UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"EXTENSIONES DE SEGURIDAD PARA DNS EN EL DOMINIO UNAM.MX"

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERA EN COMPUTACIÓN

P R E S E N T A :

VERÓNICA BADILLO TORRES

DIRECTORA DE TESIS:

ING. GLORIA GUADALUPE MARTÍNEZ ROSAS

MÉXICO, D.F. Marzo de 2011.

AGRADECIMIENTOS

El culminar el presente trabajo y así cerrar un ciclo, logrando concluír una gran meta y por ello quiero agradecer a:

Dios por darme la oportunidad de culminar algo importante para mi vida por dejarme existir.

A Mis padres

María Elena Torres de la Rosa por ser la mejor madre que me pudo tocar, por enseñarme a luchar, a no claudicar con lo que me proponía, a estar siempre escuchándome, apoyándome y por qué no, llamarme la atención cuando no seguía el camino, sé que siempre estarás en mí, ésta meta no es solo mía sino tuya y de papá Gracias por todo mamí.

José Margarito Badillo Lázaro por estar siempre conmigo, ser un amigo, enseñarme que se tiene que luchar por conseguir algo en la vida, eres el mejor papá que me pudo tocar, aunque un poco enojón y a pesar que discutíamos mucho sabes que te quiero. Mil gracias por tu trabajo, dedicación y cuidado hoy estas cosechando lo que en un momento me brindaste.

A mi hermana Minerva

Gracias por apoyarme hermanita, en levantarme el ánimo, escucharme y decirme que si se puede, ahora yo te digo si se puede aunque es trabajoso el camino y a veces con obstáculos es cuestión de levantarse con la cabeza en alto y seguir, sabes que siempre estaré a tu lado también echándote porras y sobre todo por ser mi amiga.

A Luis Enrique

Gracias amor por apoyarme cada día, apoyarme en todo lo que me propuse, respetarme en mis decisiones y siempre alentarme, por escucharme y sobre todo por ser como eres , Gracias por ser el compañero de clases, amigo que a pesar de muchas dificultades siempre estuvo conmigo y ahora como mi novio

GRACIAS

A los Muchachos

Sin temor que me falte alguno les doy las gracias chicos porque me enseñaron que con ayuda mutua se puede llegar a la meta la perseverancia y el no desistir, el repetir las cosas una vez mas no es malo si es necesario se realizara y a pesar de diferentes carreras geofísicos y petroleros siempre me apoyaron gracias por aquellos momentos de estudio siempre los llevare en mío corazón son parte importante para mí.

A Gloria Guadalupe

Por tu apoyo, amistad y darme las armas para terminar de concluir un ciclo, gracias por estar como compañera, asesora, pero sobre todo por ser amiga.

ÍNDICE

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

El presente trabajo contiene la información de cómo el conjunto de redes de computadoras interconectadas a lo largo de todo el mundo, contienen información muy valiosa, la cual se encuentra compartida para el acceso de todos los usuarios.

Pero para tener acceso a dicha información se necesita saber en donde se encuentra, para ello se consulta a un Servidor de Nombre de Dominio (DNS) que es una base de datos distribuida y delimitada que contiene la ubicación de un nombre de dominio que apunta a una IP homologa.

Es decir que para que exista una comunicación entre dos servidores es necesario que cada uno tengan su propia dirección IP y esta sea única e irrepetible, al principio esta conexión empezaron con 4 nodos, pero conforme al paso del tiempo se fue aumentando el número de nodos conectados y el número de direcciones IP por lo que resulto más complicado recordar dichas direcciones.

Esta consecuencia provocó que se creara un nuevo sistema llamado DNS (Sistema de Nombre de Dominio), con las características de un sistema jerárquico en niveles.

Pero por ser de consulta pública los servidores de nombre de dominio (DNS) no tienen la seguridad, esto ocasiona que entes ajenos a la información solicitada, generen vulnerabilidades las cuales desvíen la información que no corresponde a la IP, el no contar con las herramientas necesarias para la seguridad de los DNS traería como consecuencia el caos en la Internet, entre la suplantación de identidad, como denegación del propio servicio.

Este necesita de cierta seguridad para que al momento de realizar la consulta de un nombre o una IP sea la que realmente el usuario desea.

En la actualidad hablar de seguridad es de suma importancia, es por eso que con el uso de herramientas ayude a fortalecer un sistema, y por supuesto no podría faltara en un servidor de nombre de dominio que son los encargados de responder que zonas se encuentran a su cargo.

Cuando el usuario busca en específico una página con ayuda de algún explorador (Internet Explorer, Mozilla, etc.), éste se encarga de encontrar, lo que se solicita por medio del nombre de dominio, pero se puede encontrar con pérdida de información o suplantación de dicha información.

Con la siguiente investigación se pretende ver la funcionalidad de las **Extensiones de Seguridad en los Servidores de Nombre de Dominio (DNSSEC)** para los **Servidores de Nombre de Dominio (DNS)** de la Universidad Nacional Autónoma de México, por lo que se realizaran las pruebas correspondientes para comprobar la eficiencia de dicho protocolo.

DNSSEC brinda la seguridad mediante firmas digitalizadas para evitar la suplantación de identidad, es un protocolo que se está planeando implementar en los DNS de la Universidad Nacional Autónoma de México y estar a la vanguardia en este tipo de nueva tecnología que será de gran utilidad dada su importancia.

Reforzar la trasferencia de zonas de los DNS con la utilización de las llaves de encriptación proporcionando una mayor seguridad.
Garantizando los conjunto de subdominios que se encuentran bajo unam.mx revisando su autenticidad.

Asegurando al usuario que el dominio que están consultando se encuentra registrado en los DNS de RedUNAM y la IP se encuentra en el segmento otorgado por NIC-UNAM, reforzando la trasferencia de zonas de los DNS mediante llaves de encriptación y así evitar la suplantación de identidad y denegación de servicio.

En los antecedentes se verá todo lo referente al surgimiento y quiénes son los responsables del origen del medio de comunicación más importante de lo que hoy nos comunica con todo el mundo en poco tiempo, también del funcionamiento que realizan los Servidores de Nombre de Dominio para lograr dicha comunicación.

En el capítulo 1. Se describe todo lo referente a la ciencia, que se encarga de diseñar funciones o dispositivos capaces de generar el ocultamiento de información, que hoy en día se le conoce como criptografía, abarcando desde sus orígenes y también el estudio de los diferentes algoritmos existentes.

En el capítulo 2. Contiene todo lo referente a los problemas que contenían los Servidores de Nombre de Dominio, así como el surgimiento del grupo que su objetivo principal era proteger la información mediante el uso de firmas y éstas a su vez utiliza algoritmos vistos en el capítulo 1.

Capítulo 3. En este capítulo se habla del desarrollo de las extensiones que a lo largo de los años se han logrado implementar en los servidores de nombre de dominio logrando así una mayor seguridad a algunas vulnerabilidades anteriormente mencionadas en el capítulo 2 y revisar la implementación de RNDC, TESISG y DNSSEC.

ANTECEDENTES

HISTORIA DE INTERNET

Desde tiempos remotos el ser humano ha buscado la forma de comunicarse, no importando que tan lejos se encuentre la persona, utilizando algunos medios como: cartas, telégrafos, teléfono, tv, hasta llegar a lo que hoy conocemos como el principal medio de comunicación: la internet.

¿Pero dicho medio de comunicación cómo surgió?

La internet surge en la década de los 60 con la DARPA (*Agencia de Investigación de Proyectos Avanzados*), creada en respuesta de los desafíos tecnológicos y militares de Rusia, durante la guerra fría después renombrada ARPANET, con el propósito de tener una comunicación entre computadoras, idea original de ***Joseph Carl Robnett Licklider*** del Institute of Technology de Massachusetts, donde discute sobre su concepto de Galactic Network (Red Galáctica).

"Una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas".[1] Esto se puede visualizar en la figura 1.

[1] http://www.darpa.mil/Docs/Internet_Development_200807180909255.pdf consultada 18 de marzo 2010

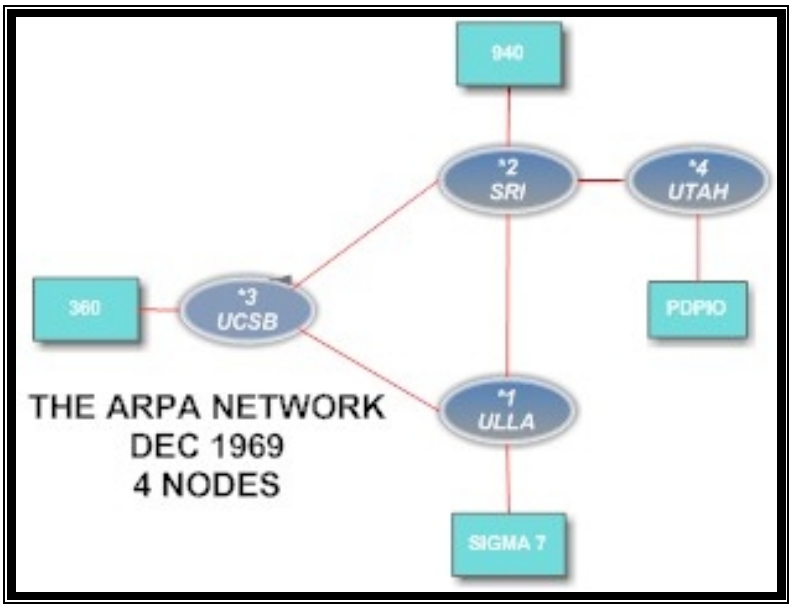


Figura 1. Esquema del primer nodo

Y fue ***Lawrence G. Roberts*** quien tras de la visión de Licklider aplica la teoría de conmutación de paquetes mediante una línea telefónica creando así, el primer nodo en la Universidad de California en los Ángeles y en el Instituto de Investigaciones de Stanford (SRI), uniéndose posteriormente la Universidad de California en Santa Barbara (UCSB) y la última en Universidad de UTHA.

Para poder establecer comunicación entre los cuatro nodos se utilizaba el Network Control Protocol (NCP) creado por ***Sthephen Crocker*** mediante las interrupciones de un grupo continuo de bits, el cual no incluía control alguno. En 1969 Crocker escribe el primer Requests for Comments (RFC[2]) dando origen a la consulta de Referencias aportaciones realizadas por diferentes personas, así como su funcionamiento.

El ingeniero ***Ray Tomlinson*** desarrollo el programa SNDMSG (acrónimo de message, enviar mensaje), así como el protocolo de transferencia CPYNE.

[2] RFC serie de documentos que sigue siendo la publicación principal para los estándares de Internet. http://www.ieee.org/portal/pages/about/awards/bios/2002internet.html

Para 1971 consiguió el intercambio de mensajes entre varios ordenadores utilizando el **‘**@’ para separar la parte del nombre del destinario del correo electrónico de receptor.

En 1971 ***Vinton Cerf*** y ***Robert E. Kahn*** publican “*A Protocol For Packet Network Interconnection*”, donde se sustituye al NCP ya que no contaba con el control de errores en el host, así como eliminar la existencia de la pérdida de información. Dando origen al "Transmisson-Control Protocol/Internet Protocol" (TCP/IP, protocolo de control de transmisión /protocolo de Internet).
La idea central del trabajo realizado por Cerf y Kahn era que cada red debería mantener por sí misma una comunicación y ésta debería de ser bajo la filosofía “best-effort” (lo menor posible) sin que ningún paquete se perdiera al llegar a su destino.

Posteriormente Cerf en 1989, conecta a internet el MCIL- Mail considerado el primer correo comercial de internet y en 1992 crea la ISOC, asociación no gubernamental sin fines de lucro, dedicada exclusivamente al desarrollo mundial de Internet, con la tarea específica de concentrar sus esfuerzos y acciones en asuntos particulares sobre la Red.

Tim Berners ocupando el protocolo TCP/IP y el hipertexto, desarrolló un método eficiente y rápido para el intercambio de datos entre la comunidad científica HTML (*Hiper Text Markup Language*, 1990), un lenguaje que permite realizar enlaces a otros documentos, dando origen a (World Wide Web, 1994) permitiendo mandar y recuperar información.

Gracias a su contribución pionera al desarrollo de la internet y de la World Wide Web, así como a la elaboración de dicha propuesta TCP/IP, aplicada actualmente son considerados los padres de internet Lawrence Roberts, Robert Kahn, ***Vinton*** Vint Cerf y Tim Berners-Lee.

Para tener comunicación con el exterior y poder tener acceso al mundo de internet, es necesario la interconexión de redes, la cual se realiza por medio de Gateway (conocido como puerta de enlace), que permite conectar las redes dependiendo de las arquitecturas y protocolos que cada una empleé.

Gracias a los sucesos anteriores y las herramientas implementadas a lo largo de estos años es que cada persona no importando idioma, ubicación, creencia, etc. Tiene acceso a diferentes partes del mundo mediante una conexión al internet.

INTRODUCCIÓN AL SERVIDOR DE NOMBRE DE DOMINIO (DNS)

La conexión entre equipos empezó con 4 nodos visto con anterioridad, cada uno de ellos contaba con una dirección numérica (IP´s), conforme al paso del tiempo creció de manera sorprendente. Por lo cual para comunicarse con diferentes equipos el usuario tendría que recordar la dirección de cada uno de ellos, conforme fue creciendo la red, era complicado que las personas recordaran muchas direcciones a la vez.

Por tal motivo el 23 de junio de 1983 en la University of Southern California School of Engineering´s Information Sciences Institute (ISI) **Jon Postel** diseña un identificador de computadoras con escalabilidad jerárquica, TLDs (Top Level Domains) .COM, .ORG y .NET., junto con Paul Mockapetris propone crear mediante una tabla, en un host una base de datos distribuida y dinámica, especificada en los RFCs 882 y 883.

Posteriormente **Paúl Vixie** desarrollo el BIND (Berkeley Internet Name Domain), implementado en un equipo que empleaba la arquitectura cliente/servidor.

BIND se ajustaba al modelo generado por postel y mockapetris, el cual se basaba en:

- **Cliente DNS**: Es el encargado de generar las consultas a los DNS, mediante el uso de buscadores.
- **Servidor de Nombres de Dominio**: son equipos encargados de dar respuesta a las consultas realizadas por clientes.
- **Zonas de Autoridad**: Son archivos cuya ubicación esta en el Servidor de Nombres de Dominio, donde se almacenan los datos y cambios realizados.

Los 3 elementos mencionados anteriormente dan origen al **DNS (Servidor de nombre de Domino)** que es una base de datos distribuida, jerárquica y descentralizada, una parte fundamental en el modelo actual de la internet. Es por esta razón que tiene un crecimiento, mediante los diferentes niveles, propuestos por Jon postel.

En cada DNS se alojan, los nombres de dominio los cuales son el conjunto de etiquetas secuenciales, separadas y finalizadas por el carácter punto (.), el último punto el cual muchas veces no se toma en cuenta por el usuario, corresponde a root o raíz, el cual es el inicio de la resolución de los mismos, la cual se realiza a partir de los root server.

Los root server son los encargados de almacenar los registros de TLDs (Top Level Domains) y ccTLDs (Country Code Top Level Domains), conocidas como zonas autoritativas, existen 13 servidores distintos alrededor del mundo los cuales se observan en la siguiente figura 2.

Letra de Identificación	Operador	Ubicación a nivel mundial	Direcciones IP
A	VeriSign, Inc.	**Sites: 6** **Global:** 6 **Local:** 0 **Los Angeles, CA, US; New York, NY, US *; Frankfurt, DE; Hong Kong, HK; Palo Alto, CA, US *; Ashburn, VA, US ***	**IPv4:**198.41.0.4 **IPv6:**2001:503:BA3E::2:30
B	Information Sciences Institute	**Sites: 1** **Global:** 0 **Local:** 1 Earth	**IPv4:** 192.228.79.201 y 192.228.79.201 **IPv6:** 2001:478:65::53 y 2001:478:65:: 53
C	Cogent Communications	**Sites:6** **Global**: 6 **Local:** 0 **Herndon, VA, US; Los Angeles, CA, US; New York, NY, US; Chicago, IL, US; Frankfurt, DE; Madrid, ES**	**IPv4:** 192.33.4.12
D	University of Maryland	**Sites: 1** **Global:** 1 **Local**: 0 **College Park, MD, US**	**IPv4**: 128.8.10.90
E	NASA Ames Research Center	**Sites: 1** **Global:** 1 **Local:** 0 **Mountain View, CA, US**	**IPv4:** 192.203.230.10

Letra de Identificación	Operador	Ubicación a nivel mundial	Direcciones IP
A	VeriSign, Inc.	**Sites: 6** **Global:** 6 **Local:** 0 **Los Angeles, CA, US; New York, NY, US *; Frankfurt, DE; Hong Kong, HK; Palo Alto, CA, US *; Ashburn, VA, US ***	**IPv4:**198.41.0.4 **IPv6:**2001:503:BA3E::2:30
B	Information Sciences Institute	**Sites: 1** **Global:** 0 **Local:** 1 Earth	**IPv4:** 192.228.79.201 y 192.228.79.201 **IPv6:** 2001:478:65::53 y 2001:478:65:: 53
C	Cogent Communications	**Sites:6** **Global**: 6 **Local:** 0 **Herndon, VA, US; Los Angeles, CA, US; New York, NY, US; Chicago, IL, US; Frankfurt, DE; Madrid, ES**	**IPv4:** 192.33.4.12
D	University of Maryland	**Sites: 1** **Global:** 1 **Local**: 0 **College Park, MD, US**	**IPv4**: 128.8.10.90
E	NASA Ames Research Center	**Sites: 1** **Global:** 1 **Local:** 0 **Mountain View, CA, US**	**IPv4:** 192.203.230.10

Letra de Identificación	Operador	Ubicación a nivel mundial	Direcciones IP
F	Internet Systems Consortium, Inc.	**Sites: 49** **Global:** 2 **Local:** 47 Ottawa, Canada *; **Palo Alto, CA, US ***; San Jose, CA, US; New York, NY, US *; **San Francisco, CA, US ***; Madrid, ES; Hong Kong, HK; Los Angeles, CA, US *; Rome, Italy; Auckland, NZ *; Sao Paulo, BR; Beijing, CN; Seoul, KR *; Moscow, RU *; Taipei, TW; Dubai, AE; Paris, FR *; Singapore, SG; Brisbane, AU *; Toronto, CA *; Monterrey, MX; Lisbon, PT *; Johannesburg, ZA; Tel Aviv, IL; Jakarta, ID; Munich, DE *; Osaka, JP *; Prague, CZ *; Amsterdam, NL *; Barcelona, ES *; Nairobi, KE; Chennai, IN; London, UK *; Santiago de Chile, CL; Dhaka, BD; Karachi, PK; Torino, IT; Chicago, IL, US *; Buenos Aires, AR; Caracas, VE; Oslo, NO *; Panama, PA; Quito, EC; Kuala Lumpur, Malaysia *; Suva, Fiji; Cairo, Egypt; Atlanta, GA, US; Podgorica, ME; St. Maarten, AN *	**IPv4:** 192.5.5.241 **IPv6:** 2001:500:2f::f
G	U.S. DOD Network Information Center	**Sites: 6** **Global:** 6 **Local:** 0 **Columbus, OH, US; San Antonio, TX, US; Honolulu, HI, US; Fussa, JP; Stuttgart-Vaihingen, DE; Naples, IT**	**IPv4:** 192.112.36.4
H	U.S. Army Research Lab	**Sites: 1** **Global:** 1 **Local:** 0 **Aberdeen Proving Ground, MD, US ***	**IPv4:** 128.63.2.53 **IPv6:**2001:500:1::803f:235

Letra de Identificación	Operador	Ubicación a nivel mundial	Direcciones IP
I	Autonomica	**Sites: 34** Stockholm, SE; Helsinki, FI; Milan, IT; London, UK; Geneva, CH; Amsterdam, NL; Oslo, NO; Bangkok, TH; Hong Kong, HK; Brussels, BE; Frankfurt, DE; Ankara, TR; Bucharest, RO; Chicago, IL, US; Washington, DC, US; Tokyo, JP; Kuala Lumpur, MY; Palo Alto, CA, US; Jakarta, ID; Wellington, NZ; Johannesburg, ZA; Perth, AU; San Francisco, CA, US; Singapore, SG; Miami, FL, US; Ashburn, VA, US; Mumbai, IN; Beijing, CN; Manila, PH; Doha, QA; Colombo, LK; Vienna, AT; Paris, FR; Taipei, TW	**IPv4:** 192.58.128.30 **IPv6:** 2001:503:C27::2:30
J	VeriSign, Inc.	**Sites: 70** **Global**: 63 **Local:** 5 **Dulles, VA, US (2 sites);** Dulles, VA, US (1 sites); **Ashburn, VA, US *; Miami, FL, US; Atlanta, GA, US;** Seattle, WA, US; Chicago, IL, US; **New York, NY, US *; Honolulu, HI, US; Mountain View, CA, US (1 sites);** Mountain View, CA, US (1 sites); **San Francisco, CA, US (2 sites) *; Dallas, TX, US; Amsterdam, NL; London, UK; Stockholm, SE (2 sites); Tokyo, JP; Seoul, KR;** Beijing, CN; **Singapore, SG; Dublin, IE; Kaunas, LT;** Nairobi, KE; **Montreal, CA; Perth, AU; Sydney, AU; Cairo, EG;** Cairo, **EG; Warsaw, PL (2 sites); Brasilia, BR; Sao Paulo, BR; Sofia, BG; Prague, CZ; Johannesburg, ZA; Toronto, CA; Buenos Aires, AR; Madrid, ES; Fribourg, CH; Hong Kong, HK (2 sites); Turin, IT; Mumbai, IN; Oslo, NO; Brussels, BE; Paris, FR (2 sites); Helsinki, FI; Frankfurt, DE; Riga, LV; Milan, IT; Rome, IT; Lisbon, PT; San Juan, PR; Edinburgh, UK; Tallin, EE; Taipei, TW; New York, NY, US *; Palo Alto, CA, US *; Anchorage, US; Moscow, RU; Manila, PH; Kuala Lumpur, MY; Luxembourg City, LU; Guam, US; Vancouver, CA; Wellington, NZ**	**IPv4:** 192.58.128.30 **IPv6:** 2001:503:C27::2:30

Letra de Identificación	Operador	Ubicación a nivel mundial	Direcciones IP
K	RIPE NCC	**Sites: 18** **Global:** 5 **Local:** 13 **London, UK ***; **Amsterdam, NL ***; **Frankfurt, DE;** Athens, GR *; Doha, QA; Milan, IT *; Reykjavik, IS *; Helsinki, FI *; Geneva, CH *; Poznan, PL; Budapest, HU *; Abu Dhabi, AE; **Tokyo, JP**; Brisbane, AU *; **Miami, FL, US ***; Delhi, IN; Novosibirsk, RU; Dar es Salaam, TZ	**IPv4:** 193.0.14.129 **IPv6:** 2001:7fd::1
L	ICANN	**Sites: 3** **Global:** 3 **Local:** 0 **Los Angeles, CA, US *; Miami, FL, US *; Prague, CZ ***	**IPv4:** 199.7.83.42 **IPv6:** 2001:500:3::42
M	WIDE Project	**Sites: 6** **Global:** 5 **Local:** 1 **Tokyo, JP (3 sites) ***; Seoul, KR; **Paris, FR ***; **San Francisco, CA, US ***	**IPv4:** 202.12.27.33 **IPv6:** 2001:dc3::35

Figura 2 Tabla de referencia a los Root Serves

CLASIFICACIÓN DNS

Los DNS se clasifican en:

- **Autoritativo:** Responden a consultas de las zonas asignadas que tienen configuradas en sus archivos.
- **No-Autoritativo:** No cuentan con la asignación de ninguna zona en particular dentro de sus archivos.
- **Primario:** Se encargan de realizar los cambios y modificaciones de archivos. Transfiriendo estos cambios a los servidores secundarios.
- **Secundario:** Dependen de un servidor primario, sirven de respaldo a los archivos configurados dentro del servidor primario**.**

- **Recursivo:** Responden a consultas del usuario, verificando en sus archivos configurados, si no encuentra la respuesta a la consulta, pregunta a otros servidores DNS.

- **No-Recursivo:** Responden consultas del usuario, solamente verificando sus archivos.

- **Cache:** Guarda por un tiempo determinado en memoria las consultas realizadas por distintos usuarios y su respectiva respuesta para el uso de consultas similares.

En la figura 3 se representa el esquema del funcionamiento de una consulta a los DNS utilizando como caso práctico www.ingeneria.unam.mx mediante los siguientes pasos:

1. El usuario hace la consulta de Nombre de Dominio.
2. La solicitud se proporciona al DNS del proveedor de servicio (ISP) para que este realice la consulta.
3. El servidor del ISP realiza la consulta de la petición a cualquiera de los 13 root server.
4. El root server busca en las zonas delegadas *.mx* registro asociado a NIC México.
5. Los servidores de NICMéxico realizan la búsqueda de la zona *.unam.mx* registro asociado a NICUNAM.
6. Los servidores de NICUNAM buscan en sus registros ingeneria.unam.mx
7. Revisan a que IP está apuntando el dominio, con la ubicación solicitada.
8. Mandando la respuesta del dominio al servidor DNS del ISP, la cual es proporcionada al usuario.
9. El usuario realiza la conexión con el servidor de la aplicación.
10. El servidor confirma la conexión con el usuario.

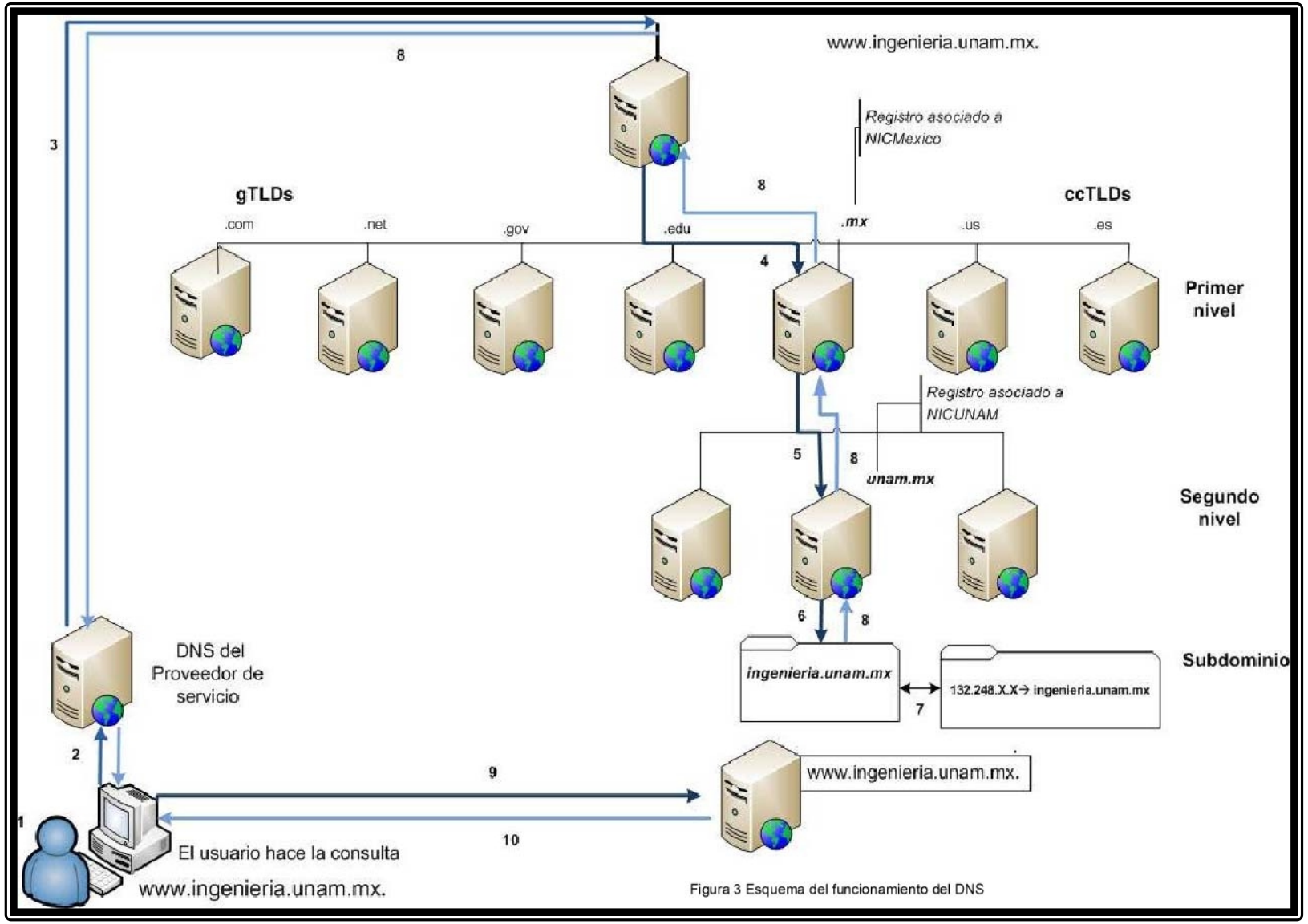


Figura 3 Esquema del funcionamiento del DNS

CAPÍTULO 1
CRIPTOGRAFÍA

1.1 CRIPTOGRAFÍA

Para dar un significado a lo que es la criptografía, debemos saber ¿Por qué y para qué fue creada?

