PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA DE SISTEMAS Y COMPUTACIÓN

TEMA

"CIFRADO DE DATOS TRANSMITIDOS A TRAVÉS DE REDES INALÁMBRICAS"

AUTOR

MARÍA BELÉN GÓMEZ RIVADENEIRA

DIRECTOR

ING. ALBERTO PAZMIÑO PROAÑO

QUITO, OCTUBRE DE 2013

DEDICATORIA

A mis padres, Walito y Janela con mucho cariño y gratitud, esperando poder retribuir de esta manera su constante apoyo, abnegación y amor que supieron enaltecer mi espíritu, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera, sacando de las flaquezas abundante energía y fortaleza. Gracias por ayudarme a cumplir mis objetivos como persona y estudiante.

A mis abuelitos, Francisco y Mirtha, a quien siempre preferí llamar mami Mirtha y papi Pancho, gracias por el orgullo que sienten por mí, por sus consejos, enseñanzas y sobre todo por las oraciones que a diario hacen por mí.

A mis tíos, primos, amigos, las palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles, sobre todo a ti mi Susy, que siempre estuviste a mi lado creyendo en mí y dándome la fuerza necesaria para triunfar en la vida.

A mi muñeca hermosa Valeria, que ha sido mi motor y mejor medicina aunque la tenga lejos.

Va por ustedes, por lo que significan para mí, porque estaré siempre agradecida por lo que han hecho por mí. No puedo dejar esta oportunidad para decirles que los amo y que gracias a ustedes estoy donde estoy.

A todos, espero no defraudarlos y contar siempre son su amor y su apoyo.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por permitirme cumplir con esta meta tan importante en mi vida. Un especial y sincero reconocimiento a mi familia por su incesante aliento, comprensión, paciencia y el ánimo recibido.

Guardo un compromiso de gratitud con la Pontificia Universidad Católica del Ecuador que me ha brindado la oportunidad de enriquecerme de conocimientos renovadores así como a sus maestros, que con amplios conocimientos han sabido orientarme y darme el respaldo necesario para hacer realidad la presente Tesis, en especial al Ing. Alberto Pazmiño Proaño, director de esta investigación, por la orientación, el seguimiento y la supervisión continua de la misma.

Especial reconocimiento merecen las sugerencias recibidas por la Ingeniera Suyana Arcos y el Ing. Xavier Castellanos, con los que me encuentro muy agradecida por la confianza en mí depositada.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN

Las redes inalámbricas tienen como característica principal, que no usan medios físicos (cables, fibra óptica, etc.) para funcionar. Esto es una gran ventaja, pero a la vez se convierte en una desventaja, ya que cualquier persona con un ordenador portátil, tablet, o un smartphone, sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Por lo anterior desde el nacimiento de las redes inalámbricas, se han implementado mecanismos como el cifrado de datos, para proporcionar la misma seguridad que la de un cable.

El presente trabajo investiga los diferentes algoritmos de cifrado de datos que existen y que son utilizados en las transmisiones de datos de redes inalámbricas, con la finalidad de garantizar la seguridad de las comunicaciones.

En el Capítulo 1 se hace una introducción a las redes informáticas: se describe su historia, componentes, topologías y los medios alámbricos e inalámbricos que existen para lograr su conexión.

El Capítulo 2 explica lo que es el cifrado de datos, sus objetivos, aplicaciones, métodos y los requerimientos mínimos de hardware y software para su implementación en una red inalámbrica.

En el Capítulo 3 se describe y se compara los diferentes algoritmos de cifrados de datos que se utilizan en la transmisión de datos de redes inalámbricas, y a continuación se hace una evaluación de sus aspectos más significativos: vulnerabilidad, tamaño de clave, uso en entidades, número de vueltas, con la finalidad de seleccionar los tres mejores.

El Capítulo 4 explica la aplicación que tienen los tres mejores algoritmos de cifrados de datos seleccionados en diversos protocolos de seguridad para redes inalámbricas. Luego muestra los resultados del estudio que establece el uso que tienen en WLAN empresariales y los resultados de una investigación de campo que determina los costos de implementar una solución de seguridad basada en ellos.

Finalmente el Capitulo 5 presenta las conclusiones y las recomendaciones a las que se llegó después de todo el trabajo investigativo.

INTRODUCCIÓN

Los seres humanos dependemos de la información que se encuentran y generan los ordenadores o computadoras, en la actualidad estos aparatos electrónicos ya no se encuentran aislados como en la década de 1980 y comienzos de la década de 1990; si no por el contrario, hoy se encuentran conectados a través de redes alambricas e inalámbricas.

Las redes inalámbricas usan medios inseguros para la transmisión de datos y esto influye mucho en la seguridad de la "información que se transmite", lo cual es algo muy preciado tanto por los propios dueños de la información como por los hackers, por ello se debe implementar una serie de seguridades para evitar que alguien no autorizado acceda a la información y ser presa fácil de robos y/o daños irreparables.

Como mecanismo de seguridad dentro de las redes tanto alambricas como inalámbricas se ha implementado el cifrado de datos, éste es un proceso por medio del cual una información comprensible se convierte por medio de un algoritmo en información incomprensible llamada criptograma. Esta información incomprensible puede ser transmitida a algún destinatario con menos riesgos de ser leída por personas no autorizadas.

Esta investigación se realiza con el propósito de proporcionar información acerca de los diferentes métodos de cifrado de datos en la transmisión de datos de redes inalámbricas, a la vez evalúa la relación costos-beneficios de implementarlos.

Al implementar la herramienta de cifrado de datos más conveniente, los principales beneficiarios serán los usuarios y propietarios de las redes inalámbricas, debido a que se solucionarán los problemas de seguridad en varios niveles, que influyen directamente en el acceso de los datos transmitidos.

Para el desarrollo del presente estudio se recolectó la información necesaria acerca de las herramientas de cifrado de datos y se seleccionó tres de ellas para realizar un análisis y demostrar que los algoritmos funcionan adecuadamente en la transmisión de datos en las redes inalámbricas.

OBJETIVOS

Objetivo general

- Realizar el estudio de los diferentes métodos de cifrado en las redes inalámbricas, para determinar y evaluar el costo-beneficio de enviar datos cifrados lo que incrementará la seguridad de este tipo de redes.

Objetivos Específicos

1. Mejora de la seguridad disminuyendo la vulnerabilidad ante amenazas de acceso no autorizado a la información.

2. Establecer costo-beneficio del cifrado de datos.

3. Realizar un estudio que determine la carga de procesamiento que demanda el cifrado de datos y su comportamiento en el ciclo de transmisión.

JUSTIFICACIÓN

En los últimos años las comunicaciones y la electrónica se han convertido en herramientas que facilitan la realización de diferentes actividades, por un lado las comunicaciones han evolucionado de tal manera que cumplen con su objetivo en casi todos los ámbitos, un ejemplo es el INTERNET y su uso masivo, dado que su implementación y su funcionamiento se realiza de una manera estandarizada, de fácil acceso y manejo, logrando así grandes avances y el soporte de una gran variedad de servicios, por otro lado, la electrónica, por medio de la generación de nuevos y mejores dispositivos contribuye en el desarrollo de nuevas tecnologías que brindan servicios que dan solución a necesidades específicas o que simplemente facilitan el diario vivir.

Esta investigación se realizará con el interés de proporcionar un análisis costo-beneficio para incluir encriptación en la transmisión de datos, debido a que siempre existen problemas de seguridad en varios niveles y que influyen directamente en el buen uso de los datos transmitidos.

Con el presente tema, los beneficiarios principales son los usuarios de redes inalámbricas al conocer el beneficio de la encriptación de información.

CAPÍTULO 1

MARCO TEÓRICO

1.1 Redes informáticas

1.1.1 Introducción

Las necesidades del ser humano por lograr comunicarse entre personas o entre personas u ordenadores o entre ordenadores y ordenadores datan a lo largo del recorrido de su historia hasta llegar a la actualidad, o tal vez futuras, autopistas de la información, que permiten a empresas y particulares conectarse e intercambiar información en todo el mundo de manera sencilla.

Una red informática es un sistema constituido por un conjunto de ordenadores conectados entre sí, con la finalidad de intercambiar información y compartir recursos o servicios, son utilizadas en abundancia para interconectar recursos tanto de hardware como de software, generando no solo ventajas en la velocidad de transmisión, ahorro de gastos, entre otros; sino también desventajas puesto que la información se encuentra expuesta ante personas que tratan de encontrar las vulnerabilidades de la red informática ya que no se puede asegurar que un sistema sea impenetrable y capaz de garantizar la privacidad de la información y la continuidad del servicio, por tanto, surgen diferentes motivos que generan preocupación ante tales repercusiones en la seguridad.

A lo largo del siglo XX las redes informáticas se han desarrollado impresionantemente de tal manera que el lugar en dónde se encuentren los ordenadores no sea obstáculo para que exista la posibilidad de poder examinar los estados actuales de organizaciones ó empresas.

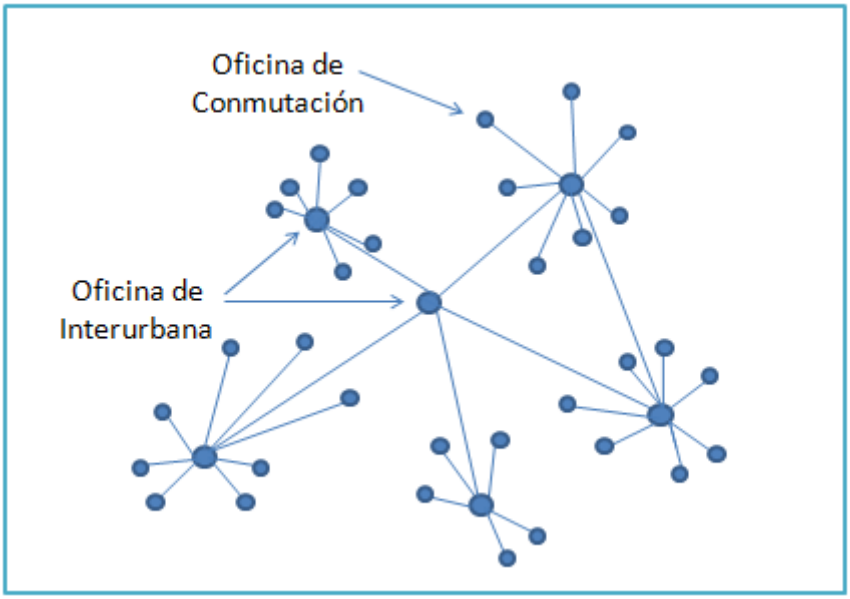
Este desarrollo ha influido enormemente en la globalización y en el desarrollo económico de los países, puesto que es un apoyo de vital importancia del cual depende el éxito de las empresas. Cabe recalcar que las empresas que manejan información verdaderamente valiosa e interesante no deberían utilizar redes inalámbricas para sus comunicaciones si no se han tomado las medidas adecuadas de protección que atraen a cualquiera que se encuentre en el espacio cubierto por la red, considerando que en las redes la unidad de

envío de datos que transporta y extrae la información, circula de forma pública pudiendo ser capturada a lo largo de la trama.

1.1.2 Antecedentes

Las redes informáticas actuales tienen sus inicios en la Advanced Research Projects Agency (ARPA), agencia del Departamento de Defensa de los Estados Unidos, creada en el año de 1960 con la finalidad de impulsar el desarrollo tecnológico. En esos tiempos las únicas redes de comunicaciones que existían eran las redes telefónicas, las cuales se consideraban vulnerables por su estructura centralizada. Estas redes estaban conformadas por oficinas de conmutación telefónica, a las cuales se conectaban miles de teléfonos. Estas oficinas a su vez estaban conectadas a oficinas de conmutación de nivel superior (oficinas interurbanas). La vulnerabilidad consistía en que la destrucción de algunas de las oficinas urbanas podía fragmentar la red dejando incomunicado a muchos integrantes de la misma (véase Figura 1).

Figura 1. Estructura de un sistema telefónico



Fuente: Tanenbaum, 2003, p. 51

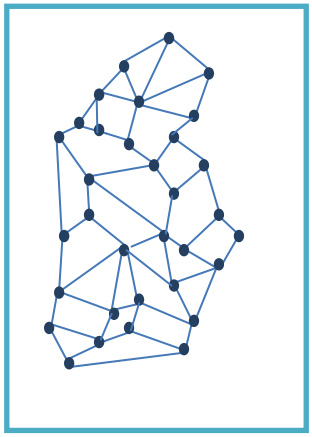
Elaborado por: María Belén Gómez

Por lo antes expuesto, el Departamento de Defensa necesitaba crear otro tipo de red de comunicación, una que fuera descentralizada y flexible, capaz de resistir cualquier ataque.

Es por eso que en este mismo año el Departamento de Defensa contrata a RAND Corporation.

Uno de los empleados de esta Corporación llamado Paul Baran ideó un sistema de comunicación que no dependía de instalaciones centralizadas capaz de operar a pesar de que muchos de sus enlaces y nodos de comunicación fueran destruidos. Todos los nodos de este sistema eran autónomos y capaces de dirigir, recibir y transmitir información (véase Figura 2).

Figura 2. Estructura de un sistema telefónico



Fuente: Tanenbaum, 2003, p. 51

Elaborado por: María Belén Gómez

Con el paso del tiempo esta idea de sistemas de comunicación se fue desarrollando y evolucionando constantemente hasta llegar a convertirse en lo que hoy se conoce como redes informáticas:

> En 1965, la ARPA patrocino un programa que trataba de analizar las redes de comunicación usando computadoras. Mediante este programa, la máquina TX-2 en el laboratorio Licoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea delicada de 1200 bits por segundo.
>
> En 1967, la ARPA convoca una reunión en Ann Arbor (Michigan), donde se discuten por primera vez aspectos sobre la futura ARPANET.
>
> En 1969, es un año clave para las redes de computadoras, ya que se construye la primera red de computadoras de la historia. Denominada ARPANET, estaba compuesta por cuatro nodos situados en la Universidad de California en los Ángeles, Stanford Research Institute, Universidad de California de Santa Bárbara y la Universidad de UTA.
>
> En 1971 la ARPANET estaba compuesta por 15 nodos y 23 maquinas que se unían mediante conmutación de paquetes. En ese mismo año Ray Tomlinson realiza un

> programa de e-mail para distribuir mensajes a usuarios concretos a través de ARPANET.
>
> En 1973, se produce la primera conexión internacional de la ARPANET. Dicha conexión se realiza con el colegio universitario de Londres (Inglaterra) En ese mismo año Bob Metcalfe expone sus primeras ideas para la implementación del protocolo Ethernet que es uno de los protocolos más importantes que se utiliza en las redes locales.
>
> En 1975, Se prueban los primeros enlaces vía satélite cruzando dos océanos (desde Hawai a Inglaterra) con las primeras pruebas de TCP de la mano de Stanford, UCLA y UCL. En ese mismo año se distribuyen las primera versiones del programa UUCP (Unís-to-Unix CoPy) del sistema operativo UNIX por parte de AT&T.
>
> En 1982 es el año en que la DCA y la ARPA nombran a TCP e IP como el conjunto de protocolos TCP/IP de comunicación a través de la ARPANET. (Scribd, 2011: http://es.scribd.com).

1.1.3 Definición

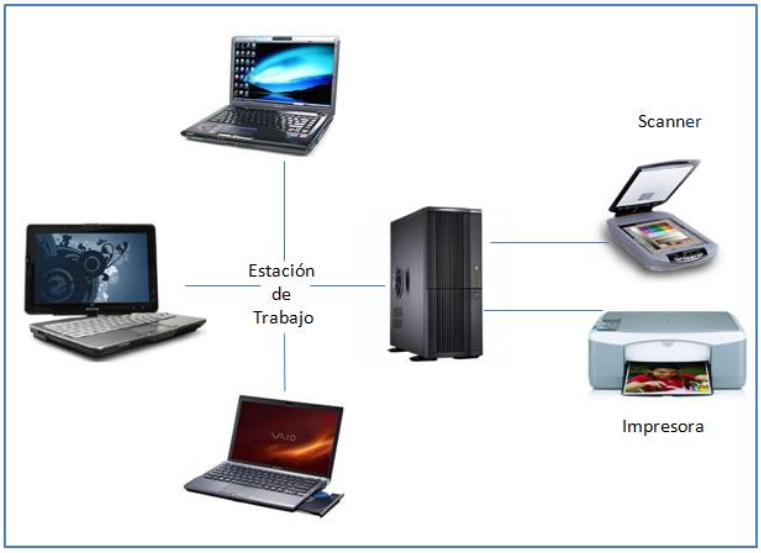
Según Atelin y Dordoigne (2006) en el libro Redes Informáticas: Conceptos fundamentales, las redes informáticas:

> Constituye el conjunto de las herramientas que permiten a los ordenadores compartir información y recursos.
>
> Las redes telefónicas forman una generación de redes de telecomunicación que precedió a la informática. La convergencia entre estos dos medios de comunicación es lo que se da actualmente. De hecho las nuevas tecnologías permiten el transporte de voz y datos con los mismos medios. (p.10)

De acuerdo a la definición anterior, una red informática es un sistema de comunicaciones que conecta a varios ordenadores o computadoras entre sí con la finalidad de compartir información (archivos, datos, software) y recursos (impresora, scanner, etc.). En una red también existen dispositivos que añaden funcionalidades a las mismas, tales como los routers, switches y hubs. La conexión puede hacerse a través de hilo de cobre, láser, satélites de comunicación microondas, etc.

En una red informática puede haber una estructura de cliente/servidor, donde existen computadoras que funcionan como clientes y puede haber una o varias computadoras que funcionan como servidores. Las estaciones de trabajo son computadoras que pueden ser utilizadas por los usuarios de una red para solicitar información y recursos a las computadoras que funcionan como servidores (véase Figura 3).

Figura 3. Red de Computadoras con estructura de cliente/servidor

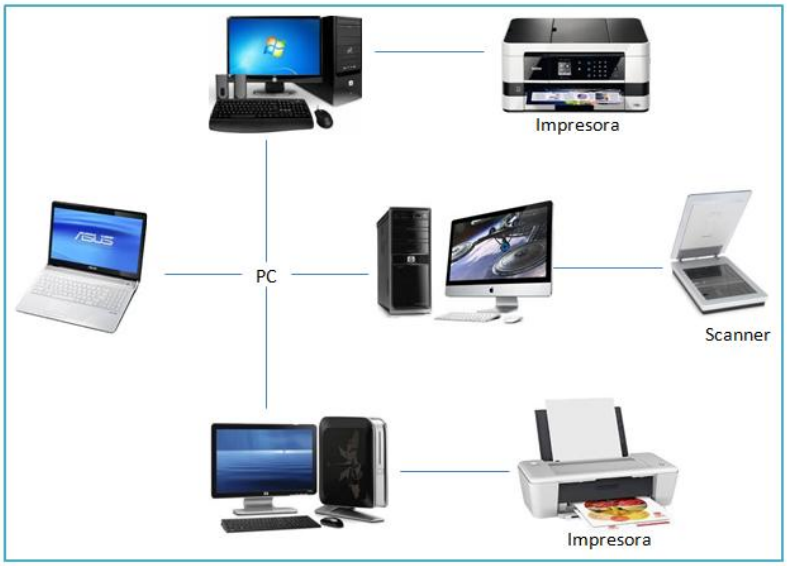


Fuente:http://www.carlospes.com/curso_de_informatica_basica/04_02_redes_cliente_servidor_e_igual_a_igual.php

Elaborado por: María Belén Gómez

También puede haber una estructura de red igual a igual en donde todas las computadoras pueden hacer las veces de cliente y servidor al mismo tiempo, en este tipo de estructura, no existen computadoras que sean clientes o servidores exclusivos (véase Figura 4).

Figura 4. Red de Computadoras con estructura de igual/igual



Fuente:http://www.carlospes.com/curso_de_informatica_basica/04_02_redes_cliente_servidor_e_igual_a_igual.php

Elaborado por: María Belén Gómez

1.1.4 Clasificación

Existen varias clasificaciones de las redes informáticas, pero las más usadas es de acuerdo a su estructura física (topología) y de acuerdo a la cobertura (alcance geográfico) del servicio.

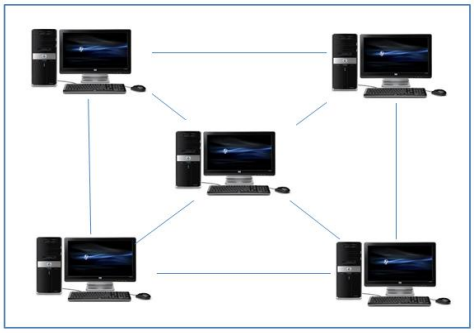
1.1.4.1 De acuerdo a la estructura física (topología)

La topología establece como se ubicaran o se distribuirán las diferentes estaciones de trabajo que forman la red, también determina el corte y tendido del cableado. La topología aporta de gran manera a la flexibilidad y dinamismo de una red en sus necesidades futuras. De acuerdo a la topología las redes informáticas pueden ser: estrella, árbol, bus, anillo y malla.

Topología en malla

En la topología malla cada ordenador tiene un enlace punto a punto y dedicado (el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta) con otro ordenador. Entre las ventajas de esta topología es que es una estructura fácilmente extensible, por ejemplo se puede conectar dos redes en mallas mediante un router auxiliar.

Figura 5. Red de Computadoras topología malla



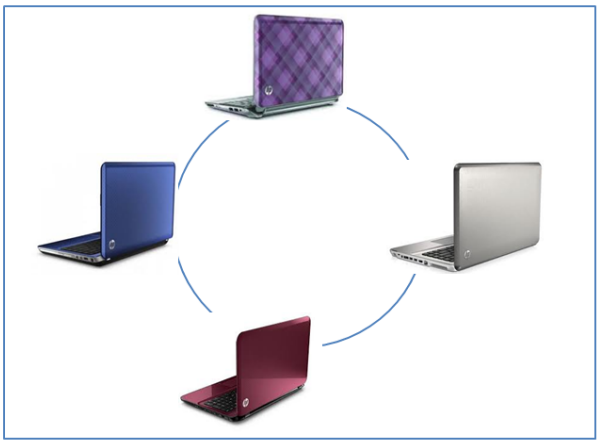
Fuente: http://topo-malla.blogspot.com/

Elaborado por: María Belén Gómez

Topología anillo

En esta estructura de red las señales viajan en una única dirección a lo largo del cable en un círculo cerrado o anillo. La desventaja de esta estructura, es si una estación de la red se cae, se rompe el anillo y la red ya no puede funciona, por esta razón es escasa este tipo de estructuras.

