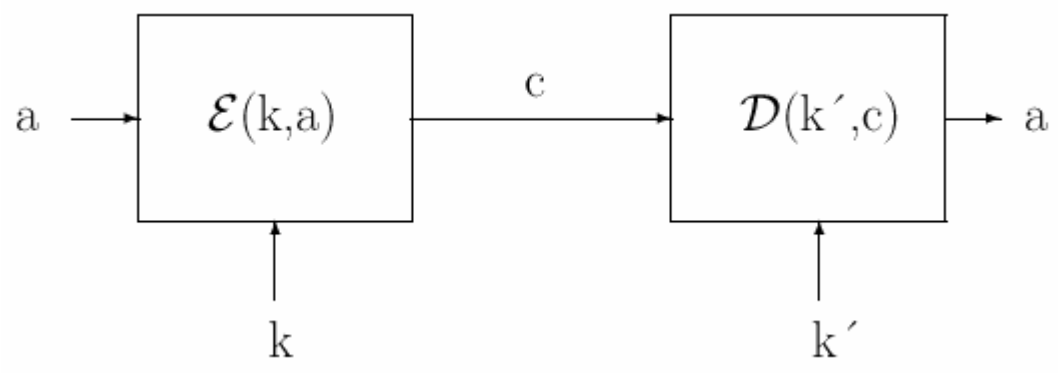


Figura 2 Ejemplo de criptosistema

1.6 Estructura de un Criptosistema

1.6.1 Clasificación de los Algoritmos de Cifrado

Los algoritmos de cifrado se pueden dividir en tres grandes grupos:

1.6.1.1 Según la naturaleza del algoritmo de cifrado

- **Sustitución:** El método de sustitución consiste básicamente en sustituir los caracteres del mensaje inicial por otros; los nuevos caracteres pueden ser de cualquier tipo: letras, símbolos, dígitos, etc. Los caracteres iniciales siguen estando en el mismo orden pero salvo que se conozca la equivalencia entre los nuevos caracteres y los antiguos el mensaje es ilegible.

Podemos considerar dos tipos de sustitución:

- **Sustitución Monoalfabética (Equivalencia entre alfabetos carácter a carácter):** A cada letra del alfabeto ordinario se le hace corresponder un símbolo y el mensaje se cifra cambiando las letras iniciales por su equivalente, si a la letra A le asignamos el símbolo "@" en el mensaje cifrado tendremos siempre @ en lugar de A.
- **Sustitución Polialfabética (Utilización de cifra o clave):** Distinto del anterior porque una vez establecida la correspondencia entre alfabetos que en este caso puede utilizar otro tipo de caracteres.

- **Permutación (Transposición):** Los algoritmos de sustitución y los códigos, preservan el orden de los símbolos en claro, pero los disfrazan. A diferencia de éstos, los algoritmos de transposición, reordenan las letras pero no las disfrazan.

  El algoritmo de transposición más común es el de tipo columnar; la clave del cifrador debe ser una palabra que no tenga ninguna letra repetida, en el ejemplo que se presenta a continuación la clave es la palabra MEGABUCK. El propósito de la clave es el de numerar las diferentes columnas que se formarán, de forma que la columna 1 es aquella que queda bajo la letra de la clave más próxima al principio del alfabeto y así sucesivamente. El texto en claro se escribe debajo de la clave en renglones horizontales; el texto cifrado se lee por columnas, comenzando por la columna cuya letra clave tiene el menor valor.

  Texto en claro:

  pleasetransferonemilliondollarstomy

Clave de cifrado: M E G A B U C K

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	L	e	a	s	e	t	R
a	N	S	f	e	r	o	N
e	M	I	l	l	i	o	N
d	O	L	l	a	r	s	T
o	M	y	a	b	c	d	E

Texto cifrado:

AFLLA SELAB TOOSD LNMOM ESILY RNNTE PAEDO ERIRC

Para desbaratar un cifrador de transposición, el criptoanalista debe estar primero enterado de que se trata efectivamente de un cifrador de transposición. Esto puede comprobarse de una forma relativamente sencilla, observando la frecuencia de las letras e, t, a, o, i, n, ... ya que en los cifradores de este tipo se cambia de lugar las letras, pero no se cambian las letras propiamente, por lo que si la frecuencia de aparición de las letras se corresponde con la observada para el lenguaje natural, es decir, la e es la que más aparece, entonces se podría afirmar con mucha seguridad que el cifrador es de transposición y no de sustitución.

El siguiente paso consistiría en determinar cuál es el número de columnas. En muchos casos una palabra o frase probable, puede llegar a adivinarse a partir del contexto del mensaje. Si el criptoanalista sabe, o supone que una determinada palabra o frase está contenida en el mensaje, entonces no le costará mucho esfuerzo determinar el número de columnas.

El último paso consistiría en ordenar las columnas.

- **Producto (Supercifrado y Recifrados):** Son los cifrados obtenidos aplicando 2 o mas veces los métodos anteriores, cuantos mas métodos se apliquen mas seguridad se tiene, siendo este método el mas aplicado en la actualidad.

1.6.1.2 Según la clave

- **Simétricos (clave privada):** Son aquellos en donde cada pareja de usuarios que deseen transmitirse un mensaje deben contar con una clave secreta, sólo conocida por ambos, este punto se lo detallara de mejor manera en el capitulo 2.
- **Asimétricos (Clave Pública):** En éstos, la clave de cifrado se hace de conocimiento general (se le llama clave pública) de forma similar este tema será tratado en el capitulo 2.
- **Irreversibles:** Cifran un texto no permitiendo su descifrado, una de sus utilizaciones es la del cifrado de contraseñas, otra aplicación es la de las claves desechables o dinámicas que se utilizan en ciertos teléfonos móviles.

1.6.1.3 Según el número de símbolos cifrados a la vez

- **Bloque:** Toman el texto en claro y lo dividen en bloques de igual longitud y cifran cada bloque independientemente. Suelen emplearse bloques de 64 bits.

  M = M1 M2 M3.....Mi

  EK (M) = EK (M1) EK (M2) EK (M3)....

- **Flujo**: El texto en claro se cifra símbolo tras símbolo, cifrándose cada uno con clave diferente.

  Con este cifrado se cumple:

  - La longitud de la clave es al menos tan grande como la longitud del texto en claro.
  - Los símbolos de la clave son aleatorios. Este cifrado alcanza el cifrado invulnerable (SECRETO PERFECTO).

1.7 Encriptación.

Encriptación es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cuál la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos. El término encriptación es

traducción literal del inglés y no existe en el idioma español. La forma más correcta de utilizar este término sería *cifrado*.

Algunos de los usos más comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas de crédito, reportes administrativo-contables y conversaciones privadas, entre otros.

La encriptación hace uso de diversas fórmulas matemáticas con el propósito de transformar el texto plano en un criptograma el cual es un conjunto de caracteres que a simple vista no tiene ningún sentido para el lector. La mayoría de los métodos de encriptación utilizan una clave como parámetro variable en las mencionadas fórmulas matemáticas de forma que a pesar de que un intruso las conozca, no le sea posible descifrar el criptograma si no conoce la clave, la cual solo se encuentra en posesión de las personas que pueden tener acceso a la información en cuestión. Algunos métodos utilizan incluso dos claves, una privada que se utiliza para la encriptación y otra pública para la desencriptación. En algunos métodos la clave pública no puede efectuar la desencriptación o descifrado, sino solamente comprobar que el criptograma fue encriptado o cifrado usando la clave privada correspondiente y no ha sido alterado o modificado desde entonces.

1.8 Data Encryption Standard (DES)

En los sistemas vistos hasta el momento, es decir, en la criptografía tradicional se ha tratado de dificultar el criptoanálisis sobre todo mediante el empleo de claves muy largas, en lugar de complicar los algoritmos.

La razón es que antes del uso de los ordenadores, un operador debía realizar las transformaciones manualmente, o con ayuda de un aparato creado específicamente para la tarea. En el primer caso, un algoritmo complicado podía comprometer muy seriamente la velocidad de cifrado o descifrado, y provocaba errores. En el segundo, además de las limitaciones técnicas, existía el problema de que fuera necesario cambiar de algoritmo.

Con la entrada en escena de los ordenadores, los criptógrafos disponen de una herramienta mediante la cual puede complicar los algoritmos sin las limitaciones anteriores, pero deben preocuparse también de ataques basados en una mayor capacidad de cálculo.

> La Oficina Nacional de Normas de los EEUU publicó en enero de 1977 una norma oficial en la que se describe el algoritmo de cifrado que las Agencias Federales deben utilizar para la protección de información no clasificada. El objetivo de la Norma de Cifrado de Datos (DES) era que los sistemas de protección de información de los distintos estados fueran compatibles.

El DES nació como consecuencia del criptosistema LUCIFER, creado por Horst Feistel quien trabajaba en IBM, este criptosistema trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente, tanto en software como en hardware.