Desde que el ser humano ha tenido la necesidad de comunicarse con una o más personas han buscado la forma de realizar dicha trasmisión de ideas, pensamientos, entre otros, dando origen a lo que hoy se le conoce como modelo de comunicación.

Pero para que exista un modelo de comunicación básico es necesario que el emisor (origen) proporcione un mensaje o texto, a trasmitir por un medio a un receptor (destinatario).como se muestra en la figura 1.1.

Figura 1.1. Modelo de comunicación básico

La comunicación ha sido necesaria desde sus orígenes por diversas razones, como son los fines bélicos. En donde no sólo se requería transmitir información, sino que además era necesario que esta información no fuese conocida por personas ajenas a ella.

Por lo que surgió la tarea de buscar métodos o técnicas para ocultar la información dando origen a lo que hoy se le conoce como criptografía. Proveniente del griego *Kryptós, criptos "ocultar"y graphe, grafos "escribir", lo que da origen a* escritura oculta.

Los primeros registros del uso de la criptografía datan del siglo V a.C. A partir de la escritura de la obra Mathematical Theory of Communication, escrito por C.E Shannon era considerado como **un arte** de escribir algún mensaje mediante el uso de claves secretas o un modo misterioso. A principios de la segunda guerra mundial se implementa la utilización de algoritmos matemáticos, de máquinas, programas, entre otros para el ocultamiento del mensaje, algunos de ellos usados aún en nuestros días considerando a la criptografía como **ciencia**.

Es decir la ciencia que se encarga de diseñar funciones o dispositivos capaces de generar el ocultamiento de información.

Por anteriores acontecimientos es por ello que se divide en:
Asesorar

- Criptografía Clásica.
- Criptografía moderna.

Como se puede visualizar en la figura 1.2

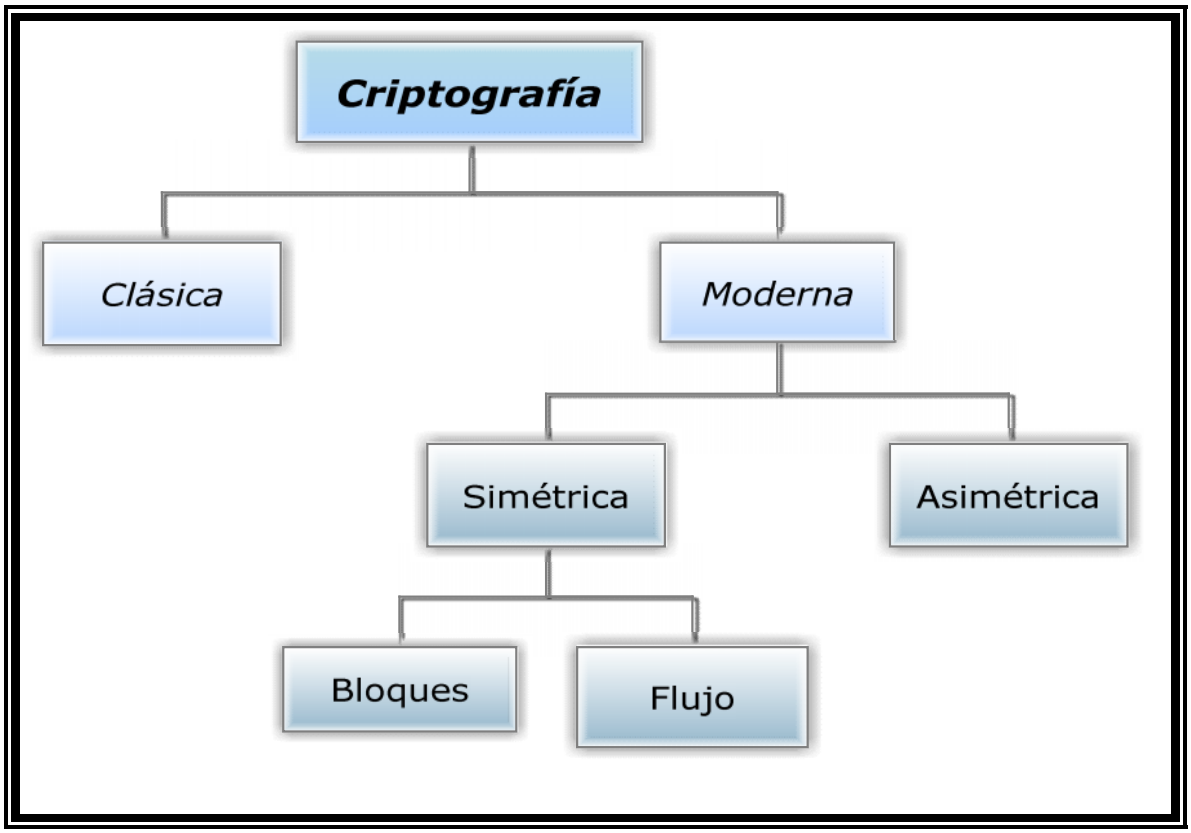


Figura 1.2. Clasificación de criptografía

1.2 CRIPTOGRAFÍA CLÁSICA

En la criptografía clásica se ocupaban diversos métodos para ocultar mensajes, que sólo podían leer o llegar a personas de mucho prestigio como reyes, jefes y monarcas. En muchos de los casos fue utilizada para la comunicación en las guerras. Es por ello que se le considero como el arte de ocultar el mensaje.

Existen diversos métodos utilizados con respecto al año o época dependiendo de los recursos disponibles (tecnológicos, humanos, etc.), para poder entender la criptografía clásica, se mencionaran algunos ejemplos sobresalientes utilizados a lo largo de la historia.

1.2.1 EVOLUCIÓN DE LOS MÉTODOS

En el siglo V a.C. durante la guerra entre Atenas y Esparta, los espartanos utilizaron la Scítala. Este método consistía en una vara o bastón, el cual era envuelto en un trozo de tela donde era escrito un texto alterado en el orden de las palabras, el cual servía para ocultar el significado del mensaje.

Para poder leerlo se necesitaba un bastón del mismo grosor y largo como se observa en la figura 1.3.

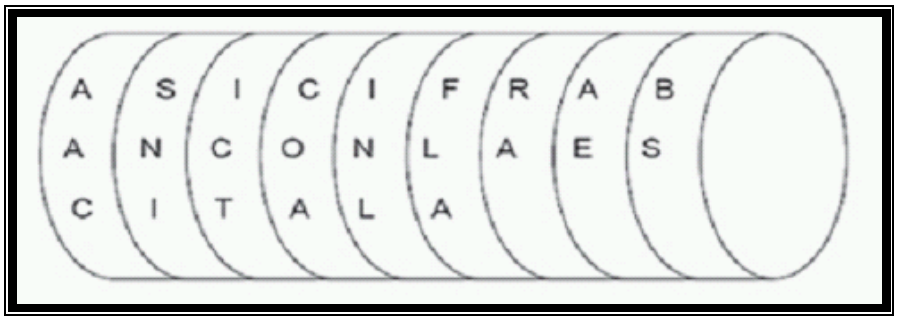


Figura 1.3. Scítala

En el sigo II a.C. Polybio, historiador griego miembro de la clase gobernante, invento un cuadro de 5x5 que permitía intercambiar símbolos, mediante el remplazo de coordenadas de dos ejes ocasionando el aumento del texto. Posteriormente se realizaron modificaciones en los símbolos, mediante la sustitución de dos letras o números, dicha sustitución se realizaba una por una, es decir dependiendo de las coordenadas de la ubicación del símbolo. Como se muestra en la figura 1.4

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N/Ñ	O	P
D	Q	R	S	T	Y
E	A	B	C	D	E

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N/Ñ	O	P
4	Q	R	S	T	Y
5	A	B	C	D	E

Figura 1.4. Cuadro de Polibybios

En el año 1466 Alberti escribe la obra “De Compendis Cifirs” dando origen al polialfabético, es decir el uso de varios alfabetos, mediante dos discos divididos en casillas designadas a cada carácter utilizado. Dicho método consiste en el movimiento de los discos, el cual consiste en una serie de saltos entre casillas, dependiendo del número asignado a cada salto era sustituido el carácter, Como se muestra en la figura 1.5.

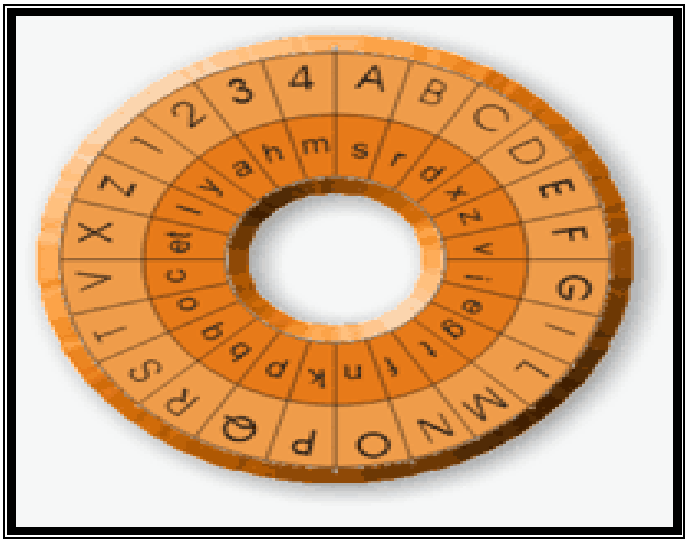


Figura 1.5. Disco de Alberti

A partir del Disco de Alberti surgen otros métodos que emplean el uso del mismo mecanismo base, uno de ellos es la rueda de Jefferson (1743). Esta máquina se conformaba por una serie de discos con letras impresas, que giraban libremente alrededor de un mismo eje, como se observa en la figura 1.6.

Figura 1.6 Rueda de Jefferson

En la primera y segunda guerra mundial (siglo XX) la criptografía juega un papel importante al hacer necesaria la utilización y desarrollo de técnicas como las máquinas de cifrado, empleadas en los sistemas de comunicación para la trasmisión de mensajes secretos.

En la primera guerra mundial se emplean los avances tecnológicos como estrategias de comunicación y armamento. Ejemplo: el espionaje de Margaret Geetruida Zelle, conocida como Mata Hari, quien empezó como espía de los alemanes para obtener información mediante la técnica de ingeniería social y posteriormente trabajando como agente doble proporcionando información a los franceses.

En 1919 se registra la primera patente de máquina de cifrado mecánica y electromecánica llamada *Enigma* creada por el holandés Alexander Koch y el alemán Arthur *Scherbius, de la cual se* obtienen diferentes versiones. Su objetivo principal era facilitar la comunicación a través de la transmisión de

documentos entre comerciantes y hombres de negocios de una manera privada.

Dicha máquina se componía de una serie de rotores que contenían el alfabeto, su funcionamiento se basaba en sustituir cada letra, al ir girando cada rotor se podía generar un gran número de alfabetos diferentes dando un total de 614,656 combinaciones. Haciendo de enigma una pieza importante para esa época, debido a que era casi imposible la obtención del mensaje sin la utilización de la misma.

Los métodos anteriormente descritos mostraban diversas vulnerabilidades. Un ejemplo de ello se presenta en la sustitución de alfabetos, al aplicar un análisis de secuencia dentro de la sustitución de caracteres, lo cual permite descifrar el mensaje oculto.

Debido lo anterior, se sustituyen los métodos manuales dando pie al uso de máquinas y la utilización de procedimientos matemáticos poniendo fin a la criptografía clásica, iniciando así una nueva era en la criptografía. Como se observa en la figura 1.7.

Figura 1.7. Enigma

1.3 CRIPTOGRAFÍA MODERNA

En 1948 Bell System Technical Journal publica el artículo llamado ***Una teoría matemática de la comunicación*** escrita por Clude Shannon y las aportaciones de Warren Weaver, se demuestra que toda fuente de información se puede medir y que los canales de comunicación tienen una unidad de medida similar, apoyado en la teoría de muestreo de Nysquit (la cual indica que se produce una pérdida de información llamada distorsión, error o ruido de cuantificación y que existe un límite para su transmisión), es decir que toda información se trasmite sobre un canal si la magnitud de la fuente no excede con la capacidad de trasmisión del canal que la conduce, sentando las bases para corrección de errores, suspensión de ruido y redundancia.

En 1949 se publicó la Teoría de las comunicaciones secretas escrito por Shannon, en donde la criptografía se apoya de otras ciencias como la estadística, la teoría de la información, la física, las matemáticas, etc.

Con los dos anteriores escritos surge la teoría de la información, que emplea el siguiente modelo de comunicación de una forma desarrollada, mostrado en la siguiente imagen 1.8.

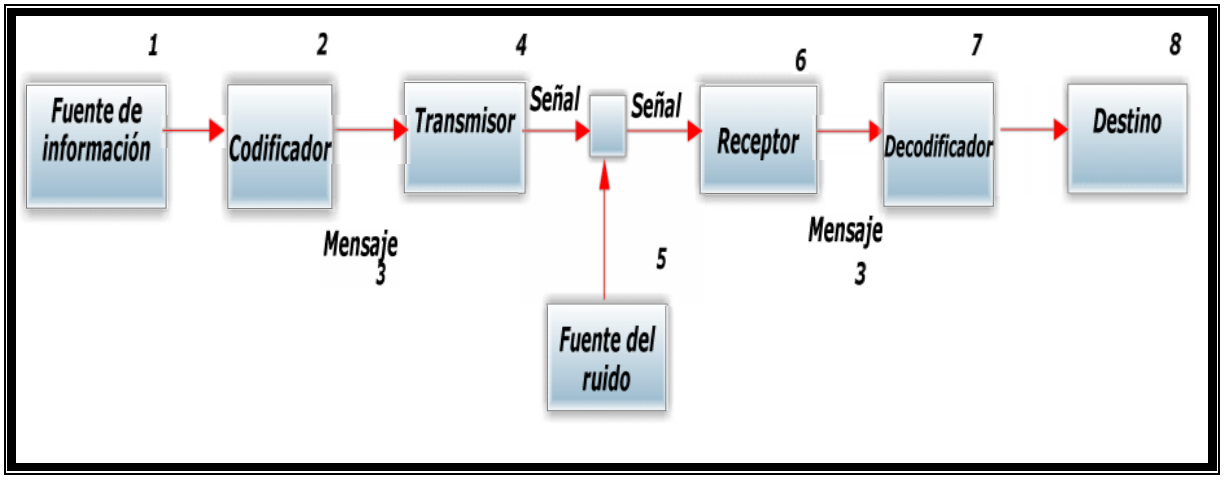


Figura 1.8. Modelo de comunicación de Shannon.

La figura anterior muestra cómo se lleva a cabo el proceso de la comunicación en donde la fuente de información genera el mensaje a trasmitir, posteriormente se aplica una codificación, es decir se trasforma el mensaje, para poder ser mandado como señal sobre un canal, en el transcurso el mensaje o señal se puede ver afectada por el ruido, el cual provocara pérdida o alteración para poder llegar al receptor. Una vez que se reciba la señal por el receptor y sea decodificado, es decir a su forma original, se manda el destino que es el punto final del proceso de comunicación.

Lo importante en este modelo es que la señal se descodifique en el transmisor de forma adecuada para que el mensaje codificado por el emisor sea el mismo que es recibido por el destino.

Con el apoyo de los dos artículos anteriores la criptografía deja de ser considerada como un arte y empieza a ser considerada como una ciencia, por lo que la criptología, se divide en criptografía que son los métodos y algoritmos que se han estado estudiando en los cuales se profundizara más adelante, y el criptoanálisis que estudia los métodos para obtener los mecanismos de cifrado para la obtención del mensaje.

Como se puede observar la criptografía toma un papel importante en la actualidad para el intercambio de información, mediante el medio de comunicación. Un ejemplo de lo anterior es la internet medio más utilizado en la actualidad, que debe proporcionar seguridad para que el medio de comunicación no tenga los siguientes problemas:

- Intercepción de los datos por un ente externo que busca obtener la información antes de que llegue a su destino y después dejar que siga su curso sin alterarla provocando el problema de **confidencialidad**.
- Falsificación: se produce cuando un ente externo obtiene el mensaje, se adueña de él y de la identidad del emisor, generando un nuevo mensaje

que manda al receptor provocando un problema de **integridad y confidencialidad**.

La criptografía moderna se dividida en dos grandes vertientes: criptografía simétrica y asimétrica.

Cabe mencionar que para fines de esta investigación se profundizara en la criptografía asimétrica.

1.4. CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE SECRETA

Los algoritmos simétricos son aquellos que utilizan ***una sola clave*** de cifrado y de descifrado, por lo que se tiene que proteger su difusión, ya que es sólo para el emisor/receptor autorizado.

Ejemplo

El usuario verónica antes de mandar la información utiliza un algoritmo con una llave para poder trasformar la información y así poder mandarla por la Internet, esta es recibida por el usuario minerva que utiliza la misma clave con la que se encripto para poder obtener la información, como se muestra en la siguiente imagen 1.9.

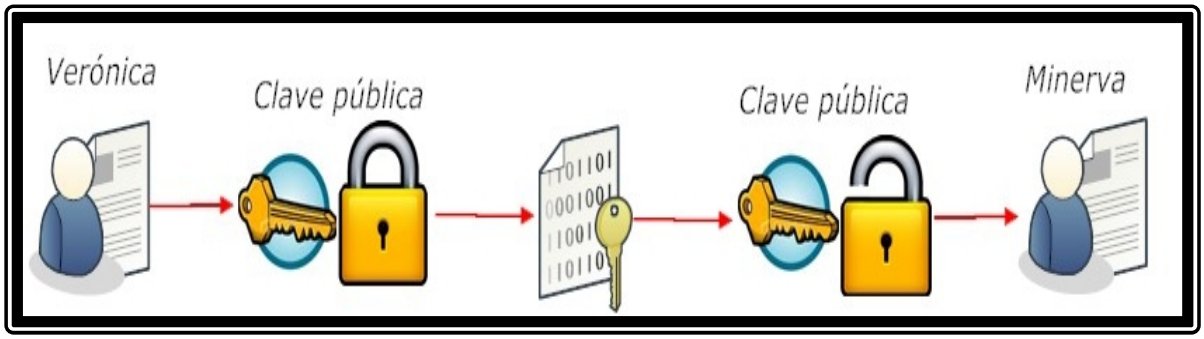


Figura 1.9 Criptografía simétrica

Es por ello que se le conoce como secreto compartido, existen dos tipos de algoritmos para poder encriptar y desencriptar por bloques y flujo.

1.4.1 ALGORITMO SIMÉTRICO EN BLOQUE

Es cuando el algoritmo divide el mensaje a cifrar en bloques de tamaño constante y cifra uno a uno los bloque con su clave del mismo tamaño, dependiendo del algoritmo utilizado, de tal forma que se va cifrando bloque por bloque como se puede observar ene la figura 1.10.

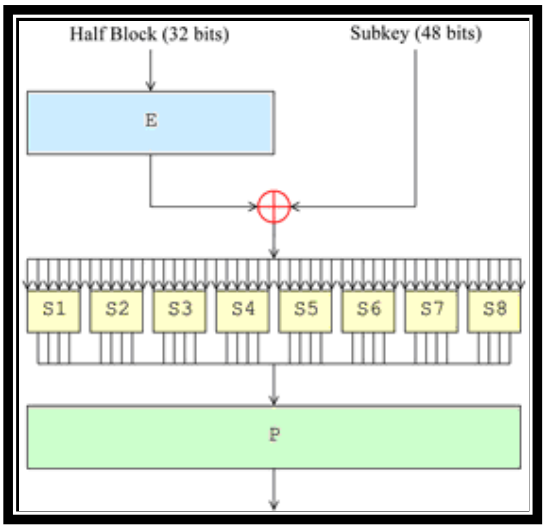


Figura 1.10. Esquema de Función de Feiste

Este algoritmo depende de los siguientes elementos:

- Transformación lineal: dependen de una o dos funciones que pueden o no depender de la clave.
- Transformación intermedia: son las iteraciones o las N veces de repeticiones para la trasformación aplicando la función y el uso de la clave.
- Transformación final: garantiza que las operaciones de cifrado y descifrado sean asimétrica es decir la operación inversa de la inicial.
- Algoritmo de expansión de clave: es la conversión de la clave del usuario en subclaves.

A continuación nombrare algunos algoritmos que fueron creados bajo un esquema simétrico en bloques

El algoritmo **Data Encryption Standard (DES)** creado en los 70’ por IBM, utiliza el esquema feister (los bloques de datos se dividen en dos partes iguales y en cada iteración trabaja de manera alternada cada una de las partes), es decir en bloques de 64 bits, su clave inicial es de 64 bits y después se genera por cada iteración una de 56 bits, en total trabaja con 16 iteraciones, implementando una permutación inicial y una final.

El Algoritmo Internacional de Cifrado de Datos **(IDEA)** fue creado por Xuejia Lai y James L. Massey y publicado en 1991, es un sistema de cifrado de bloque creado como remplazo del algoritmo DES ya que mediante fuerza bruta pudieron descifrarlo, originalmente se llamaba IPES. Se implementa mediante la utilización de claves de 128 bits las cuales se dividen en 8 bloques de 16 bits cada una, las primeras 6 claves son utilizadas en la primera ronda del cifrado y las otras dos en la segunda iteración y operación de bloques de 64 bits (Datos) y 8 ciclos.

En 1993 fue creado el **algorimo Blowfish** por Bruce Schneier, que cifra datos en bloques de 64 bits divididos en un mismo tamaño, su clave puede ser variable y puede ser hasta de 448 bits (en cada ciclo ocupa diferente subclave), es decir genera 18 iteraciones para poder obtener el mensaje encriptado.

El algoritmo **RC5** se dio a conocer en 1995 por Rivers Clipher que son las iniciales que tiene como nombre, el 5 representa la secuencia de algoritmos de cifrado simétrico, a este tipo de algoritmo se le puede especificar el tamaño de la palabra 16, 32 o 64 bits, es decir, si es diferente el tamaño de la palabra se puede producir diferentes bloques para cifrar en bloques de 32, 64 o 128 bits. El número de iteraciones a realizar van desde 1 hasta 255 dependiendo del tamaño del bloque (palabra y clave).

El National Institute of Standards and Tecnology (NIST) en 1999 da a conocer el algoritmo **3DES o TDES**, donde se modifica el problema de la utilización de clave por una más corta y consiste en aplicar 3 veces el algoritmo DES dos de cifrado y uno de descifrado utilizando 2 o 3 claves diferentes para generar las subclave.

1.4.2 ALGORITMO SIMÉTRICO EN FLUJO

Se requiere de un generador de llaves o fuente, la clave tiene que ser tan grande como el mensaje a cifrar, el inconveniente con este algoritmo es que será difícil recordar para el usuario. Donde mencionas la figura 1.11.

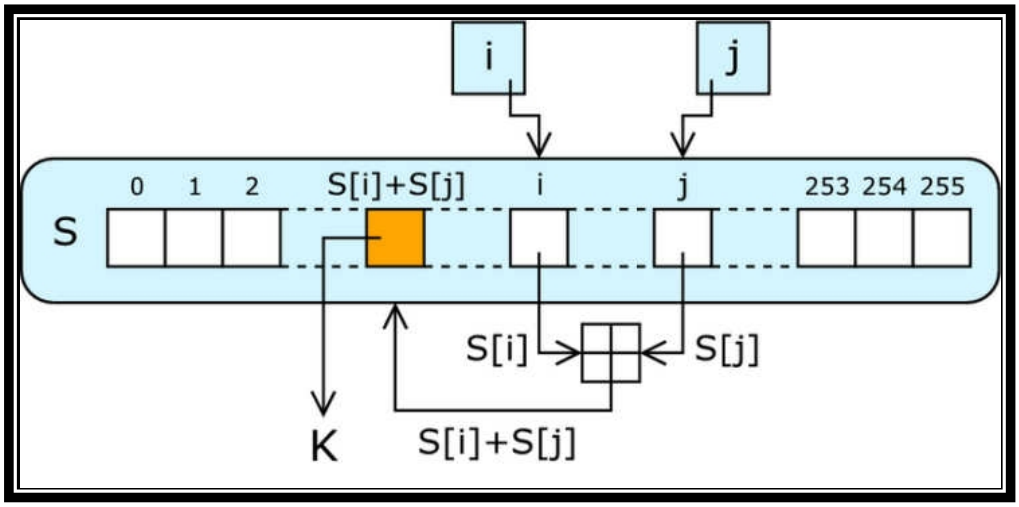


Figura 1.11. Esquema de generador de llave

Dentro de la criptografía simétrica en bloque podemos encontrar el siguiente algoritmo:

En 2001 tras un concurso por la National Institute of Standards and Tecnology (NIST) se da a conocer el nuevo Algorimo Advanced Encryption Standard (AES) que soporta un mensaje mínimo de 128 bits, las claves pueden ser de diferentes longitudes, así como las iteraciones pueden ser de 10 a 14.

1.5 CRIPTOGRAFÍA ASIMÉTRICA O DE CLAVE PÚBLICA

En 1976 la publicación de New Directions in Cryptography desarrollado por Whitfiel Diffie y Martin Hellman (Diffice-Herma), demuestra la distribución de la claves de cifrado para poder ser utilizado en los diferentes sistemas resolviendo el problema de distribución de claves.

Es un algoritmo en donde dos entidades se ponen de acuerdo en un número, a través de un medio de transmisión público, de tal forma que no pueda ser conocido por alguna otra persona, es decir que se permite el intercambio de claves a través de canales inseguros, mediante el uso de un par de claves relacionadas matemáticamente entre sí para cifrar y descifrar, se basa en funciones de un solo sentido, estas claves se generan como privada y pública, no necesitando un canal seguro para el intercambio, el cual permitirá su visibilidad de la clave por un tiempo sin poner en riesgo la información por lo cual se obtendrá como se observa en la figura 1.12.

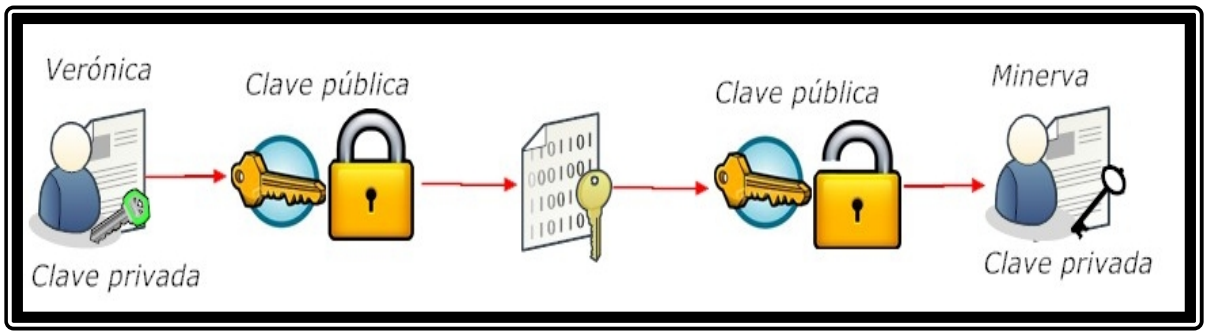


Figura 1.12 Criptografía asimétrica

Las siguientes formulas describen el procedimiento que se realiza en cualquiera de los algoritmos (f) y la utilización de un mensaje plano o claro (Mcla) así como de una clave (K) para poder obtener el criptograma y viceversa como se puede observar en la figura 1.13.

Cripto $= f(\text{Mcla}, K_{ca})$

$\text{Mcla} = g(\text{Cripto}, K_{da})$

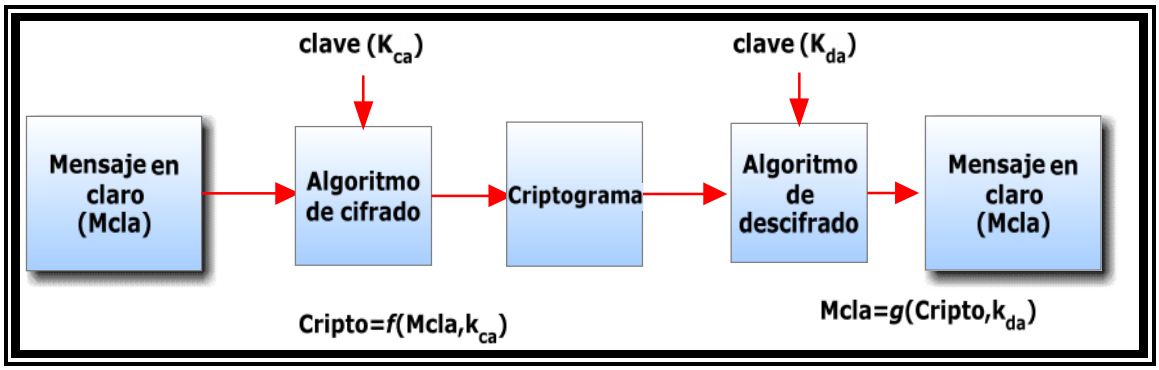


Figura 1.13 Procedimiento para generar un criptograma

Dentro de los algoritmos de criptografía asimétrica se tiene que:

En 1985 Taher Elgamal da a conocer su algoritmo **El gamal,** es un algoritmo basado en Diffie –Hellman, en un principio fue ideado para producir firmas digitales, aunque después se extendió su uso para utilizarlo en el cifrado de mensajes, es utilizado en GNU (Privacy Guard) versiones recientes de PGP, entre otros.