Figura 6. Red de Computadoras topología anillo



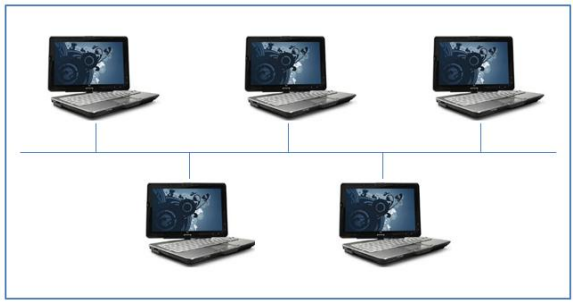
Fuente: http://topo-malla.blogspot.com/

Elaborado por: María Belén Gómez

Topología bus

En esta estructura un cable tendido a lo largo conecta a todos los ordenadores en la red. En los extremos del cable, se encuentra un terminador para que no haya reflexiones de la señal. Entre las ventajas de este tipo de red es que es fácil de instalación y sus costos son baratos ya que no existen dispositivos de interconexión, entre las desventaja es que permite un numero bastante limitado de ordenadores conectados.

Figura 7. Red de Computadoras topología bus



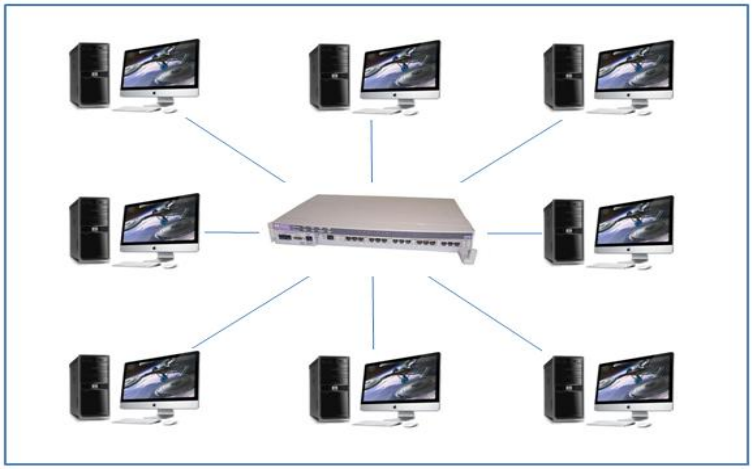
Fuente: http://topo-malla.blogspot.com/

Elaborado por: María Belén Gómez

Topología estrella

Este tipo de red consiste en un dispositivo central con una serie de puertos a los que se conectan las estaciones a través de enlaces punto a punto. En esta red cuando una estación de trabajo trasmite, sus datos son enviados al dispositivo central y éste los envía a la estación de trabajo (destino).

Figura 8. Red de Computadoras topología estrella



Fuente: http://topo-malla.blogspot.com/

Elaborado por: María Belén Gómez

1.1.4.2 De acuerdo a la cobertura (alcance geográfico)

Las redes informáticas de acuerdo a su alcance geográfico pueden ser: red de área local (LAN), red de área metropolitana (MAN) y red de área amplia (WAN).

Red de área local (LAN)

Son las redes de difusión más populares en la actualidad. Son redes de ámbito privado que cubren distancias normalmente inferiores al kilómetro. Normalmente, se ven confinadas en una sala o, como mucho, en un edificio. Una red local que pertenece a una determinada empresa u organización se suele denominar Intranet.

Las tecnologías utilizadas en redes LAN en la actualidad son, casi exclusivamente, Ethernet para las cableadas y 803.11 para las inalámbricas.

Red de área metropolitana (MAN)

Las redes de área metropolitana o acceso metropolitano se presentan en dos variantes principales.

La primera está conformada por las redes metropolitanas, que aparecieron a finales de los años 80 como evolución de las redes locales de la época. Ofrecían una distancia de cobertura mucho más amplia (50-100 km), además de una velocidad de transmisión mucho mayor para la época. La otra variante de redes de acceso metropolitano es mucho más reciente, ya que proviene de la necesidad de dar conectividad a la red a los hogares. La solución adoptada consiste en aplicar las tecnologías utilizadas en los sistemas de televisión por cable para transmitir, además de canales de televisión, datos y conexión a Internet.

Red de área amplia (WAN)

Cubren enormes distancias y permiten la comunicación de usuarios que se sitúan a kilómetros de distancia.

Están constituidas por la conexión de las redes locales y metropolitanas a redes troncales de muy alta capacidad que forman lo que se denomina un backbone. (Mouteira, 2004: pp. 41-43).

1.2 Transmisión de datos

> Es la transferencia física de datos (un flujo digital de bits) por un canal de comunicación punto a punto o punto a multipunto. Ejemplos de estos canales son cables de par trenzado, fibra óptica, los canales de comunicación inalámbrica y medios de almacenamiento. Los datos se representan como una señal electromagnética, una señal de tensión eléctrica, ondas radioeléctricas, microondas o infrarrojos (wikipedia, 2013: http://es.wikipedia.org).

La transmisión de datos es algo muy importante en el transporte de información dentro de las redes informáticas y es especial en aquellas cuyos enlaces exceden los 20 metros. Las transmisiones de datos son muy estrictas de su contenido de información, cualquier error por muy pequeño que fuera (de 1 bit), puede ser perjudicial para las mismas. Por esta razón en una red de computadoras es importante que la transmisión de datos sea muy confiable, paro lograrlo se debe tener un control adecuado del flujo de datos en el momento de la transmisión y la codificación para detectar y corregir errores. Estos factores forman parte de lo se conoce con el nombre de protocolo de comunicación, que tiene como función asegurar la comunicación completa, correcta y entendible entre las computadoras.

1.2.1 Modos de transmisión de datos

La transmisión de datos puede ser: simplex, semiduplex (Half-duple) y Duplex (Full-duplex).

1.2.1.1 Transmisión simplex

Es la transmisión en una sola dirección, del transmisor hacia el receptor, en ésta los hilo de datos se encuentran dedicados a la trasmisión de datos en un solo sentido. Por ejemplo la conexión de datos entre un ordenador y una impresora.

1.2.1.2 Semiduplex (Half-duplex)

Es cuando el mismo canal se utiliza para transmisión de datos en dos sentidos, pero no al mismo tiempo. Algunas veces se transmite los datos en un sentido y otras veces en sentido contrario, para lograr esta transmisión hay conmutadores en ambos extremos del canal.

Los ordenadores conectados en este modo de transmisión actúan tanto como emisor y como receptor, pero realiza una sola de estas funciones en su momento.

1.2.1.3 Duplex (Full-duplex)

Es cuando la transmisión de datos se realiza simultáneamente en ambos sentidos, es decir, cada extremo de la conexión puede transmitir y recibir datos simultáneamente. Es un modo muy eficiente pero implica mayores costos.

1.2.2 Tipos de transmisión de datos

1.2.2.1 Transmisión en serie

Es una transmisión de datos de bit por bit sobre un único canal. Esta transmisión es utilizada en redes de largas distancias, por ejemplo en las redes WAN.

1.2.2.2 Transmisión en paralelo

En esta transmisión el envío de datos es byte por byte. Esta transmisión es más rápida que la transmisión en serie y se la utiliza en distancias cortas, por ejemplo entre una computadora y una impresora.

1.2.3. Medios de transmisión de datos (guiados)

Dentro de las comunicaciones de red, constituye el medio físico entre el transmisor y el receptor, se entiende por medios a los cables, alambres, fibra óptica y otros medios por los cuales se transporta la información desde la fuente (origen) hasta su destino. El medio de transmisión utilizado es muy importante puesto que establece el número máximo de bits que pueden ser transmitidos en un segundo, (velocidad de transmisión máxima), la distancia máxima entre las computadoras interconectadas y el número de ordenadores conectados (véase Cuadro 1).

Cuadro 1. Tecnologías de red y principales características dependiendo del cable utilizado

Tecnología	Velocidad de transmisión	Tipo de cabe	Distancia máxima	Topología
10 Base 2	10 Mbps	Coaxial fino (50Ω)	200 m	Bus (Conector BNC-T)
10 Base 5	10 Mbps	Coaxial grueso (50Ω)	500 m	Bus (Conector AUI)
10 Base T	10 Mbps	2 pares trenzado (categoría UTP3)	100 m	Estrella (Hub o Switch)
10 Base F	10 Mbps	Fibra óptica	200 m	Estrella (Hub o Switch)
100 Base T4	100 Mbps	4 pares trenzado (categoría UTP3)	100 m	Estrella Half Duplex (hub) y Full Duplex (switch)
100 Base TX	100 Mbps	2 pares trenzado (categoría UTP3)	100 m	Estrella Half Duplex (hub) y Full Duplex (switch)
100 Base FX	100 Mbps	Fibra óptica (multimodo)	2000 m	No permite el uso de hubs
100 Base CX	100 Mbps	2 pares trenzado (STP)	25 m	Estrella (Hub o Switch)
1000 Base T	1000 Mbps	4 pares trenzado (categoría 5e ó UTP6)	100 m	Estrella Full Duplex (switch)
1000 Base SX	1000 Mbps	Fibra óptica (multimodo)	550 m	Estrella Full Duplex (switch)
1000 Base LX	1000 Mbps	Fibra óptica (monomodo)	5000 m	Estrella Full Duplex (switch)
10G Base SR	10 Gbps	Fibra óptica (multimodo)	500 m	Estrella Full Duplex (switch)
10G Base LX4	10 Gbps	Fibra óptica (multimodo)	500 m	Estrella Full Duplex (switch)
10G Base T	10 Gbps	Par Trenzado (UTP6)	55 m	Estrella Full Duplex (switch)

Fuente: (Gil, Pomares, Candelas, 2010: p.81)

Elaborado por: María Belén Gómez

Durante las transmisiones de datos pueden ocurrir alteraciones no deseadas, principalmente por atenuación (debilitamiento y deformación de la señal por causa de la distancia que recorre), para solucionar este problema se colocan dispositivos llamados repetidores, a ciertos intervalos de distancia, para que reconstruyan y amplifiquen la señal de origen. También las alteraciones pueden ser a consecuencia de los ruidos, que son tipos de señales que interfieren u obstaculizan la señal transmitida, deformándola y evitando que lleguen los datos lleguen a su lugar de destino.

1.2.3.1 Par trenzado

Es el medio más antiguo y todavía el más usado en las redes de área local. Está compuesto por dos cables de cobre entrecruzados en forma espiral, cubiertos por un aislante plástico. La disposición trenzada del cable reduce el ruido y la atenuación, de hecho mientras más número de trenzas se obtiene mayor robustez del medio al ruido y la atenuación, por consiguiente se consigue una mejor calidad en la trasmisión. Una aplicación muy conocida de este medio de transmisión es el sistema telefónico.

> Normalmente un cable de para trenzado está formado por un grupo de pares trenzados habitualmente cuatro, recubiertos de una envoltura protectora (a veces se agrupan muchos pares trenzado en un mismo cable para la transmisión de distintas líneas de comunicación a largas distancias). Cada uno de estos pares se identifica mediante un color, siendo los colores asignados y las agrupaciones de los pares de la siguiente forma.
>
> Par 1: Blanco-Azul/Azul
>
> Par 2: Blanco-Naranja/Naranja
>
> Par 3: Blanco Verde/Verde
>
> Par 4: Blanco-Marrón/Marrón (Gil, Pomares, Candelas, 2010: p.82)

1.2.3.2 Cable coaxial

Los cables coaxiales están compuestos por un conductor interno de cobre en su parte central (núcleo), por el que se envía el voltaje correspondiente a la información que se va a enviar. Este núcleo está rodeado de un material aislante, el que a su vez está rodeado por una malla conductora externa que también está cubierta de material aislante. Toda esta composición hace que tengan mayor robustez al ruido. Existen cables coaxiales de 2 tipos:

> Cable coaxial 50 Ω. Es empleado en transmisión en banda base en LANs utilizando Manchester y Manchester diferencial. Es tipo de medio ha sido remplazado por el par trenzado ya que permite una detección de errores más sencilla.
>
> Cable coaxial 75 Ω. Utilizado para la transmisión en banda modulada en televisión analógica por cable empleando multiplexión por división en frecuencia de múltiples canales. Se puede emplear para transmitir datos digitales, pero modulando para poder convertir la señal que circula por el medio a analógica. (Gil, Pomares, Candelas, 2010: pp.85-86).

1.2.3.3 Fibra óptica

El cable de fibra óptica está un fino hilo de vidrio que permite la transmisión de la información por medio de pulsos de luz. Un pulso de luz indica la existencia de un bit de valor 1 en cambio la ausencia del pulso de luz indica un bit de valor 0.

La transmisión por fibra óptica está compuesta de 3 partes: fuente de luz, el medio de transmisión y el detector. La fuente de luz puede ser un diodo emisor de luz (diodo LED), que emite pulsos de luz cuando se le aplica corriente eléctrica, el medio de transmisión es la fibra fina de vidrio o silicio fundido y el detector consiste en un fotodiodo que produce un pulso eléctrico cuando recibe un rayo de luz. La fibra óptica es actualmente el medio de transmisión de datos más utilizado en largas distancias.

1.3 Tipos de redes inalámbricas

La comunicación inalámbrica es lo nuevo en el mundo de las redes de computadoras, ofrecen la posibilidad de interconexión de distintos dispositivos en lugares de difícil acceso donde no existen otras posibilidades de servicios de telecomunicaciones, utilizan ondas de radiofrecuencia de baja potencia y una banda específica, de uso libre o privada, para transmitir entre dispositivos. Una de sus principales ventajas es notable en los costos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos. Otra ventaja de este tipo de red es que se pueden conectar fácilmente los ordenadores que se encuentran en lugares distantes, también no hace falta configurar la red cuando se realizan cambios físicos en el lugar donde se encuentran los ordenadores o se ubican los ordenadores en otro lugar.

Existen varios tipos de sistemas de transmisión inalámbrica de datos que permiten que las señales de datos sean enviadas y recibidas por otras unidades rápidamente. Por ejemplo WiFi, bluetooth, Microondas, radio e infrarrojo.

1.3.1 Ondas de radio

Las ondas de radio se emiten en todas las direcciones por lo que no se requiere que el transmisor y el receptor estén alineados físicamente. Sufre menos atenuación que las microondas, son fáciles de generar, pueden penetrar edificaciones sin problemas y viajar largas distancia, por ello su uso es generalizado en las comunicaciones tanto en interiores como en exteriores.

1.3.2 Microondas

Consiste en la emisión y recepción de ondas de radio mediante antenas parabólicas. Éstas se pueden montar sobre edificios para enviar un haz de señales hacia otra antena ubicada a varios kilómetros de distancia. Cuando aumenta la altitud de las antenas parabólicas se extiende el alcance de la transmisión. Las tormentas y otros fenómenos atmosféricos afectan la transmisión de datos por microondas.

Las hay de dos tipos:

1.3.2.1. Microondas por satelitales

Se realizan a través de bases terrestres con antenas que envían señales al satélite, este se encarga de direccionarlas hacia la estación receptora con la onda amplificada para evitar pérdidas. Tiene una frecuencia de transmisión de datos entre 4 GHz y 6 GHz ó 21 GHz y 23 GHz y la velocidad de trasmisión está entre 1 Mbps y 10 Mbps.

1.3.2.2 Microondas terrestres

Se basan en conexiones denominadas punto a punto, ya que sus antenas deben estar sin obstáculos físicos para evitar fallas en la transmisión. Su frecuencia está entre los 11 GHz y 14 GHz, y la velocidad de transmisión está entre 1 Mbps y 10 Mbps.

1.3.3 Infrarrojos

Los rayos infrarrojos tienen una largo de onda próxima a la de la luz y por tanto tienen un comportamiento similar. Una de sus características es que no puede atravesar paredes o edificios, lo que le quita capacidad de difusión, también debido a su alta frecuencia tiene resistencia a las interferencias electromagnéticas artificiales. La frecuencia de señal de transmisión en el sistema punto a punto está entre 100 GHz y 1000 terahertz (THz) y la velocidad de transmisión está entre 100 Kbps y 16 Mbps.

1.3.4. BlueTooth

Es una tecnología de transmisión inalámbrica a través de ondas de radio con corto alcance. Al transmitir los datos no se requiere de una antena externa visible sino que puede estar integrada en el mismo dispositivo. Este tipo de transmisión tiene una estandarización de independiente y una velocidad de transmisión de hasta 1 Mbps.

1.3.5. Wi-Fi

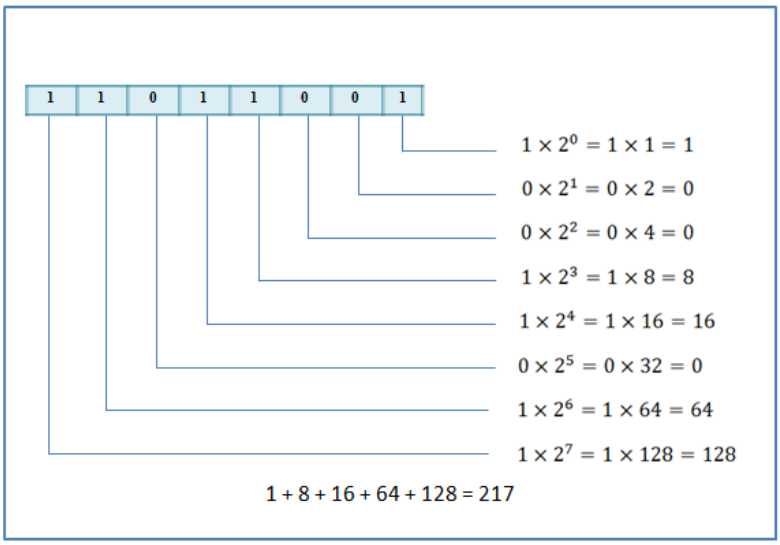
Es una tecnología de transmisión inalámbrica mediante ondas de radio, que es muy utilizada en la actualidad tiene una buena calidad para emitir en distancias cortas. Para la transmisión de datos se requiere antenas que vienen integradas en las tarjetas. Este tipo de ondas son capaces de penetrar paredes, edificios, etc., sin necesidad de que el emisor este frente al receptor.

1.4 Datos

La finalidad de las computadoras, redes y comunicación de datos es el procesamiento y transmisión de datos, por eso se debe conocer cómo los datos están representados en ellos. Los datos se guardan en el computador y son transmitidos por un sistema de comunicación en forma de dígitos binarios, o bits. Estos dígitos pueden tomar los valores de ceros o unos y están codificados de acuerdo al sistema de numeración binaria o de base 2 (véase Figura 9).

Los bits o dígitos binarios están representados dentro del computador por medio del nivel de polaridad de señales eléctricas. Por ejemplo, una señal de nivel alto en un elemento de almacenamiento del computador, representa 1 y una señal de nivel bajo representa 0. Los bits se agrupan y forman un byte (8 bits) que representa los diversos caracteres (1,2,3, A, @, etc.) que se usan en un ordenador.

Figura 9. Representación binaria del número 217



Fuente: http://programaciooao.blogspot.com/2011/05/byte-bit.html

Elaborado por: María Belén Gómez

Un dato aislado o un conjunto de datos por sí mismo no significan nada, pero mediante una tarea de ordenamiento (proceso), se convierten en información que puede ser interpretada y compartida.

1.5 Cifrado de datos

1.5.1 Definición

> Constituye uno de los métodos de protección más fiable. Consiste en la transformación de los datos, de forma que una persona no deba tener acceso a ellos no sea capaz de entenderlos. El cifrado de datos se puede realizar a través de elementos lógicos o físicos pero en cualquiera de los casos es un proceso que consume bastantes recursos. (Sampalo, Leyva, Garzón, Prieto, 2003: p. 85)

El cifrado de datos es un proceso por medio del cual una información entendible se convierte mediante un algoritmo en una información inentendible, que recibe el nombre de

criptograma. Esta información inentendible puede ser enviada a un destinatario con menos riesgos de ser leída por personas no autorizadas. El destinatario para volver a hacer entendible la información debe descifrarla, ingresando la clave del cifrado.

1.5.2. Importancia de cifrados de datos en redes inalámbricas

La seguridad es un tema muy importante cuando se habla de redes inalámbricas. Desde el comienzo de éstas, se ha intentado disponer de mecanismos que garanticen las comunicaciones. Para resolver los problemas de seguridad de una red inalámbrica, se necesita garantizar el acceso a la misma por medio de algún tipo de autorización y garantizar la privacidad de las comunicaciones que se realizan a través de medios inseguros (medios inalámbricos).

Las redes inalámbricas tienen como característica principal, el no usar medios físicos (cables, fibra óptica, etc.) para funcionar. Esto es una ventaja, pero a la vez se convierte en una desventaja, porque cualquier persona con un ordenador portátil, tablet, o un teléfono móvil, sólo requiere estar dentro del área de cobertura de la red para poder intentar ingresar a ella. Al no estar limitada el área de cobertura por paredes o por ningún medio físico, los potenciales intrusos no necesitan estar dentro de un edificio o estar conectado a un cable.

Por lo anterior, las redes inalámbricas requieren mayor seguridad que las redes alámbricas, necesitan incorporar mecanismos de seguridad que protejan los datos que se transmiten en una conexión inalámbrica.

Con la finalidad de proporcionar seguridad en las redes inalámbricas se desarrollaron diversos protocolos de cifrado de datos, entre los que se puede mencionar: WEP, WPA, WPA2, los cuales tratan de proporcionar la misma seguridad que la de un cable, a la información que circula por la red.

En conclusión el cifrado de datos es muy importante en las redes inalámbricas, porque si los datos transmitidos-recibidos (transacciones bancarias y compras en línea, envío de correos electrónicos o acceso a redes sociales, etc.), durante una conexión no se encuentran cifrados, pueden ser monitoreados y/o capturados por terceras personas.

CAPÍTULO 2

CIFRADO DE DATOS

2.1 Introducción al cifrado de datos

2.1.1 Introducción

Con el incremento y el intensivo uso de ordenadores personales, conectados a redes alámbricas e inalámbricas, también se han incrementado los problemas de seguridad en las redes. En la actualidad transacciones bancarias, compras de productos con tarjetas de crédito, envío-recepción de e-mail, etc., que se realizan a través de internet pueden ser interceptadas por terceras personas.