Tras las modificaciones introducidas por el NBS, consistentes básicamente en la reducción de la longitud de clave y de los bloques, DES cifra bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad (en realidad se usa 56 bits), produciendo así 64 bits cifrados.

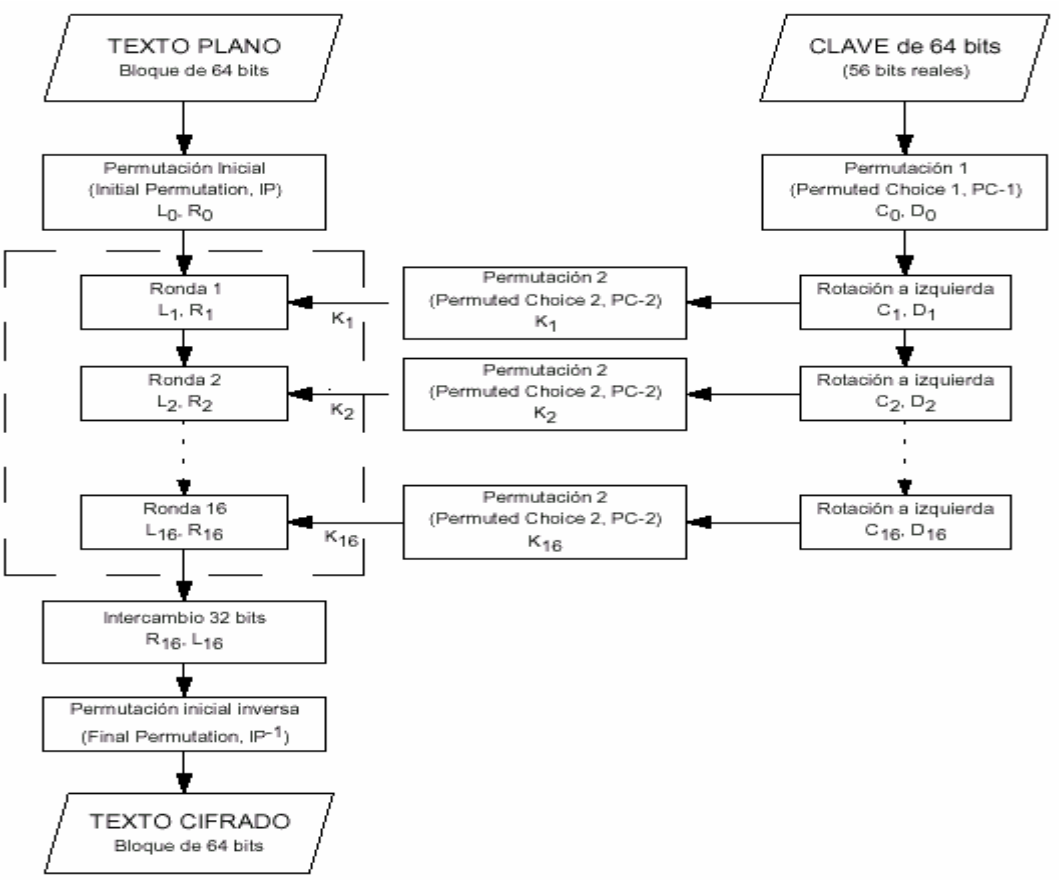


Figura 3 Data Encryption Standard (DES)

1.9 International Data Encryption Algorithm (IDEA)

El algoritmo IDEA es bastante más joven que DES, pues data de 1992. Para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits. Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar.

IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial. No presenta claves débiles, y su longitud de clave hace imposible en la práctica un ataque por la fuerza bruta.

Como ocurre con todos los algoritmos simétricos de cifrado por bloques, IDEA se basa en los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones elementales:

1. XOR.
2. Suma módulo 2^{16}.
3. Producto módulo $2^{16} + 1$.

1.9.1 Funcionamiento

El algoritmo IDEA consta de ocho rondas. Dividiremos el bloque X a codificar, de 64 bits, en cuatro partes X_1, X_2, X_3 y X_4 de 16 bits. Denominaremos Z_i a cada una de las 52 subclaves de 16 bits que vamos a necesitar. Las operaciones que llevaremos a cabo en cada ronda son las siguientes:

1. Multiplicar X_1 por Z_1.
2. Sumar X_2 con Z_2.
3. Sumar X_3 con Z_3.
4. Multiplicar X_4 por Z_4.
5. Hacer un XOR entre los resultados del paso 1 y el paso 3
6. Hacer un XOR entre los resultados del paso 2 y el paso 4.
7. Multiplicar el resultado del paso 5 por Z_5.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar el resultado del paso 8 por Z_6.
10. Sumar los resultados de los pasos 7 y 9.
11. Hacer un XOR entre los resultados de los pasos 1 y 9.

12. Hacer un XOR entre los resultados de los pasos 3 y 9.
13. Hacer un XOR entre los resultados de los pasos 2 y 10.
14. Hacer un XOR entre los resultados de los pasos 4 y 10.

La salida de cada iteración serán los cuatro sub-bloques obtenidos en los pasos 11, 12, 13 y 14, que serán la entrada del siguiente ciclo, en el que emplearemos las siguientes seis subclaves, hasta un total de 48. Al final de todo intercambiaremos los dos bloques centrales, en realidad con eso deshacemos el intercambio que llevamos a cabo en los pasos 12 y 13.

Después de la octava iteración, se realiza la siguiente transformación:

1. Multiplicar X1 por Z_{49}.
2. Sumar X2 con Z_{50}.
3. Sumar X3 con Z_{51}.
4. Multiplicar X4 por Z_{52}.

Las primeras ocho subclaves se calculan dividiendo la clave de entrada en bloques de 16 bits. Las siguientes ocho se calculan rotando la clave de entrada 25 bits a la izquierda y volviendo a dividirla, y así sucesivamente.

Las subclaves necesarias para descifrar se obtienen cambiando de orden las Z_i y calculando sus inversas para la suma o la multiplicación. Puesto que $2_{16} + 1$ es un número primo, nunca podremos obtener cero como producto de dos números, por lo que no necesitamos representar el valor. Cuando estemos calculando productos, utilizaremos el cero para expresar el número 2_{16} un uno seguido de 16 ceros. Esta representación es

coherente puesto que los registros que se emplean internamente en el algoritmo poseen únicamente 16 bits.

1.10 Sistema de claves públicas (PKI)

En el sistema de claves públicas, se utilizan distintas claves para codificar y descodificar la información. El sistema se conoce también con el nombre de "criptografía asimétrica".

En la criptografía asimétrica se crean dos claves, una pública y una privada. La clave pública, tal como implica su denominación, se hace pública y se distribuye a los diferentes colaboradores. La clave privada, naturalmente, no se hace pública. El remitente envía el mensaje codificado con la clave pública del destinatario. Después de esto, el mensaje sólo puede descodificarse mediante la clave privada del destinatario. La clave privada no puede adivinarse a partir de la clave pública o su algoritmo.

La ventaja de las claves públicas es que no hay necesidad de mandar ningún tipo de información privada por Internet. La clave pública es realmente pública: puede entregarse al destinatario mediante un mensaje de correo electrónico no codificado.

Las claves asimétricas también facilitan mucho el control de las claves: es más fácil crear y cambiar las claves cuando una de ellas es pública. El sistema criptográfico con claves públicas está especialmente indicado para sistemas grandes que requieren un gran número de claves. La desventaja es la lentitud del proceso de encriptación, que hace que el sistema no sea práctico cuando hay que codificar grandes volúmenes de información.

1.11 RSA

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye en forma autenticada preferentemente, y otra privada, la cual es guardada en secreto por su propietario.

Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.

Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes, mayores que 10100 elegidos al azar para conformar la clave de descifrado.

Emplea expresiones exponenciales en aritmética modular. La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

La computación cuántica podría proveer una solución a este problema de factorización.

1.12 Desencriptación

La desencriptación es el proceso contrario a la encriptación, mediante el cual un criptograma es transformado en el texto plano que le dio origen. En la mayoría de los

métodos o algoritmos de encriptación para que la desencriptación sea exitosa es necesario poseer una clave, ya sea pública o privada que asegura que quien realiza el proceso está acreditado para tener acceso a la información original.

1.13 El Futuro de la Encriptación.

Los actuales sistemas de llave pública y llave privada son lo suficientemente seguros siempre y cuando las llaves tienen una longitud adecuada para el estado actual de la tecnología computacional.

Pero en los últimos años se han dado pasos hacia una nueva generación de computadoras: las computadoras cuánticas, pero que muy probablemente serán una realidad en el 2020 o antes.

¿La diferencia con las computadoras actuales? A modo de ejemplo, romper un mensaje descifrarlo sin la llave privada encriptado con RSA a 2048 bits demoraría miles de años con un gran número de supercomputadoras de la actual tecnología interconectadas en paralelo. Este mismo mensaje se descifraría en cuestión de segundos con una computadora cuántica.