Para generar un par de llaves, se escoge un número primo p y dos números aleatorios α y *a* menores que *p*. Se calcula entonces la expresión:

$$y = \alpha^a \pmod p$$

Los valores p, α y β son públicos, y *a* es privado.

En 1997 se desarrollo el algoritmo **RSA** creado por Ron **R**ivest, Adi **S**hamiry Leonard **A**dleman considerado un esquema robusto, por la factorización de números muy grandes, porque para la obtención de clave pública es mediante la multiplicación de dos números primos ***p*** y ***q***, para poder calcular ***n*** que es la multiplicación de ***p*** y ***q,*** y este será de carácter público es por ello que la dificultad radica en la factorización de números grandes. Para después poder

obtener las claves para emplear este algoritmo como ejemplo se tiene la siguiente figura1.14.

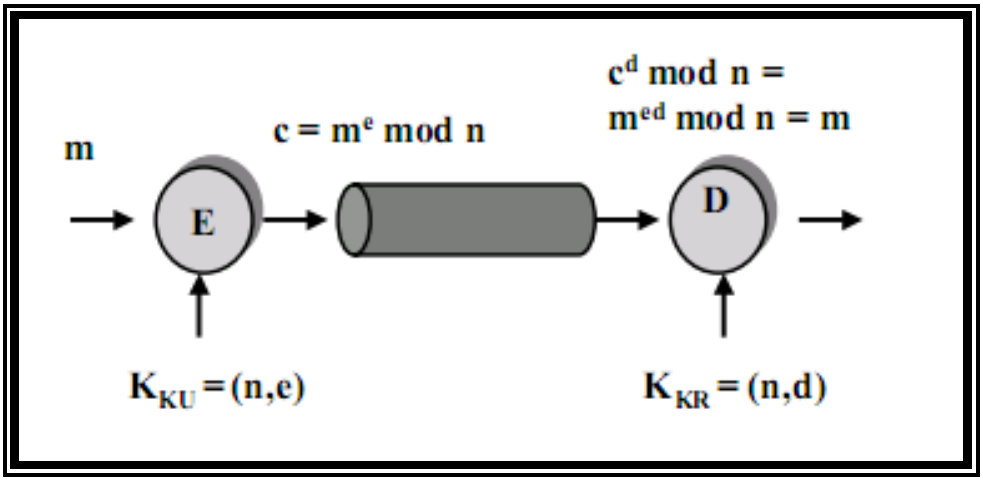


Figura 1.14. Esquema del algoritmo RSA

En 1997 **National Institute of Standards and Tecnology (NIST)** da a conocer el algoritmo de firmas digital **(Digital Signature Algorithm DSA)** y que fue para uso del estándar de firma digial o Digital Signature Standard **(DSS)** especificado en el FIPS 186, una firma digital (FD) permite identificar la autenticidad del mensaje, es decir que la información aceptada sea efectivamente enviada por quien dice ser el emisor, sin haber sufrido alguna modificación. Existen diferentes tipos de FD:

- Implícitas: que las contiene en el mismo mensaje.
- Explicitas: se añaden como una marca en el mensaje.
- Privadas ó verdadera: el remitente sólo puede verificar al usuario.
- Revocables: el remitente puede denegar su pertenencia.
- Irrevocables: el receptor prueba su origen.

Para obtener la firma es necesario tener un resumen de la información y es por ello que se utiliza las funciones hash, que son aquellas que toman como entrada una cadena de longitud variable para después con el uso de funciones

matemáticas comprimir el documento hasta generar una cadena o bloque de longitud fija llamada hash, así resolviendo el problema de integridad y autenticidad del mensaje

Existen diferentes funciones hash como son:

MD2 (128 bits)

MD4 (128 bits)

MD5(512 bits)

SHA-1 (160 bits)

SHA-256 (256 bits)

SHA-512 (512 bits)

Para realización del proyecto serán utilizados MD5 y SHA, cabe mencionar que la utilización de estas funciones en cuanto más grande sea su longitud en bites se tardara más tiempo en realizar la consulta y responder es por ello que es necesario revisar las características de servidores con los que se cuentan.

MD5 Message Digest Algorithm desarrollado en 1992 por Ron River mejorando la robustes de MD4, y se encuentra documentado en el RFC 1321, procesa mensajes de cualquier longitud, procesando uniformemente bloques de 512 bits, añadiendo bits si es necesario al final.

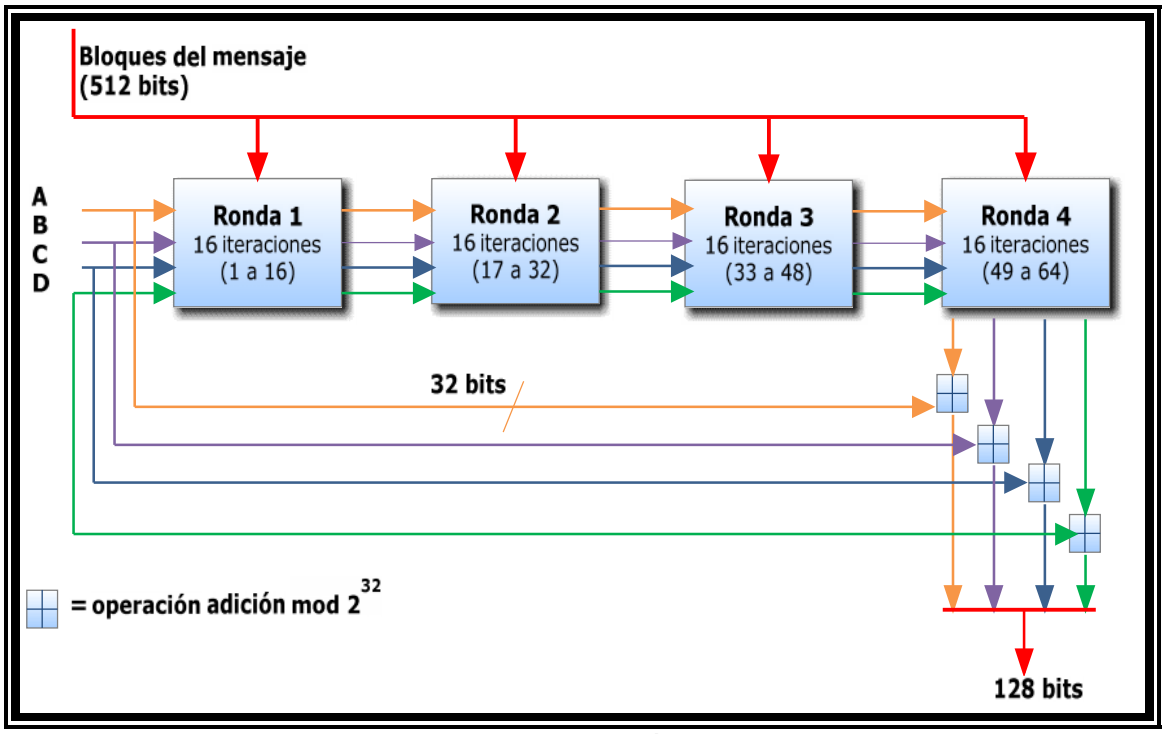


Figura 1.15. Función MD5

En la figura 1.15 se muestra como es el funcionamiento del algoritmo MD5, el cual está formado por 4 rondas cada una de 16 iteraciones en donde mediante sumas OR va generando el resumen, para después hacer una concatenación y obtener una longitud fija de 128 bits.

SHA Algoritmo Hash seguro desarrollado en 1993 y dado a conocer por FIPS 180, fue desarrollado para apoyar al estándar de firma digital DSS y se baso en el MD4, este algoritmo procesa mensajes de cualquier tamaño hasta 2^{64} bits operando en bloques de 512 bits a la vez, generando resúmenes de 160 bits.
SHA-l es la versión actualizada y especificada en el RFC 3174 consta de 5 pasos:

1. Proceso de relleno, es el agregar los bits que sean necesarios de manera que la longitud del mensaje sea long ≡ 448 mod 512 en dado caso que se requiera.

2. El mensaje original debe tener una longitud de 64 bits antes de aplicar el relleno.
3. Se inicia el registro de llamadas MD de 160 bits que permite almacenar y mantener los resultados. Este registro maneja secciones de 32 bits que son inicializadas con valores hexadecimales.
4. El mensaje se procesa a través de 16 bloques de 32 bits cada uno, por lo que se realiza 4 rondas de veinte pasos cada una dando un total de 80 iteraciones.
5. Se obtiene la concatenación que produce un bloque de 160 bits.

Como se puede observar ene la figura 1.16 el funcionamiento de SHA-l

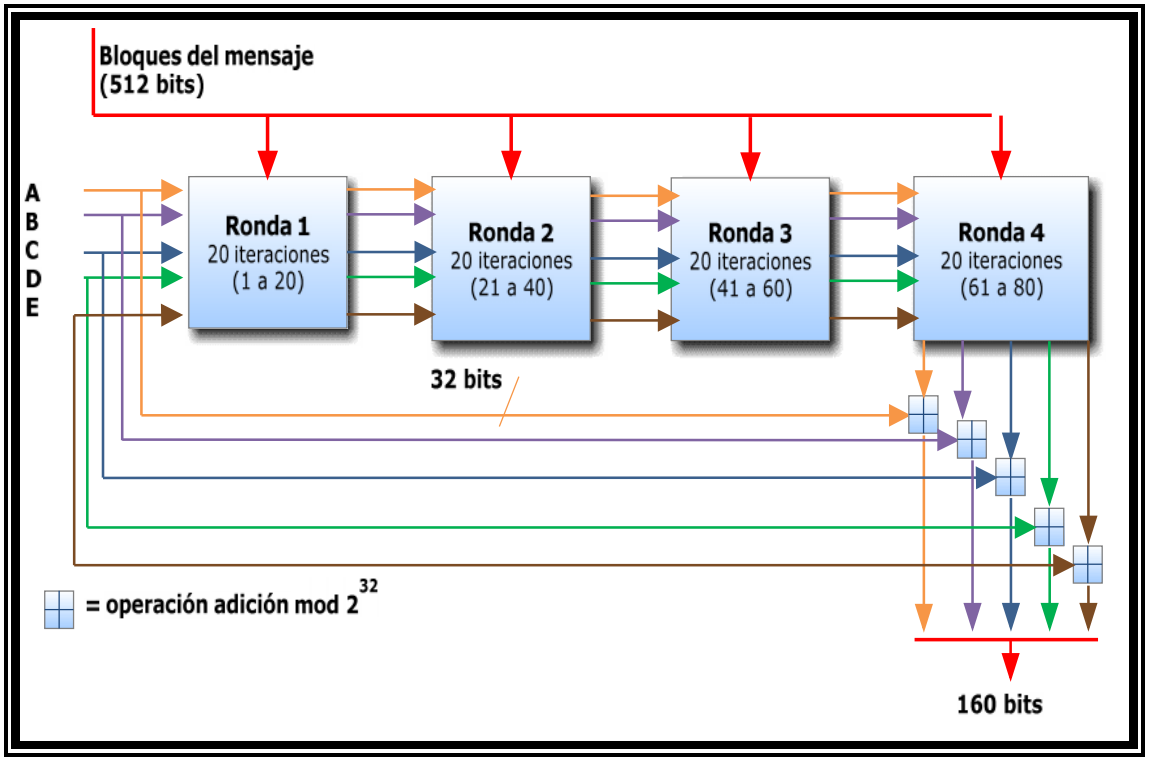


Figura 1.16. Función SHA-1

Como nota adicional se señala que el procedimiento para las otras variantes de las funciones SHA, siguen el mismo procedimiento.

CAPÍTULO 2

DNSSEC

2.1 DNSSEC

El proyecto de DNSSEC surgió en 1993 con los organismos de regularización y normalización, que se encargan de aprobar y regular las nomas y estándares elaborados para la comunidad del internet, como principal objetivo la mejora y ampliación de la existente estructura.

Esto se lleva a cabo mediante las solicitudes que son sujetas a procesos de análisis y revisión, por algunos grupos especializados en temas propuestos, para posteriormente con toda la comunidad de internet para así llegar a un conceso con las partes involucradas y así generar la aprobación y difusión de nuevas normas y estándares.

2.2 ORGANISMOS DE REGULACIÓN

2.2.1 ISOC

La Sociedad de Internet (ISOC), es un organismo sin fines de lucro fundada en 1992 dedicada a asegurar el desarrollo, evolución, cooperación y coordinación del internet a nivel mundial de protocolos, estándares y temas asociados a internet que actualmente cuenta con 100 organizaciones y más de 28,000 miembros individuales y para brindar un mejor servicio creo 5 oficinas alrededor del mundo como son:

- Oficina Africana
- Oficina de Asia
- Oficina de Europa
- América latina y Buros del Caribe
- Norte América Bureau

Su financiamiento es por los miembros, a través de organizaciones e individuos, donaciones e inscripciones a talleres, cursos y eventos se encuentra representada por el siguiente logo en la figura 2.1.

Figura 2.1 Logotipo de la ISOC

La ISOC cuenta con el premio “Jonathan Bruce Postel” premio que es entregado anual a un individuo o una organización que destaca y se dedica, al impulso de nuevas mejoras del esquema del internet.

“*Jonathan B. Postel Service Award* fue creado por la Sociedad de Internet para honrar a una persona que haya realizado contribuciones sobresalientes en el servicio a la comunidad en comunicaciones de datos. El premio se centra en las contribuciones técnicas continuas e importantes, el servicio a la comunidad, y liderazgo.”[3]

Dentro de esta asociación se encuentra un grupo dedicado a la administración de los procesos de Internet. Para cumplir sus objetivos, este grupo toma como base reglas y procedimientos anteriormente ratificados por un Consejo Administrativo. Su principal importancia, radica en el proceso establecido para la generación de nuevos estándares y protocolos de Internet, el cual va desde la documentación, publicación y difusión de especificaciones, hasta la aprobación final, por parte del Consejo.

La sociedad de Internet, cuenta con diversas organizaciones encargadas de la administración, investigación y desarrollo de algunos temas de Internet, entre las más importantes destacan las siguientes:

[3]Tomado y traducido de http://www.isoc.org/awards/postel/

- Internet Assigned Numbers Authority (IANA)
- Internet Architecture Board (IAB) que proporciona supervisión arquitectónica
- Internet Engineering Steering Group (IESG) se encarga de anunciar las mejora del internet

2.2.2 IETF

En 1986 surge la *The Internet Engineering Task Force (IETF Fuerza de Tarea de Ingenieros de Internet)*, es la comunidad internacional abierta a cualquier persona interesada, en participar en la evolución y mejora operacional de Internet, es la principal organización de la ISOC.

La IETF está organizada en diferentes grupos de trabajo encargados de un tema específico dentro de las distintas áreas de Internet. Estos grupos cuentan con un Director de Área (ADs) responsable de la dirección, administración y avance técnico, dentro del grupo de trabajo. Cada uno de estos directores es miembro activo de la Inty rnet Enginnering Steering Group (IESG), grupo responsable de la dirección técnica de las actividades y de los procesos de estandarización dentro de la IETF su logotipo es el siguiente como se muestra en la figura 2.2.

Figura 2.2 Logotipo de IETF

La IEFT se reúne tres veces al año, en las cuales se analizan las actividades y procesos de estandarización de Internet. A pesar de que este organismo tiene objetivos establecidos, una parte de su definición está basada en RFCs, ya que se encuentran en constante actualización, revisión y consulta por parte de los participantes de todo el mundo.

Dados sus objetivos y el grupo de personas que lo conforman, existen diversos mecanismos de contribución y aportación por parte de sus miembros, dentro de estas contribuciones se encuentran las participaciones orales y escritas por parte de los asistentes a los eventos y sesiones de este grupo de trabajo, además de las aportaciones realizadas en el proceso de estandarización.

2.3 ORÍGENES DE DNSSEC

En una de las publicaciones de IEFT en agosto del 2006 volumen 2 pública James M. Galvin donde describe las diferentes evoluciones que ha tenido la seguridad DNS a partir de 1999, ya que el internet va cambiando constantemente ocasionando que la seguridad no se concluirá por dicha evolución así como los requisitos.

El 30 de noviembre de 1993 identificaron las amenazas, a los servicios de seguridad así como los requisitos de interés para los DNS, dando origen al grupo de trabajo encargado de la seguridad designado por la IETF, así como evaluaría todas las propuestas con el objetivo de crear una sola propuesta.

Este grupo fue constituido hasta marzo del 2004 con la Descripción de Seguridad en el Servidor de Nombre de Dominio (DNSSEC), este se encargaría de especificar las mejoras en el protocolo DNS para evitar las posibles modificaciones no autorizadas, en la base de datos que cada servidor contiene y así la autenticación del mismo.

Así como el mecanismo que se agregaría del protocolo mediante una firma digital. Este servicio se añadiría de tal manera que los registros de recursos (RRs) del DNS serian firmados, distribuidos y verificados dando la confianza en la exactitud de datos recibidos. Esto dio dos cuestiones de estudio y revisión.

1. Los registros deben ser firmados por el DNS primario o secundario para lograr la distribución de los registros de recursos.
2. El mecanismo para identificar y verificar las claves públicas para la firma digital.

Dando origen a los supuestos como es la compatibilidad y convivencia con los servidores DNS y los clientes que no son compatibles con el servicio y los datos que se consideran de información pública, así proporcionando a la discusión de cómo realizar confidencialidad a los datos y control de acceso.

Las especificaciones se tenían claras, limitadas y estimando que se realizaría la implementación en un año (estimación que se les fue de control), debido a la falta de documentación de las discusiones que llevo a la elección de servicio de la seguridad para crear la primera obra llamada Domain Name System Security Extensions (DNSSEC) escrito por Donald Eastlake y Charlie Kaufman que se publicó en el RFC 2067 en Enero de 1997, a tres años de la creación del grupo de trabajo.

El no documentar retrasó por varios años, ya que causaba conflictos, puesto que no se entendía por qué se realizaba dicha aplicación de DNSSEC qué funcionalidad tenia y esto dio origen años después a un análisis de las amenazas más frecuentes, esto proporcionaba el estudio de todos los servidores de nombre de dominio con qué riesgos y lo que se necesitaba para realizar, este documento posiblemente habría servido como base importante para la revisión de futuras aplicaciones y para entender como implementar lo que en primera instancia se tenía.

Este documento fue publicado en agosto del 2004 llamado Análisis de Amenazas del Domain Name System (DNS) escrito a nombre de Derek Atkins y Rob Austein en el RFC 3833., en base a lo anterior las extensiones DNSSEC parecen resolver un conjunto de problemas que es necesario resolver.

Tomando en cuenta que el objetivo principal de DNS es:
"Los nombres de dominio a direcciones IP facilita la comunicación entre dos sitios. Si la información no está disponible o es inaccesible, los sitios no serán capaces de comunicarse"[4].

Aunque los datos en el DNS deben ser disponibles para ser de utilidad, el protocolo limita la rapidez de búsqueda a un dominio inherente que cualquier cliente pueda acceder a todos los datos de una zona, la seguridad añade una funcionalidad, si un cliente consulta un dominio inexistente, la respuesta sería correcta y el servidor asegurara que la firma del dominio no existe pero, además de indicar que la siguiente etiqueta del dominio es válido en la zona. A través de consultas repetidas, un cliente puede conocer y descargar todo el contenido de una zona.

Las extensiones de seguridad DNS en actualización dinámica llamo la atención de la comunidad de DNS. Esto se especifica en el RFC2065 que incluía una cobertura limitada de los problemas de actualización dinámica, pero en última actualización se especifica en el RFC 2137 de nombre Secure Domain Name System escrita por Donald Eastlake que se publicó en abril de 1997, de acuerdo a la aplicación y la experiencia operacional de los desarrolladores y los primeros usuarios. RFC2535 - Domain Name System Security Extensions escrito por Donald Eastlake se publicó en marzo de 1999.

[4] Tomado y traducido de http://isoc.org/wp/ietfjournal/?p=97#more-97

En mayo del 2000 fue publicado TSIG como el RFC 2845 que es la autentificación en la transacción de nivel mediante el uso de secreto compartido mediante la firma.

Los operadores de dominio sueco y holandés de nivel superior, NLnet Labs y RIPE NCC. Descubrieron problemas de funcionamiento con los intercambios de claves entre primarios y secundarios. Esta fue una de las principales cuestiones que dieron lugar a una reescritura importante que se convirtió en tres especificaciones en los RFC4033, RFC4034 y RFC4035 - publicado en marzo de 2005, aunque esta vez ya tenía un grupo de trabajo comprometido a resolver el problema de privacidad.

2.4 AMENAZAS DEL DNS

Las amenazas es todo aquello que intenta o pretende destruir algún sistema, explotando los fallos de seguridad que se denominan vulnerabilidades ocasionando incidentes que originan pérdida o daños a las empresas.

Una vulnerabilidad son defectos o debilidades en los diseños, implementación, controles o procedimientos de seguridad que se le proporciona a un sistema que pueden ser explotados intencionalmente.

Es por ello que las amenazas son las situaciones que pueden hacer explotar en muchas ocasiones intencionalmente para los servidores de nombre de dominio o accidentales de las vulnerabilidades que tiene.

En la red de comunicación (internet) existen muchos riesgos y es por ello que, es necesaria la implementación de seguridad para reducir los niveles de vulnerabilidades y así no tener pérdidas o alteración de la información.

2.5 VULNERABILIDADES QUE TIENEN LOS DNS

En los servidores de nombre de dominio (DNS) existen diferentes amenazas que se mencionan en el RFC 3833 comunes o que han ocasionado problemas al haber sido explotadas así como mencionando una posible solución para proteger los servidores.

2.5.1 INTERCEPTACIÓN DE PAQUETES

En el internet existe dos tipos de comunicaciones TCP (Transmission Control Protocol) es el protocolo de control de trasmisión que crea una conexión donde se mandar todo el flujo de datos es decir que se establece un canal de comunicación que garantizara la entrega de datos correctamente y UDP (User Datagram Protocol) es el protocolo basado en el intercambio de datagramas sin que se establezca una conexión ya que el datagrama contiene la información de direccionamiento, no incluye el control del flujo, por lo que los paquetes pueden llegar en diferente orden y no garantiza que llegue completamente la información. Es por ello que una es más segura que la otra los DNS trabajan con una conexión UDP es decir el usuario consulta a los DNS y este le envía la información en un solo paquete sin firmar y garantizar que realmente es lo que el usuario busca, esta información puede ser modificada y redireccionar al usuario a otra página.

La interceptación de paquetes es una de las amenazas en contra de los DNS especificado en el RFC donde es la apropiación de los paquetes en el medio de comunicación y es causada por no contener una firma o un canal seguro permitiendo a un ente ajeno a la conversación y enterarse de todo lo que el usuario busca para después poder emplear la información como a él le convenga.

Esta vulnerabilidad se puede mejorar si se firmara los servidores como en una zona de seguridad como por ejemplo TSIG donde existe una relación de confianza entre un cliente especifico y particular que comprobara la firma por

que garantiza la integridad de la comunicación de los servidores o DNSSEC que realiza la comprobación de las firmas y cuando se aplica correctamente prevé la integridad de datos.

2.5.2 ID GUESSING AND QUERY PREDICTION

Puesto que los DNS en su mayor parte se utiliza sobre el protocolo UDP/IP, es relativamente fácil para un atacante generar paquetes que coinciden con el protocolo de transporte.

Dado que el DNS crea la siguiente cabecera especificada en la figura 2.3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	Opcode				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

Figura 2.3 Cabecera del DNS

Donde:

ID es el identificador utilizado para relacionar solicitudes y respuestas.

QR identifica el mensaje como una solicitud (Query **0**) o una respuesta (1)

Opcode: de 4 bits describe el tipo de solicitud.

- 0 estándar es decir una solicitud normal (nombre a dirección).
- 1 inverso, solicitud Inversa (dirección a nombre).
- 2 status del servidor, estado del servidor.
- 3-15 reservado para un uso a futuro.

AA indica que la respuesta fue por un servidor autoritativo.

TC Indica que el mensaje fue truncado.

RD indica la solicitud de un servicio recursivo por parte del servidor de nombre. Este servicio normalmente no está disponible.

RA Indica la disponibilidad del servicio recursivo.

Z es un campo de 3 bits reservado para un uso futuro, y su valor definido por 0.

RECODE este campo lo escribe los servidores de nombre de dominio, y sirve para indicar el tipo de búsqueda como puede ser:

- ***0:*** Sin error.
- ***1:*** Format Error es decir que es imposible interpretar el formato de la búsqueda.
- ***2:*** Server Failure es el error que indica que es imposible procesar el servidor.
- ***3:*** Name Erro el nombre no existe.
- ***4:*** Not implemented es el tipo de búsqueda que no es soportada.
- ***5:*** Refused es la solicitud rechazada.

QDCOUNT indica el número de entradas en la sección de Preguntas.

ANCOUNT que indica el número de Resource Records en la sección de Respuesta.

NSCOUNT define el número de Resource Records en la sección de Autoridad.

ARCOUNT define el número de Resource Records en la sección de Archivos Adicionales.

El campo ID en la cabecera del DNS es sólo un campo de 16-bits y el puerto UDP del servidor DNS asociados a una pregunta es de 16 bits, es decir sólo hay 2^{32} posibles de que el ID y puerto UDP, sin embargo el paquete del ID en algunas implementaciones de servidores de DNS no cambian aleatoriamente y el puerto es fijado para compatibilidad con firewalls a un cliente determinado.

Es por ello que existe una posibilidad de 2^{16} de que se realice el ataque que se basa en la predicción del canal cuando éste se encuentra ocupado y que la probabilidad de éxito cuando la víctima se encuentra en un estado, ya que la

víctima reinicia continuamente o posiblemente su comportamiento sea influenciado por algún atacante o porque la víctima está respondiendo (de una manera predecible) a alguna tercera persona y esta acción es conocida por el atacante.

Este ataque no necesita estar en un tránsito o de red compartida. Es similar a la intercepción de paquetes. Una solución es que la firmas de DNSSEC controle y sean capaces de detectar la respuesta, han sido falsificadas y en caso de no ser utilizado DNSSEC se sugiere utilizar TSIG o algún mecanismo equivalente para garantizar la integridad de sus comunicaciones con un servidor de nombre recursivo que lleva a cabo la revisión de la firma.

2.5.3 NAME CHAINING

Tal vez la clase más interesante en las amenazas del DNS es la llamada name chaining, ya que son un subconjunto de ataques basados en nombres, llamadas "envenenamiento de caché". Los ataques basados en nombres pueden ser parcialmente mitigados por una la larga duración de control en los mensajes de respuesta para la consulta original, pero esas excepciones de no captura dan origen al ataque.

Hay variaciones en el ataque, pero lo que todos tienen en común es afectar los *Resource Records* (RR) en el DNS sino que directamente se asigna a un nombre. Cualquier *Resource Records* que al principio permita a un atacante introducir mal los datos en la caché de la víctima.

Los registros de tipo: CNAME, NS, y DNAME pueden redirigir la consulta de la víctima a un lugar dependiendo de la elección del atacante. *Resource Records* (RR) con MX y SRV son menos peligrosos, pero en principio también se puede utilizar para desencadenar otras búsquedas en lugar de ser asignada por el atacante.

La forma general del ataque de encadenamiento de nombre es descrita como:

- La Víctima emite una consulta, tal vez a instancias del atacante o un tercero, la consulta puede ser sin relación, bajo el nombre del ataque (es decir, el atacante sólo utiliza esta consulta como un medio para introducir información falsa acerca de algún otro nombre).
- El atacante inyecta respuesta, ya sea a través de la interceptación de paquete, o por ser un servidor de nombres legítimos que está implicado en algún momento en el proceso de respuesta a la consulta que la víctima publicará en breve.
- La respuesta del atacante incluye uno o más *Resource Records* con nombres DNS; dependiendo de la forma particular, este ataque tiene el objeto que puede inyectar datos falsos relacionados con los nombres en la caché de la víctima, o puede ser para redirigir la siguiente etapa de la consulta a un servidor de la elección del atacante (con el fin de inyectar o colocar las mentiras de la Autoridad o de *Resource Record* de una respuesta, donde tendrán una mejor oportunidad de defensas de un programa de resolución).