Por lo anterior se ha desarrollado un mecanismo que permite proteger la información que se transmite a través de las redes y proporciona seguridad a las comunicaciones y a las entidades o personas que se comunican, este mecanismo es el cifrado de datos, también conocido como encriptación.

El cifrado de datos consiste en convertir un mensaje (texto en claro) de un emisor, por medio de un algoritmo y una llave (clave) en una forma que otras personas no pueden comprender (texto cifrado), luego el receptor del mensaje utilizando el mismo algoritmo y una llave convierte el texto cifrado en el mensaje original (texto en claro).

Figura 10. Cifrado de datos

Fuente: Seoane, 2005, p. 88

Elaborado por: María Belén Gómez

Una forma común de cifrado de datos en redes, son las conexiones a sitios web seguros como: bancos, instituciones gubernamentales, buscadores (google), servidores de correo, etc., estos sitios utilizan HTTPS (Hypertext Transfer Protocol Secure - Protocolo seguro de transferencia de hipertexto), lo cual significa que la conexión entre el navegador del usuario y el sitio web está cifrado.

Figura 11. Sitio web con cifrado de datos

Fuente: https://bancavirtual.bankguay.com/nuevabancavirtual/EasyLogin/wflogin.aspx

A lo largo de la historia el cifrado de datos se lo ha utilizado principalmente para proteger información o secretos diplomáticos y militares de los gobiernos, pero hoy en día también lo utilizan muchas instituciones públicas o privadas para asegurar las comunicaciones sensibles de información confidencial.

2.1.2 Historia

La historia de la criptografía es muy extensa, los primeros en usar métodos criptográficos fueron los egipcios, quienes utilizaron jeroglíficos (sistema de escritura basado en símbolos o figuras) desde la época predinástica hasta el siglo IV a.C.

Durante la guerra entre Atenas y Esparta, se utilizó otro método de criptografía conocido como escitala espartana. Según el historiador griego Plutarco, la describe de la siguiente forma:

> “La escitala era un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero”. (Fernández, 2004, p. 121).

Los romanos también utilizaron un método criptográfico, llamado César, porque supuestamente lo utilizo el emperador Julio César para enviar mensajes secretos a sus ejércitos. Es un algoritmo criptográfico de sustitución de lo más simple, el cifrado consistía simplemente en cambiar una letra por otra situada tres lugares después en el alfabeto. Por ejemplo la letra A se transformaba en D, la letra B en E y así sucesivamente hasta que la letra Z se cambiaba a C.

Cuadro 2. Cifrario de César

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fuente: Fernández, 2004, p. 121

Elaborado por: María Belén Gómez

En 1465, Leon Battista Alberti, quien es considerado el abuelo de criptología inventó un sistema de sustitución polialfabética (uso de varios alfabetos).

En el siglo XVI, el francés Blaise de Vigenère escribió un importante tratado acerca de "la escritura secreta" y desarrollo un método de cifrado basado en varios alfabetos que hoy se lo conoce con el nombre de tablero de Vigenère, el cual consiste en una disposición de letras que contiene en orden los veintiséis alfabetos de César.

Cuadro 3. Tablero de Vigenère

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fuente: Fernández, 2004, p. 131

Elaborado por: María Belén Gómez

En 1626, Antoine y Bonaventure Rossignol, padre e hijo respectivamente, descifraron una carta capturada por el ejército francés al ejército hugonote, en recompensa, sirvieron a los reyes de Francia Luis XIII y Luis XIV como importantes criptoanalistas. Luego padre e hijo propusieron un sistema conocido como La Gran Cifra, el cual era tan robusto e indescrifrable.

A fines del siglo XIX, Etienne Bazeries, experto del departamento Criptográfico del ejército francés, después muchos años de trabajo descifró el sistema la Gran Cifra.

En este mismo siglo en el año 1854, Charles Babbage logró descifrar el método de cifrado de Vigenère. Este descubrimiento fue usado por los ejércitos ingleses en la guerra de Crimea (1853 – 1856), dándole grandes ventajas sobre los métodos criptográficos de los ejércitos rusos.

En el año de 1883, Auguste Kerckhoffs publica un tratado muy importante llamado "la criptografía Militar", en el recomienda que los sistemas criptográficos deben cumplir las siguientes reglas:

1. No debe existir ninguna forma de recuperar el texto claro a partir del criptograma (seguridad ante el primer ataque).
2. Todo sistema criptográfico debe estar compuesto por dos tipos de información:
   a) Pública: se refiere a la familia de algoritmos que definen el sistema criptográfico.
   b) Privada: es conocida sólo por el usuario. La clave de cifrado de cada usuario en particular.
3. La forma de escoger la clave debe ser fácil de recordar y modificar.
4. Debe ser posible la comunicación del criptograma con los medios de transmisión habituales.
5. La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido. (Fernández, 2004, p. 137).

En 1918, durante la Primera Guerra Mundial, los alemanes utilizaron el método de cifrado ADFGVX. Este método consistía en una matriz de 6 filas x 6 columnas, en las cabeceras de las columnas y filas se encontraban las letras A, D, F, G, V y X, dentro de la matriz se colocaban las 26 letras del alfabeto anglosajón y los diez dígitos del 0 al 9. La forma de ordenar las letras y los números dentro de la matriz forma parte de la clave y tenía que ser comunicada al receptor del mensaje.

Este método de cifrado es una mezcla de métodos de trasposición y sustitución, lo que hace que su desciframiento sea muy complicado.

Cuadro 4. Cifrado ADFGVX

	A	D	F	G	V	X
A	0	Q	9	Z	7	C
D	M	U	1	H	F	2
F	4	8	W	N	R	G
G	L	6	V	T	P	A
V	Y	3	D	5	E	K
X	J	S	I	O	B	X

Fuente: Fernández, S. 2004, p. 136

Elaborado por: María Belén Gómez

Durante la Segunda Guerra Mundial, la criptografía experimenta importantes avances, ya que se empiezan a utilizar las máquinas de cálculos, que son herramientas que permitirá conseguir mejores y más cifras seguras. La más conocida es la máquina alemana conocida con el nombre de Enigma, la cual tenía rotores que automatizaba notablemente los cálculos que eran necesarios realizar el cifrado y descifrado de mensajes.

En este mismo siglo, los americanos desarrollaron la máquina Magic usada para descifrar el código púrpura japonés.

En la década de 1970, el Departamento de Normas y Estándares de Estados Unidos publica el Estándar de Cifrado de Datos o DES, que se convertiría en el principal sistema criptográfico de finales del siglo XX.

En esta misma década se empezó a gestar, la última revolución de la criptografía teórica y práctica: los sistemas de cifrados asimétricos, los cuales son utilizados en el campo de la firma digital.

2.1.3 Objetivos del cifrado de datos

Los principales objetivos del cifrado de datos son obtener: la confidencialidad, autentificación, integridad y no repudio.

Confidencialidad.- Consiste en que los datos privados o secretos transmitidos en una red no sean revelados a personas no autorizadas. Otro aspecto de la confidencialidad consiste en la protección del flujo del tráfico frente al análisis del tráfico, es decir, el intruso no puede ver la fuente, el destinatario, la frecuencia, la longitud y otras características del tráfico en una conexión.

Autentificación.- Consiste en garantizar la autenticidad del mensaje, asegura al receptor que la información pertenece a la fuente de la que dice venir. En la conexión de un terminal con un servidor intervienen dos aspectos. En primer lugar, en el inicio de la conexión, la autentificación asegura que las dos computadoras son auténticas, es decir, cada computadora es la que dice ser. En segundo lugar, la autentificación asegura que la conexión no está intervenida de tal manera que una tercera persona pueda suplantar a una de las dos computadoras auténticas con el objetivo de hacer una transmisión o una recepción no autorizada.

Integridad. Garantiza que la información que se transmite no sea alterada por personas no autorizadas, evitando la pérdida de consistencia de los datos, es decir, garantiza que los mensajes se reciben tal cual como son enviados, sin duplicados, inserciones, modificaciones, reordenaciones y repeticiones.

No repudio.- Evita que el emisor o el receptor nieguen la transmisión de una información, es decir, cuando se envía una información, el receptor puede comprobar que efectivamente el emisor envió la información. De igual manera, cuando se recibe un mensaje, el emisor puede comprobar que, el receptor recibió el mensaje.

2.1.4 Aplicaciones del cifrado de datos

El cifrado de datos tiene muchas aplicaciones, entre las que se puede mencionar: Protocolo TLS (Transport Layer Security), VPN (Virtual Private Network), firma digital, cifrado de archivos en discos duros y memorias USB.

2.1.4.1 Protocolo TLS (Transport Layer Security - Seguridad en la capa de transporte)

El protocolo TLS (Transport Layer Security) es una evolución del protocolo SSL (Secure Sockets Layer) versión 3, es por eso que desde el punto de vista del diseño tiene los mismos módulos o protocolos (Protocolo de mutuo acuerdo TLS y Protocolo de Registro TLS) que el SSL. Las diferencias que tiene con respecto al protocolo SSL son:

- No tolera el algoritmo de cifrado de datos Fortezza, por ser un algoritmo de propiedad privada.
- El cálculo de las claves de sesión es distinto al del SSL.
- Usa 5 campos para el cálculo de la dirección MAC (Media Access Control - Control de Acceso al Medio), en cambio SSL sólo usa 3. Gracias a esta diferencia, la seguridad aumenta en el proceso de la autenticación y la integridad.

Permite comunicaciones seguras (el canal de comunicaciones está cifrado) en internet de aplicaciones del tipo cliente-servidor, garantizando la confidencialidad y la integridad de la información trasmitida-recibida. Por ejemplo, cuando un usuario (cliente) se conecta a la página web de un banco (servidor) para consultar su saldo, existe un intercambio seguro de

información entre el navegador (Internet Explorer, Google Crome, Opera, etc), del usuario y la página web del banco a través de una aplicación.

Este intercambio seguro de información se debe a que los sitios web de las instituciones financieras utilizan protocolo HTTPS (Hipertext Transfer Protocol Secure – Protocolo seguro de transferencia de hipertexto), el cual es el resultado de la combinación del protocolo HTTP (Hipertext Transfer Protocol – Protocolo de transferencia de hipertexto) con el protocolo TLS o el protocolo SSL.

Para el uso del protocolo TLS se necesita que el servidor web tenga soporte TLS y un certificado digital de seguridad emitido por una Autoridad de Certificación (Certification Authority) debidamente autorizada y que sea independiente (Ejemplo Verisign o Thawte), además se requiere que el usuario que se conecta al servidor web también tenga un navegador web con soporte TLS.

2.1.4.2 Cifrado de datos en dispositivos de almacenamiento fijos o extraíbles

El cifrado de datos se lo utiliza para restringir el acceso de personas no autorizadas, a la información confidencial (documentos, fotos, videos, etc.) que se encuentra en discos duros fijos y extraíbles y memorias USB.

Existen programas (software) de cifrado de datos que crean de unidades virtuales o volúmenes contenedores cifrados. Toda la información (archivos o carpetas) que el usuario guarda en estas unidades es cifrada.

También hay programas que cifran las carpetas del sistema operativo o creadas por el usuario. Luego del cifrado de las carpetas no se puede tener acceso a su contenido (archivos).

Además existen software que cifran archivos individuales o agrupados en carpetas (no cifran las carpetas propiamente dichas, sólo su contenido).

Los softwares antes mencionados, cifran los datos combinando la información que se quiere encriptar y la clave ingresada por el usuario, mediante uno o varios algoritmos de cifrado simétrico (son los más indicados cuando el volumen de la información a encriptarse es muy grande). Por lo anterior, se puede decir, que la clave forma parte de los

datos cifrados, lo que significa que dos archivos idénticos cifrados con distintas claves, dan como resultado dos archivos cifrados totalmente diferentes. Como ejemplos de programas gratuitos que sirven para cifrar datos en dispositivos de almacenamiento fijos o extraíbles se puede mencionar: Criptod 5.5, AxCrypt 1.7, FlashCrypt, ICE Encrypt 2.0, TrueCrypt 7.0, CryptoForge, etc.

2.1.4.3 Firma digital

Es un mecanismo de seguridad que establece una relación de autoría entre una persona u ordenador y un documento o mensaje, y además garantiza que el contenido original del documento o mensaje no haya sido modificado. Pueden ser transmitidas fácilmente, son únicas, se pueden grabar con fecha y hora automáticamente, son más difíciles de falsificar que las firmas manuales.

La firma digital combina un algoritmo hash no reversible para garantizar la integridad de los datos y cifrado asimétrico para garantizar la autenticidad del emisor del mensaje.

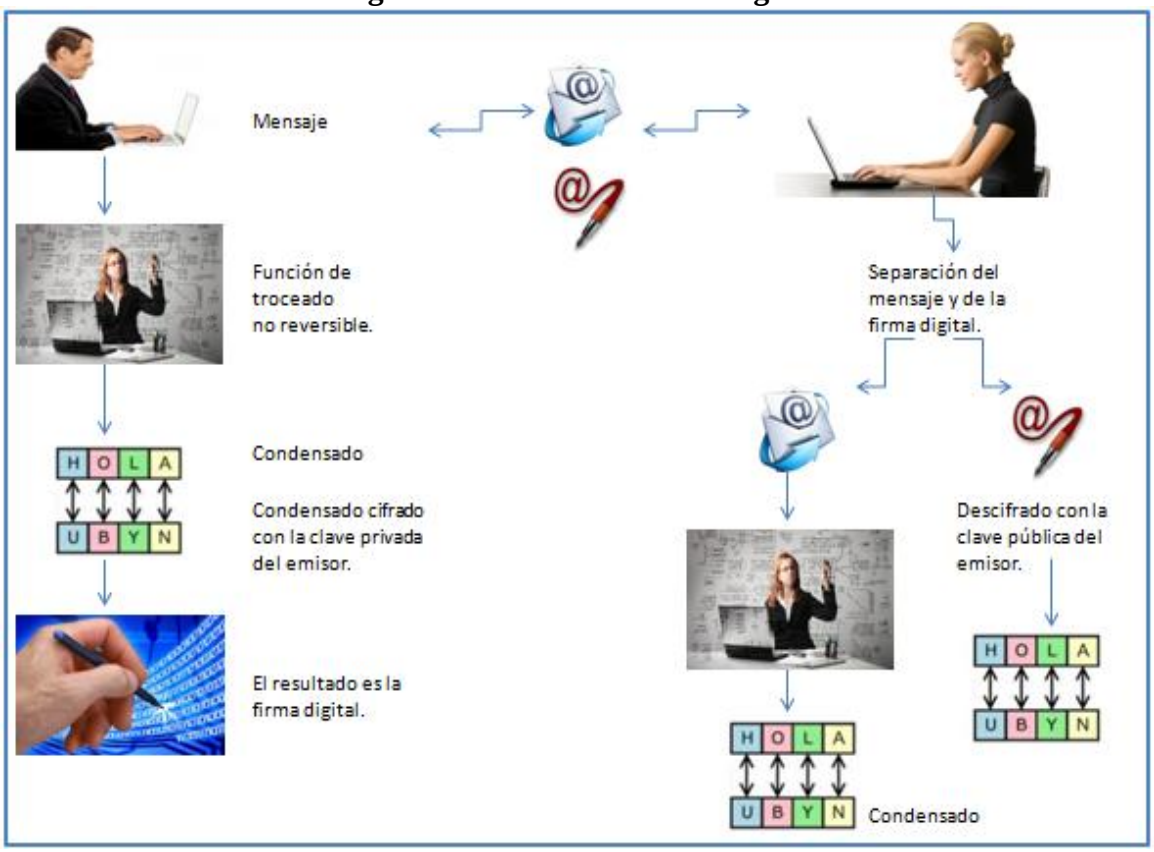
En la actualidad los algoritmos hash más utilizados son MD5 (Message Digest 5) y SHA (Secure Hash Algorithm). Ambos algoritmos utilizan bloques de 512 bits de entrada, MD5 produce un condensado de 128 bits y SHA un condensado de 160 bits. SHA es más seguro que MD5, pero a la vez consume más recursos.

Proceso de la firma digital

1. El emisor redacta el mensaje que va a enviar.
2. El mensaje del emisor es sometido a un algoritmo hash no reversible, dando como resultado una huella digital, conocida con el nombre de condesado.
3. La huella digital o condesado se cifra (por medio de un algoritmo de cifrado asimétrico) con la clave privada del emisor, dando como resultado la firma digital.
4. El emisor une su firma digital al mensaje original.
5. El emisor envía la firma digital y el mensaje original al destinatario.
6. El destinatario utiliza la clave pública del emisor para descifrar la firma digital, obteniendo como resultado la huella o condesado (primer condesado).

7. El destinatario utiliza el mismo algoritmo hash no reversible y se lo aplica al mensaje enviado por el emisor, obteniendo como resultado la huella o condesado (segundo condesado).
8. El destinatario compara los dos condesados. Si son iguales el destinatario tiene la seguridad que el mensaje no ha sido modificado. Además tiene la seguridad de quién envió el mensaje, ya que sólo el propietario de la clave privada pudo cifrar la huella o condesado.

Figura 12. Proceso de firma digital



Fuente: Mathon, P. 2004, p. 374

Elaborado por: María Belén Gómez

2.1.4.4 VPN (Virtual Private Network- Redes privadas virtuales)

Permite que una red LAN (Local Area Network – Red de Área Local) se extienda a diversos puntos remotos, por medio de una red pública como internet.

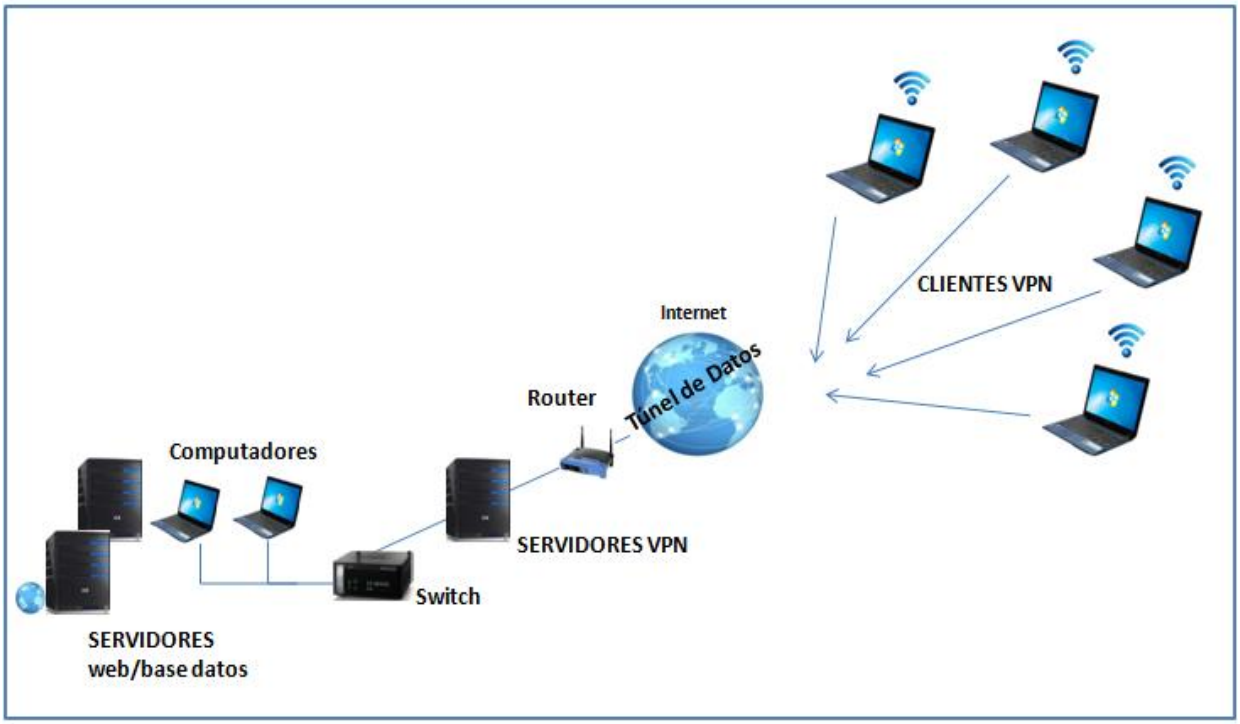
La transmisión de los paquetes de datos se realiza de manera segura, por medio de un proceso de encapsulación y cifrado de datos que funciona como un túnel (sólo ambos

extremos de la conexión pueden ver lo que se transmite) establecido en la red pública, este proceso es necesario ya que los datos viajarán en un determinado momento a través de un trayecto de red pública.

El protocolo más usado por las VPN es IPSec (Internet Protocol Security) aunque también se usan PPTP, L2F, L2TP, SSL/TLS, SSH. IPSec es un conjunto de estándares que verifican y cifran los datos en los paquetes de datos IP que se transmiten por la red pública

La implementación de una red privada virtual ofrece una conexión muy segura a bajo costo, pues sólo se necesita un router VPN de ambos lados o de un solo lado de la conexión, cómo se puede apreciar en la Figura 16.

Figura 13. Red privada virtual



Fuente: http://www.silcom.com.pe/soluciones_seguridad_redes.html
Elaborado por: María Belén Gómez

2.2 Métodos

Como se pudo ver anteriormente, el cifrado de datos, es un sistema de protección, el cual se vale de métodos para lograr su objetivo que es garantizar la seguridad de las comunicaciones. A continuación se describe los métodos de cifrados de datos que existen, cada uno con sus respectivas características, ventajas y desventajas:

2.2.1. Cifrados simétricos

El cifrado simétrico es un sistema por medio del cual a una información se la encripta aplicándole una clave y un algoritmo y se la desencripta (proceso inverso) utilizando la misma clave y el mismo algoritmo de cifrado ejecutado a la inversa. En este método de cifrado, el mensaje fuente es transformado en un mensaje cifrado (aparentemente aleatorio y sin sentido).

Este método de cifrado es rápido y permiten cifrar y descifrar eficientemente con claves relativamente grandes. El problema está en la seguridad de la clave, ya que esta debe ser transmitida sin comprometer su seguridad, al receptor del mensaje para que éste pueda descifrar el mensaje que ha sido enviado por el emisor de forma cifrada.