Para adelantarse a estos hechos, se ha venido desarrollando la criptografía cuántica, que está en una etapa de desarrollo más avanzada que las computadoras cuánticas: ya existen varios prototipos funcionales de sistemas basados en criptografía cuántica, cuando todavía existen importantes barreras para la realización de una computadora cuántica funcional.

Para tener una idea de la velocidad con la cual se está desarrollando la criptografía cuántica, en 1991 se construyó un prototipo que podía operar con una distancia máxima de 32 centímetros entre el emisor y el receptor. A mediados del 2003, esta distancia máxima ya era de 100 kilómetros. En la actualidad todavía existen problemas prácticos para su implementación, que muy seguramente se irán solucionando en los próximos años.

Para romper los sistemas actuales de encriptación solamente se requiere la potencia de computación necesaria para resolver complejos problemas matemáticos. Romper un mensaje encriptado con criptografía cuántica requeriría alterar las leyes de la naturaleza.

El experto en tecnologías de seguridad Bruce Schneier afirma: *"No tengo ninguna esperanza puesta en este tipo de productos. Tampoco tengo esperanza alguna en la comercialización de criptografía cuántica en general."*.

No vaya a ser que el Sr. Schneier pase a la historia como Thomas Watson, presidente de IBM, quien en 1943 dijo:"*Yo pienso que existe un mercado mundial para no más de cinco computadoras"*.

1.14 Conclusión.

Al final de este capitulo podemos decir que la encriptación como proceso forma parte de la criptología, ciencia que estudia los sistemas utilizados para ocultar la información.

Aunque la criptología surgió con gran anterioridad, la informática ha revolucionado los métodos que se utilizan para la encriptación y desencriptación de información, debido a

la velocidad con que las computadoras pueden realizar las fórmulas matemáticas requeridas para llevar a cabo estos métodos y a la complejidad que han alcanzado debido a este hecho.

CAPITULO 2 FIRMAS DIGITALES

2.1 Introducción

En estos tiempos cuando la seguridad de la información es un recurso sumamente valioso para una empresa, se han desarrollado metodologías que nos permiten lograr ciertos estándares de seguridad, en nuestro caso es la firmas digital, si bien estas no garantizan que nadie mas vaya a ver el contenido de un mail, al menos podremos saber si es que la persona que envía el correo electrónico es quien dice ser.

2.2 Que es la Firma Digital?

La firma digital es, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, un método criptográfico que asegura la identidad del remitente. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

La firma digital también se puede definir como una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que estos gocen de una característica que únicamente era propia de los documentos en papel.

La firma digital no implica asegurar la confidencialidad del mensaje, un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital no es un instrumento con características técnicas y normativas, es decir que hay procedimientos técnicos por medios de los cuales permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

2.3 Como funciona?

Para las firmas digitales se utiliza el sistema de claves públicas. La firma digital puede utilizarse para garantizar la integridad del mensaje. En la firma digital se usa un algoritmo de Hash (un código de comprobación) para convertir la firma digital en una cadena de longitud fija que no pueda transformarse en el mensaje original. Luego se codifica el código de comprobación mediante la clave privada del remitente. La firma digital y el mensaje original se envían entonces al destinatario. En al practica el mensaje es enviado codificado.

El destinatario utiliza la cable pública del remitente para abrir el mensaje con el código de comprobación y además recurre al mismo algoritmo de Hash para volver a poner un código de comprobación en el mensaje. Si el código de comprobación creado por el destinatario es el mismo que el enviado por el remitente, se confirma la integridad del mensaje y el hecho de que el mensaje se ha trasmitido por Internet sin sufrir alteraciones.

En la práctica, también es aconsejable asegurarse de la identidad del remitente y de que el remitente es en realidad quien dice ser. Entonces, debe añadirse el uso de una nueva clave de encriptación al procedimiento de creación de códigos de comprobación. Mediante el uso del algoritmo de hash y una clave de encriptación, podemos estar seguros de que el mensaje no ha sufrido alteraciones durante la transmisión y de que la persona que guarda la clave de encriptación es quien ha creado el mensaje original. La clave puede ser simétrica o asimétrica.

Este mismo método garantiza también la irrefutabilidad de la información. El uso de la clave de encriptación pone de manifiesto quien es remitente, incluso si este intenta alegar que no ha enviado el mensaje original.

A continuación se ilustra el proceso con el siguiente gráfico.

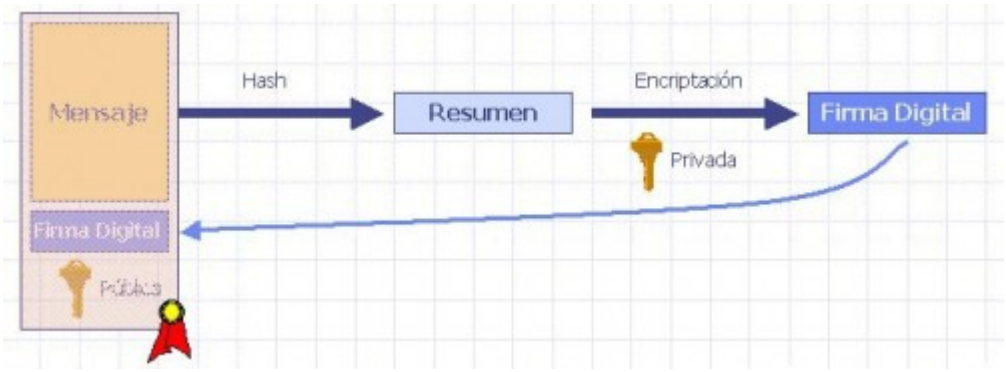


Figura 4 Funcionamiento de las Firmas digitales

2.4 ¿Claves privadas y claves públicas?

Clave Pública.

En éstos, la clave de cifrado se hace de conocimiento general (clave pública). Sin embargo, no ocurre lo mismo con la clave de descifrado (clave privada), que se ha de mantener en secreto. Ambas claves no son independientes, pero del conocimiento de la pública no es posible deducir la privada sin ningún otro dato, teniendo en cuenta que en los sistemas de clave privada sucedía lo contrario. Tenemos pues un par clave pública y clave privada; la existencia de ambas claves diferentes, para cifrar o descifrar, hace que también se conozca a estos criptosistemas como asimétricos.

Cuando un receptor desea recibir una información cifrada, ha de hacer llegar a todos los potenciales emisores su clave pública, para que estos cifren los mensajes con dicha clave. De este modo, el único que podrá descifrar el mensaje será el legítimo receptor, mediante su clave privada. Matemáticamente, si es el algoritmo cifrador y el descifrador, se ha de cumplir que, representando un mensaje, y siendo y las claves de descifrado y cifrado, respectivamente.

Clave Privada.

Son aquellos en donde cada pareja de usuarios que deseen transmitirse un mensaje deben contar con una clave secreta, sólo conocida por ambos, con la cual cifrar y descifrar.

Las dos personas dispondrían de una clave, que deberían comunicarse por un medio imposible de interceptar (canal seguro), como por ejemplo pasarla en mano. Sin embargo, no siempre es fácil disponer de ese tipo de canal. Por otra parte, seguiría necesitándose una clave para cada par de personas.

El criptosistema de clave secreta más utilizado es el Data Encryption Standard (DES), desarrollado por IBM y adaptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977.

Las desventajas de este tipo de sistemas son principalmente:

- La difícil transmisión secreta de la clave a utilizar por cada pareja.
- El gran número de claves necesarias cuando hay bastantes usuarios.

2.5 ¿Qué son los certificados digitales?

A través de los certificados digitales podemos generar la infraestructura por medio de la cual se permite dar más seguridades a los usuarios cuando utilizan el Internet y de esta manera fomentar el comercio electrónico.

Los certificados digitales, pueden acreditar la existencia de una empresa o persona en el cyber espacio, de esta manera se reducen al mínimo los fraudes en Internet que se originaron por el reemplazo virtual de personas y empresas en el mundo virtual que existió en la gran expansión del Internet, gracias a que no existía un debido control y proliferaron las Empresas fantasmas en el Internet.

Gracias a los Certificados Digitales, la transmisión de mensajes, documentos y transacciones comerciales, pueden transportarse en el Internet en un clima de absoluta seguridad y confidencialidad.

Los certificados digitales poseen mecanismos de encriptación más elaborados que permiten salvaguardar la información que navega por el Internet con esquemas muy altos de seguridad.

A continuación explicaremos qué son los certificados digitales, cuales son los formatos estándar, como podemos controlar sus periodos de validez o anularlos si se ven comprometidos, quien los genera y las infraestructuras necesarias para soportarlos.

Certificados Digitales

Un *certificado de clave pública* es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave

pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.

Los *certificados de clave pública* se denominan comúnmente *Certificado Digital*, *ID Digital* o simplemente *certificado*. La entidad identificada se denomina *sujeto del certificado* o *subscriptor*, si es una entidad legal como, por ejemplo, una persona.