Cualquier atacante que puede insertar en los *Resource Records* en la caché de una víctima puede realizar algún tipo de daño, por lo que hay ataques al envenenamiento de caché o encaminamiento de nombre. Sin embargo, en el caso del ataque de encadenamiento de nombres es la relación causa-efecto entre el ataque inicial y el resultado final puede ser mucho más compleja que en los otros las formas de envenenamiento de caché, así que el nombre encadenar ataques merecen una especial atención.

El thread común en todo el nombre del encadenamiento de los ataques es el mensajes de respuesta que permitirá al atacante la introducción del nombre al DNS de forma arbitraria y facilitar más información que las reclamaciones con el

atacante, así asociando los nombres, a menos que la víctima conozca los datos asociados con el nombres y pueda detectarlos de lo contrario la víctima va a tener dificultades para defenderse de esta clase de ataques.

Con los DNSSEC se pretende que se proporcione una buena defensa contra la mayoría de variaciones en esta clase de ataque. Al revisar las firmas, se puede determinar si los datos asociados a un nombre realmente se insertaron por la autoridad delegada por esa porción del espacio de nombres DNS.

Las firmas DNSSEC no cubren los registros de cola, dando así la posibilidad de que un nombre de encadenamiento en el ataque con la cola, pero con DNSSEC es posible detectar el ataque de forma temporal y así dando origen a la aceptación de la cola con el fin de recuperar la versión firmada autorizada de los mismos datos, a continuación, comprobar las firmas en la versión auténtica.

2.5.4 BETRAYAL BY TRUSTED SERVER

Otra variación sobre el ataque de interceptación de paquetes es la confianza del servidor que en muchos casos resulta no ser tan confiable, ya sea por accidente o por intentos del cliente servidor que es configurado como resolvers y este utiliza los servidores de confianza para realizar toda consulta del nombre de dominio.

En muchos casos la confianza del servidor es proporcionada por los usuarios ISP y de publicidad destinada al cliente a través de DHCP o por opciones de PPP. Además de la traición accidental de esta relación de confianza (A través de errores de servidor, servidor de éxito robos, etc).

El servidor puede ser configurado para devolver las respuestas que no son lo que el usuario desea, ya sea en un intento sincero de ayudar al usuario o para promover algún otro objetivo, como la promoción de una sociedad comercial entre el ISP y algunos terceros.

Este problema en particular es especialmente grave para los travelers que llevan a su propio equipo y esperar que funcione en la mayor parte, de la misma manera donde quiera que vayan. Estos travelers necesitan de confianza en el servicio DNS sin tener en cuenta que opera la red a la que su equipo está conectado.

Aunque la solución obvia a este problema sería que el cliente eligiera un servidor más confiable, en la práctica esto no puede ser una opción para el cliente. El entorno de la red de un cliente tiene sólo un número limitado de servidores de nombres recursivos que elegir, y ninguno de ellos puede ser particularmente digno de confianza. El filtrado de puertos u otras formas de intercepción de paquetes puede evitar que el cliente sea capaz de ejecutar una resolución interactiva. Así, mientras que la fuente inicial de este problema no es un ataque al protocolo de DNS, este tipo de traición es una amenaza para los clientes DNS, y simplemente cambiando a un servidor de nombre recursivo en otro diferente no es una defensa adecuada.

Visto estrictamente desde el punto de vista del protocolo DNS, la única diferencia entre este tipo de traición y un ataque de intercepción de paquetes es que el cliente ha enviado voluntariamente su solicitud al atacante. La defensa contra un ataque a la intercepción del paquete: es la resolución de cualquiera que debe comprobar las firmas de DNSSEC o el uso TSIG (o equivalente) para autenticar el servidor en el que ha depositado su confianza.

Teniendo cuenta que el uso de TSIG pero que por sí mismo no garantiza que un servidor de nombres es en absoluto fiable. TSIG puede hacer una resolución de ayudar a proteger su comunicación con un servidor de nombre que ya ha decidido confiar por otras razones. La protección de una resolución de la comunicación con un servidor que está dando falsas respuestas no es particularmente útil.

También hay que tener en cuenta que si el trozo de resolución no confía en el servidor de nombres que está realizando un trabajo en su nombre y quiere comprobar las firmas de DNSSEC, la resolución realmente tiene que tener conocimiento independiente a la clave pública DNSSEC (s) que necesita para llevar a cabo el chequeo. Por lo general, la clave pública para la zona de las raíces es suficiente, pero en algunos casos el conocimiento de claves adicionales puede también ser adecuada.

2.5.5 DNS DENEAL OF SERVICE (“NEGACIÓN DE SERVICIO” O “DNS DOS”)

Los ataques de negación de servicio utilizando la vulnerabilidad del DNS, puede llevarse a cabo de distintas maneras. Una de ellas es aprovechando las respuestas negativa que genera como respuesta un servidor de nombre de dominio ejemplo se quiere saber en la ubicación de ingeneria.unam.mx, los servidores mandan la respuesta de que no existe el nombre de dominio esto se toma como denegación del servicio. También cuando la consulta te manda a otra página que no contiene lo que el usuario requiere. El DNS es vulnerable a la denegación de servicio, y no existe mecanismo de protección, por lo que DNSSEC no ayudaría a este tipo de vulnerabilidades.

2.6 ¿QUÉ ES DNSSEC?

En la solución de las vulnerabilidades de los servidores de nombre de dominio (DNS) en el RFC 3833 se recomienda utilizar TSIG y DNSSEC, pero ¿Qué es TSIG y DNSSEC como funciona?

Como se vio anteriormente el DNS realiza una consulta en forma de árbol invertido donde parte de los Root Server (DNS), y preguntando a diferentes DNS dependiendo del nivel hasta encontrar la ubicación de donde se localiza en nombre que apunta a una IP.

Ya que la actualización de los mensaje de los Servidores de Nombre de Dominio, como son las respuestas y actualizaciones es complicado, surge el protocolo TSIG (Secret Key Trasaction Authentication for DNS Firma de transacción) publicado en el RFC 2845 utilizado sobre DNS, la implementación consta en autoriza a dos sistemas que estén intercambiando información mediante una llave compartida que permite el nivel de autenticación.

La transmisión de datos de una manera segura mediante la utilización de funciones hash para proporcionar medios de autenticación a los servidores, protección en los mensajes (como trasferencia de zonas) y actualizaciones de zonas de los DNS de una forma dinámica.

TSIG utiliza la función has MD5, con la variable HMAC-MD5 una función con un valor de 128 bits. La firma de TSIG incluye el tiempo que el mensaje firmo el DNS, esto para ayudar a combatir los ataques ya que a un hacker captura la firma.
DNSSES en el periódico El Universal se define como:

“DNSSEC es un protocolo que verifica y valida las respuestas del servidor de nombres a través de redes de confianza, lo que permite que el sistema de nombres de dominios sea más seguro.”[5]

En otras palabras el Domain Name System Security Extensions o Extensión de seguridad (DNSSEC) especificado en el RFC 2535, es el protocolo que aporta autentificación e integridad a los registros de recursos de las zonas de los DNS mediante la utilización de cadenas de confianza mediante la firma de cada servidor que realice la consulta.

[5] Periódico EL UNIVERSAL 24 de junio del 2010 http://www.eluniversal.com.mx/articulos/59265.html

Es por ello que proteger a los DNS de ciertos ataques anteriormente mencionados que requieren por lo que se necesita cambiar el protocolo del DNS tiene los *Resource Records (RR) los más conocidos o utilizados* son*:*

- **NS** (**N**ame **S**erver): Es el nombre de los servidores DNS tanto primarios como secundarios que se encuentran definidos dentro del archivo de zona es decir que disponen de la dirección y nombre para el dominio.
- **A** (**A**ddress)**:** Indica la dirección IP asociada al nombre host.
- **MX** (**M**ail E**x**changer)**:** Es el nombre del servidor encargado del correo en ese dominio asi como la prioridad.
- **CNAME** (**C**anonical **Name**)**:** Indica cuál sea el nombre canónico de un alias.
- **PTR** (**P**oin**t**e**r**)**:** Host Name – Pointer Indica el dominio asociado a una dirección IP.
- **TXT** (**T**e**xt**)**:** – datos del Host arbitrariamente utilizados para las listas negras.
- **SOA** (**S**tart **of A**uthority) indica los datos de la autoridad para el domino o zona en cuestión, por lo que cada dominio deberá de existir.

DNSSEC agrega cuatro tipos de recursos nuevo registro: registro de recursos Firma (RRSIG), DNS de Clave Pública (DNSKEY), Delegación Firmante (DS) y Next segura (NSEC).

Así también se agrega dos bits como cabecera (header) en el DNS como indicadores como son:

Checking Disabled (comparación de movilidad reducida CD).
Authenticated Data (Autenticacion de datos AD)

2.7 RRSIG

El registro Resource Record Signature (RRSIG) almacena la firma digital de un RRset.

Un RREset es un grupo de registros de recursos con el mismo propietario, clase y tipo, esto ahorra tiempo de estar buscando un registro de direcciones, es decir el propietario seria iingeneria.unam.mx se creo que registro ww2.iingeneria.unam.mx como se muestra en la figura 2.4

```
; File written on Fri Aug 13 13:02:11 2010
; dnssec_signzone version 9.4.2-P2
iingen.unam.mx.         7200    IN SOA  kate.nic.unam.mx. dns.unam.mx. (
                                        2010081100 ; serial
                                        3600       ; refresh (1 hour)
                                        1200       ; retry (20 minutes)
                                        604800     ; expire (1 week)
                                        7200       ; minimum (2 hours)
                                        )
                        7200    RRSIG   SOA 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        X9bBDUmYufjs9ImihAFm6Jgf3ncDASWDm9tZ
                                        sSEUMYF7K8m0mzWVqv5EfiYd793vqOP2/EOw
                                        1aOoCPliX6u6NQ== )
                        7200    NS      kate.nic.unam.mx.
                        7200    NS      jack.nic.unam.mx.
                        7200    RRSIG   NS 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        1VIdmco8P0ppDUbOC+hnBN1nzaSFt7vsRUSl
                                        Xo/eIzjj4OZgGhJikHqVGjxjwzBn9ucgnbyn
                                        9rTo7/+FH/uipg== )
                        7200    NSEC    ww2.iingen.unam.mx. NS SOA RRSIG NSEC DNSKEY
                        7200    RRSIG   NSEC 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        nF2LeC1+R4txo5BviP+vasF9We1oQA97FEN3
                                        iV5PoURuHoic9YbLqnFPejOzSE0ZWqUo+1Gz
                                        zVjqvMGly111rg== )
                        7200    DNSKEY  256 3 5 (
                                        AwEAAayDoYmhLfOs8baHUsqfU4yGjprYlDa5
                                        1aLiLknbPKm/3N01maneP0Yn/qwOM6mgSIyz
                                        +eE2u30TdPioojHU3ws=
                                        ) ; key id = 21306
                        7200    DNSKEY  257 3 5 (
                                        AwEAAb6JRoTbURvDYkg+qMya3LDvqaOzWali
                                        gtPdcn9LABB15A4416l1MHGyeGzgO2mfDZjS
                                        A5EUFmbQ42WdmIP75dc=
                                        ) ; key id = 12604
                        7200    RRSIG   DNSKEY 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
iingenunam.signed 52%
```

Figura 2.4 Resource Record Signature (RRSIG) con RRset

En donde el propietario es iingeneria.unam.mx y todo lo que se encuentre registrado bajo el está firmado de la siguiente manera como se visualiza en la figura 2.5.

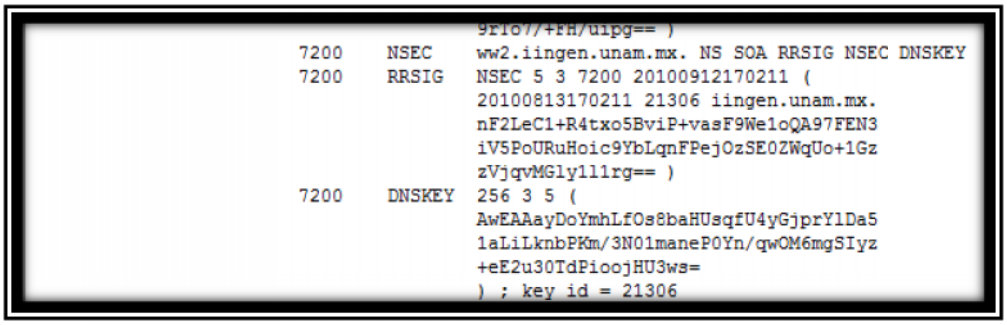


Figura 2.5 Firma de RRSIG.

- ***Tipo de cubierta*** *es el primer campo*. Eso nos dice que es NSEC que tiene por registro ww2.iingen.unam.mx
- ***Algoritmo con valor 5 es el segundo campo.*** Este es uno de los mismos valores utilizados en el registro DNSKEY, para cada RRset, es con un número 5 algoritmo RSA/SHA-1 y un 3 el algoritmo DSA.
- **Campo de etiqueta:** es el número de etiquetas que hay en el nombre del propietario de los documentos firmados ww2.iingen.unam.mx, contiene 3 etiquetas.
- **El *TTL original*** en los registros de la RRset que se firmó. (Todos los registros en un RRset se supone que tienen el mismo TTL.) El TTL necesita ser almacenado porque un servidor de nombres caché de la RRset que este en el registro se cubre RRSIG disminuir el TTL en los registros almacenados en caché. Este número es imposible reconstruir los registros de direcciones originales para verificar la firma digital.
- Los dos campos siguientes son de **inicio y expiración** de firma, respectivamente, los dos registros son almacenados con números enteros sin ningún signo de segundos son presentados en el YYYYMMDDHHMMSS (año, mes, día, hora, minuto y segundo). El

tiempo de creación de firma es por lo general el tiempo que el programa firmo la zona.

- ***Etiqueta de clave*:** es una huella digital derivada de la clave pública que corresponde a la clave privada que firmo la zona Si la zona tiene más de una clave pública, la verificación de software DNSSEC utiliza la etiqueta clave para determinar qué tecla de usar para verificar esta firma.
- **El campo de sesiones** en este caso iingen.unam.mx, es el que *firma el nombre del* campo. Es el nombre de dominio de la clave pública que un verificador debe utilizar para comprobar la firma. Es la etiqueta de clave, identifica el registro usado DNSKEY. El nombre del firmante del campo es siempre el nombre de dominio de la zona de los registros firmados.
- **El *campo de firma*:** esta es la firma digital de la clave privada de la zona en los registros de firma y del lado derecho del registro RRSIG, y esta se encuentra codificada en base 64.

RRSIG es calculada utilizando la clave privada. Un servidor con soporte DNSSEC intentará devolver los RRs solicitados y sus correspondientes registros RRSIG para poder ser chequeados posteriormente.

2.8 DNSKEY

El registro DNSKEY se utiliza para almacenar una clave pública necesaria para verificar los registros RRSIG.

La zona de clave privada se almacena en un lugar seguro, en un archivo en el sistema de archivos localizado en el Servidor de Nombre de Dominio primario o maestro, la clave pública de la zona que se anuncia como un registro vinculado al nombre de dominio de la zona y es por ello que solo almacena la clave de una zona como se muestra en la siguiente figura 2.6.

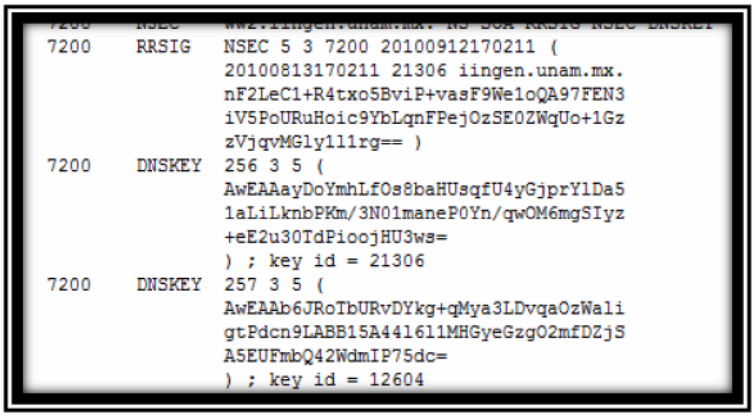


Figura 2.6 firma de DNSKEY

Después del tipo de firma que es DNSKEY siguen los siguientes campos:
Es 257 es el valor de la bandera, este es de longitud de dos bytes y codifica un conjunto de valores como se observa en la siguiente figura2.7.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
							ZK								SEP

Figura 2.7 campo de banderas disponibles

Donde los primeros bists del 0 al 6 y del 8 a 14 están reservadas y deben de tener un valor de 0.
En bit octavo es el tipo de calve:

- **0** es una clave de zona DNS y no se puede utilizar para verificar los datos firmados por la zona.
- **1** es la clave de zona DSN. El nombre de registro DNSKEY, el propietario es el nombre de dominio de al zona.3757.

El valor 3 es el campo de protocolo: es un vestigio de la versión DNSSEC.
El valor 5 es el campo de algoritmo, donde DNSSEC puede trabajar con diferentes algoritmos en la clave los valores son los siguientes:

- **0** Reservados.

- **1 RSA/MD5**. El uso de RSA/MD5 ya no se recomienda, sobre todo debido a las deficiencias descubiertas recientemente en el algoritmo de hash MD5 de un solo sentido.
- **2 Diffie-Hellman** no se puede utilizar para firmar las zonas, pero puede ser utilizado para otros fines relacionados con DNSSEC.
- **3 DSA/SHA-1** (además de cualquier algoritmo obligatorio) es opcional.
- **4Reservado** para un algoritmo de clave pública elíptica curva basada en.
- **5 RSA/SHA-1**. El uso es obligatoria.
- ***253-254*** **.**Estos números algoritmo son reservados para uso privado por RFC 4034.
- ***255*****Reservados.**

El último campo en el registro DNSKEY es la clave pública y se codifica en base 64.

DNSSEC admite claves de longitudes de muchos. Cuanto más larga sea la clave, más segura (porque es más difícil para encontrar la clave privada correspondiente), pero cuanto más tiempo se tarda en firmar datos de la zona con la clave privada y verificar con la clave pública, y más largo es el de la DNSKEY registro y firmas creadas.

2.9 NSEC

Este registro es utilizado para la comprobación de la consistencia interna. Indica qué RRset es el próximo en la zona y qué tipo de códigos están disponibles para el nombre actual.

El registro NSEC resuelve el problema de la firma de respuestas negativas. Abarca una brecha entre dos nombres de dominio consecutivos en una zona, que le dice que el nombre de dominio que sigue después de un name hacen el dominio dado el nombre del registro: "Siguiente segura"

Pero no la noción de "nombres de dominio consecutivos" implica un orden canónico a los nombres de dominio en una zona. Para ordenar los nombres de dominio en una zona, se empieza por la clasificación por la etiqueta más a la derecha en los nombres de dominio, a continuación, en la etiqueta junto a la izquierda, y así sucesivamente. Las etiquetas son ordenadas mayúsculas y minúsculas y lexicográficas (por orden de diccionario), con los números que vienen antes de las letras y los números de las etiquetas antes inexistentes como se muestra en la siguiente figura 2.8.

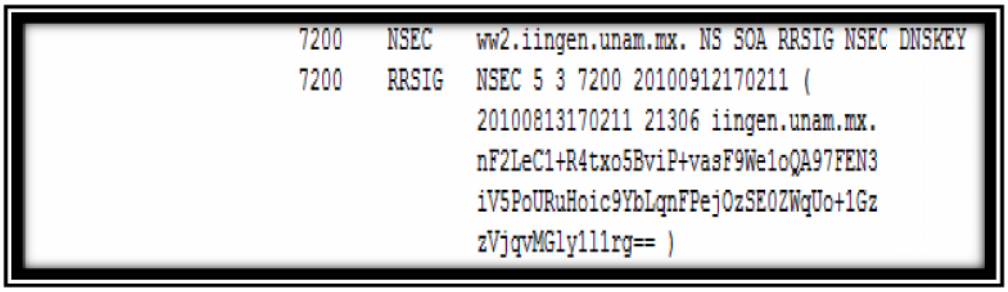


Figura 2.8 Figura NSEC

El nombre de dominio a lado en la zona después de iingen.unam.mx es ww2.iingen.unam.mx tiene registros como son NS, SOA, RRSIG, un registro NSEC y un registro DNSKEY.

El último registro NSEC en una zona contendrá el nombre de la zona, tratando el espacio de nombre como circula, dado que no hay realmente ningún nombre de dominio que sigue después, este indica que no hay otro registro de iingen.unam.mx mas que los anteriores.

El registro NSEC, en su totalidad identifica y especifica lo que existe bajo una zona, indicando “Eso no existe” y con ello reduce las demandas falsas de nombres de dominio o registros que no existen.

2.10 DS

El registro Delegation Signer (DS) es un puntero para construir cadenas de autenticación, DS o firma de delegación identifica la clave pública autorizada para firmar el iingen.unam.mx los datos de la zona. El registro DS en el registro RRSIG, da fe de que si pertenece a la zona.

2.11 COMPARACIÓN DE MOVILIDAD REDUCIDA (CD) Y AUTENTICACIÓN DE DATOS (AD)

En la cabecera del DNS como se muestra en la figura 2.9 se anexaron dos banderas de consulta AD y CD ambos son parte de la consulta estándar del encabezado como se puede visualizar en la siguiente figura 2.10.

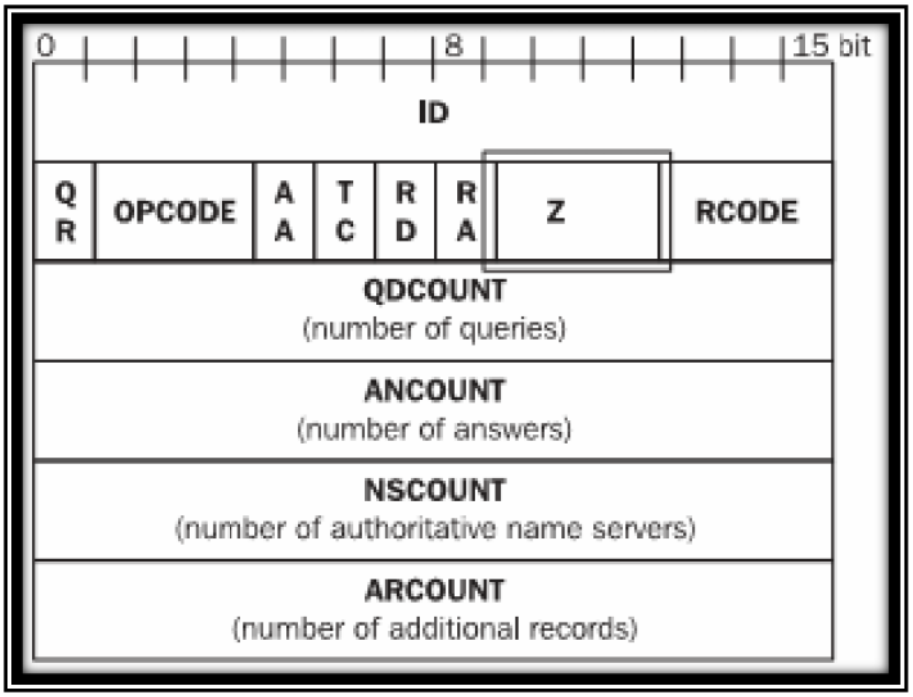


Figura 2.9 Cabeceras DNS

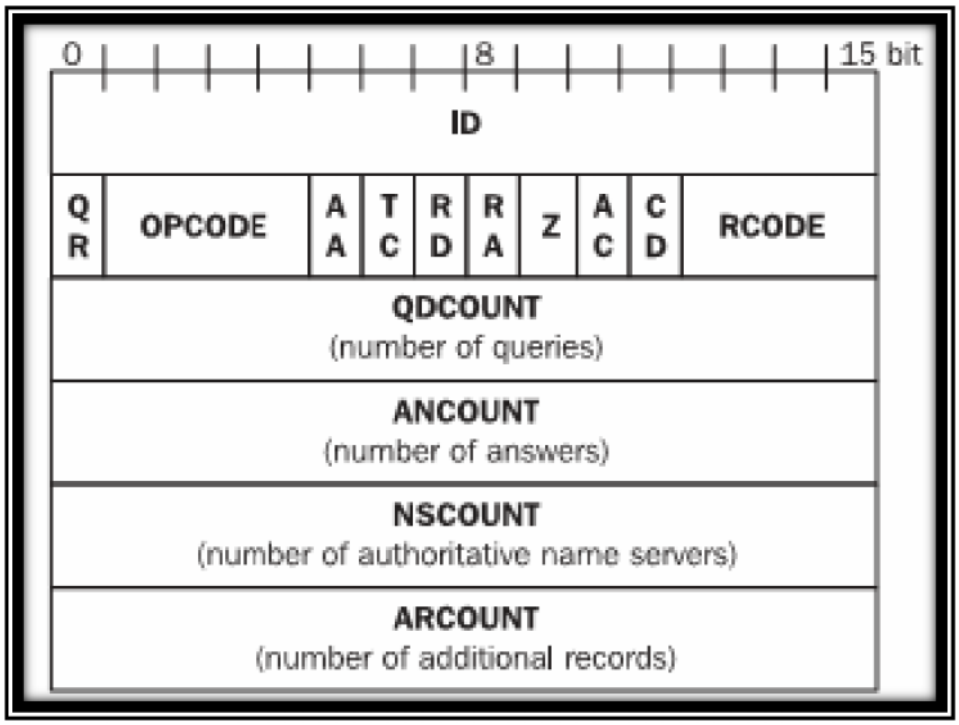


Figura 2.10 Cabeceras de DNSSEC

El bit AD está diseñado para permitir que los resultados de la consulta de un servidor de nombres que admite DNSSEC, pero no pueden comprobar los registros DNSSEC para determinar si una respuesta ha sido validada. Sin embargo, estos solucionadores sólo deben confiar en el valor del bit AD si su canal de comunicación con el servidor de nombres es secureusing IPSEC o TSIG, por ejemplo.

El bit de CD, por el contrario, es para el uso de resultados que *pueden* comprobar los registros DNSSEC, que es una abreviatura para la comprobación de movilidad reducida, le dice al servidor de nombres para no molestar a la verificación de los registros DNSSEC en la resolución de nombre, ya que puede manejar el trabajo en sí.

CAPÍTULO 3
DESARROLLO E IMPLEMENTACIÓN

3.1 SISTEMA OPERATIVO

Antes de abordar el tema del funcionamiento e implementación de DNSSEC es necesario saber, en donde se implementa, si funciona sobre algún sistema operativo en específico, etc. Antes de seguir, definiré ¿Qué es un sistema operativo?

Un sistema operativo es el conjunto de programas que controlan y gestionan de una manera más eficiente, las acciones y recurso de un dispositivo u computadora. Proporcionando la base sobre la cual se pueden escribir programas de aplicación, estableciendo comunicación entre el usuario y la máquina.

Es por ello que la implementación y desarrollo han sido de varios años y aun en nuestros días no se llega a su total culminación.

DNSSEC son las medidas de seguridad que son implementadas en los servidores de nombre de dominio (DNS).

Pero recordemos que un Servidor de Nombre de Dominio, es aquel que administra la información de una parte del nombre de dominio llamada zona, dando origen a una base de datos, esta es distribuida, jerárquica y descentralizada, formando una parte fundamental para el funcionamiento en la internet.

Es por esta razón que tiene un crecimiento, mediante los diferentes niveles, propuesto por los creadores Jonathan B. Postell y Paul Mockapetris, especificado en los RFC’s 882 y 883.

Para llevar a cabo el servicio del Servidor de Nombre de Dominio en 1980 Paul Vixie conocido en programas de sistemas UNIX diseña la arquitectura de un Software de licencia libre llamado **Berkeley Internet Name Domain (BIND)**, el más utilizado por el protocolo DNS, es conveniente mencionar que BIND se

puede implementar en cualquier sistema operativo, aunque para aquellos administradores que trabajan en plataformas Windows, Microsoft desarrollo sus propios DNS Server Windows.

Retomando lo anterior Paul Vixie trabajo y modifico el BIND hasta la versión 8 resolviendo las diferentes vulnerabilidades de seguridad con respecto a la primera versión liberada que fue la versión 4.3BSD, posteriormente deja el mantenimiento y distribución a la ISC (Internet Software Consortium) fundada en 1994, la cual es una organización que se encarga de la distribución y elaboración de software de código abierto, para el apoyo de la infraestructura de conectividad a la Internet.

"BIND proporciona una plataforma sólida y estable sobre la cual se pueden crear sistemas de computación distribuida con el conocimiento de que esos sistemas son totalmente compatibles con las normas publicadas DNS." [6]

Actualmente BIND se encuentra en la versión 9, esta contiene aspectos de seguridad que anteriormente no se contemplaban como son: DNS Security Extensions, IPV6, algunas mejoraras en los protocolos IXFR, DDNS etc.
Teniendo en cuenta que existe una variedad de sistemas operativos se debe de elegir uno que soporte el BIND para un mejor funcionamiento, para ello los estudios realizados comentan que depende de las necesidades y recursos con los que se cuenten influirá en la decisión.