La seguridad en este método de cifrado depende enormemente del secreto de la clave, más que del secreto del algoritmo, es decir, no se puede descifrar un mensaje teniendo el texto cifrado y sabiendo el algoritmo de cifrado/descifrado.

El nivel de seguridad del método de cifrado simétrico está condicionado por dos factores:

1. Mayor o menor resistencia a los intentos de descubrir la clave por medio del mecanismo de prueba y error, también conocido como fuerza bruta, el cual es común a cualquier método de cifrado. Para incrementar la resistencia es aconsejable aumentar el tamaño de la clave.
2. Falta de certeza acerca de la identidad del emisor, ya que no hay nada que garantice la identidad de la persona que ha cifrado la información. Este inconveniente si se ha podido solucionar y es por eso que este método de cifrado se lo utiliza en los sitios web seguros (aquellos que utilizan protocolo HTTPS).

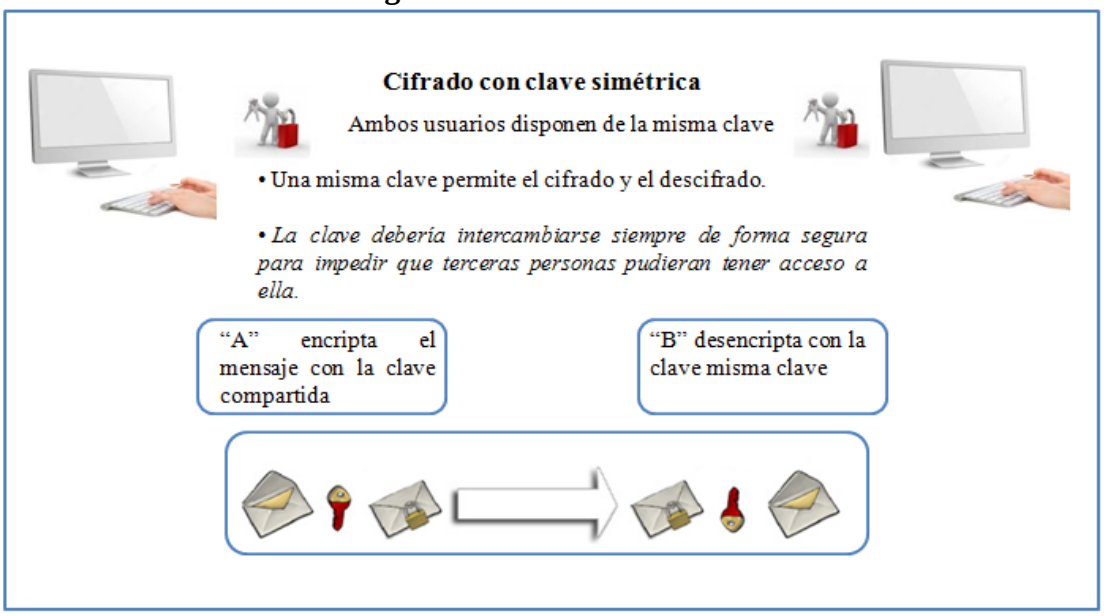
2.2.1.1 Esquema de cifrados simétricos

El cifrado simétrico tiene 5 componentes

1. **Texto claro (texto plano)**.- Es el mensaje o los datos fuentes que se ingresa en el algoritmo como entrada.
2. **Algoritmo de cifrado**.- Es el que realiza las sustituciones y transformaciones del texto claro.

3. **Clave**.- Es también una entrada del algoritmo, Las sustituciones y transformaciones del texto claro dependen de ella.
4. **Texto cifrado**.- Es el mensaje incomprensible que se produce como salida, este depende del texto claro y de la clave.
5. **Algoritmo de descifrado**.- Es el algoritmo de cifrado ejecutado a la inversa. Recibe el texto cifrado y la misma clave y produce el texto claro.

Figura 14. Cifrado simétrico



Fuente: http://www.rinconastur.com/php/php19.php

Elaborado por: María Belén Gómez

2.2.2. Cifrados asimétricos

En este método de cifrado cada usuario tiene dos claves: una privada que sólo conoce él y otra clave pública, la cual es conocida por todos los usuarios. La ventaja que ofrece este método es que, aunque un atacante pueda ser capaz de obtener el texto cifrado, tenga las claves públicas del emisor y receptor, y conozca el algoritmo de cifrado/descifrado, no será capaz de obtener el texto en claro (texto plano).

Cuando el funcionamiento de este método está basado en la factorización de números primos, ayuda a que el cifrado de datos se calcule con relativa facilidad, pero al momento de descifrarlo se necesita mayor procesamiento. La desventaja que tiene este método es que es más lento y hace que la información cifrada tenga mayor volumen.

El funcionamiento de este método es el siguiente:

El emisor A cifra el mensaje con la clave pública del receptor B, la cual es de conocimiento de todos los usuarios del sistema. Para decifrar el mensaje, el receptor B utilizará su clave privada, la cual sólo la conoce él. Con este procedimiento se garantiza la confidencialidad del mensaje, cualquiera puede cifrar, pero sólo la persona que tenga la clave privada podrá descifrar.

El emisor A cifra el mensaje con su clave privada, que sólo él conoce, pero una vez descifrado con esa clave A, la naturaleza del algoritmo estará garantizando que se ha cifrado con la clave B, por lo que la utilización del algoritmo en este sentido se usa para asegurar la autenticidad, y no para ocultar información. Cualquiera tendrá acceso a la información, pero podrá saber a ciencia cierta de dónde procede. El cifrado asimétrico en esta dirección se usa para certificar la autenticidad de las firmas digitales.

El emisor A cifra el mensaje con su clave privada, que sólo él conoce y se la envía al receptor B. Luego el receptor B descifra el mensaje con la clave pública del emisor A, como el mensaje descifrado contiene la clave privada del emisor A, entonces el receptor B puede tener la certeza que el mensaje se lo envió el emisor A, de esta forma queda asegurada la autenticidad de la persona que envió el mensaje. El método de cifrado asimétrico en este sentido, se utiliza para certificar la autenticidad de las firmas digitales.

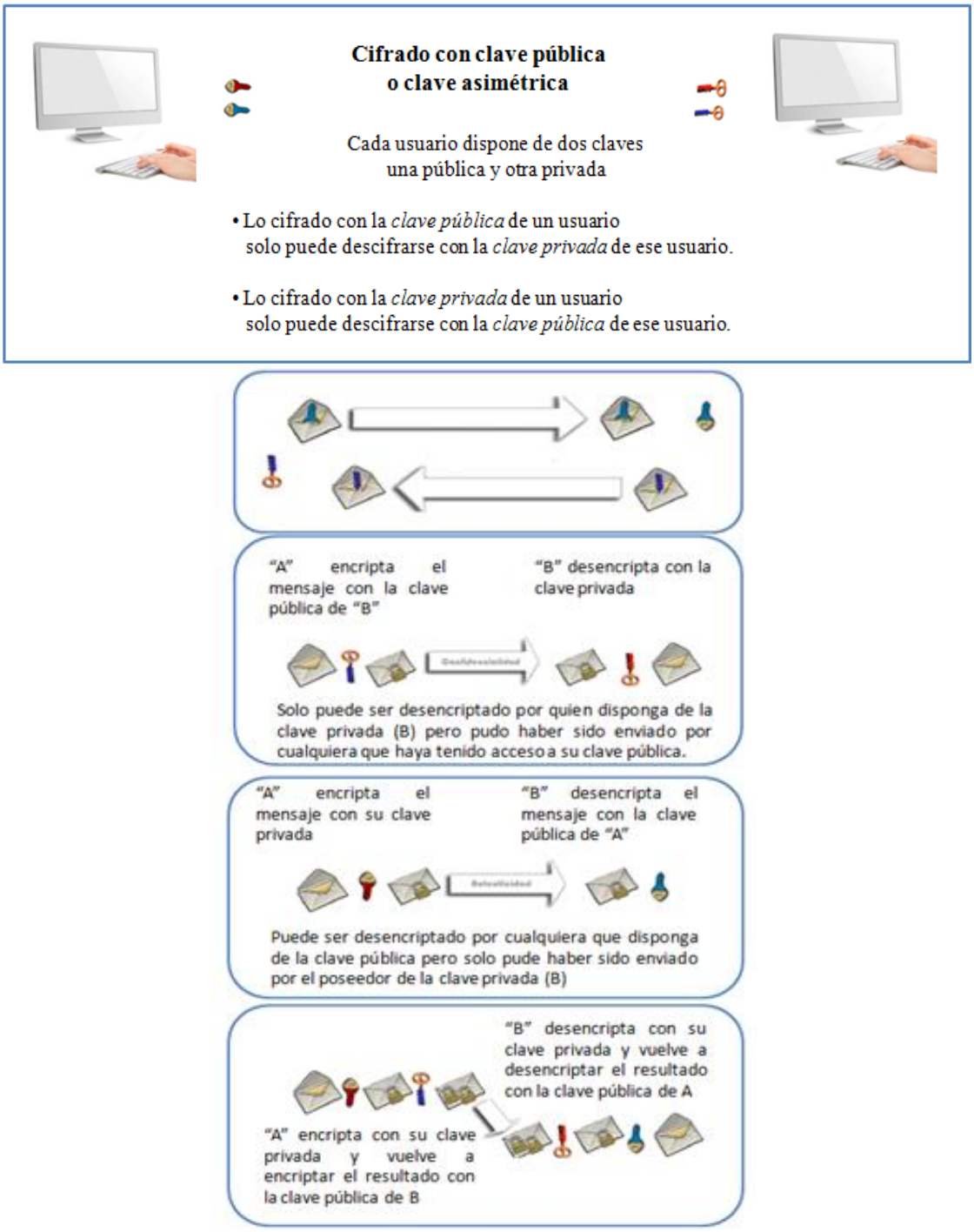
2.2.2.1 Esquema de cifrados asimétricos

El cifrado asimétrico tiene 6 componentes

1. **Texto claro (texto plano)**.- Es el mensaje comprensible que se ingresa en el algoritmo como entrada.
2. **Algoritmo de cifrado**.- Es el que realiza las sustituciones y transformaciones del texto claro.
3. **Clave pública y privada**.- Son una pareja de claves que ha sido previamente seleccionadas, de estas una se usa para el cifrado y la otra para el descifrado. Las sustituciones y transformaciones exactas del texto claro realizadas por el algoritmo de cifrado dependen de la clave pública o privada que se da como entrada.

4. **Texto cifrado**.- Es el mensaje incomprensible que se produce como salida, este depende del texto claro y de la clave.
5. **Algoritmo de descifrado**.- Es el algoritmo de cifrado ejecutado a la inversa. Recibe el texto cifrado y la clave correspondiente y produce el texto claro.

Figura 15. Cifrado asimétrico



Fuente: http://www.rinconastur.com/php/php20.php

Elaborado por: María Belén Gómez

2.3 Algoritmos

2.3.1 Antecedentes

El término algoritmo se origina del nombre Mohamed Ibn Moussa al-KHwarizmi, eminente científico, matemático y astrónomo de Persia, que escribió la obra titulada "Quitab Al Mugabala" entre los años 800 y 825, en la cual se exponía: el sistema de numeración hindú, el concepto del número cero, las reglas del cálculo algebraico, el estudio de ecuaciones de segundo grado, entre otros temas.

Los primeros algoritmos se originaron en Mesopotamia cerca de la ciudad de Babilonia entre los años 3000-1500 a.C. Históricamente los algoritmos siempre estuvieron relacionados con las matemáticas. Ejemplos de esto, es el algoritmo del matemático griego, Euclides (330 a. C – 275 a.C), que consistía en resolver el problema de cómo obtener el máximo común divisor de dos números naturales y la Criba de Eratóstenes que es un algoritmo que permite encontrar todos los números primos menores que un número natural dado.

En el siglo XIX, la analista y metafísica, Ada Augusta Byron, hija del poeta inglés Lord Byron, escribió el primer algoritmo para una computadora. Ella colaboró en el proyecto de Charles Babbage de construir una máquina que pudiera realizar cálculos.

En la actualidad los algoritmos están muy ligados a la informática y a otras disciplinas relacionadas.

2.3.2 Definición

Existen diversas definiciones de lo que es un algoritmo, a continuación se describe algunas de ellas:

> Un procedimiento matemático o lógico para resolver un problema. Es un método para encontrar la respuesta correcta a un problema difícil. Para ello, el problema se divide en un número específico de pasos sencillos. Tiene un principio y un fin, aunque no un tamaño predeterminado. (Sánchez, 2007, p.5).

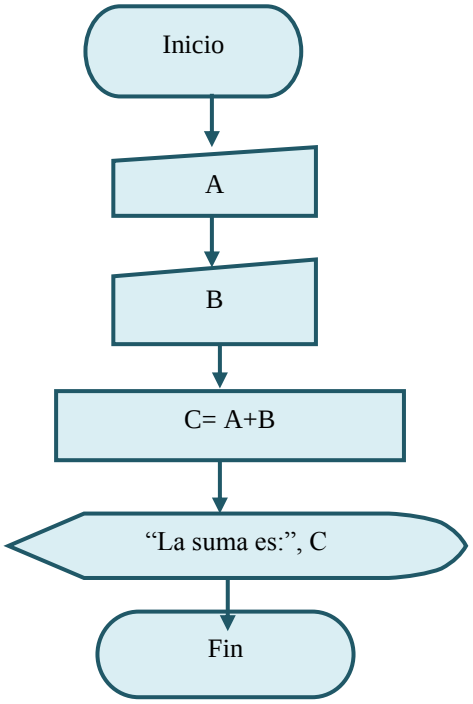
> A la secuencia de instrucciones precisas que lleva a una solución, se le llama algoritmo. Algunas palabras equivalentes son receta, método, instrucciones, procedimiento y rutina. Las instrucciones pueden expresarse en lenguaje de programación o en lenguaje coloquial (Savitch, 2006, p.13).

De acuerdo a las definiciones anteriores se puede concluir, que un algoritmo es una secuencia lógica de operaciones que se requieren para resolver un problema y que tiene principio y fin.

2.3.3 Representación

En informática para desarrollar un software o una aplicación, primeramente se diseña el algoritmo, luego para su mejor entendimiento suelen ser representados por medio de símbolos gráficos llamados diagramas de flujos (véase Figura 18), finalmente son llevados a lenguajes de programación (conjunto de reglas sintácticas y semánticas, que se usan para escribir las instrucciones que realizará una máquina u ordenador para resolver un problema) tales como: C++, Visual basic, Java, etc. y se obtiene como resultado el software (véase Cuadro 2).

Figura 16. Diagrama de flujo de algoritmo que calcula la suma de dos números naturales



Elaborado por: María Belén Gómez

Cuadro 5. Algoritmo que calcula la suma de dos números naturales y su equivalente en un lenguaje de programación

Pasos	Algoritmo	Lenguaje de Programación
1	Ingresar el primer número a sumar	INPUT A
2	Ingresar el segundo número a sumar	INPUT B
3	Calcular la suma	LET C=A+B
4	Mostrar el resultado	PRINT “La suma es:”, C

Elaborado por: María Belén Gómez

2.4 ¿Qué se necesita para cifrar datos?

Como se ha visto anteriormente, es importante cifrar los datos para evitar la pérdida, la interceptación o la sustracción de los datos transmitidos en una red alámbrica o inalámbrica. Para implementar un sistema de cifrado de datos se requiere de ciertos elementos de hardware y software diseñados para este propósito.

La mayoría de soluciones para cifrar datos proporcionan AES de 256 bits como estándar de cifrado, pero hay otras características que se deben considerar antes de implementar cualquier solución:

Administración: Consiste en la facilidad y sencillez con la que se instala, implementa y se gestiona la solución.

Transparencia: Es el grado en que la solución afecta las operaciones de la red y las aplicaciones que hay en la misma.

Flexibilidad: La solución debe ser compatible con cualquier aplicación, topología y protocolos.

Una buena solución debe ser excelente en estos tres aspectos, porque de lo contrario afectaría a su eficacia general.

2.4.1 Requerimiento de hardware

Los requerimientos mínimos de hardware para la implementación un sistema de cifrado en una red inalámbrica local son:

Ruteador inalámbrico.- Son dispositivos especialmente desarrollados para redes domesticas, pequeñas empresas, instituciones educativas, etc. Son de bajo costo y de fácil instalación (no requiere de cableado y de mucho conocimiento técnico), por lo que tienen una alta demanda.

Este dispositivo tiene varias funcionalidades, entre las que se puede mencionar:

- Es el encargado de crear la infraestructura de la red inalámbrica local.
- Trabaja como un punto de acceso porque permite conectar los dispositivos inalámbricos (teléfono movile, notebook, etc) a la red existente.
- Opera como un switch porque permite la conexión por cable de algunos equipos, creando de esta manera una infraestructura de red Ethernet.
- Tiene la función de servir como puerta de enlace, ya que este equipo se conecta al modem del proveedor de internet y luego suministra la conexión a internet a todos los equipos de la red, ya sea que se encuentren conectados por cable o de manera inalámbrica.
- Proporciona el sistema de cifrado de datos (en combinación con el software suministrado por el fabricante), la velocidad inalámbrica y la cobertura necesaria, para compartir archivos, compartir impresoras, navegar por Internet, etc., de manera segura.
- Funciona como puente entre la red inalámbrica y la red inalámbrica.
- Realiza funciones de control de acceso, a través de establecer las direcciones MAC de las computadoras autorizadas para ingresar a la red local, o por medio de consultas a un servidor RADIUS externo a la red.
- Ejecuta el cifrado de datos entre el cliente inalámbrico y el punto de acceso, para lo cual ambos intercambian la clave del cifrado.

Tarjetas de red inalámbrica.- Permiten conectar los equipos a la red inalámbrica, existen de varios tipos, siendo las más utilizadas las tarjetas PCI y las USB.

Las tarjetas PCI se instalan (o vienen instaladas de fábrica) a las computadoras de escritorio o las portátiles.

Las tarjetas USB son las más utilizadas en la actualidad, porque permiten fácilmente conectar un ordenador de escritorio o portátil a la red inalámbrica a través de un puerto USB.

Figura 17. Requerimientos mínimos de hardware para implementar un sistema de cifrado en una red inalámbrica.

Fuente: http://www.trendnet.com/langsp/products/proddetail.asp?prod=225_TEW-711BR&cat=173

2.4.2 Requerimiento de software

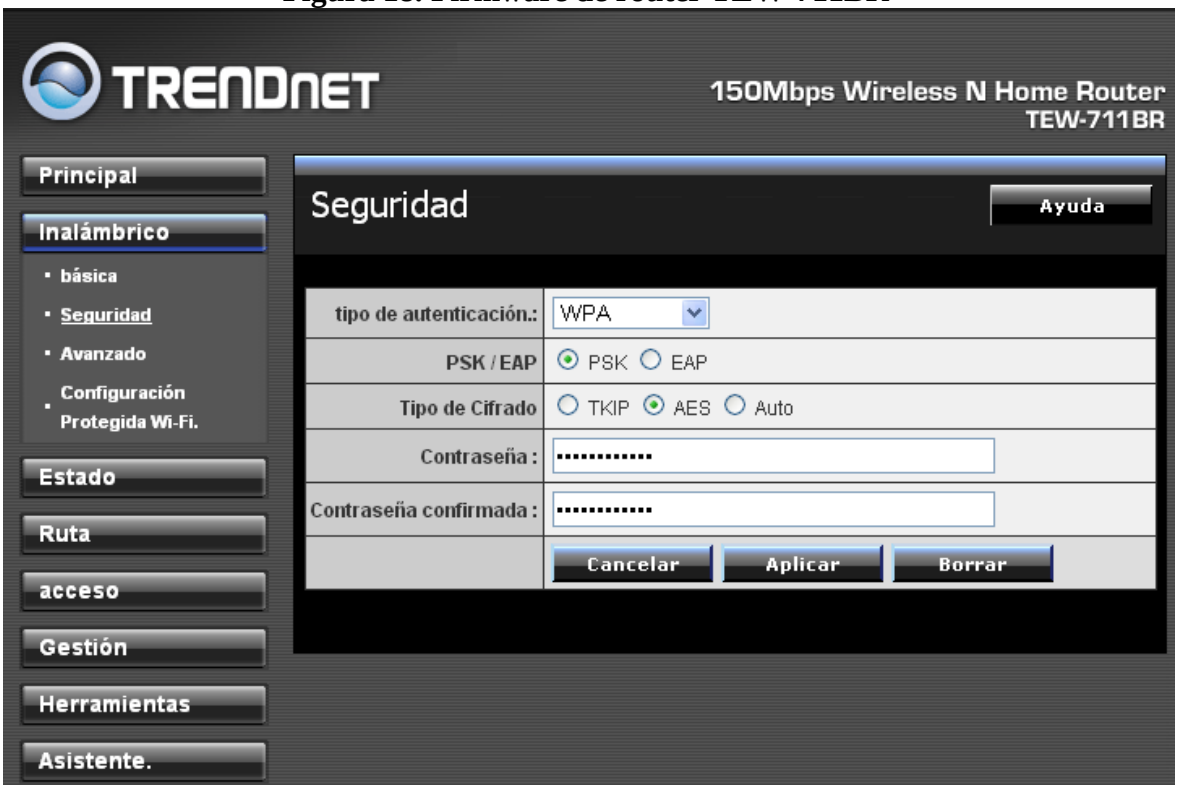
Al adquirir un ruteador inalámbrico este viene acompañado de su respectivo software para instalarlo y configurarlo. Este software también conocido con el nombre de Firmware, es un programa que permite controlar los circuitos electrónicos del dispositivo. Se lo considera parte del hardware porque está integrado en la parte electrónica del dispositivo, pero a la vez es software, porque proporciona la interfaz entre el usuario y el ruteador, y está programado en algún lenguaje de programación. Este software recibe las órdenes del usuario y responde manipulando al dispositivo.

Por medio del firmware se pueden establecer los siguientes parámetros de comunicaciones inalámbricas para la función LAN inalámbrica del ruteador:

- Habilita e inhabilitar la red LAN inalámbrica a través del ruteador.

- Establece el nombre de la LAN inalámbrica, con la finalidad de que los dispositivos inalámbricos la reconozcan y se conecten a ella.
- Oculta o muestra el nombre de red inalámbrica de modo que los clientes inalámbricos para poder conectarse a ella necesitaran conocer el nombre de la LAN inalámbrica.
- Establece el protocolo de cifrado de datos (WEP, WPA WPA2) para transmisiones inalámbricas seguras.