Los certificados digitales sólo son útiles si existe alguna *Autoridad Certificadora* (*Certification Authority* o *CA*) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los *certificados digitales* proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes.

Certificados X.509

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization / International Electrotechnical Commission*) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para

incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

- **Limitaciones básicas**. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- **Política de certificación**. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- **Uso de la clave**. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado *sintaxis abstracta uno* (*Abstract Sintax One* o ASN-1). Para la transmisión de los datos se aplica el DER (*Distinguished Encoding Rules* o *reglas de codificación distinguible*), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

2.6 ¿Qué contiene un certificado digital?

Los elementos del formato de un certificado X.509 v3 son:

- **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.

- **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.
- **Extensiones**. Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

    1. **Tipo de extensión**. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
    2. **Valor de la extensión**. Este subcampo contiene el valor actual del campo.
    3. **Indicador de importancia**. Es un *flag* que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

2.7 ¿Qué valor legal tiene la firma digital?

En términos legales "Firma Digital" y "Firma Electrónica" tienen un significado diferente. La principal diferencia esta en que el valor probatorio a cada uno de los mismo, en el caso de "Firma Digital" existe una presunción "iuris tantum" a favor de la misma; esto quiere decir que si un *documento firmado digitalmente* es verificado correctamente, el mismo se presume *salvo prueba en contrario* que proviene del suscriptor del certificado asociado y que este no fue alterado. En su defecto el caso de *firma electrónica*, de no ser de conocimiento por su titular, corresponde quien la invoca acredita su validez.

Para reconocer que un documento tenga una firma digital se necesita que el certificado digital del firmante haya sido emitido por certificador licenciado o en su defecto que cuente con la aprobación del Ente Licenciante.

Esto es debido a que si bien entendemos que en los ambientes técnicos se utiliza constantemente el término Firma Digital para hacer transferencia al instrumento tecnológico, es independiente su importancia legal.

2.8 ¿Qué es una Infraestructura de Firma Digital?

Se puede definir como un conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades, ya sean estos individuos u organizaciones, se identifiquen entre sí de manera segura al realizar transacciones de información a través de redes, como por ejemplo el Internet.

Esta definición es conocida mundialmente con las PKI que significan Public Key Infraestructura o Infraestructura de clave pública. La Infraestructura de clave pública utiliza métodos de encriptación asimétrica de modo que se cumplan bases relativas a las transacciones electrónicas seguras: firma digital con una clave privada del firmante y además encriptación con la clave pública del destinatario.

Una parte esencial de este método es la confianza, a fin de confirmar las identidades de dos partes que no se conocen entre sí, es necesaria una tercera parte para hacer la certificación. Dicha parte debe ser alguien de confianza para ambas partes. La función de un certificado procedente de un proveedor de certificados de confianza es conectar la clave pública y la clave del usuario entre si. De este modo, es posible realizar una comunicación

confidencial y utilizar una comunicación confidencial y utilizar incluso firmas digitales si las partes no se conocen entre si.

2.9 Conclusión.

Como hemos podido observar a lo largo del capitulo 2 si bien las firmas y los certificados digitales no son una seguridad de que alguien mas no pueda acceder a nuestra información pero si nos sirve para autentificar a la persona que envía el mail y saber si es que algún usuario mal intencionado ha accedido o modificado de alguna manera nuestro correo.

Es de vital importancia que se utilice de manera correcta a las firmas digitales para poder salvaguardar la integridad en una empresa ya que la información es su recurso mas preciado.

CAPITULO 3 CONFIGURACIÓN DE LAS APLICACIONES

3.1 Introducción.

En el presente capítulo presentaremos dos propuestas de configuración, una sobre Windows utilizando el sistema operativo Windows Server 2003, utilizando Microsoft Exchange para el intercambio de correo y la configuración respectiva para el cliente de correo que en este caso utilizaremos Microsoft Outlook, luego en el capítulo siguiente tendrá una demostración práctica, y además de una propuesta teórica en la cual detallaremos los pasos para configurar un servidor de correo en Linux utilizando sendmail, y como cliente correo de electrónico utilizaremos Mozilla Thunderbird.

3.2 Configuración del Servidor de Correo.

3.2.1 Configuración del DNS.

Los DNS es una base de datos distribuida y jerárquica que guarda los datos de asociados a nombres de Dominio en redes como Internet, la asignación de nombres a direcciones IP es sin duda la función mas conocida de los protocolos DNS, y que es mas fácil recordar un nombre que una secuencia de números.

Para configurar el DNS procedemos a modificar tres archivos básicos y se lo hace en el Terminal del Centos y realizamos los siguientes pasos:

1.- Se configura el primer archivo que se encuentra el la siguiente dirección y que corresponde a la interfaz.

/etc/sysconfig/network-scripts/ifcfg-eth0

BOOTPROTO=static

IPADDR=192.168.47.1

NETMASK=255.255.255.0

GATEWAY=192.168.47.1

ONBOOT=yes

TYPE=Ethernet

2.- Procedemos a configurar los servidores DNS

/etc/resolv.conf

search miservidor.com	busca dentro del mismo dominio
nameserver 192.168.47.1	servidor primario
nameserver 127.0.0.1	secundario no importa el nombre

3.- En la misma red vamos a definir el dominio.

/etc/sysconfig/network

NETWORKING=yes

HOSTNAME=miservidor.com

4.- Luego se reinicia los servicios con el siguiente comando.

service network restart

3.2.2 Configuración del Named.

Este servicio contiene la configuración de los servidores DNS y provee información de los root servers.

1.- En este archivo creamos nuestras 3 zonas agregando el siguiente contenido.

```
//Nuestra Zona
zone "miservidor.com" IN) {  La zona
type master;                 Primario o secundario
file "miservidor.zone";      Nombre del archivo en el que se guarda la configuración
allow-update {none;};        Para que no actualice de forma remota
};
//Zona Inversa
zone "47.168.192.in-addr.arpa" IN) {
type master;
file "47.168.192.in-addr.arpa.zone";
allow-update {none;};
};
```

2.- Luego se crea los archivos de la configuración de la zona, que se encuentran en la siguiente dirección.

/var/named/chroot/var/named

Copiamos el siguiente archivo para la zona principal

cp localhostdomain.zone miservidor.zone

De igual manera para la zona inversa

cp localhostdomain.zone 47.168.192.in-addr.arpa.zone

Ahora los modificamos

miservidor.zone

Agregamos lo siguiente, primero se coloca el nombre del administrador que será

admin..miservidor.com

Un número que nos permita identificar la modificación del archivo, por ejemplo

0101200701 día/mes/año/numero de cambio

Luego pasamos a incluir los siguientes campos

miservidor.com.	IN NS	ns1
miservidor.com.	IN NS	ns2
ns1.miservidor.com.	IN A	192.168.47.1
www	IN CNAME	ns1
ns2	IN A	192.168.47.2
mail	IN CNAME	ns1
ftp	IN CNAME	ns1
miservidor.com	IN MX 10	mail
192-168-47-1.miservidor.com	IN A	192.168.47.1

En el archivo que corresponde a la zona inversa agregamos lo siguiente

admin..miservidor.com

Un número que nos permita identificar la modificación del archivo

0101200701 día/mes/año/numero de cambio

Luego incluimos los siguientes campos:

47.168.192.in-addr.arpa.	IN NS	ns1.miservidor.com
47.168.192.in-addr.arpa	IN NS	ns2.miservidor.com
1	IN PTR	192-168-47-1.miservidor.com

3.- Luego se reinicia el servicio.

service named restart

3.2.3 Configuración del Sendmail.

Primero se comprueba si esta instalado el sendmail mediante el siguiente comando.

rpm -q sendmail sendmail-cf imap

La ejecución de este commando nos devuelve la versión del SendMail, sendmail-cd e imap que se tienen instaladas en el computador. Antes de continuar, debemos modificar el archivo.

/etc/mail/local-hosts-names

En el cual se lista todos y cada uno de los aliases que tenga el servidor que estamos configurando, así como los posibles dominios.

miservidor.com	192.168.47.1
localhost	127.0.0.1
Laptop	192.168.47.2

Luego modificamos el archivo

/etc/mail/sendmail.mc

Donde cmentamos la siguiente linea

dnl # DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

Después generamos la macro para obtener el siguiente archivo /etc/sendmail.cf:

m4 sendmail.mc > /sendmail.cf

Luego modificamos el archivo vi /etc/mail/access y agregamos algunas líneas para definir quienes podrán hacer uso de nuestro servidor de correo

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
192.168.47	RELAY

Debemos compilar este archivo para generar otro en formato de base de datos a fin de ser utilizado por Sendmail

makemap hash /etc/mail/access.db < /etc/mail/access

3.2.4 Configuración del Dovecot.

1.- Se configura el archivo

/etc/dovecot.conf

Parámetros a configurar en el archivo

protocols = imap pop3 (pop3s es encriptado)

pop3_listen='::' cambiar por '*'

imap_listen='::' cambiar por '*'

2.- Reiniciamos el servicio con el comando

service dovecot restart

El último paso es crear los usuarios para las cuentas de correo con el siguiente comando

Useradd Patricio

Y luego utilizamos el comando passwd para agregar el password para el usuario patricio

Passwd uda2007

Finalmente hemos realizado toda la configuración para la parte del servidor de correo

3.2.5 Generación de Certificados Digitales.

Crearemos un directorio donde procederemos a guardar los certificados que generaremos, por razones de seguridad este directorio estará solamente al alcance del administrador del Sistema (root).

mkdir -m 0700 /etc/ssl

Procedemos a crear una carpeta específica para almacenar los certificados para nuestro servidor, y también procedemos a otorgar permisos para que este solo accesible al root.

mkdir -m 0700 /etc/ssl/miservidor.com

Accedemos al directorio que creamos.