Para la implementación de dicha investigación y las pruebas se decidió utilizar un sistema operativo tipo UNIX, llamado OpenBSD versión 4.6.

[6] Tomado y traducido de http://www.isc.org/software/bind

3.2 UNIX Y SUS DERIVADOS

UNIX es un Sistema operativo que controla los recursos de un equipo o dispositivo compartido, entre varios usuarios (multiusuario), es decir este acepta el acceso de más de un usuario al mismo tiempo, dando como principal objetivo el proporcionar una asignación ordenada y controlada de su uso del o los procesadores, la memoria y los dispositivos tanto de entrada como salida para los distintos usuarios y programas.

Estos sistemas operativos tienen la característica principal de ser multitarea, ya sea cooperativa (no existe prioridad en los procesos, el proceso decide cuando deja de utilizar los recursos) o de asignación de prioridad (el sistema puede intervenir en cualquier momento en la asignación de prioridades de los procesos), es decir, ejecutar más de un programa o proceso al mismo tiempo.

UNIX contiene un núcleo del sistema llamado kernel y diversos programas esenciales como son: los compiladores, editores, lenguajes de comandos, programas para copiado e impresión de archivos y programas desarrollados por el propio usuario formando así un sistema operativo sencillo, elegante y consistente.

UNIX fue creado por los Laboratorios Bell de AT & T y el MIT (Massachussets Institute of Technology) a finales de los 60’s, bajo el nombre de MULTICS. En la década de de los 70 fue retomado por Dennis Ritchie, quien desarrollando un compilador para el lenguaje C (Lenguaje en el que fue desarrollado UNIX), dado este suceso surgió lo que hoy es UNIX.

Gracias a su portabilidad, su ambiente y programación en un lenguaje de alto nivel, el código fuente fue difundido y utilizado por las universidades de Estados Unidos.

Una de las versiones más significativas y difundida fue la Universidad de California en Berkeley, la cual fue la base de diversas versiones.

A partir de la década de los 80 AT & T, comienza a comercializar UNIX.
Una de las funciones que se ejecutaba era
"controla el hardware y proporciona una interfaz de llamada al sistema para todos los programas" [7]

Estas interfaces permiten a los programas desarrollados por el usuario, participar en la creación y manejo de procesos, archivos y otros recursos.

Los programas realizan llamadas al sistema al colocar valores en los registros (a veces utilizan pilas), y en el momento de ejecutar las instrucciones de señalamientos, para alternar entre el modo usuario y el modo núcleo.

El shell de este sistema operativo, permite a los usuarios escribir comandos para su ejecución, permitiendo también redireccionar la entrada y salida. La base de UNIX se centra en tres aspectos fundamentales:

1. El modelo de memoria, el cual consta de un segmento de texto, de datos y de pilas de proceso.
2. El sistema de archivos que maneja, un sistema de orden jerárquico, parecido a un árbol
3. Las Entradas / Salidas se dan a través de llamadas al sistema.

Del UNIX original se han desprendido una amplia gama de sistemas operativos, los cuales, han adoptado comandos, base estructural y algunas otras ventajas que este sistema ofrece, permitiendo establecer una nueva gama de sistemas operativos que cubren con las diversas necesidades presentadas por los usuarios, algunos de estos sistemas operativos son Linux y OpenBSD.

[7] SISTEMAS OPERATIVOS MODERNOS

Linux es un software libre de código abierto. Surge del proyecto GNU, el cual inicia en 1983.

Este proyecto tiene el objetivo de crear un sistema operativo tipo UNIX. En 1991 se libera la primera versión de Linux, gracias a la programación ejercida por miles de voluntarios principalmente de la Universidad de Helsinki, y principalmente por las aportaciones realizadas por Linus Torvals, quien es el creador del Kernel que maneja Linux.

Actualmente existen diferentes soluciones algunas comerciales basadas en Linux, distribuidas alrededor del mundo, cada una de estas soluciones se enfoca a diversas necesidades presentadas por los usuarios.

Una de ellas es OpenBSD que en su primera versión surgió en 1995 desarrollado por voluntarios de distintas partes del mundo, que se unen para cumplir normas y regulaciones, correcciones del código seguridad y criptografía que integran en él para su funcionalidad es por ello que se actualiza mediante parches y suites de seguridad que se puede obtener de su página de una manera gratuita, si se requiere anexar algún otro componente se puede descargar de las páginas del fabricante tanto de Software como de Hardware.
Anteriormente OpenBSD contaba con BIND en la versión 4.3 y para realizar alguna actualización se realizaba mediante los parches, pero a partir de la versión 4.6 ya se cuenta con la BIND versión 9 solo se necesita realizar los parches que se sugiere en la página de OpenBSD.

“OpenBSD produce un sistema operativo LIBRE, multi-plataforma, se orientan principalmente en la portabilidad, estandarización, seguridad proactiva y criptografía integrada” [8] su logotipo se muestra en la figura 3.1.

[8]Tomado y traducido de http://www.openbsd.org/es/

Figura 3.1 Logotipo de OpenBSD 4.6

3.3 CARACTERÍSTICAS DEL BIND

BIND ofrece un Servidor de Nombre de Dominio a través del archivo Named. Named además de ser una biblioteca de resolución de sistemas de nombres de dominio, es un paquete de herramientas para monitorizar el correcto funcionamiento de todo el sistema (bind-utils).

Gracias a su arquitectura mejorada se ha conseguido una mejor portabilidad entre sistemas.

Como se vio anteriormente el servidor de nombre de dominio realiza una consulta en forma de árbol invertido donde parte de los Root Server, pregunta a diferentes servidores de nombre de dominio dependiendo del nivel hasta encontrar la ubicación de donde se localiza el nombre que apunta a una IP, para que pueda ser posible la consulta es necesario configurar el archivo *named.conf* en el Servidor de Nombre de Dominio (DNS), donde se configura las distintas zonas a su cargo así como los dominios que se almacenan y todo el conjunto forma la base de datos. Como se muestra en la siguiente figura 3.2.

```
// $OpenBSD: named-simple.conf,v 1.9 2008/08/29 11:47:49 jakob Exp $
//
// Example file for a simple named configuration, processing both
// recursive and authoritative queries using one cache.


// Update this list to include only the networks for which you want
// to execute recursive queries. The default setting allows all hosts
// on any IPv4 networks for which the system has an interface, and
// the IPv6 localhost address.
//
acl clients {
        localnets;
        ::1;
};

options {
        version "";     // remove this to allow version queries

        listen-on    { any; };
        listen-on-v6 { any; };

        empty-zones-enable yes;

        allow-recursion { clients; };
        dnssec-enable yes;

};

logging {
        category lame-servers { null; };
};
```

Figura 3.2 named.conf

```
# End of named.conf
// Standard zones
//
zone "." {
        type hint;
        file "etc/root.hint";
};

zone "localhost" {
        type master;
        file "standard/localhost";
        allow-transfer { localhost; };
};

zone "127.in-addr.arpa" {
        type master;
        file "standard/loopback";
        allow-transfer { localhost; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" {
        type master;
        file "standard/loopback6.arpa";
        allow-transfer { localhost; };
};
```

Figura 3.2 named.conf

Como se vio con anterioridad uno de los servidores que configuraremos es de tipo maestro (Master) y esclavo-(Slave).

Por ejemplo para la configuración de zona maestra se configura de la siguiente manera:

zone "myzone.net" ---------- Nombre de la zona

{

type **master;**

file "master/myzone.net"; ---------- Archivo de configuración

}

Para la configuración en un esclavo es:

zone "otherzone.net" ---------- Nombre de la zona

{

type **slave;**

file "slave/otherzone.net"; ----------> Archivo de configuración
masters { 192.0.2.1; [...;] };
};

Donde cada zona es asociada a un archivo de de configuración donde contienen la información de la misma como se puede ver en la siguiente figura 3.3.

```
;  RR NS Name Servers
;  ____________________
;
        IN      NS      kate.nic.unam.mx.
        IN      NS      jack.nic.unam.mx.

;  RR MX Mail Exchangers
;  _____________________
;


;
;  RR A Name-to-Address Mapping
;  ____________________________

www             IN      A       132.248.120.137
;
;  RR CNAME Canonical Name (Alias)
;  _______________________________
;
ww2             IN      CNAME   www
```

Figura 3.3 Archivo de configuración

Donde se encuentran los RRs (*Resource Records) su formato es:*

[nombre] [TTL] [class] <type> <RDATA>

Donde:

- ***nombre**: Dominio o máquina a la cual se agrega un RR.*
- ***TTL**: Time to Live (tiempo de vida del registro).*
- ***Class**: tipo de red (IN, CHAOS).*
- ***Type**: Función del registro.*
- ***RDATA**: Datos del Registro.*

Los RRs (Resource Record) más conocidos son:

- **NS** (**N**ame **S**erver): Es el nombre de los servidores DNS tanto primarios como secundarios que se encuentran definidos dentro del archivo de zona es decir que disponen de la dirección y nombre para el dominio.
- **A** (**A**ddress)**:** Indica la dirección IP asociada al nombre host.
- **MX** (**M**ail E**x**changer)**:** Es el nombre del servidor encargado del correo en ese dominio así como la prioridad.
- **CNAME** (**C**anonical **Name**)**:** Indica cuál sea el nombre canónico de un alias.
- **PTR** (**P**oin**t**e**r**)**:** Host Name – Pointer Indica el dominio asociado a una dirección IP.
- **TXT** (**T**e**x**t)**:** – datos del Host arbitrariamente utilizados para las listas negras.
- **SOA** (**S**tart **of A**uthority) indica los datos de la autoridad para el domino o zona en cuestión, por lo que cada dominio deberá de existir.

Siendo el SOA el principal RRs porque contiene la siguiente información:

- ***Serial***: número de modificaciones que se realizaron a la tabla y debe de ser incrementada cada vez que se realicen cambios en los datos de la zona.de lo contrario el servidor no releerá la nueva información y el servidor secundario no se actualizara.

- ***Refresh*** es el intervalo de tiempo que cuenta desde la última vez que se realizo la actualización del archivo de zona en el Slave, es decir que desde la última actualización a partir tiene cierto tiempo para actualizar el Slave.

- ***Retry:*** es el tiempo que el secundario debe esperar para reintentar la actualización de la zona encaso de que falle la conexión al hacer el ***refresh.***

- ***Expire:*** tiempo después del cual si no se ha llegado a realizar la actualización se desecha la zona y el Slave deja de responder a actualizaciones y peticiones con respecto al dominio u zona.

- ***TTL***: Intervalo de tiempo asociado a cada uno de los RRs por cuánto tiempo guarda en cache el registro.

Como se muestra en la siguiente figura 3.4.

```
$TTL 2h
;
;  RR SOA Start of Authority
;  ------------------------
;
@       IN      SOA     kate.nic.unam.mx.       dns.unam.mx. (
                        2010081100              ; Serial   [yymmddss]
                        3600                    ; Refresh  [secs]
                        1200                    ; Retry    [secs]
                        604800                  ; Expire   [secs]
                        7200 )                  ; TTL      [secs]
;
```

Figura 3.4 Configuración SOA

Pero como no es solo la implementación que se tiene que realizar a un servidor de nombre de dominio conforme el tiempo han surgido problemas ya que existen diferentes vulnerabilidades que conforme el tiempo ha surgido y que ocasionan dificultades para la administración de DNS.

3.4 IMPLEMENTACIÓN DE EXTENSIONES DE SEGURIDAD

Para la administración del servidor de nombre de dominio necesitamos que este, pueda permitir la manipulación de él remotamente para ello es necesario configurar las llaves de RNDC.

3.4.1 RNDC

BIND incluye la utilidad llamada rndc, la cual permite la administración de línea de comandos del demonio named desde el host local o desde un host remoto. Para ello BIND utiliza dos puertos en sus comunicaciones, el 53 TCP, que se usa para las transferencias y el 53 UDP, que se utiliza para las consultas. Es necesario no aplicar reglas de cortafuegos sobre estos puertos si queremos que el servicio DNS funcione de forma correcta. Mientras que la herramienta rndc utiliza el puerto 953 UDP para el control remoto.

Para prevenir el acceso no autorizado al demonio named, BIND utiliza un método de clave secreta compartida para otorgar privilegios a hosts.

Esto es que si se utiliza utiliza una clave idéntica, estas se obtiene con el comando ***rndc-congen*** y debe estar presente en los archivos de configuración como son:

- **/etc/named.conf**
- **/etc/rndc.conf**

En la siguiente figura 3.5 se muestras el resultado al aplicar el comando.

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "D6CwiMmF474nHfhl/ZKBcw==";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-md5;
#       secret "D6CwiMmF474nHfhl/ZKBcw==";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
kate#
```

Figura 3.5 Llaves de rndc

Pero para el caso práctico están colocados en diferentes rutas como son:

- /var/named/etc/named.conf como se muestras en la siguientes figura 3.6.

```
# pwd
/var/named/etc
# ls
named-dual.conf       named.conf
named-simple.conf     root.hint
#
```

Figura 3.6 ubicación del archivo named.conf

La declaración *controls* permite a *rndc* conectarse desde un host local, como se observa en la siguiente figura 3.7.

```
options {
        version "";     // remove this to allow version querie

        listen-on    { any; };
        listen-on-v6 { any; };

        empty-zones-enable yes;

        allow-recursion { clients; };
};

logging {
        category lame-servers { null; };
};

key "rndc-key" {
       algorithm hmac-md5;
       secret "Qg1BmBbUXRY0zeONkWpYxg==";
};

controls {
       inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

Figura 3.7 declaración *controls* en el *named.conf*

En esta declaración le proporciona al documento named, que en el puerto 953 por TCP se encuentre a la escucha de la dirección loopback y que permita al comandos rndc provenientes del host local, autentificarse y realizar comunicación controlando al demonio named, si se proporciona la clave correcta.

- /etc/rndc.conf como se muestra en la siguiente imagen 3.8

```
# pwd
/etc
# cat rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "Qg1BmBbUXRY0zeONkWpYxg==";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf
#
```

Figura 3.8 rndc.conf

El valor <*key-name*> se relaciona con la declaración *key*, la cual está también en el archivo */etc/named.conf*

3.4.2 OPCIONES DE RNDC

El comando rndc tiene la siguiente forma:

rndc <*options*> <*command*> <*command-options*>

Están disponibles las siguientes opciones:

- **-c <*configuration-file*>** indica a rndc que use un archivo de configuración diferente a /etc/rndc.conf.
- **-p <*port-number*>** Especifica la utilización de un número de puerto diferente del predeterminado 953 para la conexión del comando rndc.
- **-s <*server*>** Indica a rndc que envié el comando a un servidor distinto al default-server especificado en su archivo de configuración.
- **-y <*key-name*>** Le permite especificar una clave distinta de la opción default-key en el archivo /etc/rndc.conf.

Y cuando se ejecuta rndc en una máquina local configurada de la forma correcta se pueden ejecutar los siguientes comandos:

- **halt** Detiene el servidor sin grabar los updates pendientes del servicio named.
- **querylog** Registra todas las peticiones de logueo hechas a este servidor de nombres.
- **refresh** Refresca la base de datos del servidor de nombres.
- **reload** Recarga los archivos de configuración de zona pero mantiene todas las respuestas precedentes situadas en caché. Esto le permite realizar cambios en los archivos de zona sin perder todas las resoluciones de nombres almacenadas.

  Si los cambios sólo afectaron una zona específica, vuelva a cargar una zona añadiendo el nombre de la zona después del comando reload.
- **stats** Descarga las estadísticas actuales de named al archivo /var/named/named.stats.
- **reconfig** relee la configuración y verificando toda el contenido actual.
- **stop** Graba los updates pendientes en archivo maestro y detiene al servidor, guardando todas las actualizaciones dinámicas y los datos de las transferencias de zona incremental (IXFR) antes de salir.

Para mayor información sobre estas opciones se puede consultar el manual de rndc.

Las llaves de rndc ayudan a los servidores de nombre de dominio a reconocer cuales son los servidores maestros o primarios ante los secundarios.

Para revisar que la sintaxis del archivo de configuración comprobando si hay errores del tipo de sintaxis o topográficos, se puede utilizar una herramienta llamada **named-checkconf** para comprobar servidor BIND DNS (nombre demonio), pero no puede comprobar si hay mal MX o una dirección asignada por nosotros. Sin embargo, esta es una herramienta excelente para solucionar problemas relacionados con el servidor DNS.

3.5 HERRAMIENTAS DE DIAGNÓSTICO

Para poder realizar, un monitoreo adecuado de los cambios y buen funcionamiento de los equipos, los administradores utilizan una serie de herramientas, que permiten consultar las operaciones realizadas por el equipo.

Algunas de estas herramientas, pueden ser descargadas de la red, dependiendo del sistema operativo que utilice el administrador, otras son creadas a partir de sus necesidades especificas.

Dentro de la amplia gama de opciones de herramientas, existen 3 herramientas básicas que son las más utilizadas por los administradores, PING, DIG y NSLOOKUP. A continuación se muestra una breve descripción y algunas opciones básicas de estas.

Nota: Las opciones de las herramientas dependen directamente del sistema operativo, en el cual se instalen y apliquen.

3.5.1 PING

Esta herramienta comprueba la conectividad a nivel red, de forma rápida la conexión entre 2 equipos. Su creador Mike Mususs, le asigno este nombre a esta herramienta, tomando en cuenta la opción de sonar para localizar un objeto.

Con ayuda de ping podremos determinar si el nivel de red funciona adecuadamente, así como los niveles físicos y de enlaces sobre los que descansa.

La forma básica de invocar a PING es:

ping <opcion> <ip>

Donde:

- **opción**: es el complemento de opciones a realizar, dentro de la herramienta. Algunas opciones son:

- **-c**: especifica el número de paquetes enviados.
- **-s**: tamaño del paquete enviado
- **-t:** especifica el tiempo de vida (tiempo de respuesta del paquete enviado)
- **ip**: dirección ip del equipo destinatario al que se le va a realizar el ping.

PING, trabaja bajo la funcionalidad "echo request" y "echo reply" del protocolo ICMP (Internet Control Message Protocol), donde, una entidad ICMP emisora envía un paquete pequeño, a un equipo destinatario, el cual es determinado por el usuario al momento de invocarlo, el ICMP del equipo destinatario, recibe el paquete y lo reenvía a la entidad emisora. Como se muestra en al siguiente figura 3.9.

```
# ping 132.248.10.1
PING 132.248.10.1 (132.248.10.1): 56 data bytes
64 bytes from 132.248.10.1: icmp_seq=0 ttl=62 time=0.768 ms
64 bytes from 132.248.10.1: icmp_seq=1 ttl=62 time=0.520 ms
64 bytes from 132.248.10.1: icmp_seq=2 ttl=62 time=0.557 ms
64 bytes from 132.248.10.1: icmp_seq=3 ttl=62 time=0.334 ms
64 bytes from 132.248.10.1: icmp_seq=4 ttl=62 time=0.608 ms
64 bytes from 132.248.10.1: icmp_seq=5 ttl=62 time=0.509 ms
64 bytes from 132.248.10.1: icmp_seq=6 ttl=62 time=0.411 ms
64 bytes from 132.248.10.1: icmp_seq=7 ttl=62 time=47.534 ms
--- 132.248.10.1 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.334/6.405/47.534/15.545 ms
#
```

Figura 3.9 Ejemplo de la herramienta ping

La salida del comando PING, nos muestra el nombre y la dirección IP del equipo al que se hace realiza el PING, además de la cantidad de datos que se envían en cada paquete (suelen ser por lo general 64 bytes), esta línea se repite en cada una de las respuestas a los paquetes enviados.
Esta herramienta se interrumpe con las teclas Ctrl. + C, al finalizar muestra una pequeña estadística basada en el número de paquetes enviados y recibido.

3.5.2 DIG (DOMAIN INFORMATION GROPER)

DIG, es una herramienta que realiza consultas de diversos tipos a un DNS. Esta herramienta, muestra las respuestas recibidas de acuerdo a la pregunta realizada. Es muy útil para detectar problemas en la configuración de los DNS debido a su claridad, flexibilidad y facilidad de uso.

La herramienta DIG tiene dos modos de invocarse: comando modo-simple línea para preguntas simples o múltiples, y el modo batch para la lectura de peticiones lookup de un archivo.

La forma básica de invocar a DIG es:

dig <servidor> <nombre> [tipo]

Donde:

- **Servidor:** es el nombre o la dirección IP del servidor a consultar.
- **Nombre:** es el nombre de dominio del record por el cual se quiere preguntar.
- **Tipo:** es el tipo del record por el que se consulta (ANY, NS, SOA, MX, etc.). De no indicarse un tipo especifico, dig asumirá el tipo A.

Algunas opciones básicas de DIG son:

- **@:** Especifica los servidores DNS que son utilizados en cada pregunta. Si no se provee un nombre especifico de Servidor, DIG intenta con cada servidor listado en el /etc/resolv.conf.

- **-h:** muestra la ayuda del comando.
- **-x:** hace consultas inversas, o sea, a partir de las direcciones IP determina nombres de dominio.
- **-f <filename>**: toma las consultas a partir de un fichero. Estas se definen una por línea y con la misma sintaxis que en la línea de comando.
- **-b <dirección>:** indica la dirección IP a partir de la cual se realizará la consulta dado el caso en que se tenga más de una interfaz de red configurada.

La sintaxis de esta herramienta en modo **–** simple línea es:

dig [servidor] [opciones] [nombre] [tipo] [clase] [opciones de consulta]

La sintaxis de esta herramienta en modo batch es:

dig [servidor-global] [opciones-d-global] dominio [servidor] [opciones] [q-opciones] [q-tipo] [q-clase] [dominio [servidor][opciones] [q-opciones] [q-tipo] [q-clase] [...]]

Las opciones de preguntas de dominio global controlan las búsquedas y despliegan los resultados de preguntas múltiples y afectan todas las preguntas.

Nota: Cada conjunto global de opciones de pregunta deben ser sobrescritas por cada conjunto de opciones de pregunta, por cada pregunta individual

En la salida de esta herramienta, hay una serie de campos identificados con una serie de letras. Estas letras indican la información específica, con respecto a la consulta realizada, no todas estas letras aparecen, en la salida arrojada por DIG.

Como se muestra en la siguiente figura 3.10.

```
jack# dig www.iingen.unam.mx

; <<>> DiG 9.4.2-P2 <<>> www.iingen.unam.mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.iingen.unam.mx.            IN      A

;; ANSWER SECTION:
www.iingen.unam.mx.     7200    IN      A       132.248.120.137

;; AUTHORITY SECTION:
iingen.unam.mx.         7200    IN      NS      kate.nic.unam.mx.
iingen.unam.mx.         7200    IN      NS      jack.nic.unam.mx.

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jun 29 17:21:32 2010
;; MSG SIZE  rcvd: 94

jack#
```

Figura 3.10 Ejemplo de la aplicación DIG

3.5.3 NSLOOKUP (*NAME SYSTEM LOOKUP*)

Es una herramienta que permite consultar un servidor de nombres para obtener información relacionada con el dominio o el host, así se diagnostica los eventuales problemas de configuración que pudieran haber surgido en el DNS. Basta con introducir el nombre de un dominio en la invitación de comando para detallar las características. De la misma manera, es posible solicitar información sobre un host indicando su nombre seguido del comando nslookup.

Nslookup tiene dos modos: interactivo y no interactivo.

- **Interactivo** este permite al usuario consultar servidores de nombres para obtener información sobre diversos huéspedes y dominios o para imprimir una lista de hosts en un dominio.

- **No interactivo** se utiliza para imprimir sólo el nombre y la solicitó información de un host o de dominio.

Su sintaxis es

nslookup[nombre | -] [-opciones] [servidor]

Para la forma interactiva

- **host [servidor]** Buscar información para el host utilizando el valor predeterminado actual servidor o utilizando el servidor.
- **Server** busca el servidor del dominio
- **lserver**: busca información acerca del dominio.
- **set [palabras] = valor** Este comando se utiliza para cambiar la información de estado que afecta a las búsquedas palabras como: **q= ns** busca la zona.

Nota: Las opciones de las herramientas dependen directamente del sistema operativo, en el cual se instalen y apliquen es recomendable revisar el manual.

Como por ejemplo la siguiente figura 3.11.

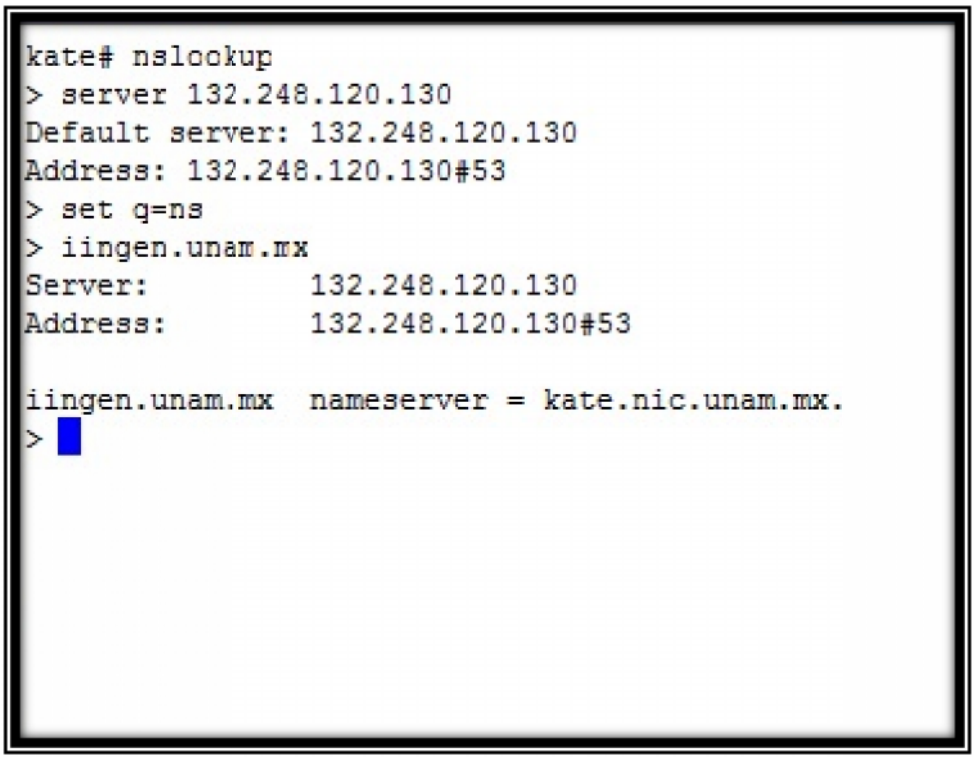


Figura 3.11 Ejemplo de Nslookup

3.6 TSIG

Para llevar a cabo la implementación de TSIG (Firma de transacción) es un protocolo que se define en el RFC 2845, se utiliza para proporcionar un medio de autenticación en la actualización de la base de datos en un DNS dinamico

TSIG utiliza para autentifica unas claves secretas mediante el one-way hashing para proporcionar medios seguro criptográficamente de identificación de cada punto final de una conexión, permitiendo realizar o responder a una actualización de DNS.

Aunque las consultas al DNS se pueden hacer de forma anónima, las actualizaciones de DNS deben ser autenticadas, puesto que al hacer cambios que duraderan en la estructura del sistema de nombres de Internet. El uso de

una clave compartida por el cliente que realiza la actualización y el servidor DNS garantiza la autenticidad de la solicitud de actualización.
Sin embargo, la solicitud de actualización se puede pasar sobre un canal inseguro. Una función unidireccional utilizada por one-way hashing se utiliza para prevenir los observadores malintencionados de aprendizaje de la clave secreta y usarla para hacer sus propias modificaciones.

Con la utilización de las funciones de hash, se permitirá asegurar que el que produce el mensaje es quien dice ser, y que el mensaje no ha sido alterado en un paso de la red.

Las actualizaciones de DNS, como consultas, que normalmente se transportan a través de UDP, ya que requiere menor sobrecarga que TCP. Sin embargo, los servidores DNS de apoyo tanto en las peticiones UDP y TCP.

“Para proporcionar la autenticación de clave secreta, se utiliza un nuevo tipo de RR cuya nemotécnica es TSIG y cuyo tipo de código es de 250. TSIG es un meta-RR y No debe ser almacenado en caché. TSIG RR´s se utilizan para la autenticación entre el DNS entidades que han establecido una clave secreta compartida. TSIG RR se ha calculado dinámicamente para cubrir una transacción de DNS.”[9]

3.6.1 GENERACIÓN DE LLAVES TSIG

Para la generación de llaves TSIG ocupa el algoritmo especificado en el RFC 1321 y 2104 “HMAC-MD5” para la aplicación de su operatividad, mediante la herramienta ***dnssec-keygen***.