Figura 18. Firmware de router TEW-711BR



Fuente: http://www.trendnet.com/langsp/products/proddetail.asp?prod=225_TEW-711BR&cat=173

2.5 Clases/ Niveles

2.5.1 Cifrado de datos por bloques

El cifrado de datos por bloques es una unidad de cifrado simétrico que trabaja en grupos de bits de longitud fija de tamaños de 64-256 bits cada uno, conocidos con el nombre de bloques, a los cuales se les aplica una transformación que no varía. Cuando se efectúa el

cifrado, una unidad de cifrado por bloques recibe un bloque de texto claro como entrada y lo transforma en un bloque igual tamaño de texto cifrado. La transformación exacta es controlada por una segunda entrada que es la clave secreta. El proceso de descifrado es igual, ingresan bloques de texto cifrado y se transforman en bloques de texto claro. Cuando se requiere cifrar datos más grandes que el tamaño del bloque, se utiliza un modo de operación.

El cifrado de datos por bloque usa combinaciones muy complejas que se basan en sustituciones y cambios de posición que se rigen por la clave de cifrado. Generalmente este tipo de cifrado es más robusto y representa costos más altos que los cifrados por flujo tanto a nivel de creación de dispositivos como a nivel computacional.

2.5.2 Cifrado de datos por flujo

El cifrado de datos por flujo es otra una unidad de cifrado simétrico, realiza el cifrado incrementalmente, es decir, transforma el texto claro en texto cifrado bit por bit, esto se consigue construyendo un generador de flujo de clave, que es una sucesión de bits de tamaño arbitrario.

Se puede crear un generador de flujo de clave repitiendo una función matemática sobre un rango de valores de ingreso para lograr un flujo continuo de valores de salida, estos se concatenan para crear bloques de texto plano, y los bloques se cifran utilizando una clave que la comparten el emisor y el receptor.

Para que la calidad de servicio del flujo de datos se conserve, los bloques del flujo de clave deben producirse con un poco de anticipación sobre el momento en que van a ser utilizados, por otro lado el proceso que los crea no debe exigir mucho esfuerzo de procesamiento que retrase el flujo de datos.

Este tipo de cifrado se lo usa mucho en las telecomunicaciones. Por ejemplo en las conversaciones de telefonía celular, donde la voz se digitaliza, es decir, se convierte a un flujo de bits, una vez cifrada se la envía por la red de telecomunicaciones.

CAPÍTULO 3

SELECCIÓN DEL MÉTODO DE CIFRADO DE DATOS

3.1 Herramientas de cifrado de datos

Son los algoritmos que existen para el cifrado de datos. En la antigüedad la robustez de un método de cifrado de datos se fundamentaba en el secreto del algoritmo de cifrado, es decir, que no fuera del dominio público. Pero en la actualidad los algoritmos de cifrado pueden ser conocidos por todo el mundo y la fuerza del método de cifrado está exclusivamente en la clave de cifrado, la cual se puede cambiar si en algún caso está en riesgo o comprometida.

Los algoritmos de cifrado de datos, son funciones matemáticas utilizadas en los procesos de cifrado y descifrado. Trabajan en combinación con una llave en el proceso de transformar texto claro en texto cifrado, para que usuarios sin autorización no puedan revertirlos con facilidad.

El algoritmo, para cifrar los datos realiza un cálculo matemático, combinando el mensaje a proteger con la llave provista de antemano, dando como resultado de este cálculo los datos cifrados. Para decifrar los datos, el algoritmo realiza otro cálculo matemático, combinando los datos cifrados con la llave provista, obteniendo los datos descifrados.

El objetivo de un algoritmo de cifrado de datos es hacer difícil el proceso de decifrar los datos sin usar la llave. Un algoritmo de cifrado se lo considera bueno, cuando un intruso al ver lo complejidad del mismo recurre a la fuerza bruta, es decir, intentar metódicamente con cada llave posible. Por ejemplo para un algoritmo con una llave de 48 bits, se tendrían que hacer 2^{48} (más de 281 trillones) de intentos de llaves posibles.

Es importante conocer que, para un ataque para obtener la clave no es suficiente probar todas las posibles claves, también se requiere conocer el texto claro. Además, si el algoritmo de cifrado es atacado con fuerza bruta, la manera de contrarrestar ese ataque es usando claves más largas.

Los algoritmos de cifrado de datos para llevar a cabo su labor utilizan como técnicas criptográficas básicas: la sustitución y la permutación o transportación.

La técnica de la sustitución consiste en cambiar el alfabeto del texto plano por un nuevo alfabeto llamado alfabeto de texto cifrado. Por Ej. Se puede establecer un alfabeto de texto cifrado, que sea el alfabeto del texto plano con un desplazamiento de n posiciones.

La técnica de la permutación o transposición consiste básicamente en cambiar la posición de un carácter del texto plano a otra posición. Por Ej. Un carácter que se encuentra en la segunda posición del texto plano, puede ser cambiado a la posición novena del texto cifrado.

3.2 Algoritmos de cifrado de datos existentes

Los algoritmos de cifrado de datos existentes se clasifican en: algoritmos de cifrado simétrico y algoritmos de cifrado asimétrico.

3.2.1 Algoritmos de cifrado de datos simétricos

Estos algoritmos usan una misma clave para encriptar como para desencriptar el mismo texto claro. El proceso para encriptar está formado por dos elementos: un algoritmo y una clave ingresada por un usuario, la cual es independiente del texto que se va cifrar.

La clave es un factor importante para el proceso de encriptación, ya que si se ingresan dos claves distintas para un mismo mensaje, el algoritmo de cifrado va a producir dos textos cifrados distintos para el mismo mensaje.

Los algoritmos de cifrado simétrico existen de 2 tipos: algoritmos simétricos de cifrado de bloques y algoritmos simétricos de cifrado de flujo.

Los algoritmos de cifrado de flujo son los más indicados para trabajar en transmisiones de datos de alta velocidad. Por ejemplo en aplicaciones como el cifrado de conversaciones por teléfono, donde los flujos de datos se efectúan en tiempo real y en pequeñísimos fragmentos (8 bits o 1 bit). Gracias a estos algoritmos las comunicaciones entre receptor-emisor son seguras y fluidas, y no entrecortadas. Entre los algoritmos de este tipo se puede mencionar el algoritmo RC4.

Por otro lado, los algoritmos simétricos de cifrado de bloques son más utilizados en redes de datos alámbricas e inalámbricas. Entre los algoritmos de este tipo se puede mencionar los algoritmos DES, 3DES, RC2, RC5, AES, IDEA, BLOWFISH, CAST, entre otros.

3.2.2 Algoritmos de cifrado de datos asimétricos

Estos algoritmos necesitan de dos claves, una pública usada para cifrar el texto y una privada usada para descifrar el texto cifrado, las dos claves están relacionadas en un cálculo matemático.

La diferencia de los algoritmos asimétricos con respecto a los algoritmos simétricos, está en la longitud de la clave, en un algoritmo simétrico una clave de 128 bits es considerada segura, en cambio en los algoritmos asimétricos es recomendable claves de al menos 1024 bits para alcanzar un nivel similar. Otra diferencia es la rapidez que tienen los algoritmos, los simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos, estos últimos tienen una complejidad de cálculo que los hace lentos, por esta razón no pueden ser utilizados para cifrar grandes cantidades de información.

También existe una diferencia en el proceso de cifrado y descifrado, en los algoritmos simétricos se realizan los dos procesos con la misma clave, en cambio en los algoritmos asimétricos se usa una clave para cifrar el mensaje y otra para descifrarlo.

Entre los algoritmos de este tipo se puede mencionar: Diffie- Hellman, RSA, DSA, Merkle-Hellman, Goldwasser-Micali.

3.2.3 Algoritmos de cifrado de datos utilizados en la transmisión de datos de redes inalámbricas.

En las comunicaciones de las redes inalámbricas, es muy importante lograr que los datos se transmitan de forma segura, es decir, asegurar la autenticidad, no repudio, integridad y la confidencialidad de los mismos. Estas características solamente se las puede conseguir por medio de un algoritmo de cifrado, los cuales ayudan a evitar ataques pasivos y activos.

En los ataques pasivos los datos no son alterados, pero son escuchados y monitoreados, obteniendo de esta manera la información transmitida. Por lo anterior son difíciles de

detectar, puesto que no producen ningún cambio en los datos. Los objetivos de estos ataques son interceptar los datos y el análisis de tráfico, una forma muy sutil de conseguir información de las transmisiones de datos.

En los ataques activos los datos son alterados. Dentro de estos tipos de ataques están la suplantación de identidad, cuando el atacante se hace pasar por otro ente; reactuación, cuando uno o varios datos originales son capturados y repetidos sin ninguna autorización; modificación de datos, cuando el atacante cambia los mensajes transmitidos.

Tanto los ataques activos como los pasivos son posibles evitar por medio de algoritmos de cifrado datos, los cuales operan en algún protocolo de la red, proporcionándole seguridad al mismo y por consiguiente a la red.

Los algoritmos de cifrados de datos más indicados para garantizar la seguridad en la transmisión de datos de redes inalámbricas son los algoritmos simétricos, puesto que usan menos los recursos de los sistemas computacionales y son más rápidos que los algoritmos asimétricos cuando se trata de cifrar y descifrar grandes volúmenes de información.

Para su implementación en una red inalámbrica se comparte la clave secreta entre el dispositivo o equipo inalámbrico y el punto de acceso (router inalámbrico) al que se conecta.

Los algoritmos simétricos cifran el documento o mensaje, una vez cifrado es transmitido por la red. Para descifrar o recuperar el mensaje original se utiliza el mismo algoritmo (en forma inversa) y la misma clave usada para el cifrado.

Entre los protocolos que utilizan algoritmos de cifrado simétricos se pueden mencionar: WEP (Wired Equivalent Privacy) y WPA (WiFi Protected Access) que utilizan el algoritmo RC4, WPA2 (WiFi Protect Access 2) que utiliza el algoritmo AES y el protocoló IPSec (Internet Protocol security) que puede utilizar los algoritmos IDEA, DES, 3DES, AES, RC5.

Los algoritmos de cifrado simétrico que se describirán a continuación son utilizados en los protocolos antes citados, los cuales son utilizados en las transmisiones de datos de las redes inalámbricas, proporcionando seguridad a las comunicaciones.

DES (Data Encription Standard)

El algoritmo DES (Data Encription Standard - Estándar de Encriptación de Datos), es el algoritmo de cifrado simétrico más estudiado, mejor conocido en el mundo. Fue desarrollado originalmente por IBM y adoptado en 1977 por National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología), perteneciente al del Departamento de Comercio de Estados Unidos. En 1998 dejó de ser utilizado por el gobierno de los Estados Unidos, cuando Electronic Frontier Foudation anunció que había descifrado un mensaje cifrado con algoritmo DES en menos de tres días.

Características

Al inicio operaba sobre bloques de 128 bits y claves de igual tamaño, y se lo podía implementar fácilmente en software y en hardware. Pero con el tiempo la NBS (National Bureau of Standards - Oficina Nacional de Estandarización) le realizó algunas modificaciones, que consistían en la disminución de la longitud de la clave y de los bloques, quedando en 64 bits respectivamente.

El DES era un algoritmo muy seguro, pero dejo de serlo, porque con hardware específico se puede hacer ataques por fuerza bruta que revelen una clave en pocos días. El problema se debe al tamaño de clave que maneja de 64 bits, de los cuales 56 bits son utilizados para cifrar (lo cual es muy pequeño para la potencia de cálculo que manejan los ordenadores actuales) y los 8 bits restantes son de paridad y se utilizan para detectar errores en el proceso.

En este algoritmo el texto claro se divide en bloques de 64 bits y el proceso de descifrado es básicamente el mismo que el de cifrado.

Su funcionamiento está basado en un sistema monoalfabético y consiste en la aplicación secuencial de varias permutaciones y sustituciones.

Funcionamiento

El funcionamiento del algoritmo DES no es secreto, la fuerza de su cifrado está en la complejidad de algunos procesos interiores de permutación y sustitución no sometidos a las reglas del algoritmo. Pero su mayor fuerza está en la longitud de las claves utilizadas y en la dimensión del campo de claves, puesto que una de las formas de criptoanálisis consiste en la de prueba-ensayo (fuerza bruta).

En términos generales el algoritmo DES tiene 19 etapas distintas. La etapa 1 es una transposición (Permutación Inicial IP) del texto claro de 64 bits o múltiplo de 64 (independiente de la clave ingresada por el usuario). Luego viene una red de Feistel (método de cifrado en bloque) compuesta de 16 vueltas. En cada una de estas 16 vueltas se utiliza un valor K_n, que se obtiene de la clave de 56 bits, el cual es distinto en cada vuelta.

1. Procesamiento de la clave (véase Figura 19)

1.1. El usuario ingresa una clave de 64 bits (8 bytes).

Ésta puede ser ingresada directamente o podría ser el resultado de una operación anterior, puesto que no hay ninguna descripción al respecto. Se divide la clave en 8 bytes y se elimina el último bit (el menos significativo) de cada byte, quedando como resultado sólo 56 bits de los 64 bits iníciales.

1.2. Cálculo de las subclaves (véase Figura 20).

1.2.1. Se realiza la siguiente permutación con la clave de 64 bits, quedando reducida a 56 bits (El bit 1, el más significativo, de la clave convertida u obtenida es el bit 57 de la clave original; el bit 2, de la clave convertida es el bit 49 de la clave original).

Cuadro 6. Permuted Choice 1 (PC-1)

57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

1.2.2. Se divide la clave permutada en 2 partes de 28 bits cada una. C(0) es el bloque que tiene los 28 de mayor peso y D(0) los otros 28 bits que restan.

1.2.3. Se calculan las 16 subclaves (Se empieza con i=1).

1.2.3.1. Se rotan 1 ó 2 bits a la izquierda C(i-1) y D(i-1), y se obtiene C(i) y D(i) respectivamente. El número de bits de desplazamiento se sujeta a la siguiente tabla:

Cuadro 7. Número de bits de desplazamiento

Vuelta	1	3	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits desplaz.	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

1.2.3.2. Se concatenan C(i)y D(i) y se permuta como se indica en la siguiente tabla. Como resultado se obtiene K(i), la cual posee una longitud de 48 bits.

Cuadro 8. Permuted Choice 2 (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

1.2.3.3. Se regresa al punto 1.2.3.1 hasta que se calcule K(16).

Procesamiento del texto claro (véase Figura 19)

1. El texto claro se divide en bloques de 64 bits (si un bloque posee menos de los 64 bits, se debe completar el bloque hasta que tenga los 64 bits).
2. Se aplica la siguiente permutación (Permutación inicial) al bloque de 64 bits.

Cuadro 9. Permutación inicial

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

3. El bloque que se obtuvo como resultado se divide en 2 partes de 32 bits cada una L(0) y R(0) . L(0) es el bloque con los 32 bits de mayor peso y R(0) tiene los 32 bits restantes.
4. Se aplican las 16 subclaves obtenidas durante el **procesamiento de la clave**
   a) Se expande R de 32 bits a 48 bits realizando la siguiente permutación. Como se puede ver en el cuadro siguiente se repiten algunos bits, esto se hace con la intención de expandir de 32 bits a 48 bits.

Cuadro 10. Expansión (E)

32	1	2	3	4	5	4	5
6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27
28	29	28	29	30	31	32	1

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

   b) Se hace la operación XOR entre el bloque obtenido con K(i).

c) El resultado obtenido en el literal anterior se divide en 8 bloques de 6 bits cada uno (B1, B2, B3,….B8).

d) Para cada bloque se toma el primer y último bit y se forma un número llamado m compuesto de 2 bits.

e) Para cada bloque se toma los bits 2,3, 4 y 5 y se forma un número llamado n de 4 bits.

f) El número m representan una fila y el número n representa una columna. En el siguiente cuadro se puede observar las cajas de sustitución para cada bloque. Se tiene que seleccionar la fila y la columna obtenidas de m y n, y reemplazar el valor de Bj por el de Sj en cada uno de los 8 bloques. Cada bloque Bj es originalmente de 6 bits, luego de la sustitución quedan bloques de 4 bits.

Cuadro 11. S-cajas del algoritmo DES

Fila	Columna																S-Caja
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5

1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	**S_6**
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	**S_7**
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	16	15	11	1	10	9	3	14	5	0	12	7	**S_8**
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

g) Después de la sustitución se concatenan los 8 bloques y quedará un solo bloque de 32 bits.

h) Se realiza la siguiente permutación.

Cuadro 12. Permutación P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

i) Se realiza una or-exclusiva entre la permutación anterior y el bloque L que se obtuvo en el paso 3.

j) El resultado del literal anterior será la entrada para la siguiente iteración (se repite desde el literal a) hasta que se apliquen las 16 subclaves.

5. Se realiza la siguiente permutación del bloque R(16) L(16).

Cuadro 13. Permutación final

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

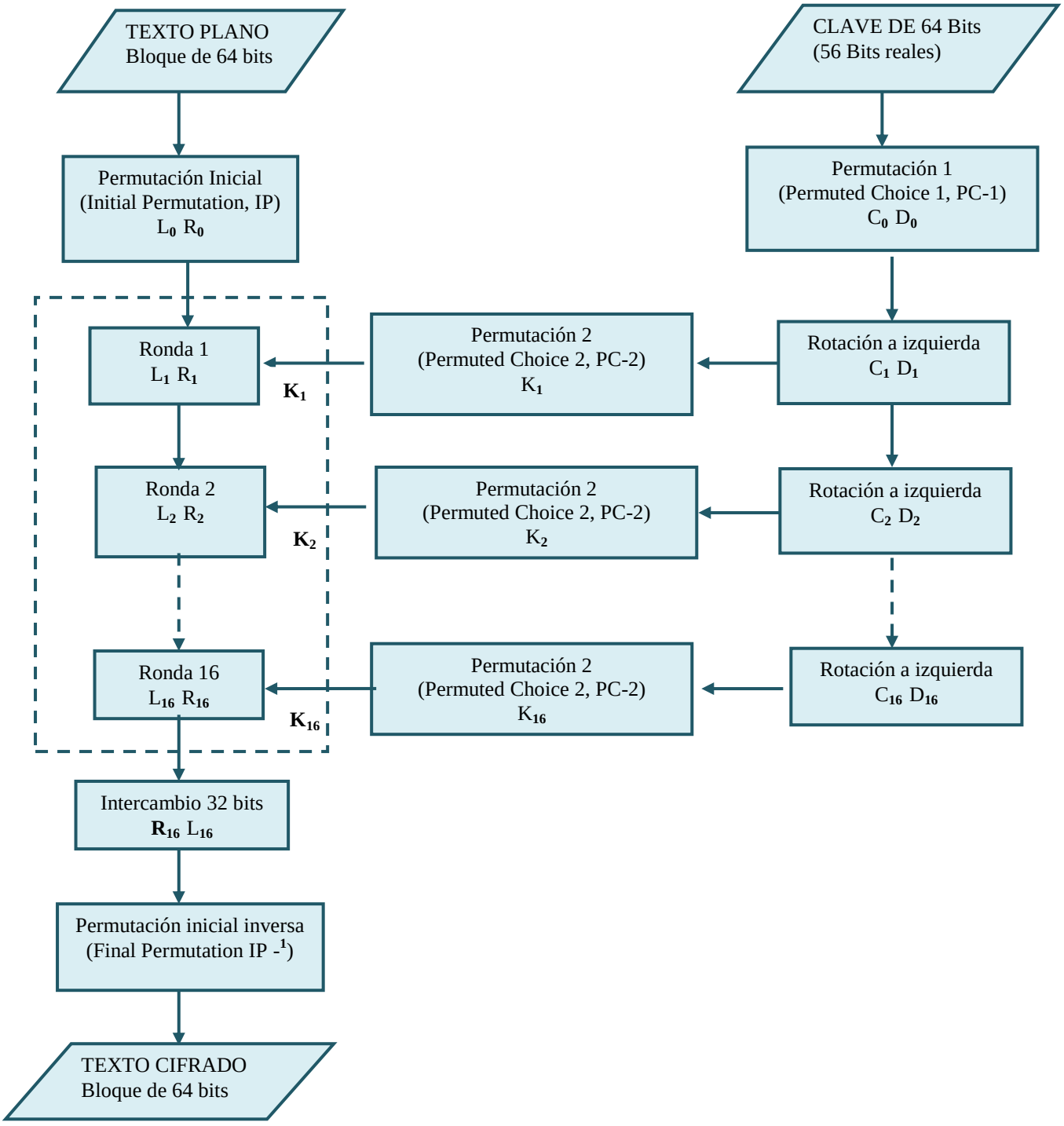
Elaborado por: María Belén Gómez

6. Se obtiene el texto cifrado de 64 bits.

Descifrado

Para el descifrado se usa el mismo proceso descrito anteriormente pero utilizando las subclaves en orden inverso, es decir, aplicar K(16) para la primera iteración, aplicar K(15) para la segunda, aplicar K(14) para la tercera y así sucesivamente hasta aplicar K(1) en la última iteración.