/etc/ssl/miservidor.com

Procedemos a Generar el Certificado para el Sendmail.

Sendmail necesita una llave creada con el algoritmo DSA de 1024 octetos, para esto creamos primero el archivo de parámetros DSA.

openssl dsaparam 1024 -out dsa1024.pem

A continuación utilizamos el fichero DSA que acabamos de crear para generar la una llave con algoritmo DSA y estructura X.509, así como también el correspondiente certificado. Establecemos una duración de 730 días para la validez del certificado.

openssl req -x509 -nodes -newkey dsa:dsa1024.pem -days 730 -out **sendmail.crt** -keyout **sendmail.key**

Nos pedirá que ingresemos los siguientes datos, código de dos letras para el país, estado o provincia, Ciudad, nombre de la empresa o razón social, unidad o sección, nombre del anfitrión, y dirección de correo.

Nosotros Ingresaremos

- EC
- Azuay
- Cuenca
- Universidad del Azuay

- Sistemas
- Miservidor.com
- paul@miservidor.com

Una vez que hayamos realizado el paso anterior ya podemos eliminar el fichero dsa1024.pem con toda seguridad.

```
rm -f dsa1024.pem
```

Es necesario que los archivos de certificados y claves tengan permisos de lectura para el usuario root.

```
chmod 400 /etc/ssl/miservidor.com/sendmail.*
```

Dentro del archivo /etc/mail/sendmail.mc tenemos que agregar las siguientes líneas para que Sendmail utilice la clave y el certificado que acabamos de crear.

```
define(`confCACERT_PATH',`/etc/ssl/miservidor.com')
define(`confCACERT',`/etc/ssl/miservidor.com/sendmail.crt')
define(`confSERVER_CERT',`/etc/ssl/miservidor.com/sendmail.crt')
define(`confSERVER_KEY',`/etc/ssl/miservidor.com/sendmail.key')
```

Y también activamos el puerto que será utilizado para SMTPS (465 por TCP)

```
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
```

Procedemos a guardar los cambios realizados en el archive sendmail.cf y reiniciamos el servicio de sendmail.

```
service sendmail restart
```

Realizamos una comprobación al sistema con introduciendo.

```
Telnet 127.0.0.1 25
```

Ingresamos el comando EHLO miservidor.com

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is '^]'.

220 midominio.org ESMTP Sendmail 8.13.1/8.13.1; Mon, 2 Oct 2006 13:18:02 -0500

ehlo midominio.org

250-midominio.org Hello localhost.localdomain [127.0.0.1], pleased to meet you

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-8BITMIME

250-SIZE

250-DSN

250-ETRN

250-AUTH LOGIN PLAIN

250-STARTTLS

250-DELIVERBY

250 HELP

Note que el servicio STARTTLS se encuentra activo. Ahora procedemos a realizar un proceso similar al anterior pero ahora con el objetivo de obtener la llave y el certificado para el dovecot.

Establecemos que la duración del certificado sea de dos años igual, y procedemos a insertar el comando openssl para generarlos.

openssl req -x509 -nodes -newkey rsa:1024 -days 730 -out dovecot.crt -keyout dovecot.key

Ahora procedemos a ingresar los datos de forma similar a sendmail nos pedirá, código de dos letras para el país, estado o provincia, Ciudad, nombre de la empresa o razón social, unidad o sección, nombre del anfitrión, y dirección de correo.

Ingresaremos

- EC
- Azuay
- Cuenca
- Universidad del Azuay
- Sistemas
- Miservidor.com
- paul@miservidor.com

El computador nos devolverá una confirmación de todos los datos que hemos ingresado

Generating a 1024 bit RSA private key

.....++++++

.++++++

writing new private key to 'dovecot.key'

You are about to be asked to enter information that will be

incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name

or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:**EC**

State or Province Name (full name) [Berkshire]:**Azuay**

Locality Name (eg, city) [Newbury]:**Cuenca**

Organization Name (eg, company) [My Company Ltd]:

Mi servidor

Organizational Unit Name (eg, section) []:UDA

Common Name (eg, your name or your server's hostname) []:

Miservidor.com

Email Address []: **Paul@miservidor.com**

Luego de haber generado la llave y el certificado correspondientes al dovecot procedemos a restringir los permisos a todos los archivos nuevos.

chmod 400 /etc/ssl/**miservidor.com**/dovecot.*

Ahora vamos a cambiar los parámetros de /etc/dovecot.conf en el parámetro protocols, se activan todos los servicios (imap, imaps, pop3 y pop3s)

protocols = imap imaps pop3 pop3s

Verificamos que el parámetro #ssl_disable tenga el valor “no” o bien que esta línea se encuentre documentada.

#ssl_disable = no

Seguimos y especificamos las rutas del certificado y clave con las siguientes líneas.

ssl_cert_file = /etc/ssl/miservidor.com/dovecot.crt

ssl_key_file = /etc/ssl/miservidor.com/dovecot.key

Finalmente grabamos los cambios y procedemos a reiniciar el servicio para lo cual ingresamos el código.

```
service dovecot restart
```

3.2.6 Configuración del Cliente.

A continuación se detallan los pasos para la instalación de un Certificado Digital en el Mozilla Thunderbird.

El primer paso es configurar una cuenta de correo para esto hacemos clic en “Tools”, “Account Settings”.

En la ventana que aparece a continuación en la parte inferior encontramos un botón que dice “Add Account”, hacemos clic.

En la siguiente ventana hacemos clic en la opción “Email account” y seguimos Clic en “Next”.

Aparece una ventana que tiene como titulo “Identify” procedemos a introducir el nombre de la persona dueña de la cuenta de correo por ejemplo “Paúl Carrión” y también introducimos nuestra dirección de correo “paul@miservidor.com” y damos clic en “Next”.

En la siguiente ventana que hace referencia a la Información del Servidor “Information Server” dejamos marcada la opción POP 3 y en la casilla “Incommng Server” ingresamos “miservidor.com” o “192.168.47.1” ambas opciones son validas ya que el servicio de DNS esta configurado en el servidor de Correo.

Seguimos configurando la cuenta de correo y llegamos a la parte del nombre de usuario e introducimos el nombre de usuario correspondiente a la cuenta en nuestro caso colocamos “Paul” en la casilla “Incoming User Name” y hacemos clic en “Next”, en la siguiente ventana confirmamos los datos que hemos introducido en el proceso.

El siguiente paso es acceder al menú opciones donde podemos configurar varias alternativas de configuraciones acerca del funcionamiento del Mozilla Thunderbird.

Clic en options, tools.

Hacemos clic en el icono “Privacy” y en la parte de “Security” encontramos cuatro botones hacemos clic en “View Certificates” y hacemos clic en import y seleccionamos los certificados que generamos en el servidor.

Ahora procedemos como ultimo paso a configurar la conexión segura para esto hacemos clic “Tools”, “Account Settings” y en la ventana se abre hacemos clic en la parte “Secure Settings” seleccionamos la opción “TLS” y dejamos activada la opción de “Use secure authentication”

Con esto hemos terminado la alternativa de la configuración de cliente y servidor para la parte de Linux, a continuación de Igual manera explicaremos la configuración respectiva para Microsoft Exchange

3.3 Configuración de Servidor de Microsoft Exchange.

3.3.1 Creación de la Entidad Emisora de Certificados.

El primer paso es dirigirnos al panel de control y elegimos la opción de agregar o quitar programas y pulsamos el botón agregar o quitar componentes de Windows, señalamos la opción con el nombre Actualizar Certificados de Raíz y hacemos clic en el botón de detalles.