Dnssec-keygen genera claves para DNSSEC especificado en el RFC 2535 y RFC 4034.A su vez también puede generar claves para su uso con TSIG (transacciones firmas), como definida en el RFC 2845.
Su sintaxis para TSIG es la siguiente.

[9] Tomado y traducido del rfc 2845

dnssec-keygen {-a algoritmo}{-b tamaño de la clave}{-n el tipo de nombre} nombre

A continuación explico las diferentes opciones:

- **- a algoritmo**: selecciona el algoritmo criptográfico a utilizar, para el caso de TSIG es obligatorio utilizar HMACMD5, eso especificado en el RFC 2845. Para el caso de DNSSEC se puede ocupar RSAMD5 (RSA) o RSASHA1, DSA, DH (Diffie-Hellman) o HMAC-MD5.

  Nota 1: que para DNSSEC se recomienda utilizar RSASHA -k.
- **-b el tamaño de la clave**: se especifica el número de bits en la clave. La elección del tamaño de la clave depende del algoritmo utilizado.

  RSAMD5 o RSASHA1 debe estar entre 512 y 2048 bits.

  DH(Diffie-Hellman) debe estar entre 128 y 4096 bits.

  DSA deben de ser entre 512 y 1024 bits y con exactitud de múltiplo de 64.

  HMAC-MD5 debe estar entre 1 y 512 bits.
- **-n tipo de nombre**: se especifica el tipo de propietario de la clave, es decir el valor de tipo de nombre o de ZONA (para una clave de zona DNSSEC(CLAVE / DNSKEY)), HOST o entidad (por una clave asociada con una gran cantidad (KEY)), usuario (por una clave asociada a unausuario (KEY)) u otros (DNSKEY). Estos valores son insensible.

Como se muestra en la siguiente figura 3.12.

```
kate# dnssec-keygen -a hmac-md5 -b 128 -n user rndc
Krndc.+157+30333
```

Figura 3.12 implementación de TSIG

En la imagen al momento de dar el comando nos proporciona dos llaves como son:

Krndc.+157+30333.key
Krndc.+157+30333.private

Como se muestra en la siguiente figura 3.13

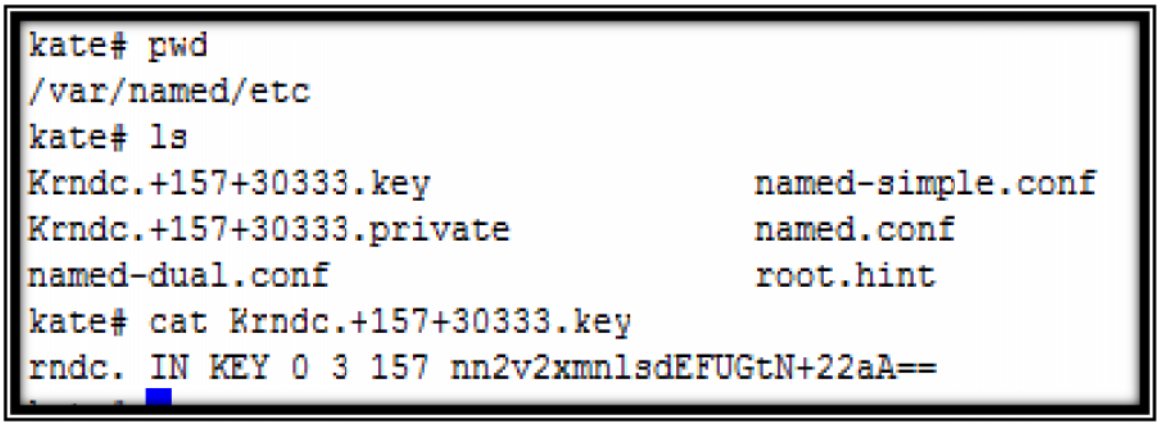


Figura 3.13 Llaves de TSIG obtenidas

La llave proporcionada un formato, el significado de cada campo se describe en el RFC 1035 como se muestra en la siguiente tabla 3.14.

Campo	Bytes	Descripción
NOMBRE	max 256	Nombre de clave, que debe ser único en el cliente y el servidor
TIPO	2	TSIG (250)
CLASE	2	CUALQUIER (255)
TTL	4	0 (desde que los registros TSIG no debe ser almacenado en caché)
RDLENGTH	2	Duración de la RDATA campo
RDATA	variable	Estructura que contiene la fecha y hora, el algoritmo de hash y datos

Tabla 3.14 Campos de registro de TSIG

Por los que rndc. IN KEY 0 3 157 nn2v2xmnlsdEFUGtN+22aA== siendo la última la llave que se anexara a el archivo named.conf del servidor primario o maestro como se muestra en la figura 3.15 y del secundario o esclavo como se observa en la figura 3.16.

```
//Pruebas dnssec

key kate.secreta.jack {
        algorithm hmac-md5;
        secret "nn2v2xmnlsdEFUGtN+22aA==";
};

server 132.248.120.129 {
        keys {kate.secreta.jack.;};
};

zone "iingen.unam.mx" {
        type master;
        file "master/iingenunam";
        allow-transfer {key kate.secreta.jack.;};
};

zone "120.248.132.in-addr.arpa" {
        type master;
        file "master/inverso248/120.132";
        allow-transfer {key kate.secreta.jack.;};
};
```

Figura 3.15 implementación de TSIG en el DNS maestro

```
//Pruebas dnssec

key kate.secreta.jack {
        algorithm hmac-md5;
        secret "nn2v2xmnlsdEFUGtN+22aA==";
};

sever 132.248.120.130 {
        keys {kate.secreta.jack.;};
};

zone "iingen.unam.mx" {
        type slave;
        file "slave/iingenunam";
        masters {132.248.120.130;};
};

zone "120.248.132.in-addr.arpa" {
        type slave;
        file "slave/120.132";
        masters {132.248.120.130;};
```

Figura 3.16 Implementación de TSIG en el DNS secundario o esclavo

3.7 GENERACIÓN DE LLAVES DNSSECBIS

En el anterior capítulo dnssecbis provee la integridad de datos, incluyendo mecanismos para verificación de negación de existencia.

Existen dos tipos de llaves llamadas:

- KSK solo es utilizada en la firma de ZSK, ya que el nodo padre valida la autenticidad de la llave KSK del hijo, esta llave se considera de mayor cantidad de bist
- ZSK es una llave que se utiliza para la firma de registros de la zona, es más sencillo porque su actualización es local.

Como se muestra en la siguiente figura 3.17

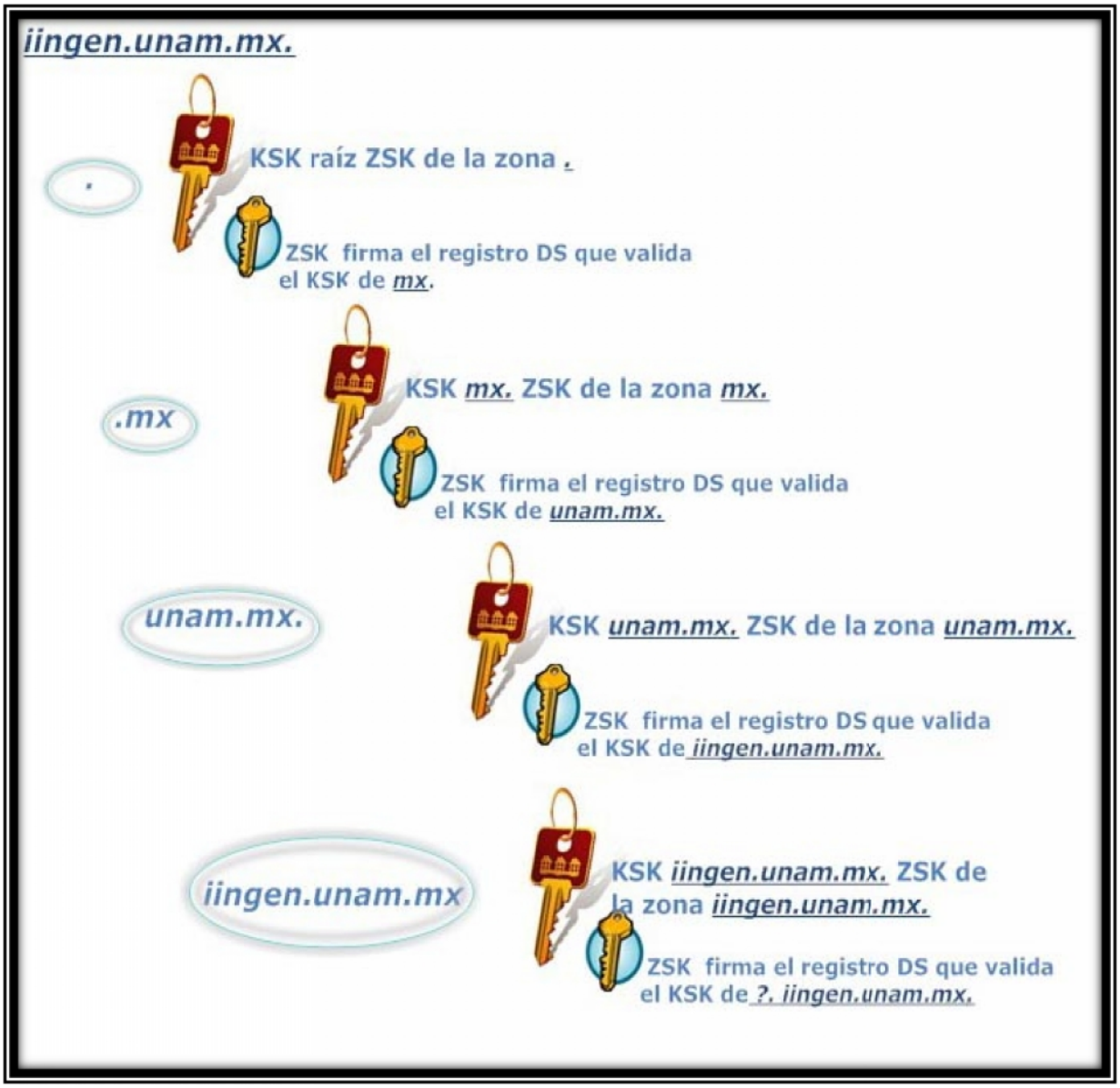


Figura 3.17 Estructura de firmas KSK y ZSK

Los servidores que resuelven mediante dnssec esta constituye la cadena de autenticación desde la raíz de la jerarquía hasta la zona.

Pero debido que aun no está completa la firma desde la raíz, se decidió realizar la firma desde unam.mx ya que se está realizando las pruebas en los servidores mx. y no se cuenta con su KSK.

Por esta razón realizaremos las pruebas en los servidores de la Universidad Nacional Autónoma de México (UNAM) creando así una isla de confianza. Para ello se llevara a cabo la firma DNSKEY, RRSIG y NEC.

3.7.1 DNSKEY

El RR de DNSSEY contiene la llave pública se utiliza para firmar, esta se obtiene con el siguiente comando:

dnssec-keygen –a RSASHA1 –b 512 –n Zone iingen.unam.mx para ZSK y
dnssec-keygen –a RSASHA1 –b 512 –f ksk –n Zone iingen.unam.mx para KSK

Como se menciona anteriormente se especifica que se utilizara el algoritmo RSASHA1 con 512 bits si ampliáramos mas bits el sistema se volvería muy lento por la generación de claves.
Donde contiene:

- Banderas del archivo donde indica el tipo de llave existen dos tipos 256 para ZSK y consultas como se muestra en la siguiente figura 3.18

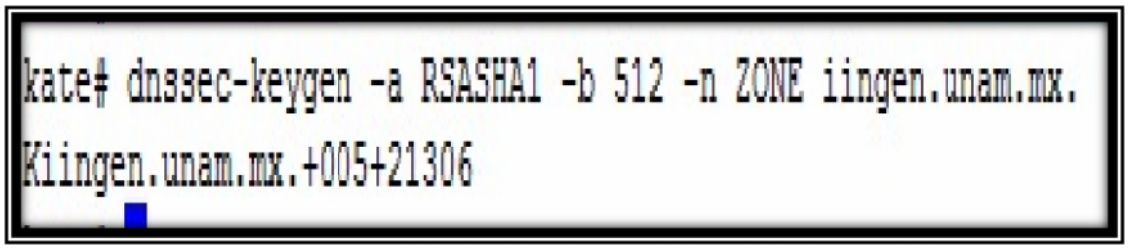


Figura 3.18 Generación de llave DNSKEY ZSK

Este entrega dos archivos que son
Kiingen.unam.mx.+005+21306.key figura 3.19.

Kiingen.unam.mx.+005+21306.private

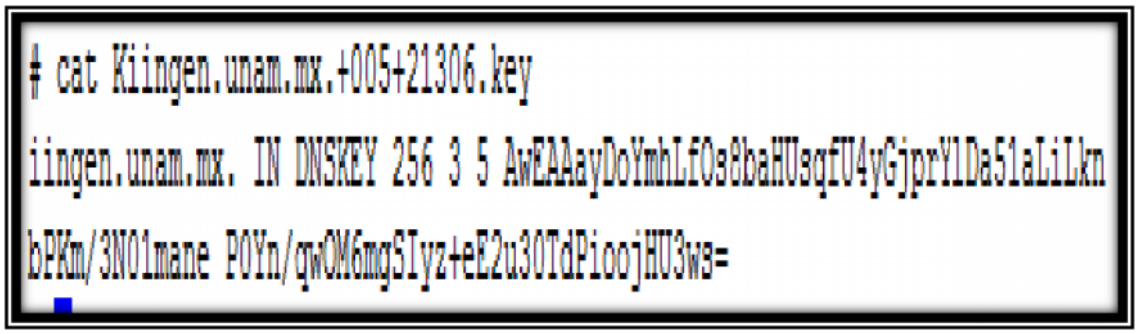


Figura 3.19 ZSK Kiingen.unam.mx.+005+21306.key

257 para KSK y consultas donde se entregan los siguientes archivos: Kiingen.unam.mx.+005+12604.key como se muestra en la siguiente figura 3.20 Kiingen.unam.mx.+005+12604.private

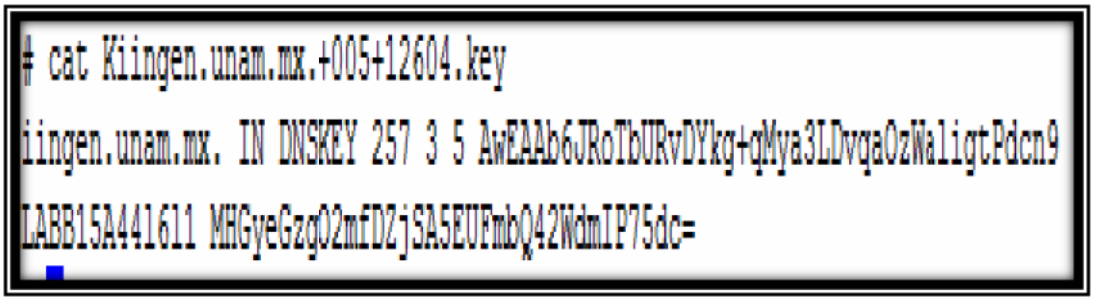


Figura 3.20 SKS Kiingen.unam.mx.+005+21306.key

Este entrega dos archivos que son:

- El protocolo del archivo que tiene de valor 3
- El algoritmo del archivo donde se indica el tipo de algoritmo para generar la llave como se muestra en la siguiente tabla 3.21

Valor	Algoritmo	Status
0	Reservado	
1	RSA7MD5[RSAMD5]	No recomandado
2	Diffie-Herllman[DH]	
3	DSA/SHA-1 [DSA]	Opcional
4	Eliptic Curve [ECC]	
5	RSA/SHA-1[RSASHA1]	Mandatorio
252	Indirect [INDIRECT]	
253	Private[PRIVATEDNS]	Opcional
254	Private[PRIVATEOID]	Opcional
255	reservado	

Tabla 3.21 algoritmos para emplear

- La publicación de la llave del archivo en base 64

Esta será clocada en el archivo de configuración como se observa en la siguiente figura 3.22.

```
$TTL 2h
;
;  RR SOA Start of Authority
;  ------------------------
;
@       IN      SOA     kate.nic.unam.mx.       dns.unam.mx. (
                        2010081100              ; Serial  [yymmddss]
                        3600                    ; Refresh [secs]
                        1200                    ; Retry   [secs]
                        604800                  ; Expire  [secs]
                        7200 )                  ; TTL     [secs]
;

;Llave DNS KEY  ZSK

iingen.unam.mx. IN DNSKEY 256 3 5 AwEAAayDoYmhLfOs8baHUsqfU4yGjprYlDa51aLiLknbPK
m/3N01mane POYn/qwOM6mgSIyz+eE2u30TdPioojHU3ws=

;Llave DNS KEY KSK

iingen.unam.mx. IN DNSKEY 257 3 5 AwEAAb6JRoTbURvDYkg+qMya3LDvqaOzWaligtPdcn9LAB
```

Figura 3.22 Implementación de DNSKEY en archivo de resolución

Y al momento de consultar la base de datos con la herramienta dig nos muestra la firma que se realizó como se observa en la siguiente figura 3.23.

```
kate# dig @132.248.120.130 iingen.unam.mx dnskey

; <<>> DiG 9.4.2-P2 <<>> @132.248.120.130 iingen.unam.mx dnskey
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46905
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;iingen.unam.mx.                        IN      DNSKEY

;; ANSWER SECTION:
iingen.unam.mx.         7200    IN      DNSKEY  256 3 5 AwEAAayDoYmhLfOs8baHUsqf
U4yGjprYlDa51aLiLknbPKm/3N01mane P0Yn/qwOM6mgSIyz+eE2u30TdPioojHU3ws=
iingen.unam.mx.         7200    IN      DNSKEY  257 3 5 AwEAAb6JRoTbURvDYkg+qMya
3LDvqaOzWaligtPdcn9LABB15A441611 MHGyeGzgO2mfDZjSA5EUFmbQ42WdmIP75dc=

;; AUTHORITY SECTION:
iingen.unam.mx.         7200    IN      NS      kate.nic.unam.mx.
iingen.unam.mx.         7200    IN      NS      jack.nic.unam.mx.

;; Query time: 1 msec
;; SERVER: 132.248.120.130#53(132.248.120.130)
```

Figura 3.23.Consuta de DNSKEY

3.7.2 RRSIG

Es un archivo que contiene la firma digital que valida a otros registros o RR Mediante el siguiente comando Dnssec-sigzone –o zona-k llave zona ZSK.

Generando así un archivo, como se muestra en la siguiente figura 3.24.

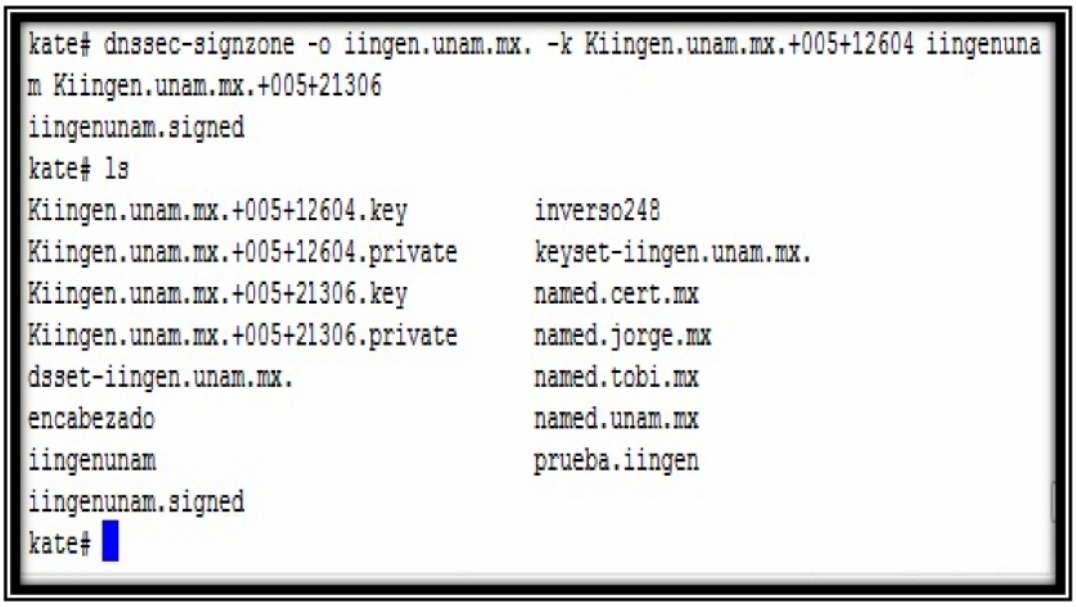


Figura 3.24.Implementación RRSIG

El nuevo archivo a consultar es iingen.unam, después de ejecutar el comando se creó el siguiente archivo iingenunam.signed donde firma todas los RR que se encuentran configurados como se observa en la siguiente figura 3.25.

```
; File written on Fri Aug 13 13:02:11 2010
; dnssec_signzone version 9.4.2-P2
iingen.unam.mx.         7200    IN SOA  kate.nic.unam.mx. dns.unam.mx. (
                                        2010081100 ; serial
                                        3600       ; refresh (1 hour)
                                        1200       ; retry (20 minutes)
                                        604800     ; expire (1 week)
                                        7200       ; minimum (2 hours)
                                        )
                        7200    RRSIG   SOA 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        X9bBDUmYufjs9ImihAFm6Jgf3ncDASWDm9tZ
                                        sSEUMYF7K8m0mzWVqv5EfiYd793vqOP2/EOw
                                        1aOoCPliX6u6NQ== )
                        7200    NS      kate.nic.unam.mx.
                        7200    NS      jack.nic.unam.mx.
                        7200    RRSIG   NS 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        lVIdmco8P0ppDUbOC+hnBN1nzaSFt7vsRUSl
                                        Xo/eIzjj4OZgGhJikHqVGjxjwzBn9ucgnbyn
                                        9rTo7/+FH/uipg== )
                        7200    NSEC    ww2.iingen.unam.mx. NS SOA RRSIG NSEC DNSKEY
                        7200    RRSIG   NSEC 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        nF2LeC1+R4txo5BviP+vasF9We1oQA97FEN3
                                        iV5PoURuHoic9YbLqnFPejOzSE0ZWqUo+1Gz
                                        zVjqvMGly111rg== )
                        7200    DNSKEY  256 3 5 (
                                        AwEAAayDoYmhLfOs8baHUsqfU4yGjprYlDa5
                                        1aLiLknbPKm/3N01manePOYn/qwOM6mgSIyz
                                        +eE2u30TdPioojHU3ws=
                                        ) ; key id = 21306
                        7200    DNSKEY  257 3 5 (
                                        AwEAAb6JRoTbURvDYkg+qMya3LDvqaOzWali
                                        gtPdcn9LABB15A441611MHGyeGzgO2mfDZjS
                                        A5EUFmbQ42WdmIP75dc=
                                        ) ; key id = 12604
                        7200    RRSIG   DNSKEY 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
iingenunam.signed 52%
```

Figura 3.25 archivo firmado por RRSIG

CONCLUSIONES

CONCLUSIONES

En el presente trabajo se puede observar que la seguridad al 100% no existe y ni existirá porque la tecnología cambia día a día y las necesidades de los usuarios también.

Una implementación de medidas de seguridad han sido de años atrás el buscar las extensiones al protocolo de DNS, el no documentar, el no tener fija la meta han logrado que dicha implementación no se logre.

Las extensiones de seguridad a los Servidores de Nombre de Dominio, es lograr la seguridad e integridad mediante el firmado de *Resource Records*.
Y DNSSEC es sólo el firmar los *Resource Records* que no es más que la base de datos que conforman un Servidor de Nombres de Dominio, pero es importante no dejar a un lado a TISG o RNDS que como se vio son también claves de seguridad que se brindan al servidor de nombre de dominio y también son parte de las extensiones de seguridad, por lo que yo considero que todo en conjunto es realmente las extensiones de seguridad a DNS y no sólo DNSSEC como se maneja.

Ya que RNDS sea para la autentificación remota de los servidores, TSIG para la autentificación de servidores de una forma dinámica y DNSSEC para la integridad de la base de datos que contiene se puede, aunque este conjunto de medidas son manejadas por separado.

El protocolo DNSSEC no se ha logrado a su totalidad la implementación dado que se tiene que firmar desde la raíz (.) es decir desde los root servers y empezar a compartir la firma a las diferentes etiquetas como por ejemplo se tiene que www.ingenieria.unam.mx.

En este caso la llave que es generada por los root server y que le asignan a .mx. conocida como ZSK, para después que ésta genere sus llaves privada y pública ésta proporcionara su llave publica a NIC México, para que obtenga

éste la firma de la etiqueta .mx y a su vez comparte ZSK con nic UNAM para que firme la etiqueta unam.mx y a su vez firme todas las dependencias que se encuentran a cargo como es ingenieria.unam.mx.

Todo esto se tiene que realizar para que se concluya en su totalidad pero dado que existe una infinidad de direcciones es laborioso realizar la implementación.
Y tomando en cuenta que se realizó un cambio en la dirección y ahora es www.ingenieria.unam.mx se tiene que hacer todo lo anterior para realizar la firma al registro.

En la Universidad Nacional Autónoma de México se le asigno el segmento de red 132.248 y 132.247 y próximamente a liberar ipv6 se tiene una infinidad de dependencias exteriores a la cual se le brinda servicio, así como interiores como facultades, posgrados, centro de investigación, preparatorias, cch y entre otras, es laborioso realizar dicha implementación.

Lo que yo propondría es que se realice un análisis de las facultades que han tenido problemas de phising, o problemas con sus URLS para generar la llave de DNSSEC para que el usuario que consulta la página conosca realmente la página que está explorando está dentro de la base de datos, es la que realmente se visualiza y esto se logrará mediante la aparición de un candado en la parte superior.

Pero dicha prueba no pudo ser realizada, el visualizar el candado en la parte de la URL, ya que por problemas del equipo que no permitió la configuración debido a que se debe configurar en una red que no contenga firewall ya que no permitía confirmar de la implementación, aunado que se necesita realizar en los DNS que tiene la Universidad Nacional de México con todos los permisos de responder y autorizados por NIC UNAM.

Solo quedaría la seguridad, que el administrador de la red le proporcione a sus cuarto de telecomunicación así como del personal sea el encargado de tenga

las medidas adecuadas del equipo que es asignada la ip, porque solo con DNSSEC se garantizaría que la ip con etiqueta está en la base de datos, pero no se hace responsable del equipo.

DNSSEC es un protocolo funcional que sólo es cuestión de analizar el equipo, Sistema Operativo y que base de datos contendrá

Con esto se reforzaría la transferencia de zonas de los DNS con la utilización de las llaves de encriptación proporcionando una mayor seguridad, garantizando que el conjunto de subdominios que se encuentran bajo unam.mx revisando su autenticidad.

ANEXOS

ANEXO1 RAÍZ DE BASE DE DATOS DE ZONA

La raíz de la Zona de base de datos representa los datos de delegación de dominios de nivel superior, incluidos los gTLD como". COM", y el código de dominios de nivel superior del país, tales como “. Reino Unido". Como el gerente de la zona raíz de DNS, IANA es responsable de la coordinación de estas delegaciones, de conformidad con sus políticas y procedimientos.

Gran parte de esta información también está disponible a través del protocolo WHOIS en whois.iana.org .