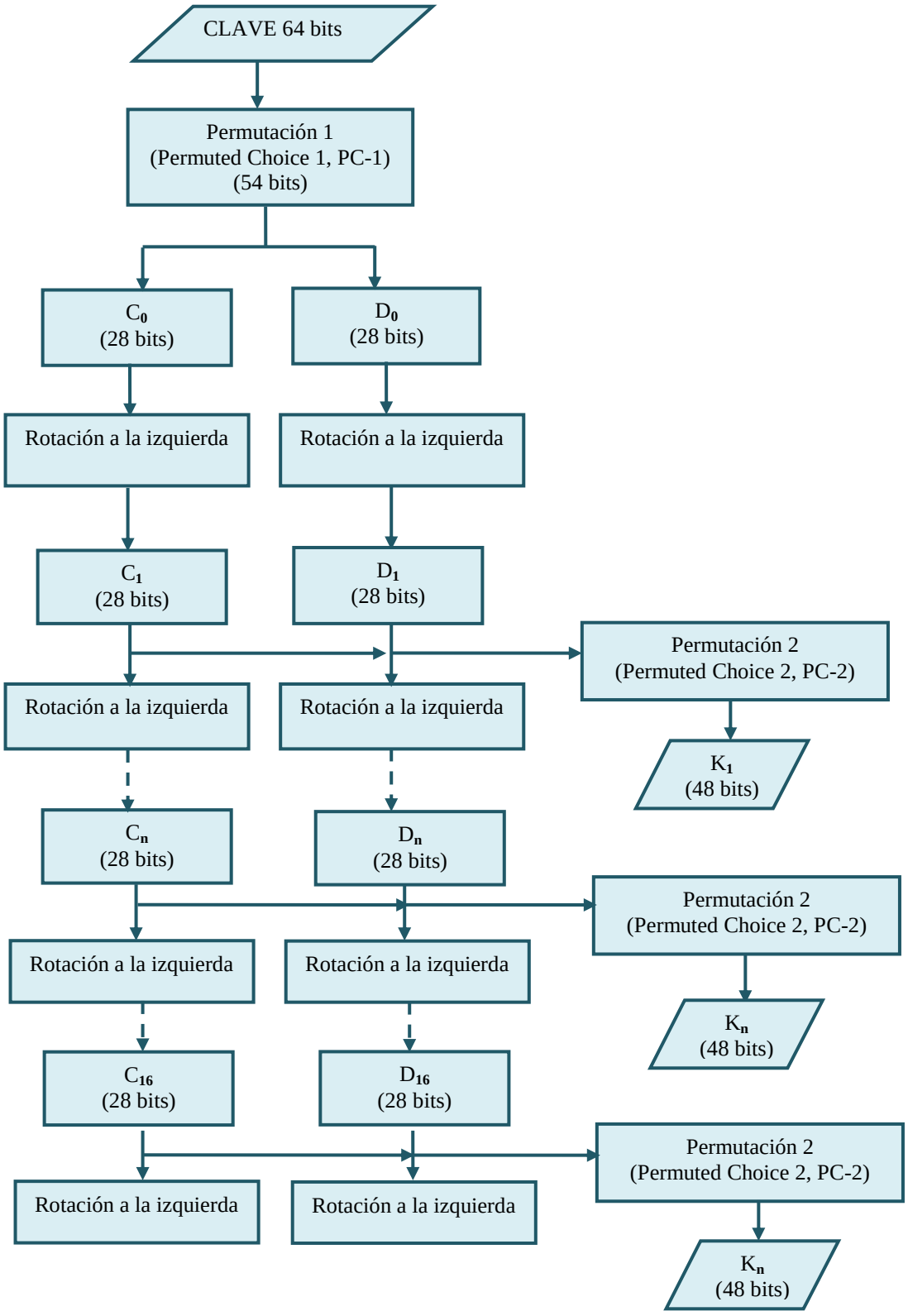
Figura 19. Diagrama de flujo general del algoritmo DES



Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

Figura 20. Diagrama de flujo del cálculo de las subclaves del algoritmo DES



Fuente: http://www.tierradelazaro.com/public/libros/des.pdf

Elaborado por: María Belén Gómez

3DES (3 Data Encription Standard)

Fue planteado por Tuchman y publicado en el año 1999 por el FIP (Federal Infomation Processing), como una mejora del algoritmo DES, puesto que dejó de ser un algoritmo seguro por el aumento del poder de cálculo de las computadoras.

Características

Existen versiones de este algoritmo que usa claves de 128 bits (112 bits para la clave y 16 bits de paridad), lo que equivale a 2 claves de 64 bits (56 bits para la clave y 8 bits de paridad) de las usadas en el DES. La razón de usar esta longitud de clave es que sea compatible con el algoritmo DES. También existen versiones modernas con claves de 192 bits (168 bits para la clave y 24 bits de paridad) que son más robustas.

Aplica el algoritmo de cifrado DES a los mismos datos tres veces con la finalidad de aumentar el nivel de cifrado, con esto aumenta la longitud de la clave de cifrado 192 bits, lo cual no lo hace más lento que otros algoritmos de cifrado. No es un algoritmo de cifrado múltiple, porque todas sus subclases no son independientes, esto se debe a que este algoritmo tiene la característica de no ser un grupo, lo que implica que si se cifra el mismo bloque en dos ocasiones con 2 claves distintas, aumenta el tamaño efectivo de la clave.

Cuando se supo que la clave de 56 bits del algoritmo DES no era suficiente para impedir un ataque de fuerza bruta, se prefirió 3DES como una forma de agrandar el largo de la clave sin tener que cambiar de algoritmo de cifrado.

El algoritmo 3DES es inmune a ser atacado por encuentro a medio camino, aumentando la longitud efectiva de la clave, pero a cambio se logra triplicar el número de operaciones de cifrado, haciendo de este algoritmo de cifrado más seguro que el DES.

Actualmente el 3DES está desapareciendo poco a poco, por ser un algoritmo lento (AES puede ser hasta 6 veces más rápido), y está siendo reemplazado por el algoritmo AES. Pero todavía gran cantidad de tarjetas de crédito y otros medios de pago electrónico utilizan el 3DES.

AES (Advanced Encryption Estándar)

En 1997, el National instite for Standars and Technolgy de los Estados Unidos, convocó a concurso al público en general para desarrollar un algoritmo de cifrado que reemplazará al DES, como resultado se diseño un algoritmo de cifrado simétrico conocido como Rjindael por los apellidos de los diseñadores (Vincent Rijmen y Joan Daemen, estudiantes de la Katholieke Universiteit Leuven de Bélgica).

En el año 2002 se convirtió en un estándar y posteriormente se le realizaron algunas modificaciones por lo que fue renombrado como AES (Advanced Encryption Estándar-Estándar de cifrado avanzado).

En el año 2003 fue declarado como un algoritmo seguro por el gobierno de los Estados Unidos. Hasta la actualidad no se conoce que haya tenido ataques eficientes.

Características

El algoritmo de cifrado AES utiliza una clave de cifrado que puede tener una longitud de 128, 192 ó 256 bits y cifra los textos claros en bloques de 128 bits (el algoritmo original Rjindael puede manejar bloques de entre 128 y 256 bits). Este algoritmo es aplicado a los datos 10, 12, o 14 veces (rondas), lo que lo hace muy seguro.

Está formado por 4 funciones invertibles desarrolladas para resistir criptoanálisis lineal y diferencial.

Para descifrar los datos en cada ronda se aplica las inversas de las funciones en orden contrario al utilizado en el cifrado.

Es rápido, fácil de implementar en hardware y software, y consume poca memoria.

Opera en matrices de 4x4 bytes, que reciben el nombre de estado.

Todavía no se sabe de ataques eficientes que hayan vulnerado este algoritmo.

RC5 (Rivest Cipher 5)

El algoritmo Rivest Cipher 5 más conocido como RC5, fue diseñado en 1994 por Ron Rivest para la RSA Data Security. Difiere de otros algoritmos porque es configurable en

todos sus aspectos, puede usar diversos tamaños de bloque (32, 64 ó 128 bits), permite longitud variable de clave (de 8 a 2048 bits) y numero de rotaciones (vueltas) de 0 a 255.

Características

La combinación propuesta originalmente era bloques de 64 bits, claves de 128 bits y 12 rotaciones (vueltas). Este algoritmo es usado por el navegador Netscape en su implementación Secure Sockets Layer (SSL).

Tiene tres rutinas: expansión de la clave, cifrado y descifrado. En la primera rutina la clave ingresada por el usuario se expande hasta llenar una tabla de claves cuyo tamaño depende del número de vueltas, esta tabla se utiliza en el cifrado y el descifrado.

La combinación de vueltas dependientes de los datos y de distintas operaciones hace que sea resistente al criptoanálisis lineal y diferencial. Su implementación y análisis es fácil, y se lo considera por el momento seguro.

IDEA (International Data Encription Algorithm)

El algoritmo IDEA (International Data Encription Algorithm- Cifrado de datos internacional) fue desarrollado en 1990 y mejorado en 1992 por X. Lai y J. Massey.

Características

Trabaja con bloques de 64 bits de longitud y emplea claves de 128 bits, lo que lo hace muy robusto frente a ataques de fuerza bruta y al criptoanálisis diferencial. Este algoritmo funciona de la misma manera para cifrar como para descifrar (excepto en el cálculo de las subclaves). Se lo puede implementar fácilmente en hardware y software, pero algunas de las operaciones que hace en software no son eficientes.

A diferencia del algoritmo DES, no presenta problemas de claves débiles, y la longitud de clave que tiene, hace que sea imposible los ataques por fuerza bruta, aunque sea con la capacidad de procesamiento de los actuales ordenadores. Es robusto frente al criptoanálisis diferencial y diferencial y no tiene debilidades algebraicas.

El IDEA tiene un funcionamiento que consta de 8 etapas o vueltas y divide el bloque de datos en cuatro partes de 16 bits.

RC4 (Rivest Cipher 4)

Desarrollado en 1987 por Ron Rivest, uno de los fundadores de la empresa RSA Security. El nombre de este algoritmo se debe a la inicial del apellido Rivest (creador) y la inicial de la palabra Cipher (cifra). Lo anterior se aplica también a los algoritmos RC2, RC5 y RC6.

En sus comienzos era comercializado como secreto, es decir, que sólo se conocía el código binario del algoritmo y no se conocía cómo estaba implementado ni tampoco su algoritmo teórico. Pero en 1994 una descripción de este algoritmo fue anónimamente publicada y se esparció por muchos sitios web, por tal razón dejó de comercializarse como algoritmo secreto.

Características

Usa la misma información de entrada que va a cifrar para crear un número pseudoaleatorio que usará como clave, ejecutando un XOR entre la información de entrada y la clave.

El cifrado como el descifrado son operaciones similares.

Es un algoritmo de cifrado de flujo y la clave varía de 8 a 2048 bits.

Es seguro pero algunos modos de utilizar el algoritmo lo han llevado a ser muy inseguro. Por ejemplo su uso en el protocolo WEP.

Es rápido y está compuesto de 2 algoritmos: Key Scheduling Algorithmn (KSA) y Pseudo-Random Generation Algorti(PRGN).

Es sencillo de implementar tanto en software como en hardware y se requiere de pocos recursos para lograr un rendimiento eficiente.

Entre las debilidades se puede mencionar: En la clave existen patrones sin variantes que se propagan al interior del algoritmo, lo que hace que los primeros bytes creados sean predecibles. Además presenta debilidad cuando la clave procede de una concatenación con un vector inicial público, al recolectar gran cantidad de mensajes y vectores iníciales la clave que descubierta.

3.2.4 Uso de algoritmos de cifrado de datos en servidores Web de entidades públicas y privadas.

A continuación se detalla importantes entidades del país que utilizan algoritmos de cifrado en sus sitios web.

Cuadro 14. Entidades del país que utilizan algoritmos de cifrado en sus sitios web

Institución	Algoritmo utilizado	Sitio web
BANCO DE GUAYAQUIL MULTIBANCO	AES-256	http://www.bancoguayaquil.com/
BANCO PICHINCHA En confianza.	RC4-128	http://www.pichincha.com/web/index.php
Banco Bolivariano	RC4-128	http://www.bolivariano.com.ec/
BANCO DEL PACÍFICO GRUPO FINANCIERO	RC4-128	https://www.bancodelpacifico.com/inicio.aspx
Banco de Machala El Oro es nuestro respaldo	3DES	http://www.bancomachala.com/home.aspx
BancoAmazonas Su Banca Personalizada	RC4-128	https://www.bancoamazonas.com/portal/index.jsp
SRI Servicio de Rentas Internas	AES-256	http://www.sri.gob.ec/web/guest/home
Instituto Ecuatoriano de Seguridad Social IESS	RC4-128	http://www.iess.gob.ec/
BANCO INTERNACIONAL	AES-256	http://www.bancointernacional.com.ec
BANCO CENTRAL DEL ECUADOR	RC4-128	http://www.bce.fin.ec/
BGR BANCO GENERAL RUMIÑAHUI	AES-256	http://wwwp2.bgr.com.ec/portal/web/guest/inicio
Claro	AES-256	http://www.claro.com.ec/portal/ec/
movistar	AES-256	http://www.movistar.com.ec/site/

Elaborado por: María Belén Gómez

3.3 Cuadro comparativo

Cuadro 15. Cuadro comparativo de algoritmos de cifrados

Algoritmo	T. de clave	T. bloque	No. de vueltas	Uso en Entid.	Vulnerabilidad	Observaciones
DES	56 bits	64 bits	16	NADA	Dejo de ser utilizado en 1998 Por EE.UU. por haber sido vulnerado	Creado en 1977
3DES	168 bits	64 bits	48	BAJO	Es 3 veces más seguro que el DES pero a la vez es 3 veces más lento.	Publicado en 1999 por el FIP Está en desuso
AES	128, 192, 256 bits	128 bits	10,12,14	ALTO	No ha sido vulnerado	Desarrollado en 1997 En el 2003 fue declarado seguro por EE.UU Fue creado para reemplazar al 3DES Es más rápido que el 3DES
IDEA	128 bits	64 bits	8	NADA	Es robusto frente al criptoanálisis diferencial y diferencial Imposible los ataques por fuerza bruta	Fue desarrollado en 1990 y mejorado en 1992
RC4	Hasta 2048 bits	Cifrador de flujo	Cifrador de flujo	ALTO	Es seguro pero algunos modos de utilizar el algoritmo lo han llevado a ser muy inseguro. Por ejemplo su uso en el protocolo WEP	Fue desarrollado en 1987
RC5	Hasta 2048 bits	32, 64, 128 bits	Hasta 255	NADA	Es resistente al criptoanálisis lineal y diferencial Se lo considera seguro	Fue diseñado en 1994

Elaborado por: María Belén Gómez

3.4. Tres herramientas seleccionadas

A continuación se realizará una evaluación de los aspectos más significativos (vulnerabilidad, tamaño de la clave, número de vueltas o rondas en la estructura del algoritmo, uso en entidades públicas y privadas) de cada uno de los algoritmos de cifrados estudiados, con la finalidad de seleccionar los tres mejores.

Para evaluar los aspectos más significativos, en primer lugar se realizará la ponderación de cada uno de ellos. El peso asignado establece el grado de importancia de dicho aspecto.

En el cuadro 17 se puede observar que los aspectos que tienen mayor importancia son: En primer lugar la seguridad, puesto que esta es la razón de ser de un algoritmo. En segundo lugar es el tamaño de la clave, mientras más grande sea es más fuerte el algoritmo. En tercer lugar el número de vueltas que posee en la estructura el algoritmo, y en último lugar el uso que tiene en instituciones.

Cuadro 16. Ponderación de los aspectos significativos

Aspectos significativos	Ponderación	%	
Vulnerabilidad	4	40%	0.4
Uso en entidades	3	30%	0.3
Tamaño de clave	2	20%	0.2
No. Vueltas	1	10%	0.1

Elaborado por: María Belén Gómez

Para calificar cada uno de los aspectos anteriores se utilizará la siguiente escala de calificación.

Cuadro 17. Escala de calificación de aspectos significativos

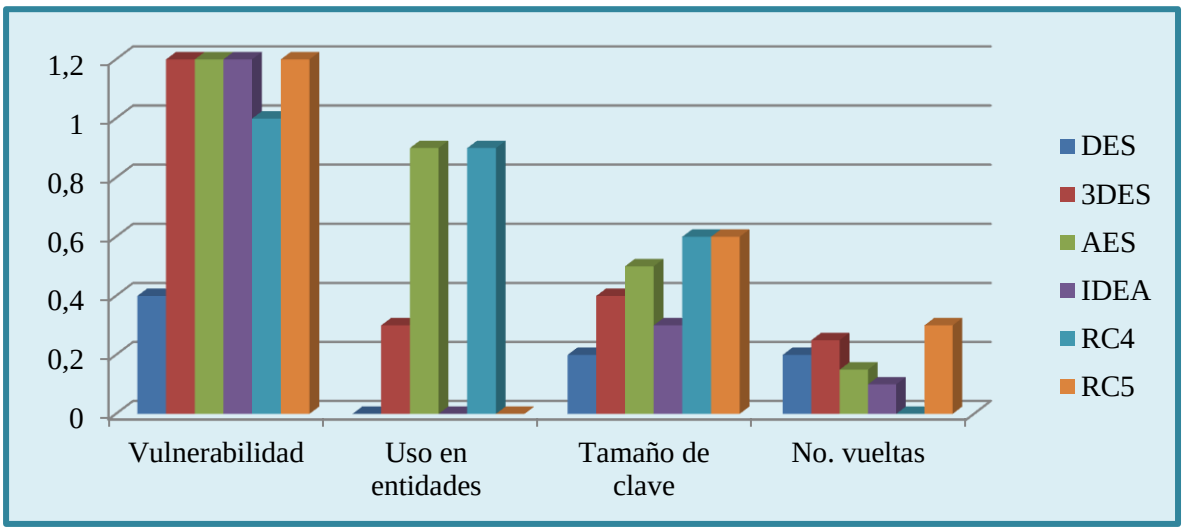
Muy alta	3
Alta	2,5
Media	2
Baja	1,5
Muy baja	1
Nada	0

Elaborado por: María Belén Gómez

3.4.1. Evaluación de los algoritmos estudiados

Para seleccionar los 3 mejores algoritmos utilizados en la transmisión de datos de redes inalámbricas, se hizo una evaluación de los aspectos significativos.

Gráfico 1. Evaluación de los aspectos significativos de los algoritmos estudiados



Elaborado por: María Belén Gómez

Vulnerabilidad: La calificación más alta (3) la obtuvieron los algoritmos AES, IDEA, 3DES y RC5, porque son algoritmos que no han presentado ninguna vulnerabilidad ante ninguna circunstancia. Al algoritmo RC4 se le dio la calificación de (2,5) porque esté pierde seguridad de acuerdo al modo como se lo utiliza. Al algoritmo DES se le asignó la calificación muy baja (1) porque ya ha sido vulnerado.

Tamaño de clave: La calificación más alta (3) la obtuvieron los algoritmos RC4 y RC5, porque son los algoritmos que poseen una longitud de clave grande (Hasta 2048 bits). Al algoritmo AES se les dio la calificación (2,5) porque tiene una longitud de clave de hasta 256 bits. Al algoritmo 3DES se les dio la calificación (2) porque tiene una longitud de clave de 168 bits. Al algoritmo IDEA se les dio la calificación (1,5) porque tiene una longitud de clave de 128 bits. Al algoritmo DES se le asignó la calificación muy baja (1) porque una longitud de clave de 56 bits.

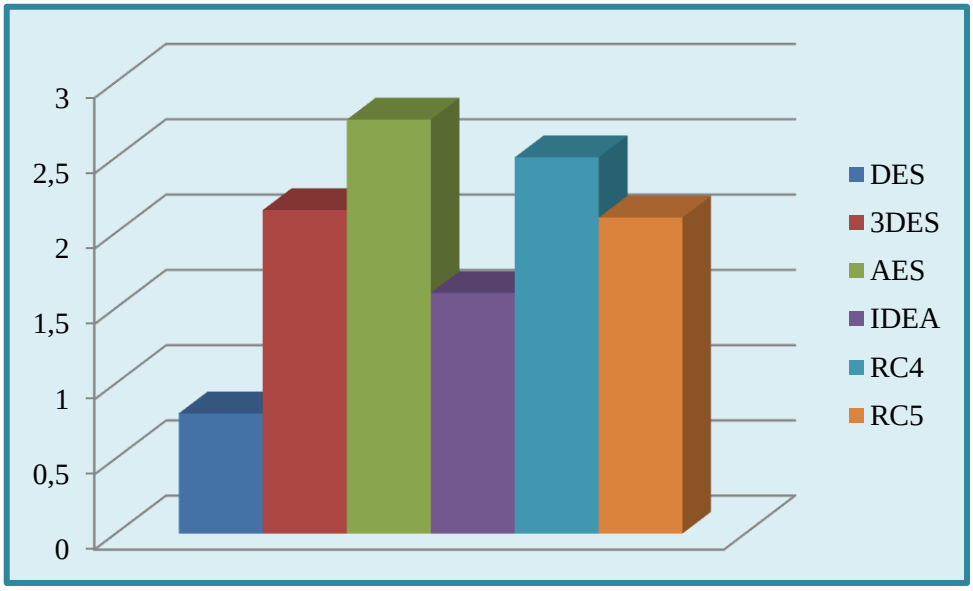
Uso en entidades: La calificación más alta (3) la obtuvieron los algoritmos AES y RC4, porque son los algoritmos más utilizados en los sitios web de entidades privadas y públicas del país. Al algoritmo 3DES se les dio la calificación (1) porque su uso es muy bajo en las

entidades del país. A los algoritmo DES, RC5 y IDEA se le asignó la calificación (0) porque no fueron utilizados por ninguna de las entidades que se investigaron.

Número de vueltas: La calificación más alta (3) la obtuvo el algoritmo RC5, porque es el algoritmo que más vueltas poseen en su estructura. Al algoritmo 3DES se le dio la calificación de (2,50) porque en su estructura posee 48 vueltas. Al algoritmo DES se le dio la calificación de (2) porque en su estructura posee 16 vueltas. Al algoritmo AES se le asignó la calificación (1,50) porque en su estructura posee 14 vueltas. Al algoritmo IDEA se le asignó la calificación (1) porque en su estructura posee 8 vueltas. Finalmente al algoritmo RC4 se le dio la calificación (0) porque no posee vueltas en su estructura, ya que es un algoritmo de cifrado de datos por flujo.

Después de la evaluación de los aspectos significativos, los algoritmos que obtuvieron mayores puntajes fueron: en primer lugar AES, en segundo lugar RC4 y en tercer lugar 3DES, por lo tanto son los más recomendados en la transmisión de datos de redes inalámbricas.

Gráfico 2. Algoritmos evaluados con mayores puntajes



Elaborado por: María Belén Gómez

El detalle de la evaluación (calificación y puntaje) de los aspectos significativos de los algoritmos se los puede observar en el cuadro 19.