- En la primera ventana que aparece señalamos la opción entidad emisora raíz de la empresa y marcamos la opción usar la configuración personalizada para generar el par de claves y certificado de entidad emisora y pulsamos siguiente.
- Escogemos la pareja de clave publica y privada el proveedor de servicios de cifrado que va ha ser Microsoft Strong Cryptographic Provider y algoritmo hash SHA-1 con la longitud de clave de 2048 bits y pulsamos siguiente.
- Vamos a dar la Identificación de la Entidad Emisora de Certificados en el nombre común colocamos para esta entidad miservidor, en sufijo del nombre completo se coloca lo siguiente “DC=Miservidor,DC=local” y en vista previa de nombre completo “CN=miservidor,DC=Miservidor,DC=local” con un periodo de validez de 5 años y pulsamos siguiente.
- El campo de la base de datos de certificados escribimos la ruta donde se va ha almacenar para nuestro ejemplo “C:/WINDOWS/system32/CertLog” de igual manera para el Registro de la base de datos de certificados y pulsamos siguiente.
- En ese instante nos aparece un mensaje de advertencia para completar la instalación de Servicios Certificate Server y pulsamos en “Si”.
- Y luego se muestra una ventana donde se esta realizando la configuración de los componentes y al final se hace clic en el botón de finalizar.

3.3.2 Configuración del Administrador del Sistema Exchange.

Lo primero que se debe realizar es ir al Administrador de Sistema Exchange:

- Abrir la carpeta de servidores.
- Pulsar el icono Server que es el nombre de nuestro servidor y dirigimos a la carpeta de Protocolos.
- Ahora abrimos el fólder de SMTP y ponchamos el icono con el nombre Servidor Virtual SMTP predeterminado.
- Pulsamos el botón derecho del ratón y damos clic en propiedades.

En la parte de propiedades:

- La primera viñeta “General” en el campo Dirección IP seleccionamos la opción “Todos sin asignar”.
- La siguiente viñeta es la de “Acceso” pulsamos el botón de Certificados donde se muestra el Asistente para Certificados de Servidor de Correo.
- En la próxima ventana que aparece señalamos la opción Crear un certificado nuevo y pulsamos siguiente.
- Marcamos la opción enviar la petición inmediatamente a una entidad emisora de certificados en línea en este caso seria nuestro servidor de correo y pulsamos siguiente.

- Escribimos ahora el nombre del nuevo certificado para nuestro ejemplo “Miservidor Correo” y la longitud en bits que es 1024.
- Colocamos el nombre de la organización y la unidad organizativa que será “UDA” y “Sistemas” respectivamente.
- Y luego el nombre común de nuestro Sitio Web que es “server”.
- Registramos la información geografía, donde ingresaremos la información del país “Ecuador”, estado o provincia “Azuay” y la ciudad o localidad “Cuenca”.
- Como nosotros somos la entidad emisora seleccionamos la opción SERVER.Miservidor.local\miservidor y pulsamos siguiente hasta terminar el asistente.
- Al terminar la generación del certificado se debe tomar en cuenta un punto muy importante que es la seguridad entonces en la viñeta de “Acceso” en el botón de comunicación señalamos las opciones de Requerir un canal seguro y Requerir cifrado de 128 bits y pulsamos clic en aceptar.

3.3.3 Creación de los Usuarios.

Nos dirigimos al Administrador de Servidores donde buscamos la opción de usuarios y pulsamos en el vínculo de agregar un nuevo usuario en el cual aparece el asistente para agregar usuarios y se realiza los siguientes pasos:

- En este punto llenamos la información de la cuenta del usuario que consta de los siguientes campos:
  - Nombre: Paul
  - Apellidos: Carrion
  - Nombre de inicio de sesión: Paul Carrion
  - Alias de correo electrónico: PaulCarrion@miservidor.com
  - Teléfono: (593)-072887866
- La siguiente ventana es la contraseña de usuario ingresamos una contraseña y la confirmamos en el cual también tenemos la opción de permitirle cambiar la contraseña o no para la practica escogimos la primera y pulsamos siguiente.
- En la selección de plantilla escogemos la de User Template y pulsamos siguiente.
- La ventana de configuración de equipo cliente seleccionamos la opción no configurar el equipo y finalizamos el asistente.
- En ese momento se crea la cuenta y se configura la pertenecías de grupo al final cerramos la ventana y se muestra un mensaje de información y pulsamos aceptar.

3.3.4 Creación del Certificado.

Hay que considerar 2 aspectos si se crea desde el servidor en la ventana del Internet Explorer en la barra de direcciones se debe colocar el link http://server/certsrv/ o si se lo realiza desde el cliente se digitara http://miservidor.com/certsrv/, con esto se muestra una pantalla de bienvenida donde realizaremos lo siguiente:

- En la selección de tareas pulsamos el link Solicitar un Certificado.
- Lo que nos lleva a otro screen en el que seleccionamos el tipo de certificado q para la práctica es de usuario.
- Ahora nos aparece la pantalla de Identificar información pero es adquirida automáticamente por la cuenta de usuario de correo que se creo anteriormente y presionamos el botón de enviar.
- Se nos muestra un mensaje de advertencia y pulsamos “Si”, mostrando que se emitió el certificado solicitado.
- Luego pulsamos el link instalar este certificado, mostrándonos un mensaje de agregación de certificados en donde pulsamos en “Si”, enviándonos a una pantalla que muestra que se ha instalado satisfactoriamente su certificado nuevo.

3.4 Instalación del Certificado en el Cliente de Correo Microsoft Outlook 2003.

Para la implementación de la firma digital en la parte del correo de en Windows XP vamos a utilizar el Cliente de correo Microsoft Outlook 2003.

Nuestro primer paso será crear un cliente de correo para esto realizamos los siguientes pasos:

- Clic en Inicio, luego panel de control y hacemos doble clic en el icono Correo
- Hacemos clic en el botón “Cuentas de correo Electrónico”
- En la ventana que aparece señalamos la opción “Agregar una nueva cuenta de correo electrónico” y hacemos clic en “Siguiente”.
- Seleccionamos la opción “Servidor de Microsoft Exchange”
- A continuación en la nueva ventana que aparece en el cuadro de texto “Microsoft Exchange Server” insertamos el siguiente texto “SERVER.Miservidor.local” el cual hace referencia a nuestro servidor de correo.
- En el cuadro de texto de la parte inferior “Nombre de usuario” introducimos el nombre del cliente “Paul Carrion” y pulsamos sobre el botón “Comprobar Nombre” al realizar esto el cliente se comunica con el servidor y verifica la existencia del usuario Paul Carrion en su base de datos de usuarios y si el usuario existe subraya el nombre del usuario en el cuadro de texto.
- Hacemos clic en el botón “Más Configuraciones” tiene que encontrarse la opción “Detectar automáticamente el estado de la conexión” señalada si no es así procedemos a señalarla.
- En la viñeta de Seguridad encontramos la opción “Cifrar datos entre Microsoft Office Outlook y Microsoft Exchange Server” la cual debemos activarla.
- Hacemos clic en Siguiente.

Para instalar el certificado en el computador del cliente realizamos los siguientes pasos.

- Abrimos el Internet Explorer e introducimos la siguiente dirección "http://miservidor.com/certsrv/"
- Nos conectamos al servidor para instalar el certificado ya generado y pulsamos sobre el link "Solicitar un certificado"
- En la siguiente pagina hacemos clic sobre "Certificado de usuario"
- Luego hacemos clic sobre el botón Enviar, e inmediatamente nos aparece un mensaje preguntando si queremos aceptar el certificado, clic en Sí
- Por ultimo nos aparece una pagina con un link con el texto "Instalar este certificado"
- Hacemos clic sobre el mismo, y aparece un mensaje que nos informa que un certificado va a ser instalado en nuestro computador y solo debemos hacerlo si es que realmente confiamos en este sitio Web, respondemos que si.
- Llegamos a la ultima pagina que nos dice que el certificado a sido instalado de forma satisfactoria en nuestro computador

Procedemos ha abrir la aplicación Microsoft Outlook 2003 para instalar el certificado digital que generamos en el servidor, realizamos los siguiente pasos.

- Hacemos Clic en el menú "Herramientas", e inmediatamente en "Opciones".
- En la ventana que se despliega nos dirigimos la Viñeta Seguridad y ahí seleccionamos las opciones "Agregar Firma Digital y datos adjuntos para mensajes salientes" y "Solicitar Confirmación S/MIME para todos los mensajes S/MIME firmados"

- Hacemos un clic en el botón “Configuración” y en la venta que aparece damos un nombre a la configuración de seguridad “Mi configuración S/MIME ”
- Hacemos clic en el formato de cifrado y seleccionamos S/MIME
- Presionamos sobre el botón “Elegir” y seleccionamos nuestro certificado de firma digital que en nuestro caso es para Paul Carrion para el uso en Mi servidor.
- Repetimos el mismo procedimiento para el paso seleccionar el certificado de encriptación.