Dominio	Tipo	Objetivo / Organización Patrocinadora
. AC	country-code	Isla de la Ascensión Red de Centros de Información (Registro de dominio de CA) c / o Cable and Wireless (Isla de la Ascensión)
. AD	country-code	Andorra Andorra Telecom
. AE	country-code	Emiratos Árabes Unidos Reglamentación de las Telecomunicaciones (TRA)
. AERO	patrocinado	Reservados para los miembros de la industria del transporte aéreo Société Internationale de Aeronáutica de Telecomunicaciones (SITA INC EE.UU.)
. AF	country-code	Afganistán Secretaría de Comunicaciones y TI
. AG	country-code	Antigua y Barbuda UHSA la Facultad de Medicina
. AI	country-code	Anguila Gobierno de Anguila
. AL	country-code	Albania Electrónica y Comunicaciones Autoridad Postal - AKEP
. AM	country-code	Armenia Internet Society
. AN	country-code	Antillas Holandesas (retirado) Universidad de las Antillas Neerlandesas
. AO	country-code	Angola Faculdade de Engenharia da Universidade Agostinho Neto
. AQ	country-code	La Antártid Mott y Asociados
. AR	country-code	Argentina MRECIC (Ministerio de Relaciones Exteriores, Comercio Internacional y Culto)
. ARPA	infraestructura	Reservados exclusivamente para apoyar operativamente crítica de infraestructura identificador de espacios según las recomendaciones de la Junta de Arquitectura de Internet Asignación de Números de Internet

Dominio	Tipo	Objetivo / Organización Patrocinadora
. AS	country-code	Samoa Americana Como registro de dominio
. ASIA	patrocinado	Limitado a la Pan-Asia y la comunidad Asia-Pacífico DotAsia Organización Ltd.
. A	country-code	Austria Verwaltungs NIC.AT Internet und mbH Betriebsgesellschaft
. UA	country-code	Australia . Au Administración del Dominio (de auDA)
. AW	country-code	Aruba SETAR
. AX	country-code	Islas Aland Ålands landskapsregering
. AZ	country-code	Azerbaiyán Intrans
. BA	country-code	Bosnia y Herzegovina De universidades Telinformatic Centro (UTIC)
. BB	country-code	Barbados Gobierno de Barbados Ministerio de Economía y Desarrollo Telecomunicaciones Unidad
. BD	country-code	Bangladesh Ministerio de Correos y Telecomunicaciones Bangladesh Secretaría
. SER	country-code	Bélgica DNS BE vzw / asbl
. BF	country-code	Burkina Faso DELGI Informática Generale Delegacional
. BG	country-code	Bulgaria Register.BG
. BH	country-code	Bahrein BATELCO
. BI	country-code	Burundi Centro Nacional de Informática
. BIZ	genéricos con restricción	Restringidos para los negocios NeuStar, Inc.
. BJ	country-code	Benin Oficinas de Correos y Telecomunicaciones
. BL	country-code	Saint-Barthélemy No asignado
. BM	country-code	Bermudas Registro General Ministerio de Trabajo e Inmigración
. BN	country-code	Brunei Darussalam Jabato Telekom Brunei
. BO	country-code	Bolivia Agencia Para El Desarrollo de la Información de la Sociedad en Bolivia

Dominio	Tipo	Objetivo / Organización Patrocinadora
. BQ	country-code	Bonaire, San Eustaquio y Saba-
. BR	country-code	Brasil Comite Gestor da Internet no Brasil
. BS	country-code	Bahamas El Colegio de las Bahamas
. BT	country-code	Bhután Ministerio de Información y Comunicaciones
. BV	country-code	Isla Bouvet UNINETT Norid A / S
. BW	country-code	Botswana Universidad de Botswana
. POR	country-code	Belarús Abrir contacto Ltd.
. BZ	country-code	Belice Universidad de Belice
. CA	country-code	Canadá Autoridad de Registro de Internet de Canadá (CIRA) Autorite Canadienne pour les enregistrements Internet (IECA)
. CAT	patrocinado	Reservado para la comunidad lingüística y cultural catalán Fundació puntCAT
. CC	country-code	Cocos (Keeling) ENIC Cocos (Keeling) Islas Pty. Inc. d / b / a de Servicios Isla de Internet
. CD	country-code	Congo, República Democrática del Congo NIC - SARL Interpunto
. CF	country-code	República Centroafricana Société Centrafricaine de Telecomunicaciones (SOCATEL)
. CG	country-code	Congo ONPT Congo y Suiza Interpunto
. CH	country-code	Suiza SWITCH La educación suiza y la Red de Investigación
. IC	country-code	Cote d'Ivoire INP-HB Institut Nacional Polytechnique Houphouet Boigny Felix
. CK	country-code	Islas Cook Telecom Islas Cook Ltd.
. CL	country-code	Chile NIC Chile (Universidad de Chile)
. CM	country-code	Camerún Camerún Telecomunicaciones (CAMTEL)
. NC	country-code	China Academia China de Ciencias La Red de Centros de Informática
. CO	country-code	Colombia . CO Internet SAS

Dominio	Tipo	Objetivo / Organización Patrocinadora
. COM	genéricos	Genéricos de nivel superior de dominio Servicios de VeriSign Global Registry
. COOP	patrocinado	Reservado para las asociaciones cooperativas DotCooperation LLC
. RC	country-code	Costa Rica Academia Nacional de Ciencias Academia Nacional de Ciencias
. CU	country-code	Cuba CENIAInternet Industria y San José Capitolio Nacional
. CV	country-code	Cabo Verde Das Comunicações Agência Nacional (ANAC)
. CW	country-code	Curaçao-
. CX	country-code	Isla de Navidad Isla de Navidad de Internet Administration Limited
. CY	country-code	Chipre Universidad de Chipre
. CZ	country-code	República Checa CZ.NIC, zspo
. DE	country-code	Alemania DENIC eG
. DJ	country-code	Djibouti Djibouti Telecom SA
. DK	country-code	Dinamarca Dansk Foro de Internet
. DM	country-code	Dominica DotDM Corporation
. NO	country-code	República Dominicana Pontificia Universidad Católica Madre y Maestra Recinto Santo Tomás de Aquino
. DZ	country-code	Argelia CERIST
. CE	country-code	Ecuador NIC.EC (NICEC) SA
. EDU	patrocinado	Reservado para las instituciones de enseñanza postsecundaria acreditado por una agencia del Departamento de Educación de EE.UU. la lista de las agencias de acreditación reconocidos a nivel nacional EDUCAUSE
. EE	country-code	Estonia Instituto Nacional de Física Química y Biofísica
. EG	country-code	Egipto Red de Universidades de Egipto (EUN) Supremo Consejo de Universidades
. EH	country-code	Sáhara Occidental No asignado

Dominio	Tipo	Objetivo / Organización Patrocinadora
. ER	country-code	Eritrea Corporación de Servicios de Telecomunicaciones de Eritrea (EriTel)
. ES	country-code	España Red.es
. ET	country-code	Etiopía Corporación de Telecomunicaciones de Etiopía
. UE	country-code	La Unión Europea EURid vzw / asbl
. FI	country-code	Finlandia Comunicaciones Finlandés Autoridad Regulatoria
. FJ	country-code	Fiji La Universidad del Pacífico Sur Servicios de TI
. FK	country-code	Islas Malvinas (Falkland) Gobierno de las Islas Malvinas
. FM	country-code	Micronesia, Estados Federados de Corporación de Telecomunicaciones de Estados Federados de Micronesia
. FO	country-code	Islas Feroe Por el Consejo
. FR	country-code	Frange AFNIC (Francia NIC) - Immeuble Internacional
. GA	country-code	Gabón Gabón Telecom
. GB	country-code	Reino Unido Dominio Reservados - IANA
. GD	country-code	Granada La Comisión Reguladora Nacional de Telecomunicaciones (NTRC)
. GE	country-code	Georgia Caucasus Online
. GF	country-code	Francés Guayana Neto más
. GG	country-code	Guernesey Isla Networks Ltd.
. GH	country-code	Ghana Red Informática de Sistemas Limitada
. IG	country-code	Gibraltar Zafiro Redes
. GL	country-code	Groenlandia TELE Greenland A / S
. GM	country-code	Gambia GM-NIC
. GN	country-code	Guinea Centro Nacional de las Ciencias Pesqueras de Boussoura

Dominio	Tipo	Objetivo / Organización Patrocinadora
. GOB	patrocinado	Reservados exclusivamente para el Gobierno de los Estados Unidos Administración de Servicios Generales Attn: QTDC, 2E08 (. Registro de Dominios gov)
. GP	country-code	Guadalupe Grupo de Redes de Tecnologías
. GQ	country-code	Guinea Ecuatorial GETESA
. GR	country-code	Grecia ICS-Forth GR
. GS	country-code	Georgia del Sur e Islas Sandwich del Sur Gobierno de Georgia del Sur e Islas Sandwich del Sur (GSGSSI)
. GT	country-code	Guatemala Universidad del Valle de Guatemala
. GU	country-code	Guam Universidad de Guam Centro de Cómputo
. GW	country-code	Guinea-Bissau Fundación IT & MEDIA de la Universidad Bissao
. GY	country-code	Guyana Universidad de Guyana
. HK	country-code	Hong Kong Hong Kong Corporación Registro Internet Ltd.
. HM	country-code	Islas Heard y McDonald SM el Registro de Dominio
. HN	country-code	Honduras Red de Desarrollo Sostenible Honduras
. HR	country-code	Croacia CARNet - Red Académica y de Investigación de Croacia
. HT	country-code	Haití Consorcio FDS / RDDH
. HU	country-code	Hungría Consejo de Proveedores de Internet húngaro (CHIP)
. ID	country-code	Indonesia Mikroelektronika IDNIC-ppau
. IE	country-code	Irlanda University College Dublin Servicios Informáticos Centro de Cálculo
. IL	country-code	Israel Internet Society de Israel
. IM	country-code	Isla de Man Isla de Man Gobierno
. EN	country-code	La India Nacional del Mercado de Internet de la India

Dominio	Tipo	Objetivo / Organización Patrocinadora
. INFO	genéricos	Genéricos de nivel superior de dominio Afilias Limited
. INT	patrocinado	Sólo se utiliza para el registro de las organizaciones establecidas por tratados internacionales entre gobiernos Asignación de Números de Internet
. / S	country-code	Territorio Británico del Océano E / S del registro de dominio de nivel superior Cable and Wireless
. IQ	country-code	Irak Comisión de Comunicaciones y Medios de Comunicación (CMC)
. IR	country-code	Irán, República Islámica del Instituto de Investigación en Ciencias Fundamentales
. ES	country-code	Islandia ISNIC - Islandia Internet ltd.
. TI	country-code	Italia IIT - CNR
. JE	country-code	Jersey Isla de Redes (Jersey) Ltd.
. JM	country-code	Jamaica Universidad de las Indias Occidentales
. JO	country-code	Jordania Nacional de Información Centro de Tecnología (NTIC)
JOBS.	patrocinado	Reservado para los gerentes de recursos humanos Emplear los medios de comunicación LLC
. JP	country-code	Japón Servicios de Registro de Japón Co., Ltd.
. KE	country-code	Kenya Red de Kenia Centro de Información (Kenic)
. KG	country-code	Kirguistán AsiaInfo Empresa de Telecomunicaciones
. KH	country-code	Camboya Ministerio de Correos y Telecomunicaciones
. KI	country-code	Kiribati Ministerio de Comunicaciones, Transporte, Turismo y Desarrollo
. KM	country-code	Comoras Comoras Telecom
. KN	country-code	Saint Kitts y Nevis Ministerio de Finanzas, Información y Tecnología para el Desarrollo Sostenible
. PK	country-code	Corea, República Popular Democrática de Corea del Centro de Cómputo
. KR	country-code	Corea del Sur Corea del Internet y la Agencia de Seguridad (KISA)

Dominio	Tipo	Objetivo / Organización Patrocinadora
. KW	country-code	Kuwait Ministerio de Comunicaciones
. KY	country-code	Las Islas Caimán La información y la Autoridad de Tecnología de las Comunicaciones
. KZ	country-code	Kazajstán Asociación de Empresas de TI de Kazajstán
. LA	country-code	República Democrática Popular Lao Lao Comité Nacional de Internet (LANIC) Ciencia Tecnología y Medio Ambiente
. LB	country-code	Líbano Universidad Americana de Beirut Computación y Servicios de red
. LC	country-code	Santa Lucía Universidad de Puerto Rico
. LI	country-code	Liechtenstein Hochschule Liechtenstein
. LK	country-code	Sri Lanka Consejo para la Tecnología de la Información LK Secretario de dominio
. LR	country-code	Liberia Datos de Technology Solutions, Inc.
. LS	country-code	Lesotho Universidad Nacional de Lesotho
. LT	country-code	Lituania Universidad Tecnológica de Kaunas Tecnología de la Información del Instituto de Desarrollo
. LU	country-code	Luxemburgo Restena
. LV	country-code	Letonia Universidad de Letonia Instituto de Matemáticas y Ciencias de la Computación Departamento de Soluciones de red (DNS)
. LY	country-code	Jamahiriya Árabe Libia General de Correos y la Empresa de Telecomunicaciones
. MA	country-code	Marruecos Agencia Nacional de Telecomunicaciones réglementation des (ANRT)
. MC	country-code	Mónaco Gouvernement de Mónaco Dirección de Comunicaciones des Electroniques
. MD	country-code	Moldova, República de MoldData SE
. ME	country-code	Montenegro Gobierno de Montenegro
. MF	country-code	San Martín (parte francesa) No asignado

Dominio	Tipo	Objetivo / Organización Patrocinadora
. MG	country-code	Madagascar NIC-MG (Red de Información Centro de Madagascar)
. MH	country-code	Las Islas Marshall Oficina del Gabinete
. MIL	Patrocinado	Reservados exclusivamente para los militares de Estados Unidos Red Centro de Información del Departamento de Defensa
. MK	country-code	Macedonia, Antigua República Yugoslava de Ministerio de Relaciones Exteriores
. ML	country-code	Malí SOTELMA
. MM	country-code	Myanmar Ministerio de Comunicaciones, Correos y Telégrafos
. MN	country-code	Mongolia Para comunicación de datos Co., Ltd.
. MO	country-code	Macao Universidad de Macao
. MOBI	Patrocinado	Reservado para los consumidores y los proveedores de productos y servicios móviles mTLD Top Level Domain dba limitada dotMobi
. MP	country-code	Islas Marianas del Norte Para comunicación de datos Saipan, Inc.
. MQ	country-code	Martinica SYSTEL
SR.	country-code	Mauritania Universidad de Nouakchott
. MS	country-code	Montserrat MNI Networks Ltd.
. MT	country-code	Malta NIC (Malta)
. MU	country-code	Mauricio Directo a internet Ltd
.MUSEUM	patrocinado	Reservado para los museos Museo de la Asociación de Gestión de Dominio
. MV	country-code	Maldivas SA de Dhiraagu. Ltd. (DHIVEHINET)
. MW	country-code	Malawi Malawi Desarrollo Sostenible Programa de redes (Malawi PRDS)
. MX	country-code	México NIC-México ITESM - Campus Monterrey
. MI	country-code	Malasia MYNIC Berhad
. MZ	country-code	Mozambique Centro de Informática de la Universidad Eduardo Mondlane

Dominio	Tipo	Objetivo / Organización Patrocinadora
. NA	country-code	Namibia Red de Namibia Centro de Información
.NAME	genéricos con restricción	Reservado para las personas VeriSign Information Services, Inc.
.NC.	country-code	Nueva Caledonia Oficina de Correos y Telecomunicaciones
. NE	country-code	Níger SONITEL
. NET	genéricos	Genéricos de nivel superior de dominio Servicios de VeriSign Global Registry
. NF	country-code	Isla Norfolk Norfolk Isla de los servicios de datos
. GN	country-code	Nigeria Internet Nigeria Registro de Asociación
. NI	country-code	Nicaragua Universidad Nacional del Ingernieria Centro de Computo
. NL	country-code	Países Bajos Stichting Nederland Internet Domeinregistratie
. NO	country-code	Noruega UNINETT Norid A / S
. NP	country-code	Nepal Mercantil de Comunicaciones SA. Ltd.
. NR	country-code	Nauru CENPAC NET
. NU	country-code	Niue La Fundación IUSN
. NZ	country-code	Nueva Zelanda InternetNZ
. OM	country-code	Omán Compañía de Telecomunicaciones de Omán
. PF	country-code	Polinesia francés Ministère des Postes et Télécommunications et des Sports, encargado des Nouvelles Technologies de l'information
. PG	country-code	Papua Nueva Guinea PNG absoluto de Administración Los rectores de Office La Universidad de Papua Nueva Guinea de Tecnología
. PH	country-code	Filipinas PH Fundación de dominio
. PK	country-code	Pakistán PKNIC
. PL	country-code	Polonia Red de Investigación y Computación Académica
. PM	country-code	San Pedro y Miquelón AFNIC (Francia NIC) - Immeuble Internacional

Dominio	Tipo	Objetivo / Organización Patrocinadora
. PN	country-code	Pitcairn Isla Pitcairn Administración
. PR	country-code	Puerto Rico Gauss Research Laboratory Inc.
. PRO	genéricos con restricción	Limitado a los profesionales acreditados y entidades relacionadas Registro de la Corporación de Servicios dba RegistryPro
. PS	country-code	Territorio palestino, ocupado Ministerio de Telecomunicaciones y Tecnología de la Información, Gobierno de Centro de Cómputo.
. PT	country-code	Portugal Fundación para a Computação Científica Nacional
. PW	country-code	Palau Micronesia de Inversiones y la Corporación de Desarrollo
. PY	country-code	Paraguay NIC-PY
. QA	country-code	Qatar El Consejo Supremo de la Información y Tecnología de la Comunicación (ictQATAR)
. RE	country-code	Reunión AFNIC (Francia NIC) - Immeuble Internacional
. RO	country-code	Rumania Instituto Nacional de I + D en Informática
. RS	country-code	Serbia Registro Nacional de Serbia Los nombres de dominio (RNIDS)
. RU	country-code	Federación de Rusia Centro de Coordinación para la empresa ferroviaria TLD
. RW	country-code	Rwanda Congo NIC - SARL Interpunto
. SA	country-code	Arabia Saudita Comisión de Comunicaciones y Tecnología de la Información
. SB	country-code	Las Islas Salomón Salomón de la empresa Telekom Limitada
. SC	country-code	Seychelles VCS Pty Ltd
. SD	country-code	Sudán Sudán Internet Society
. SE	country-code	Suecia La Fundación de la Infraestructura de Internet
. SG	country-code	Singapur Red Centro de Información México (SGNIC) Pte Ltd
. SH	country-code	Santa Elena Gobierno de Santa Elena

Dominio	Tipo	Objetivo / Organización Patrocinadora
. SI	country-code	Eslovenia Académicas y de investigación de redes de Eslovenia (ARNES)
. SJ	country-code	Svalbard y Jan Mayen UNINETT Norid A / S
. SK	country-code	Eslovaquia SK-NIC, como
. SL	country-code	Sierra Leona Sierratel
. SM	country-code	San Marino Telecom Italia SpA San Marino
. SN	country-code	Senegal Université Cheikh Anta Diop NIC Senegal
. SO	country-code	Somalia Ministerio de Correos y Telecomunicaciones
. SR	country-code	Suriname Telesur
ST.	country-code	Santo Tomé y Príncipe Tecnisys
. UB	country-code	Unión Soviética (retirado) Instituto Ruso para el Desarrollo de las Redes Públicas (ROSNIIROS)
. SV	country-code	El Salvador SVNet Col. Medica El Dr. Emilio Alvarez
. SX	country-code	Sint Maarten (parte holandesa)-
. SY	country-code	República Árabe Siria Telecomunicaciones Establecimiento Siria (STE)
. SZ	country-code	Swazilandia Universidad de Swazilandia Departamento de Ciencias de la Computación
. TC	country-code	Islas Turcas y Caicos Melrex TC
. TD	country-code	Chad Société des télécommunications du Tchad (Chad SOTEL)
. TEL	patrocinado	Reservado para las empresas y las personas a publicar sus datos de contacto Telnic Ltd.
. TF	country-code	Francés tierras australes AFNIC (Francia NIC) - Immeuble Internacional

Dominio	Tipo	Objetivo / Organización Patrocinadora
. TG	country-code	Togo Servicio de Informática y Telecomunicaciones
. TH	country-code	Tailandia Información de Red Tailandesa Fundación Centro
. TJ	country-code	Tayikistán Centro de Información de Tecnología
. CC.TT.	country-code	Tokelau Corporación de Telecomunicaciones de Tokelau (Teletok)
. TL	country-code	Timor-Leste Ministerio de Infraestructura División de Información y Tecnología
. TM	country-code	Turkmenistán Registro de Dominio TM Ltd
. TN	country-code	Túnez Agence Tunisienne d'Internet
. A	country-code	Tonga Gobierno del Reino de Tonga SAR el Príncipe de la Corona Tupouto'a c / o Consulado de Tonga
. TP	country-code	Timor Portugués (retirado) -
. TR	country-code	Turquía Medio Oriente de la Universidad Técnica Departamento de Ingeniería Informática
.TRAVEL	patrocinado	Reservado para las entidades cuyo principal ámbito de actividad es en el sector de los viajes Registro Tralliance Management Company, LLC.
. TT	country-code	Trinidad y Tobago Universidad de las Indias Occidentales Facultad de Ingeniería
. TV	country-code	Tuvalu Ministerio de Hacienda y Turismo
. TW	country-code	Taiwan Red Centro de Información de Taiwán (TWNIC)
. TZ	country-code	Tanzania, República Unida de Tanzania Network Information Centre (tzNIC)
. UA	country-code	Ucrania Los sistemas de comunicación Ltd
. UG	country-code	Uganda Uganda Online Ltd.
. Reino Unido	country-code	Reino Unido Nominet Reino Unido

Dominio	Tipo	Objetivo / Organización Patrocinadora
. UM	country-code	Estados Unidos Islas Menores No asignado
. EE.UU.	country-code	De los Estados Unidos NeuStar, Inc.
. UY	country-code	Uruguay SeCIU - Universidad de la República
. UZ	country-code	Uzbekistán Tecnologías de informatización y de la Información Centro de Desarrollo UZINFOCOM
. VA	country-code	Santa Sede (Ciudad del Vaticano) Santa Sede Secretaría de Estado Oficina de Internet de la Santa Sede
. VC	country-code	San Vicente y las Granadinas Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria
. VE	country-code	Venezuela, República Bolivariana de Centro Nacional de Tecnologias de Información
. VG	country-code	Islas Vírgenes Británicas Evolución Pinebrook Ltd
. VI	country-code	Islas Vírgenes, EE.UU. Islas Vírgenes Sistema Telcommunications Pública c / o Servicios de Internet COBEX
. VN	country-code	Viet Nam Ministerio de Información y Comunicaciones de la República Socialista de Viet Nam
. VU	country-code	Vanuatu Telecom Vanuatu Limitada
. WF	country-code	Wallis y Futuna AFNIC (Francia NIC) - Immeuble Internacional
. WS	country-code	Samoa Gobierno de Samoa Ministerio de Relaciones Exteriores
.测试 test:zh-Hans	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.परीक्षा test:hi-Deva	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.испытание test:ru-Cyrl	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.테스트 test:ko-Hang	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet

Dominio	Tipo	Objetivo / Organización Patrocinadora
.טעסט test:yi-Hebr	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.中国 zhongguo:zh-Hans	country-code	China Internet de China Network Information Center
.中國 zhongguo:zh-Hant	country-code	China Internet de China Network Information Center
._____ lanka:si-Sinh	country-code	Sri Lanka LK Registro de Dominio
.測試 test:zh-Hant	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.عش‌یآزما test:fa-Arab	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.பரிட்சை test:ta-Taml	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.香港 hongkong:zh-Hans	country-code	Hong Kong Hong Kong Corporación Registro Internet Ltd.
.δοκιμή test:el-Grek	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.اختبـــار test:ar-Arab	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
.台湾 taiwan:zh-Hans	country-code	Taiwán, Provincia de China Red Centro de Información de Taiwán (TWNIC)
.台灣 taiwan:zh-Hant	country-code	Taiwán, Provincia de China Red Centro de Información de Taiwán (TWNIC)
.امارات emarat:ar-Arab	country-code	Emiratos Árabes Unidos Autoridad de Regulación de Telecomunicaciones (TRA)
.الاردن alordon:ar-Arab	country-code	Jordania Nacional de Información Centro de Tecnología (NTIC)
.السـعودية alsaudiah:ar-Arab	country-code	Arabia Saudita Comisión de Comunicaciones y Tecnología de la Información
.ไทย thai:th-Thai	country-code	Tailandia Información de Red Tailandesa Fundación Centro

Dominio	Tipo	Objetivo / Organización Patrocinadora
.рф rf:ru-Cyrl	country-code	Federación de Rusia Centro de Coordinación para la empresa ferroviaria TLD
.تونس tunis:ar-Arab	country-code	Túnez Agence Tunisienne d'Internet
.مصر misr:ar-Arab	country-code	Egipto Autoridad Nacional de Reglamentación de las Telecomunicaciones - NTRA
.قطر qatar:ar-Arab	country-code	Qatar Supremo Consejo para las Comunicaciones y Tecnologías de la Información (ictQATAR)
.இலங்கை llangai:ta-Taml	country-code	Sri Lanka LK Registro de Dominio
.فلسطين falasteen:ar-Arab	country-code	Territorio palestino, ocupado Ministerio de Telecomunicaciones y Tecnología de la Información (MTIT)
.テスト test:ja-Kana	prueba	Reservado para pruebas de nombres de dominio internacionalizados Asignación de Números de Internet
. YE	country-code	Yemen TeleYemen
. YT	country-code	Mayotte AFNIC (Francia NIC) - Immeuble Internacional
. ZA	country-code	Sudáfrica ZA Nombre de Dominio Autoridad
. ZM	country-code	Zambia ZAMNET Sistemas de Comunicación SL
. ZW	country-code	Zimbabwe Correos y Telecomunicaciones de la Autoridad Reguladora de Zimbabwe (POTRAZ)

BIBLIOGRAFÍA

BIBLIOGRAFÍA

LIBROS

- Albitz, Paul, Liu, Cricket. "*DNS AND BIND*", Editorial O'Reilly, Estados Unidos, 4ª edición, 2001.
- Albitz, Paul, Liu, Cricket. "*DNS AND BIND*", Editorial O'Reilly, Estados Unidos, 3ª edición, 1998.
- Kabelova Alena "*DNS IN ACTION A DETAILED AND PRACTICAL GUIDE TO DNS IMPLEMENTATION, CONFIGURATION AND ADMINISTRATION*" Editorial Packt publishing Birmingham- Mumbai
- López Barrientos Ma. Jaquelina "*CRIPTOGRAFÍA*", Universidad Nacional Autónoma de México, Facultad de Ingeniera, División de ingeniera eléctrica departamento de computación, 2009
- Tanenbaum, Andrew. "SISTEMAS OPERATIVOS MODERNOS", Editorial Prentice Hall, México, 1ª edición, 1993.