Cuadro 18. Detalle de la evaluación de los algoritmos

Aspectos significativos	POND.	DES		3DES		AES		IDEA		RC4		RC5	
		Calif.	Punt.	Calif.	Punt.	Calif.	Punt.	Calif.	Punt.	Calif.	Punt.	Calif.	Punt.
Vulnerabilidad	0,40	1	0,40	3	1,20	3	1,20	3	1,20	2,50	1,00	3	1,20
Uso en entidades	0,30	0	0	1	0,30	3	0,90	0	0	3	0,90	0	0
Tamaño de clave	0,20	1	0,20	2	0,40	2,5	0,50	1,5	0,30	3	0,60	3	0,60
No. vueltas	0,10	2	0,20	2,50	0,25	1,5	0,15	1	0,10	0	0	3	0,30
Puntaje total			0,80		2,15		2,75		1,60		2,50		2,10

Elaborado por: María Belén Gómez

CAPÍTULO 4

HERRAMIENTAS DE CIFRADO DE DATOS

4.1 Tecnología de cifrado simétrico

En el capítulo 3 se estudiaron seis conocidos algoritmos de cifrado simétrico que son utilizados en diferentes protocolos de seguridad para redes inalámbricas. Se evaluaron estos algoritmos de cifrado tomando en consideración aspectos significativos como: vulnerabilidad, tamaño de clave, uso en entidades, número de vueltas ó rondas en la estructura del algoritmo. Luego de esta evaluación se determinó que los tres mejores algoritmos de cifrado de datos eran: AES, RC4 y 3DES.

A continuación se explica el funcionamiento de estos tres algoritmos.

4.1.1 Algoritmo AES

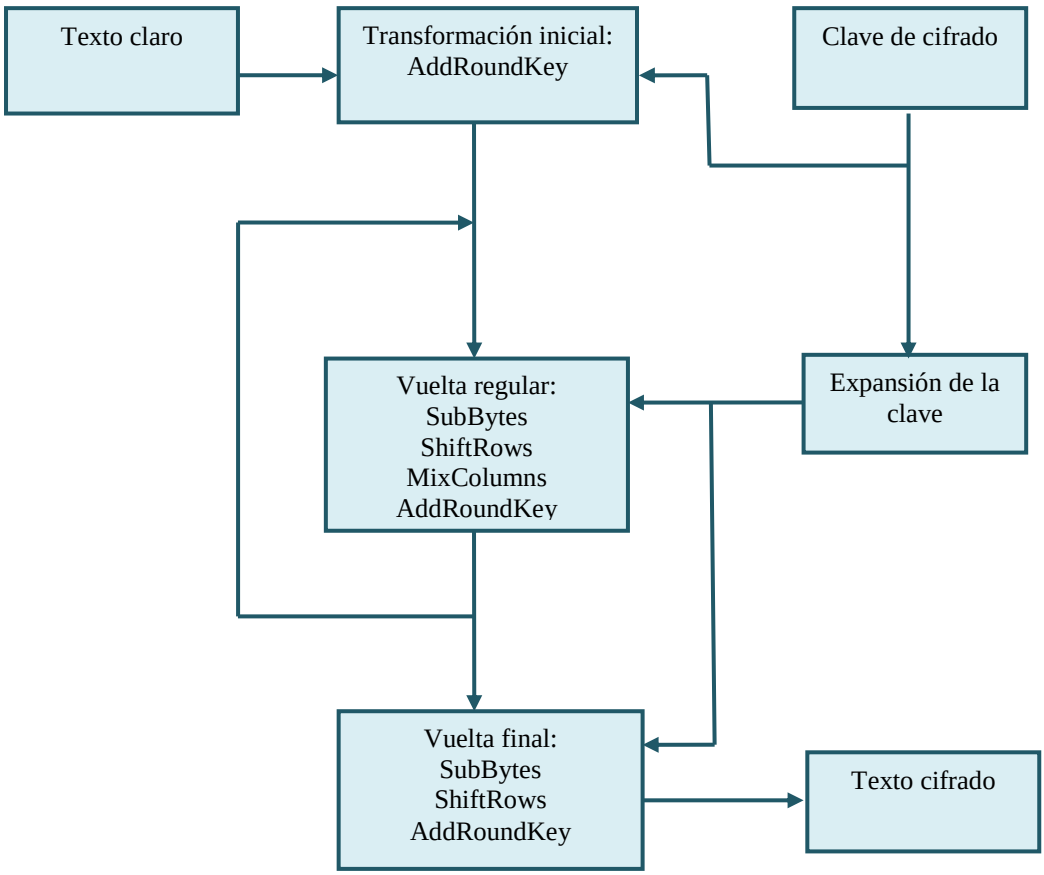
El AES tiene una longitud de bloque de 128 bits y el tamaño de la clave puede ser de 128, 192 ó 256 bits.

A continuación se describe el funcionamiento del algoritmo AES con una longitud de clave de 128 bits:

1. El texto claro empieza una transformación inicial con una fase de suma de clave de etapa, después siguen 9 rondas de cuatro fases cada una (véase figura 21), y termina con una décima etapa de tres fases.
2. La clave ingresa por el usuario se agranda en un vector de 44 palabras de 32 bits, 4 palabras distintas (128 bits) se usan como clave de etapa en cada vuelta
3. Cada una de las rondas de este algoritmo realiza cuatro operaciones básicas (una de permutación y tres de sustitución):
    - Sustitución de bytes (SubBytes).- Se utiliza una tabla denominada caja S^4, para hacer una sustitución byte a byte de todo el bloque.

- Desplazamiento de filas (ShiftRows).- Se realiza una permutación simple fila por fila.
- Mezcla de columnas (MixColumns).- Se realiza una sustitución que cambia cada byte de una columna en relación de todos los bytes de la columna.
- Suma de la clave de etapa (AddRoundKey).- Se realiza una operación lógica XOR bit a bit del bloque presente con una porción de la clave agrandada.

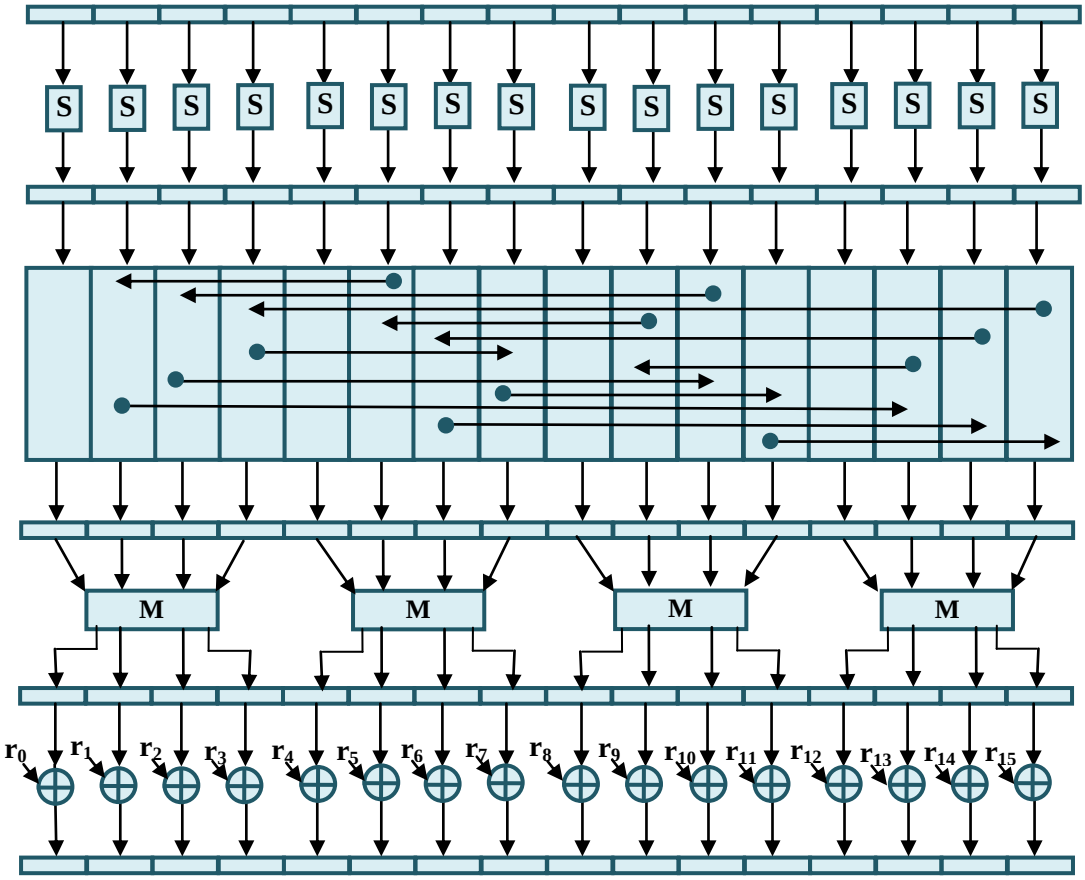
Figura 21. Funcionamiento del algoritmo AES



Fuente: http://www.fup.edu.co/investigacion/fupcric/images/pdf/aes.pdf

Elaborado por: María Belén Gómez

Figura 22. Diagrama de una ronda del algoritmo AES



Fuente: (Stallings, 2004: p.41)

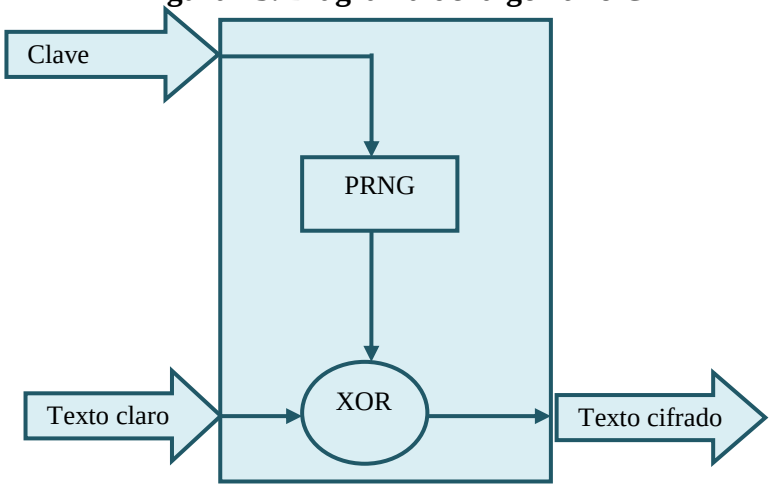
Elaborado por: María Belén Gómez

4.1.2 Algoritmo RC4

El funcionamiento de este algoritmo se detalla a continuación.

1. A partir de una clave de 8 a 1024 bits se inicializa una tabla de estados.
2. Esta tabla crea bytes pseudoaleatorios.
3. Estos bytes se mezclan por medio de la función XOR con el texto en claro, dando como resultado el texto cifrado.

Figura 23. Diagrama del algoritmo CR4



Fuente: http://www-ma2.upc.es/~cripto/Q1-02-03/wep.pdf

Elaborado por: María Belén Gómez

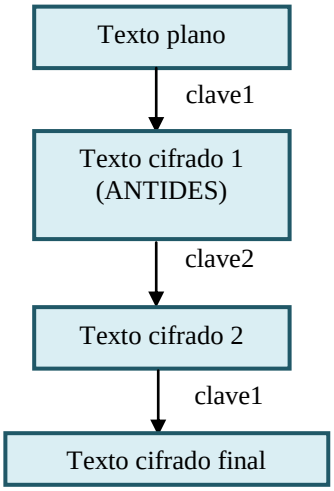
4.1.3 Algoritmo 3DES

A continuación el funcionamiento de un algoritmo 3DES con clave de 128 bits.

1. Se divide la clave de 128 bits en 2 partes de 64 bits cada una: clave1 y clave2.
2. Se cifrar el texto plano con clave1 (Este resultado tiene el nombre de ANTIDES).
3. Se cifrar ANTIDES con clave2.
4. El resultado del punto anterior se cifrar con clave1.

Si clave1 = clave2 el resultado es similar si hubiera sido cifrado con DES.

Figura 24. Diagrama de flujo del algoritmo 3DES



Elaborado por: María Belén Gómez

4.1.4 Aplicación de los algoritmos en protocolos de seguridad de redes inalámbricas

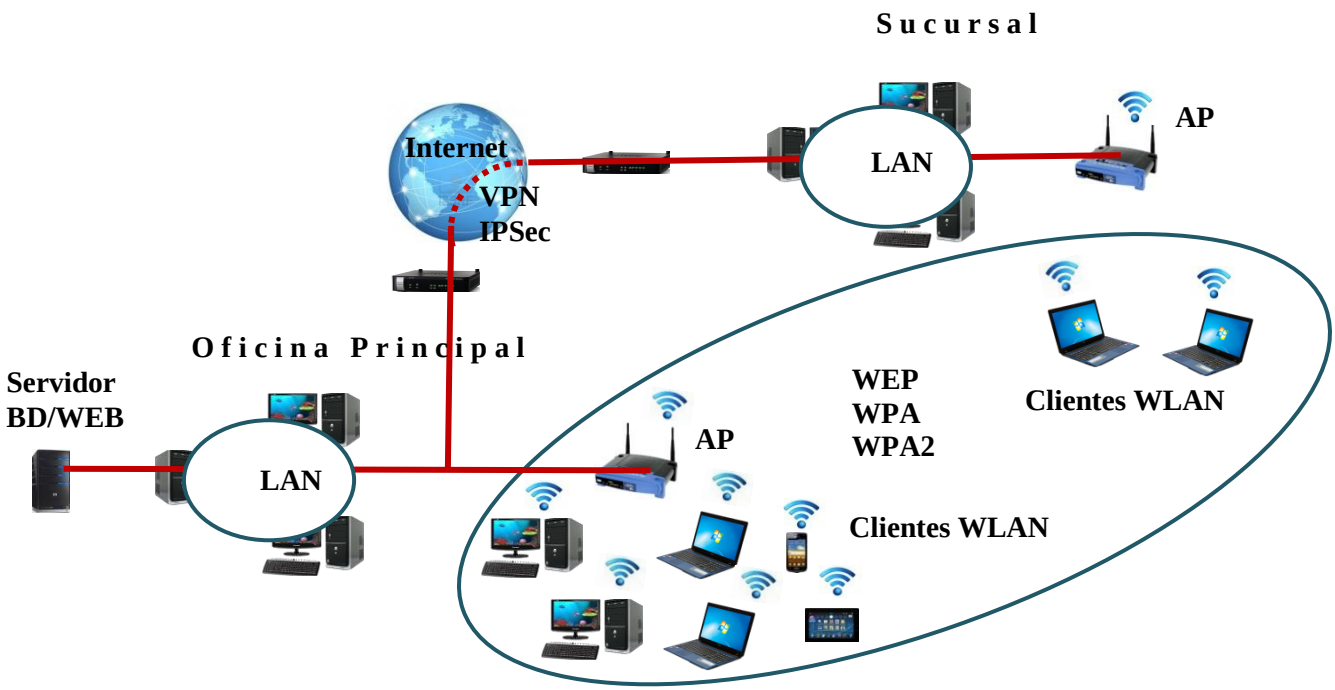
Los algoritmos AES, RC4 y 3DES son aplicados en el desarrollo de protocolos seguros, los cuales proporcionan seguridad a las redes inalámbricas durante la transmisión de datos en canales inseguros como Internet.

La utilización de estos protocolos seguros evita la interceptación de la información que circulan a través de las redes inalámbricas, muy aparte de otras medidas de seguridad que se adopten. A la vez garantiza la integridad, puesto que si no es interceptado tampoco es modificable.

También garantizan la confidencialidad de la información. Aunque esta resulte accesible a personas sin autorización no podrán entender su contenido.

Entre los protocolos que proporcionan las características anteriores se encuentran: WEP, WPA, WPA2, IPSec.

Figura 25. Protocolos utilizados en las transmisiones de datos de redes inalámbricas



Fuente: http://www.ipsd.cl/net_red2.html

Elaborado por: María Belén Gómez

4.1.4.1 Protocolo WEP (Wired Equivalent Privacy-Privacidad equivalente al cableado)

Este protocolo encripta las comunicaciones usando el algoritmo RC4 y usando una cadena prefija como clave, la cual debe ser conocida por el punto de acceso de la red inalámbrica y los ordenadores autorizados.

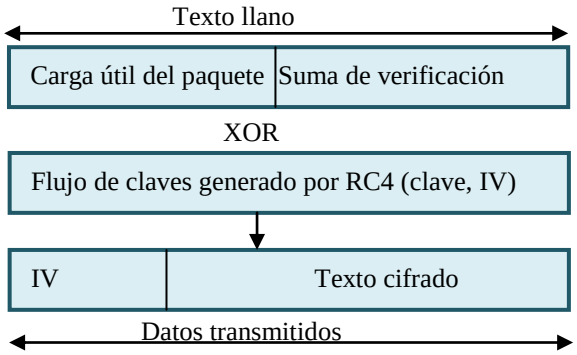
Es un protocolo de cifrado de datos simple, que estuvo presente en la primera versión de las redes inalámbricas (estándar 802.11). Al estar activo este cifrado, el emisor tiene que cifrar la información y el receptor tiene que decifrar la misma introduciendo la clave en cada ordenador. Utiliza claves estáticas de 64 ó 128 bits, cada clave tiene dos partes, la primera parte la configura el usuario/administrador en cada una de las tarjetas de red o puntos de acceso de la red. La segunda parte se genera de forma automática y recibe el nombre de vector de inicialización, la finalidad de este es conseguir claves distintas para repeler cualquier ataque que pueda capturar suficiente tráfico encriptado con la misma clave y que termine descubriendo la clave. En este diseño los dos extremos deben saber la clave y el vector de inicialización. La debilidad de este diseño es que al viajar el vector de inicialización en cada trama puede fácilmente ser interceptado por un atacante.

Este protocolo de cifrado no es muy fuerte y tiene muchas vulnerabilides, puesto que no es tan difícil obtener la información cifrada (Ejemplo la contraseña WEP) y por lo tanto podrían acceder usuarios no autorizados a la red.

Aplicación del algoritmo RC4

1. Se hace una suma de verificación de la carga útil usando CRC-32 (Comprobación de redundancia cíclica) polinomial y esta suma se agrega a la carga útil formando el texto llano.
2. Al texto llano se le aplica una operación lógica (OR exclusivo) junto con un fragmento de flujo de claves de su propio tamaño.
3. Se obtiene el texto cifrado.
4. El vector de inicialización (IV), usado para iniciar el algoritmo RC4, se une con el texto y cifrado, formando el paquete que será transmitido.

Figura 26. Aplicación del algoritmo RC4



Elaborado por: María Belén Gómez

4.1.4.2 Protocolo WPA (WiFi Protected Access-Acceso a WiFi protegido)

Este tipo de protocolo también utiliza el algoritmo RC4 y se lo creó con la finalidad de mejorar la seguridad WEP. En este protocolo la generación de la clave es dinámica y sin limitaciones en el largo de la cadena de caracteres. Para la administración de las claves dinámicas usa el estándar TKIP (temporary Key Integrity Protocol), el cual es un protocolo de gestión de claves dinámicas que usa una clave distinta en cada paquete que se transmite.

4.1.4.3 Protocolo WPA2 (WiFi Protect Access 2- Acceso a WiFi protegido 2)

Este protocolo utiliza el algoritmo AES, que lo hace ser el más seguro dentro de las redes inalámbricas. Se creó con la finalidad de corregir los defectos del protocolo WPE y a la vez mejorar la seguridad del protocolo WPA. Usa para la administración de claves el estándar CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), el cual fue desarrollado para reemplazar al TKIP.

4.1.4.4 Protocolo IPSec (Internet Protocol security – Protocolo de seguridad de internet)

IPsec está formado por un conjunto de protocolos estandarizados por el IETF (Internet Engineering Task Force - Grupo de Trabajo de Ingeniería de Internet), cuya finalidad es proporcionar seguridad al protocolo de internet (IP) autentificando y cifrando cada paquete IP en un flujo de datos. La protección que da se basa en el cifrado de datos y la administración de la clave dinámica.

El protocolo IPSec trabaja de extremo a extremo, es decir, solamente los ordenadores de origen y destinos requieren soportar este protocolo, gracias a ello se puede atravesar dispositivos de red como routers, sin la necesidad de que estos conozcan este protocolo. Pero si los paquetes IPSec deben atravesar routers filtrantes o cortafuegos, se deberán abrir los respectivos puertos para que los paquetes puedan atravesar estos equipos.

Este protocolo trabaja en la capa de red (capa 3 del modelo TCP/IP) y utiliza dos protocolos de seguridad: de autenticación AH (Authetication Header) que asegura que los datos no han sido modificado y que proviene de quién dice ser, y el de cifrado ESP (Encapsulating Security Payload) que cifra los datos. Los algoritmos de cifrado que se pueden usar en el protocolo IPSec son: DES, 3 DES, RC5, IDEA, AES. El protocoló IPSec es utilizado en soluciones de seguridad de redes inalámbricas como las VPN(Virtual Private Network).