3.5 Conclusión.

En principio se configuro el servidor de correo sobre la plataforma Linux (Sendmail), pero debido a que no existe mucha información sobre la aplicación de las firmas digitales sobre esta, decidimos realizar la aplicación sobre la plataforma Windows con su producto Microsoft Windows Server 2003 y el servidor de correo con el programa Microsoft Exchange que nos permitió una mayor flexibilidad durante la configuración del servidor, que consta de varios asistentes ya sea para la creación de los usuarios y certificados de manera mas rápida y segura, y a su vez la aplicación del certificado sobre el cliente de correo electrónico Microsoft Outlook 2003 proporcionando una mayor cantidad de información condescendiéndonos un mas alto entendimiento, tomando en cuenta un aspecto importante; que estas herramientas no son libres, representando un costo para su implementación.

CAPITULO 4 PRUEBAS

4.1 Introducción

En este capitulo hablaremos de las diversas pruebas que realizamos en el transcurso del desarrollo práctico de nuestra investigación, en donde hablaremos desde los pasos que realizamos para comprobar el correcto estado de la conexión de la red entre el servidor y el cliente, hasta las pruebas finales sobre la implementación de las firmas digitales.

4.2 Pruebas del estado de la red.

Una vez conectadas las 2 computadoras a través de un enlace punto a punto con un cable cruzado procedes a utilizar el comando ping entre ambas.

El servidor cuenta con la dirección IP 192.168.47.1 y el cliente cuenta con la dirección de IP 192.168.47.2, para realizar un ping entre el cliente y el servidor procedemos de la siguiente manera.

Ping 192.168.47.1

Y obtenemos la respuesta:

Reply from 192.168.47.1: bytes=32 time<1ms TTL=128

Reply from 192.168.47.1: bytes=32 time<1ms TTL=128

Reply from 192.168.47.1: bytes=32 time<1ms TTL=128

Reply from 192.168.47.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.47.1:

Packets: sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Con estos resultados podemos interpretar que el estado de la conexión es óptimo, ahora procedemos a probar la correcta configuración de los DNS para esto volvemos a utilizar el comando ping pero en vez de apuntar a la dirección IP del servidor lo llamaremos por su nombre de Dominio.

Ping miservidor.com

Obtenemos resultados exactos a los que obtuvimos realizando un ping apuntado a la dirección IP del servidor.

Una vez configurado la red procedemos a enviar una prueba de correo entre las dos maquinas.

4.3 Pruebas de Correo.

Mandamos un mail desde Microsoft Outlook 2003 al servidor desde el cliente PaulCarrion@miservidor.com en este caso en el servidor esta configurado con la cuenta de correo PatricioMonsalve@miservidor.com, y el correo se envía sin ningún problema y llega de manera inmediata al destinatario, la cuenta de correo PatricioMonsalve@miservidor.com

recibe el correo electrónico que se envió desde el cliente y responde el correo para probar que el correo funciona sin inconvenientes en ambos sentidos. La cuenta de correo PaulCarrion@miservidor.com recibe de igual manera el correo de respuesta del servidor sin ningún inconveniente ni demora.

Ahora procedemos a enviar un correo electrónico incluyendo la firma digital desde PatricioMonsalve@miservidor.com a PaulCarrion@miservidor.com el correo se envía perfectamente y cuando el cliente PaulCarrion@miservidor.com recibe el mensaje se puede constatar de que esta firmado Digitalmente ya que en la esquina superior derecha encontramos un icono con un listón rojo que indica que el documento esta firmado digitalmente al hacer clic sobre el mismo podemos ver información sobre el la firma digital como de donde se mando el correo y así podemos verificar que el destinatario es realmente quien dice ser y alcanzando un alto de nivel de confianza en el correo electrónico.

4.4 Conclusión

Finalmente podemos demostrar de manera práctica el uso de las firmas y Certificados digitales en un sistema de correo electrónico generando así confianza en el usuario al comunicarse a través de este medio. Si bien es una técnica sencilla cuando se sabe como implementarla es de gran ayuda en las comunicaciones dentro y fuera de una empresa.

CONCLUSIONES

Al término de la presente monografía logramos el entendimiento de los orígenes de la encriptación, basándonos en el estudio de ciencias que fueron las fundadoras o predecesoras de la misma como la criptografía, criptologia y criptosistemas que permitieron la proliferación de los métodos de ocultamiento de información.

Las mismas que permitieron crear además sistemas como los certificados y firmas digitales que garantizan a los usuarios el envió seguro de nuestros emails a través del correo electrónico, que aseguran que nuestra información no haya sido alterada y que están validadas por una entidad seria y legalizada.

Al terminar el capitulo número tres vimos la manera en que se puede configurar un sistema de firmas digitales ya sea utilizando la plataforma Linux o sistemas operativos de la casa de Microsoft, dando un entendimiento práctico de la teoría expuesta en los dos capítulos anteriores.

Finalmente de manera práctica logramos con éxito sustentar y a través del funcionamiento del una aplicación de firmas y certificados digitales todo el esfuerzo que se entregó en el desarrollo de esta investigación.

RECOMENDACIONES

Un aporte muy importante que se pudo obtener durante la elaboración de la monografía, es que con el crecimiento de las empresas en todos sus niveles, su necesidad de seguridad crece, por lo que se debería tratar de fomentar la implementación de mecanismos de autentificación de correo electrónico como son las firmas digitales, con el constante flujo de entrada y salida de los datos corren un peligro de no saber si la información que se recibe es valida o esta certificada.

Tomando en cuenta que no es necesario invertir demasiados recursos sino en tratar de buscar medios alternativos como la plataforma Linux que se encuentra libre en el mercado, pero también con personal competente que permitan una mayor investigación sobre temas que no se han explorado a fondo, por la falta de información o expertos capacitados en el tema, para que sirvan de apoyo a la implantación de nuevos sistemas de seguridad en las empresas.

BIBLIOGRAFÍA

- **www.wikipedia.org** Enciclopedia Virtual, Wikimedia Foundation, Inc., 04-01-2007.

- **http://ieee.udistrital.edu.co/concurso/ciencia_tecnologia_info_3/index.html#indice** Universidad Distrital Jose Fracisco Caldas (Colombia) – Materia de Ciencia y Tecnologia de la Informacion III, 04-01-2007**.**

- **http://www.pki.gov.ar/index.php?option=content&task=view&id=91&Itemid=102** Proyecto Firma Digital de la República Argentina, Subsecretaria de la Gestion Publica – Jefatura de Gabinete de Ministros de la Republica Argentina, 04-01-2007.

- **http://www.diphuelva.es/area_principal.asp?idArea=56** Diputacion de Huelva (España) – Firma Digital, 04-01-2007.

- **http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=como-sendmail-dovecot-tls-ssl** Como configurar Sendmail y Dovecot con soporte SSL y TLS 21-02-2007

- **http://www.microsoft.com/spain/exchange/techinfo/seguridad/default.aspx Microsoft información sobre seguridad en Exchange Server**

GLOSARIO

ASN-1 (Abstract Sintax One) - Sintaxis de Abstracto Uno.

CA (Certification Authority) - Autoridad Certificadora.

DER (Distinguished Encoding Rules) - Reglas de Codificación Distinguible.

DES (Data Encryption Standard) - Norma de Cifrado de Datos.

DNS.

El **Domain Name System** (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

DSA

DSA (Digital Signature Algorithm, en español Algoritmo de Firma digital) Es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales

IBM (International Business Machines) - Maquinas de Negocio Internacional.

IDEA (International Data Encryption Algorithm) - Algoritmo Internacional de Cifrado de Datos.

ISO/*IEC* (International Standards Organization / International Electrotechnical Commission) - Organización de Estándares Internacionales / Comisión Electrotécnica Internacional.

ITU-T (International Telecommunication Union /Telecommunication Standarization Sector) - Union Internacional de Telecomunicaciones / Sector de Estandarización de las Telecomunicaciones.

MX.

Mail Exchange, Intercambio de Correo.

NBS (National Bureau of Standards) - Oficina Nacional de Estándares.

PKI (Public Key Infrastructure) - Infraestructura de Clave Pública.

RSA.

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

SMTP.

Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos

TLS.

(Transport Layer Security en castellano Seguridad para Capa de Transporte) es una versión estandarizada por el IETF del protocolo SSL que pretende abarcar toda la capa de transporte de la pila OSI.

ANEXOS

Cuenca, 9 de Enero del 2007

Señor Economista
Luís Mario Cabrera
Decano de la Facultad de Ciencias de la Administración
De la Universidad del Azuay
Ciudad

Señor Decano:

Quienes suscribimos comunicamos a usted que hemos procedido a revisar el Diseño de Monografía presentado por Paúl Sebastián Carrión Martínez y Patricio Esteban Monsalve Espinoza, estudiantes de la Escuela de Ingeniería de Sistemas con el tema: ***"Utilización de Firmas Digitales en el Correo Electrónico"***, como requisito previo a la obtención del titulo de Ingenieros de Sistemas, sobre el cual presentamos el siguiente informe:

- El contenido propone un trabajo de investigación objeto y coherente sobre el estudio e implementación de una aplicación que agrega una firma digital a los correos dentro de un servidor de correo electrónico basado en una plataforma Linux (Sendmail).