LISTA DE FIGURAS

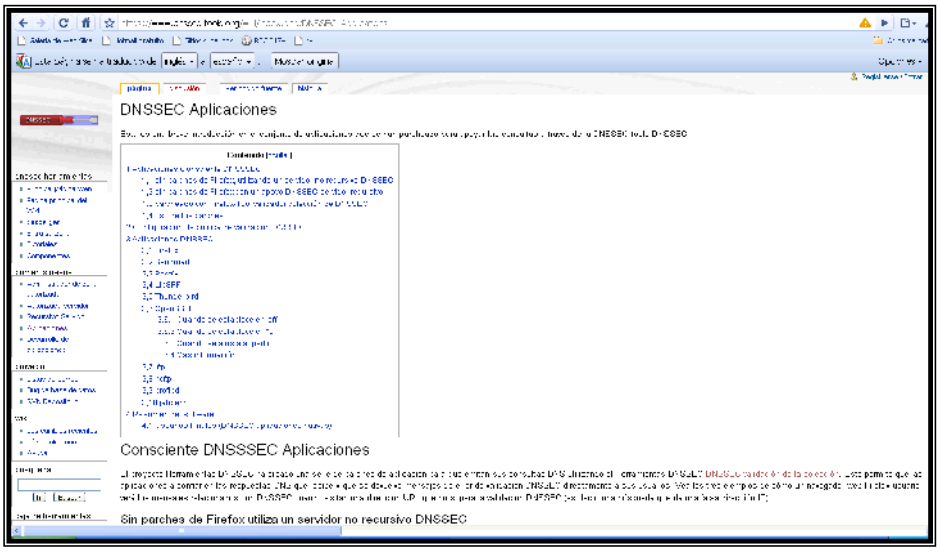
- Figura 1 Fuente: [19 de mayo del 2010 http://inza.wordpress.com/2008/10/page/2/
- Figura 2 Fuente: [19 de mayo del 2010http://www.andymeneely.com/blog/science/computer-security/public-key-cryptography/#more-95
- Figura 1.3 Fuente: [04 de Abril 2010 http://www.outono.net/elentir/?p=606]
- Figura 1.6 Fuente: [04 de Abril 2010 http://library.thinkquest.org/07aug/01676/spanish/downtheages_wars_toolsanddevices_jeffersonswheel.html]
- Figura 1.7 Fuente http://redyseguridad.fi-p.unam.mx/pp/aldo/criptografia/notasclase/tema_4.pdf

- Figura 1.10 Fuente http://redyseguridad.fi-p.unam.mx/pp/aldo/criptografia/notasclase/tema_4.pdf
- Figura 1.11 Fuente: http://www.inf.utfsm.cl/~rmonge/seguridad/cripto-03-bn.pdf 16 de junio del 2010
- Figura 1.15 Imagen tomada de Criptografía por Ing Ma. Jaquelina López Barrientos página 233
- Figura 1.16 Imagen tomada de Criptografía por Ing Ma. Jaquelina López Barrientos página 238

MESOGRAFÍA

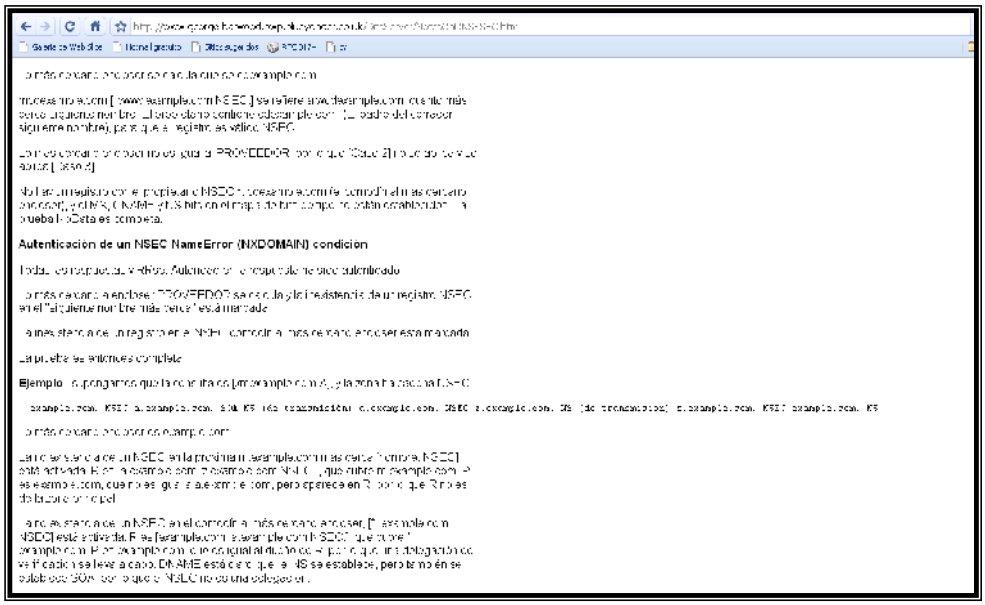
Fuente 8 de Junio del 2010
http://www.internetnews.com/security/article.php/3758566/Is+DNSSEC+the+Answer+to+Internet+Security.htm

https://www.dnssec-tools.org/wiki/index.php/DNSSEC_Applications

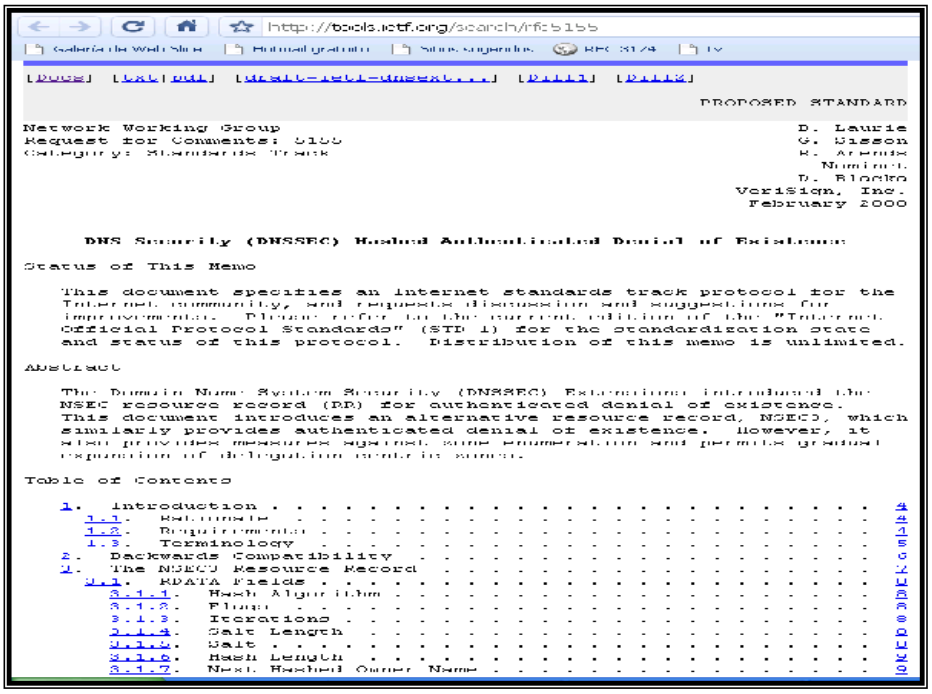


http://www.linuxsecurity.com/content/view/117551/49/

http://www.george-barwood.pwp.blueyonder.co.uk/DnsServer/NotesOnDNSSSEC.htm



http://tools.ietf.org/search/rfc5155



Network Working Group
Request for Comments: 5155

D. Laurie
G. Sisson
R. Arends
Nominet
D. Blacka
VeriSign, Inc.
February 2008

DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

Status of This Memo

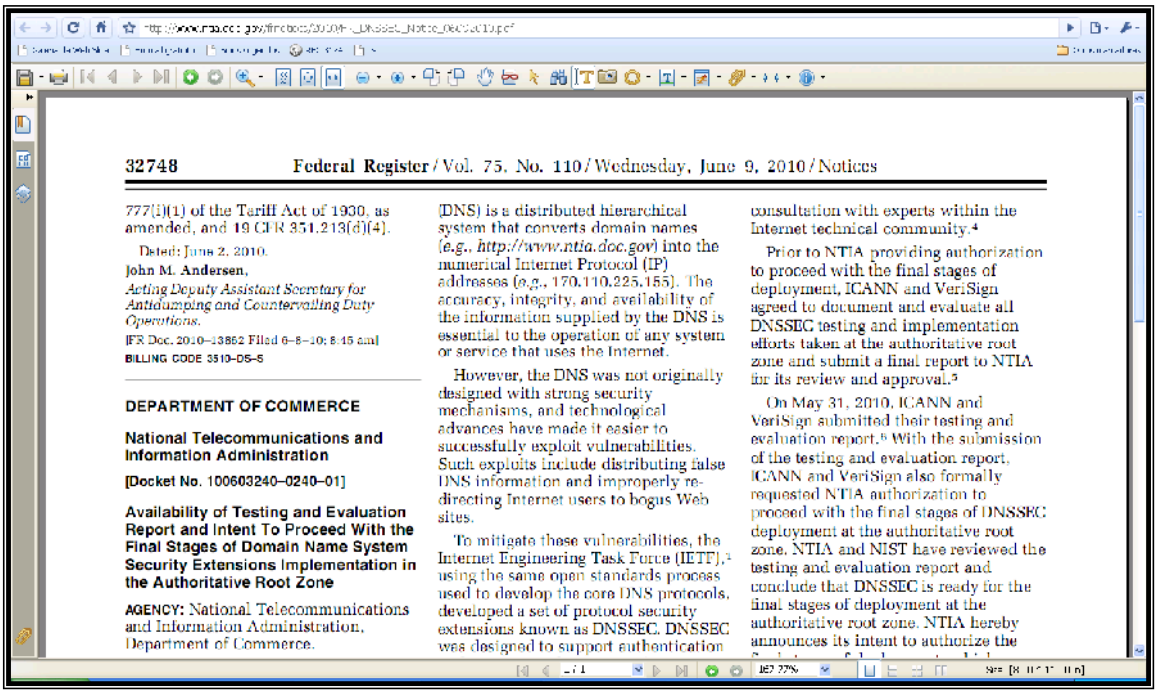
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Domain Name System Security (DNSSEC) Extensions introduced the NSEC resource record (RR) for authenticated denial of existence. This document introduces an alternative resource record, NSEC3, which similarly provides authenticated denial of existence. However, it also provides measures against zone enumeration and permits gradual expansion of delegations using Opt-Out.

Table of Contents

http://www.ntia.doc.gov/frnotices/2010/FR_DNSSEC_Notice_06092010.pdf



32748 Federal Register / Vol. 75, No. 110 / Wednesday, June 9, 2010 / Notices

777(i)(1) of the Tariff Act of 1930, as amended, and 19 CFR 351.213(d)(4).

Dated: June 2, 2010.

John M. Andersen,

Acting Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.

[FR Doc. 2010–13862 Filed 6–8–10; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 100603240–0240–01]

Availability of Testing and Evaluation Report and Intent To Proceed With the Final Stages of Domain Name System Security Extensions Implementation in the Authoritative Root Zone

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

(DNS) is a distributed hierarchical system that converts domain names (*e.g., http://www.ntia.doc.gov*) into the numerical Internet Protocol (IP) addresses (*e.g.*, 170.110.225.155). The accuracy, integrity, and availability of the information supplied by the DNS is essential to the operation of any system or service that uses the Internet.

However, the DNS was not originally designed with strong security mechanisms, and technological advances have made it easier to successfully exploit vulnerabilities. Such exploits include distributing false DNS information and improperly re-directing Internet users to bogus Web sites.

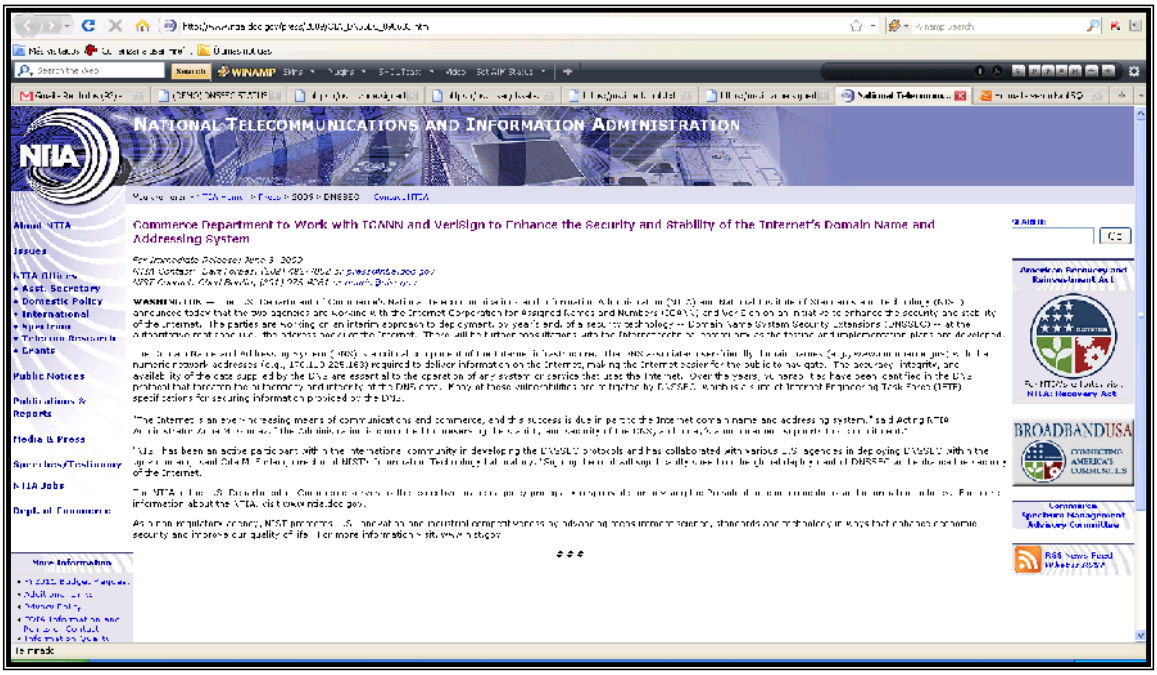
To mitigate these vulnerabilities, the Internet Engineering Task Force (IETF),[3] using the same open standards process used to develop the core DNS protocols, developed a set of protocol security extensions known as DNSSEC. DNSSEC was designed to support authentication

consultation with experts within the Internet technical community.[4]

Prior to NTIA providing authorization to proceed with the final stages of deployment, ICANN and VeriSign agreed to document and evaluate all DNSSEC testing and implementation efforts taken at the authoritative root zone and submit a final report to NTIA for its review and approval.[5]

On May 31, 2010, ICANN and VeriSign submitted their testing and evaluation report.[6] With the submission of the testing and evaluation report, ICANN and VeriSign also formally requested NTIA authorization to proceed with the final stages of DNSSEC deployment at the authoritative root zone. NTIA and NIST have reviewed the testing and evaluation report and conclude that DNSSEC is ready for the final stages of deployment at the authoritative root zone. NTIA hereby announces its intent to authorize the

http://www.ntia.doc.gov/press/2009/OIA_DNSSEC_090603.html



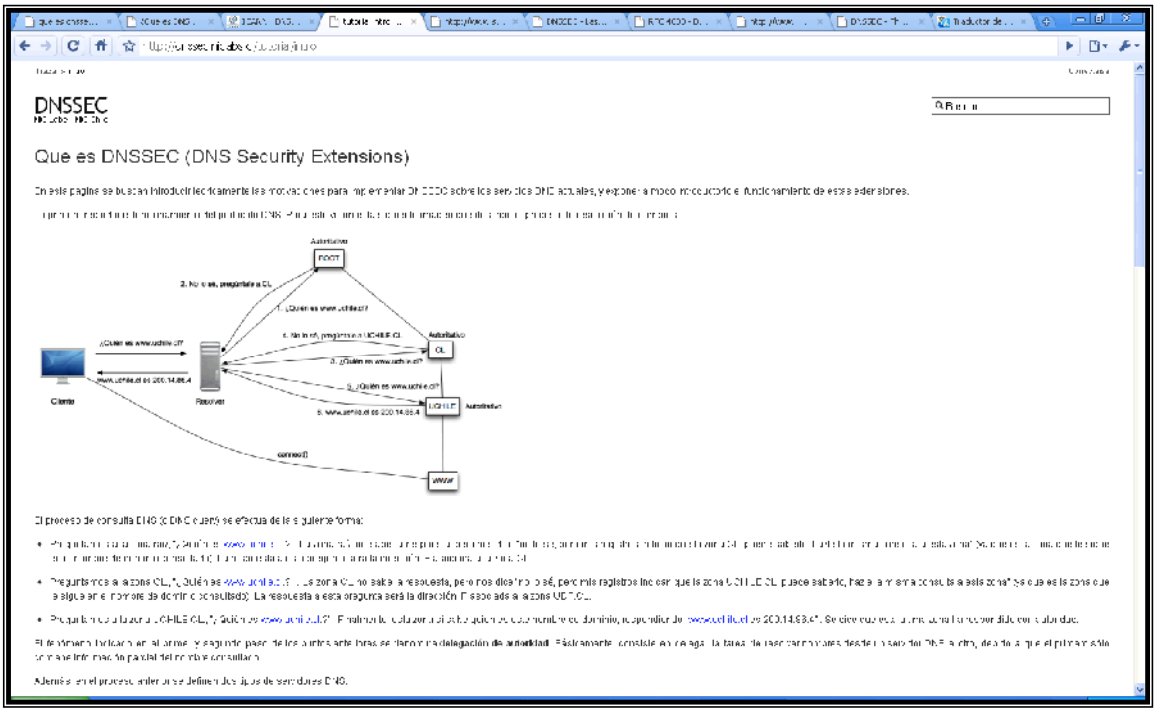
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Commerce Department to Work with ICANN and VeriSign to Enhance the Security and Stability of the Internet's Domain Name and Addressing System

13 de julio del 2010

Descritpcion breve de que es dnssec http://teleobjetivo.org/blog/que-es-dnssec.html

http://dnssec.niclabs.cl/tutorial/intro



http://www.saulo.net/des/DNSSEC-pre.pdf

Descripción de dnssesc con la implementación explicada paso a paso

http://www.codigolibre.org/index.php?view=article&catid=91:practicas&id=5221:dns&option=com_content

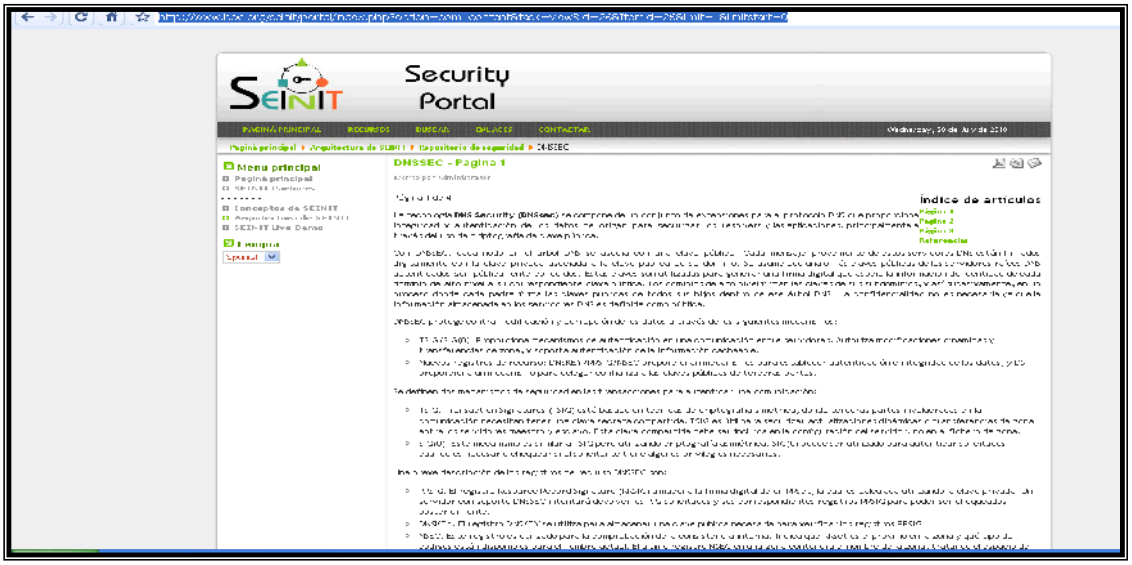
Como configurar un dns y los componentes que tiene

Periódico el universal se da de alta la zona .eu y .org

http://www.eluniversal.com.mx/articulos/59265.html

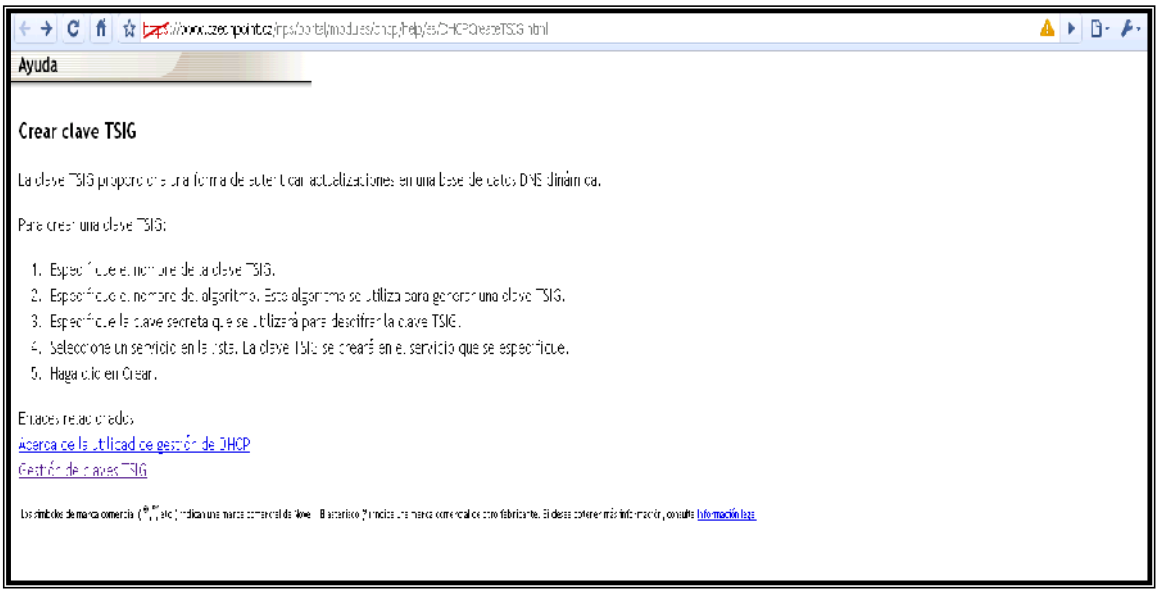
Descripción de DNSSEC 27 de julio del 2010

http://www.isoc.org/seinit/portal/index.php?option=com_content&task=view&id=26&Itemid=26&limit=1&limitstart=0



TSIG descripción del protocolo

https://www.czechpoint.cz/nps/portal/modules/dhcp/help/es/DHCPCreateTSIG.html



Descripción del protocolo TSIG

http://www.worldlingo.com/ma/enwiki/es/TSIG

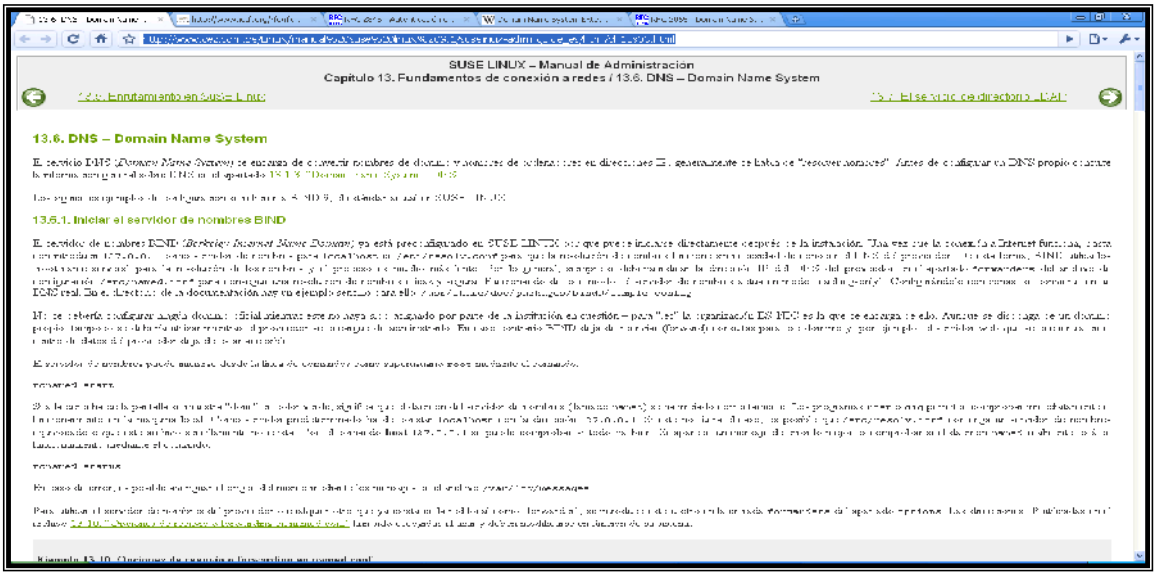
DNSSEC cadenas de confianza publicación que presenta el cómo funciona DNSSEC

http://www.linux-magazine.es/issue/41/058-064DNSSECLM41.pdf

2 de julio del 20 10

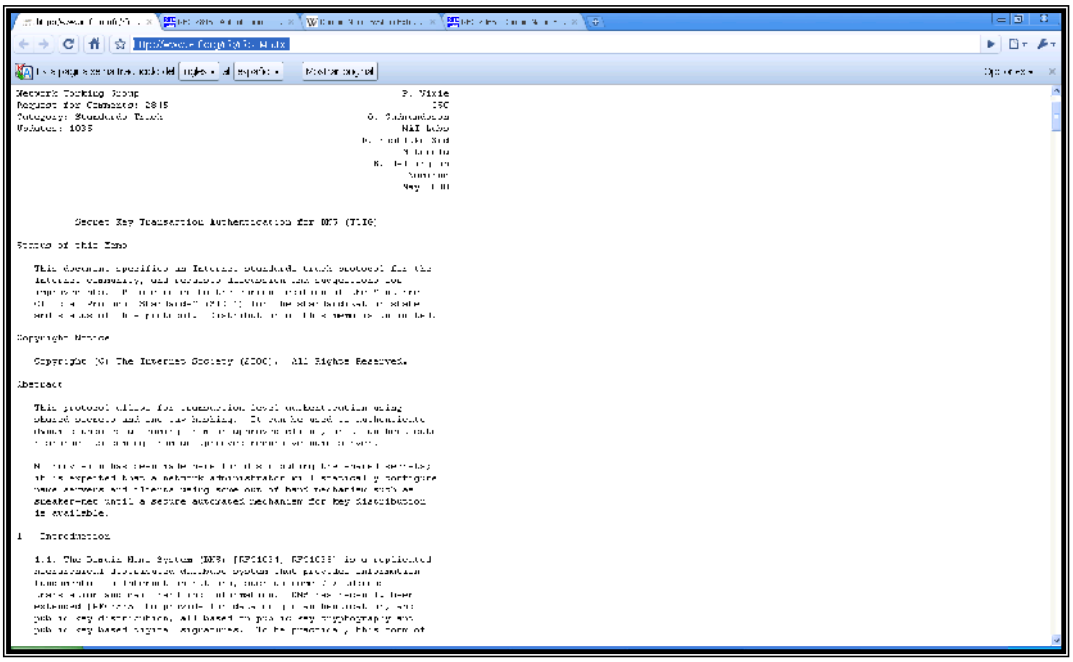
Descripción del DNS

http://www.cez.com.pe/Linux/manual%20suse%20linux%209.1/suselinux-adminguide_es/html/ch13s06.html



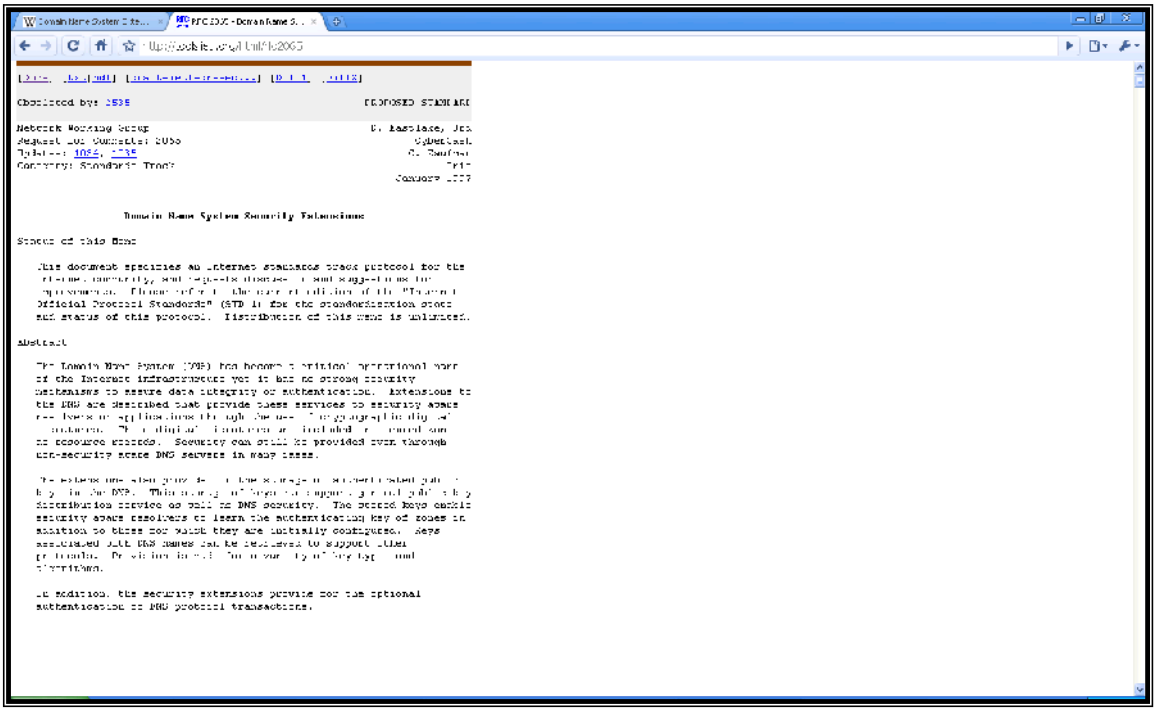
RFC 2845 descripción del protocolo RNDSIG

http://www.ietf.org/rfc/rfc2845.txt



Primera publicación del protocolo DNSSEC en el RFC 2065

http://tools.ietf.org/html/rfc2065



http://www.cs.jhu.edu/~ateniese/papers/dnssec.pdf
http://net.educause.edu/ir/library/pdf/EST1001.pdf
http://www.ripe.net/training/dnssec/material/dnssec.pdf
http://www.dnssec.net/links
http://ws.edu.isoc.org/workshops/2008/cctld-ams/Documentation/DNSSEC_Key_maintenance.pdf
http://www.infoweapons.com/content/why-do-you-need-dnssec
http://computerworld.nl/article/11819/wat-is-dnssec.html
https://st.icann.org/alac-docs/index.cgi?problemas_de_seguridad_del_sistema_de_nombres_de_dominio_dns_dentro_del_ambito_de_competencia_de_la_icann_al_alac_st_0309_5_es
http://pedrollo.com.co/pdf/SIC_68_Riesgos%20en%20el%20Sistema%20de%20DNS.pdf
http://www.intgovforum.org/cms/2010/Background/Spanish-IGF-Background-Funcionamiento de DNS
http://www.ldc.usb.ve/~yudith/docencia/ci-4821/PRESENTACION-DNS.pdf
http://www.icann.com/es/public-comment/public-comment-201012-es.htm
http://www.ripe.net/training/dnssec/material/dnssec.pdf
ROOT dnssec
http://www.root-dnssec.org/
http://www.iis.se/pdf/Routertester_en.pdf
http://www.cert.uy/historico/pdf/DNSSEC_-_parte1_-_CERTificate.pdf
https://www.iana.org/dnssec/