- El diseño cumple con los requisitos metodológicos básicos exigidos por la facultad, en cuanto a la descripción del objeto de estudio, resumen del proyecto, contexto, justificación-impactos, objetivos, marco teórico, esquema tentativo, procedimientos metodológicos y bibliografía necesaria para el desarrollo de la monografía.

Por las consideraciones anotadas, se emite un informe favorable y salvo su mejor criterio, se recomienda su aprobación.

Atentamente

Ing. Osvaldo Merchán
Director de Escuela de Ingeniería de Sistemas

Ing. Pablo Esquivel
Director de Monografía

Cuenca, 9 de Enero del 2006

Señor Economista
Luís Mario Cabrera
Decano de la Facultad de Ciencias de la Administración
De la Universidad del Azuay
Ciudad

Señor Decano:

Nosotros, Paúl Sebastián Carrión Martínez y Patricio Esteban Monsalve Espinoza, estudiantes de la Escuela de Ingeniería de Sistemas, nos dirigimos a usted, y por su digno intermedio al Honorable Consejo de Facultad, para solicitarle la aprobación del Diseño de Monografía con el tema: ***"Utilización de Firmas Digitales en el Correo Electrónico"***, así como la asignación de Director de Monografía, el mismo que nos permitimos sugerir al Ing. Pablo Esquivel, por cuanto el a sido nuestro asesor y contamos con su aprobación.

Por la favorable acogida que brinde a la presente, le anticipamos nuestros agradecimientos.

Atentamente

Paul Sebastián Carrión Martínez
Código: 26094
CI. 0103673489

Patricio Esteban Monsalve Espinoza
Código: 27776
CI. 0103777298

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACION

ESCUELA DE INGENIERÍA DE SISTEMAS

DISEÑO DE MONOGRAFIA

TEMA:

"Utilización de Firmas Digitales en el Correo Electrónico"

AUTORES:

Paúl Sebastián Carrión Martínez
Patricio Esteban Monsalve Espinoza

Cuenca - Ecuador
2007

1. Titulo del Proyecto.

"Utilización de Firmas Digitales en el Correo Electrónico"

2. Selección y Delimitación del Tema.

Contenido.

El proyecto abarca el tema de la encriptación de la información de los correos electrónicos ya que estos son altamente susceptibles a usuarios mal intencionados que desean leer el contenido de los correos que transitan en la red.

Para lo cual implementaremos una aplicación que agrega una firma digital en base al contenido del correo electrónico utilizando una clave privada, el destinatario realizará la verificación de la firma utilizando una clave pública, en este proceso se comprueba que el contenido no ha sido modificado.

La monografía se realizada de manera teórico-practica demostrando el funcionamiento de la aplicación y la explicación de las tecnologías y conocimientos empleados en el tema.

3. Contexto sobre la Monografía.

En la actualidad el correcto manejo de la información es de vital importancia en todos los aspectos de nuestra sociedad y es utilizado a todos los niveles socioeconómicos y por usuarios de todas las edades y posiciones dentro de una empresa.

Con el uso del correo electrónico se permitió grandes avances en la comunicación de las personas, hace 50 años el envío de un correo podía tomar semanas hasta incluso meses en llegar a su destinatario dependiendo de la ubicación en que se encontraba, con la llegada del correo electrónico un mensaje puede ser enviado a cualquier parte del mundo en cuestión de segundos.

Esto contribuyo a que la comunicación en los negocios avance a pasos agigantados reduciendo los costos, y optimizando el uso de personal en las empresas, esto ha traído sus consecuencias negativas ya que los correos electrónicos son fácilmente falsificables, por eso es que creemos que es necesario la implementación de un sistema de autentificación y seguridad de correos electrónicos.

4. Impacto Tecnológico.

Al implementar un sistema de encriptación que brinde seguridad y confianza a los usuarios del correo electrónico se puede optimizar el uso de equipos y mejorar el proceso de la información en los servidores, aparte de poder asegurar un nivel de confianza a la información que es enviada por correo electrónico.

5. Impacto Social.

Dar a los usuarios de correo electrónico seguridad y confianza al momento de enviar y recibir información, conseguido esto se puede promover el correo electrónico como un método muy económico y eficaz de uso.

6. Objetivos.

6.1 Objetivo General.

Implementar un sistema con la utilización de Firmas Digitales.

6.2 Objetivos Específicos.

- Configurar un servidor de correo con la utilización de Firmas Digitales.
- Configurar un cliente de correo electrónico para Firmas Digitales.

7. Teoría Referencial.

- Linux.

  Linux es la denominación de un sistema operativo y el nombre de un núcleo. Es uno de los paradigmas del desarrollo de software libre (y de código abierto), donde el código fuente está disponible públicamente y cualquier persona, con los conocimientos informáticos adecuados, puede libremente estudiarlo, usarlo, modificarlo y redistribuirlo.

- Firmas Digitales.

  La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma en el que se emplea una clave privada al resultado de la operación anterior, generando la firma electrónica o digital.

- Encriptación.

  Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cuál la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos.

8. Esquema Tentativo.

Capitulo 1. Introducción

1.1 Encriptación.
    1.1.1 Tipos de Claves.
1.2 Métodos de Encriptación.

Capitulo 2. Firmas Digitales.

2.1 ¿Qué es la firma digital?
2.2 ¿Cómo funciona?
2.3 ¿Claves privadas y claves públicas?
2.4 ¿Qué son los certificados digitales?
2.5 ¿Qué contiene un certificado digital?
2.6 ¿Qué valor legal tiene la firma digital?
2.7 ¿Qué es una Infraestructura de Firma Digital?
2.8 Instalación de un Certificado Digital.

Capitulo 3. Configuración de las Aplicaciones.

3.1 Configuración del Servidor de Correo.
3.2 Configuración del Cliente.

Capitulo 4. Pruebas.

Conclusiones.

Recomendaciones.

Bibliografía.

Anexos.

9. Recursos humanos.

- 1 Director de Monografía.
- 2 Estudiantes Egresados.

10. Recursos Materiales.

Hardware.

- 3 computadores con soporte para red.
  - 1 computador que servirá como servidor de correo electrónico.
  - 1 computador que trabajara como remitente.
  - 1 computador que será el destinatario.
  - 1 Hub/Switch.

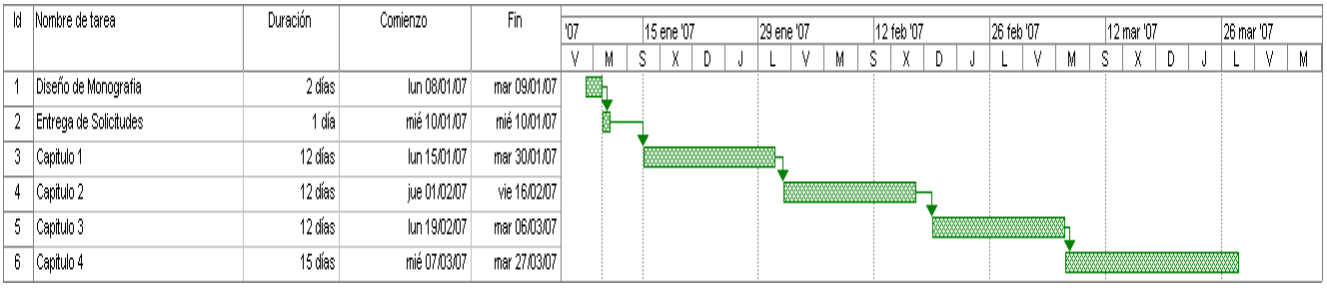
Software.

- Sistema Operativo Centos 4.2 plataforma Linux
- Aplicación SendMail.

11. Recursos Financieros.

Recurso	Cantidad	Valor unitario	Valor Total
Papel Bond	150	0,01	**1,50**
Carpeta	5	0,25	**1,25**
Internet	30	0,80	**24**
Tinta	1	45	**45**
Otros		20	**20**
		Total	**91.75**

13. Cronograma.



Id	Nombre de tarea	Duración	Comienzo	Fin
1	Diseño de Monografía	2 días	lun 08/01/07	mar 09/01/07
2	Entrega de Solicitudes	1 día	mié 10/01/07	mié 10/01/07
3	Capitulo 1	12 días	lun 15/01/07	mar 30/01/07
4	Capitulo 2	12 días	jue 01/02/07	vie 16/02/07
5	Capitulo 3	12 días	lun 19/02/07	mar 06/03/07
6	Capitulo 4	15 días	mié 07/03/07	mar 27/03/07

14. Bibliografía.

- **es.wikipedia.org/wiki/Firma_digital** Firma digital - Wikipedia, la enciclopedia libre 07-01-2007.
- **www.pki.gov.ar/index.php?option=content& task=view&id=91&Itemid=102** Proyecto Firma Digital de la República Argentina 07-01-2007.
- **www.iec.csic.es/CRIPTONOMICON/articulos/expertos32.html** Cómo funcionan las firmas digitales 07-01-2007.