4.1.5 Uso de los algoritmos de cifrado simétricos en WLAN (Wireless Local Area Network) empresariales

Para determinar el uso de los algoritmos de cifrado simétricos en WLAN empresariales se realizó una encuesta a profesionales del área de sistemas (Especialista en Informática, Jefe de Unidad TIC, Analista Senior TIC´s, Coordinador servicios informáticos, Director de Sistemas, Ingeniero en Network SIS) de importantes instituciones y empresas de la ciudad de Guayaquil que poseen varias WLAN dentro de su infraestructura de redes. Las empresas e instituciones encuestadas fueron las siguientes:

Cuadro 19. Empresas e instituciones encuestadas

Institución	Información
SRI (Servicio de Rentas Internas) 	La institución: Es una entidad técnica y autónoma que tiene la finalidad de recaudar los impuestos internos Agencia: World Trade Center Dirección: Av. Francisco de Orellana y Justino Cornejo Cargo de la persona encuestada: Especialista en Informática Teléfonos: (04)2685150

Subsecretaría de Educación Coordinación Zonal 8 	La institución: Administra el sistema educativo en Guayaquil, Samborondón, Durán y diseña las estrategias y mecanismos para asegurar la calidad de los servicios educativos. Edificio: Makro Dirección: Avenida Carlos Luis Plaza Dañin y Calle Francisco Bolaña Cargo de la persona encuestada: Jefe de Unidad TIC Teléfonos: 04) 268 4350
Coordinación Zonal 8 del MIES 	La institución: Es una extensión del MIES (Ministerio de Inclusión Económica y Social) que ejecuta políticas, regulaciones, estrategias, programas y servicios para la atención de grupos de atención prioritaria y aquellos que se encuentran en situación de pobreza y vulnerabilidad, en Guayaquil, Samborondón, Durán Edificio: Makro Dirección: Avenida Carlos Luis Plaza Dañin y Calle Francisco Bolaña Cargo de la persona encuestada: Analista SeniorTIC´s Teléfonos: 043714780
IESS (Instituto Ecuatoriano de Seguridad Social) 	La institución: Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del sistema nacional de Seguridad Social. Agencia: Urdesa Dirección: Víctor Emilio Estrada y Guayacanes Cargo de la persona encuestada: Coordinador servicios informáticos Teléfonos: 042380927

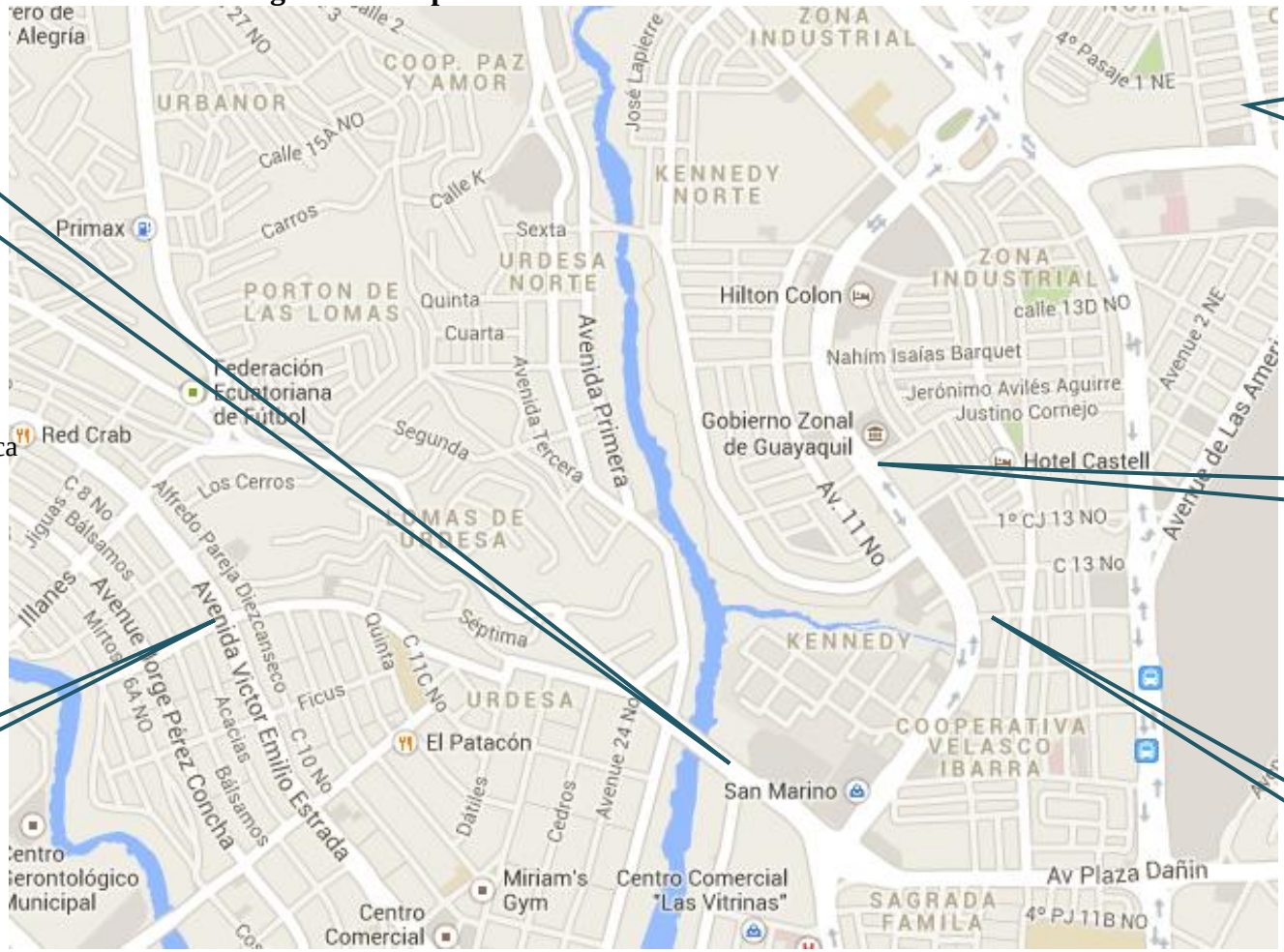
Institución	Información
MSP (Ministerio de Salud Pública) 	La institución: Planifica, gestiona, coordina y controla la salud pública Edificio: Makro Dirección: Avenida Carlos Luis Plaza Dañin y Calle Francisco Bolaña Cargo de la persona encuestada: Especialista en Informática Teléfonos:
TELE-RED 	La institución: Empresa que proporciona soluciones en telecomunicaciones, servicios IP y Voip. Edificio: Trade Building, torre B, oficina 632-633 Dirección: Leopoldo Benítez Vinueza y Joaquín J. Orrantia Gonzalez Cargo de la persona encuestada: Gerente Teléfonos: 043731366
CONECEL (CLARO) 	La institución: Empresa de telefonía celular que proporciona soluciones integrales y de calidad en telecomunicaciones. Edificio: Centrum Dirección: Av. Francisco de Orellana y Alberto Borges Cargo de la persona encuestada: Ingeniero en Network SIS Teléfonos: 045004040

Fuente: Investigación de campo

Elaborado por: María Belén Gómez

Figura 27. Mapa de ubicación de las instituciones encuestadas

- Sub. de Educación Coord. Zonal 8
- Coordinación Zonal 8 del MIES
- Ministerio de Salud Pública



- IESS

- TELE-RED

- Servicio Rentas Internas

- Claro

Fuente: Investigación de campo

Elaborado por: María Belén Gómez

ENCUESTA PARA EL PERSONAL DE SISTEMAS

Nombre de la Institución/organización: ……

Dirección: ……..

Cargo de la persona encuestada:……

Fecha:……..

OBJETIVO:

Conocer los algoritmos de cifrado de datos de las soluciones de seguridad que existe en las redes área local inalámbrica (WLAN)

1. ¿Cuál es la solución de seguridad más usada por las WLAN?

___WEP ___WPA ___WPA2

___VPN (Redes virtuales privadas) ___Otro(Especifique)_____

2. ¿Cuál es el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

___AES ___RC4

___3DES ___Otro(Especifique)_____

3. Califique el nivel de seguridad del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

___Alta ___Media ___Baja

4. Califique la velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

___Alta ___Media ___Baja

5. Califique la carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

___Alta ___Media ___Baja

6. ¿Cuáles son las ventajas/desventajas (técnicas), del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

Ventajas:_____

Desventajas:_____

7. ¿Cuáles son los beneficios del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

_____

_____

_____

Análisis e interpretación de datos

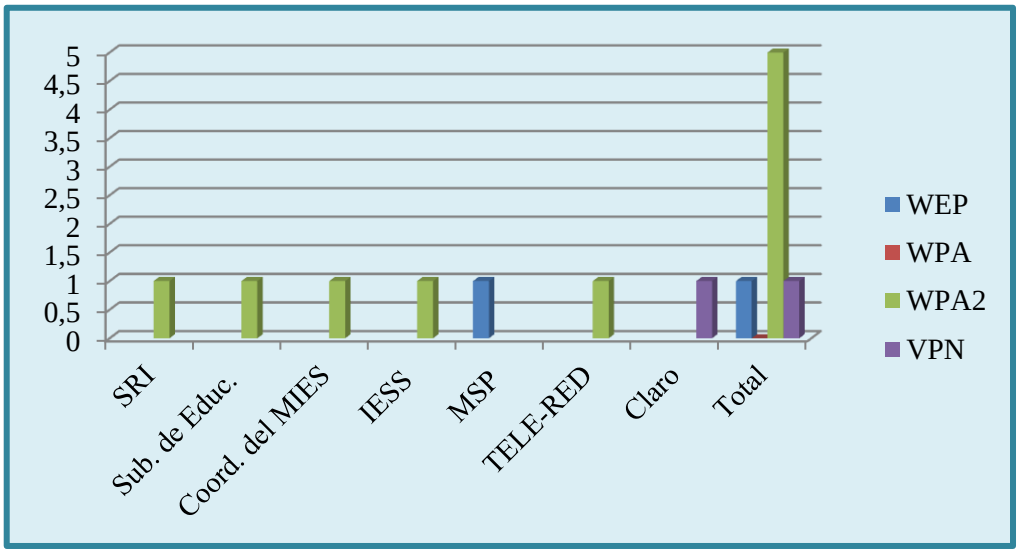
1.- ¿Cuál es la solución de seguridad más usada por las WLAN?

Cuadro 20. Solución de seguridad más usada por las WLAN

Instituciones	SRI	Sub. de Educ.	Coord. del MIES	IESS	MSP	TELE-RED	Claro	Total	F. Relativa %
WEP					1			1	14%
WPA								0	0
WPA2	1	1	1	1		1		5	71%
VPN							1	1	14%

Elaborado por: María Belén Gómez

Gráfico 3. Solución de seguridad más usada por las WLAN



Elaborado por: María Belén Gómez

Las instituciones públicas a excepción del Ministerio de Salud Pública usan como solución de seguridad para sus redes inalámbricas WPA2, la cual es una solución de seguridad muy fuerte, de bajo costo y de fácil implementación. El MSP usa WEP, una solución que está en desuso porque ha demostrado ser vulnerable. La empresa Claro usa VPN, que es mucho mejor que WPA2 pero su costo es más alto y su implementación requiere de personal calificado, lo cual no es un impedimento puesto que es una de las empresas más grandes del país. Como se puede observar en el gráfico en términos globales la solución más usada es WPA2 con el 71% y las menos usadas son WEP y VPN con el 14% respectivamente, por lo anteriormente mencionado.

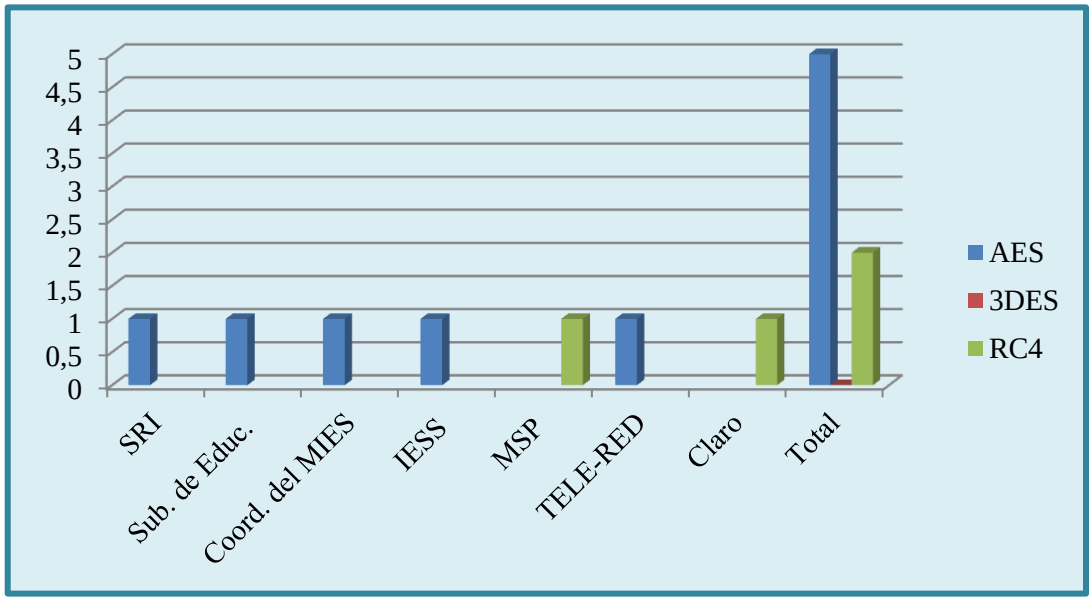
2.- ¿Cuál es el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

Cuadro 21. Algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

Instituciones	SRI	Sub. de Educ.	Coord. del MIES	IESS	MSP	TELE-RED	Claro	Total	F. Relativa %
AES	1	1	1	1		1		5	71
3DES								0	0
RC4					1		1	2	29

Elaborado por: María Belén Gómez

Gráfico 4. Algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN



Elaborado por: María Belén Gómez

Esta pregunta tiene una relación directa con la anterior pregunta, ya que el algoritmo de cifrado está muy relacionado con la solución de seguridad que usan las empresas o instituciones en sus WLAN. Podemos observar que las entidades que utilizan como solución WPA2, el algoritmo implementado en la misma es AES.

Hay que destacar que tanto la empresa Claro como el Ministerio de Salud utilizan el algoritmo de flujo RC4 pero en diferentes soluciones.

Claro utiliza RC4 en VPN, el cual es un algoritmo muy usado en las conversaciones de telefonía celular, donde la voz se digitaliza, es decir, se convierte a un flujo de bits, una vez

cifrada se la envía por la red de telecomunicaciones. En cambio el Ministerio de Salud Pública utiliza RC4 en WEP, lo cual hace muy vulnerable a la solución.

WEP usa como algoritmo sólo RC4, mientras que VPN puede utilizar distintos algoritmos tales como: 3DES, AES, IDEA, RC4, RC5, entre otros.

En términos globales el algoritmo de cifrado de datos más usado es AES con el 71% y el menos usado es el algoritmo RC4 con el 29%.

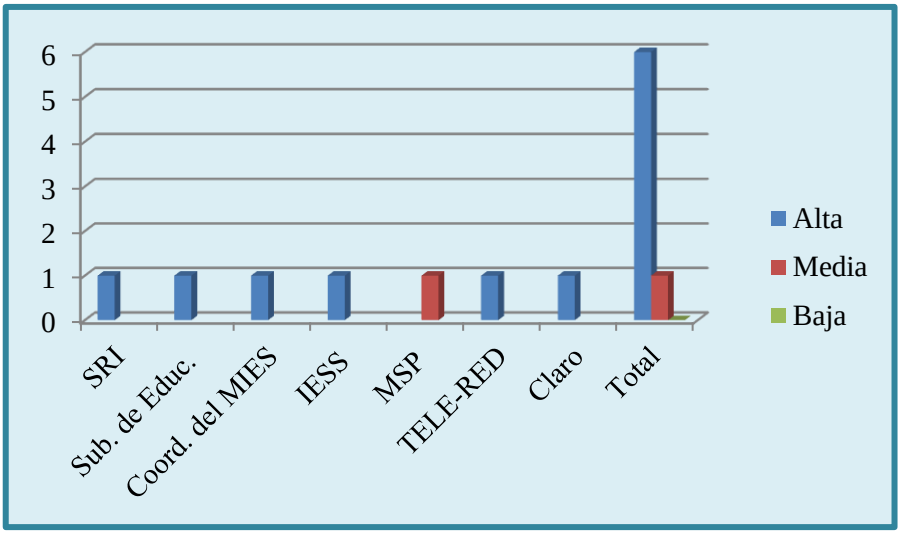
3. Califique el nivel de seguridad del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

Cuadro 22. Nivel de seguridad del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

Instituciones	SRI	Sub. de Educ.	Coord. del MIES	IESS	MSP	TELE-RED	Claro	Total	F. Relativa %
Alta	1	1	1	1		1	1	6	86
Media					1			1	14
Baja								0	0

Elaborado por: María Belén Gómez

Gráfico 5. Nivel de seguridad del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN



Elaborado por: María Belén Gómez

Servicio Rentas Internas, Subsecretaría de Educación Coordinación Zonal 8, Coordinación Zonal 8 del MIES, IESS y TELE-RED afirmaron que es alto el nivel de seguridad que alcanzan con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por sus redes inalámbricas. El algoritmo que utilizan estas instituciones en su solución de seguridad es el AES, el cual hasta la actualidad no ha sido vulnerado.

Ministerio de Salud Pública afirmó que el nivel de seguridad del algoritmo de cifrado es medio, lo cual es comprensible porque tiene implementado el algoritmo RC4 en la solución de seguridad WEP, lo cual lo hace vulnerable.

En cambio la empresa Claro afirmó que el nivel de seguridad del algoritmo de cifrado es alto porque tiene implementado el algoritmo RC4 en la solución de seguridad VPN, lo cual lo hace más robusto frente a los ataques.

En términos globales el 86% de las instituciones y empresas encuestadas afirmaron que el algoritmo de cifrado de datos que utilizan les ofrece un alto nivel de seguridad frente al 14% que afirmaron que sólo les ofrece un nivel medio de seguridad.

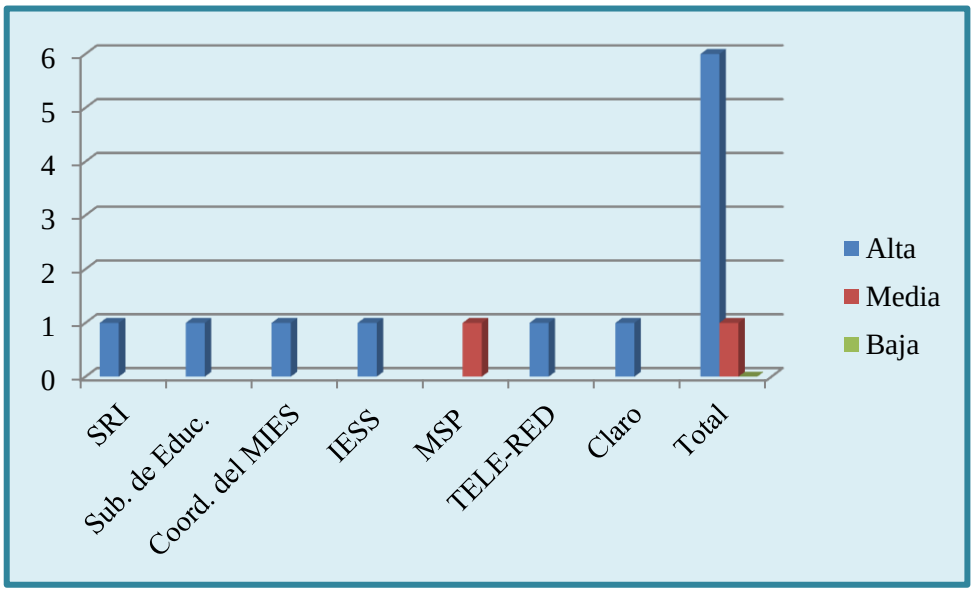
4. Califique la velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

Cuadro 23. Velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN

Instituciones	SRI	Sub. de Educ.	Coord. del MIES	IESS	MSP	TELE-RED	Claro	Total	F. Relativa %
Alta	1	1	1	1		1	1	6	86
Media					1			1	14
Baja								0	0

Elaborado por: María Belén Gómez

Gráfico 6. Velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN



Elaborado por: María Belén Gómez

Servicio Rentas Internas, Subsecretaría de Educación Coordinación Zonal 8, Coordinación Zonal 8 del MIES, IESS y TELE-RED y Claro afirmaron que es alta la velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por sus redes inalámbricas. El algoritmo que utilizan estas instituciones y empresas en su solución de seguridad es el AES a excepción de Claro que utiliza RC4 implementado en VPN.

Ministerio de Salud Pública afirmó que es media la velocidad de transmisión de un archivo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por sus redes inalámbricas. Ésta institución tiene implementado el algoritmo RC4 en la solución de seguridad WEP.

En el global el 86% de las instituciones y empresas encuestadas afirmaron que el algoritmo de cifrado de datos que utilizan les ofrece una alta velocidad de transmisión de un archivo frente al 14% que afirmaron que sólo les ofrece un nivel medio de velocidad.

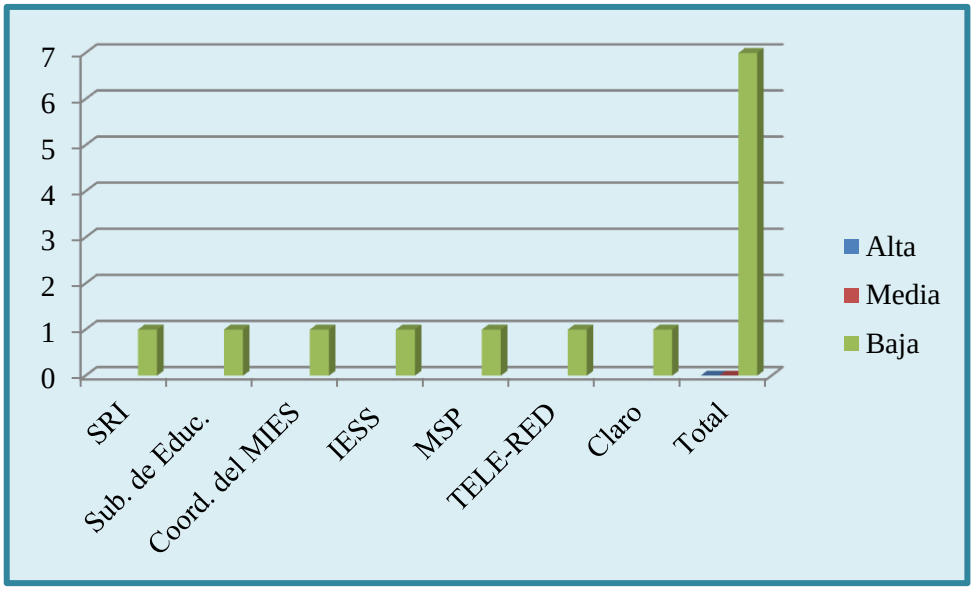
5. Califique la carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

Cuadro 24. Carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema con el algoritmo de cifrado de datos

Instituciones	SRI	Sub. de Educ.	Coord. del MIES	IESS	MSP	TELE-RED	Claro	Total	F. Relativa %
Alta								0	0
Media								0	0
Baja	1	1	1	1	1	1	1	7	100%

Elaborado por: María Belén Gómez

Gráfico 7. Carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema con el algoritmo de cifrado de datos



Elaborado por: María Belén Gómez

Servicio Rentas Internas, Subsecretaría de Educación Coordinación Zonal 8, Coordinación Zonal 8 del MIES, IESS, MSP y TELE-RED y Claro afirmaron que es baja la carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema de computo con el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por sus redes inalámbricas.

En esta pregunta el 100% de las empresas e instituciones encuestadas respondieron que es baja la carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema de computo con el algoritmo de cifrado de datos, lo que significa que con ninguno de los 2 algoritmos que utilizan (AES o RC4) estas entidades consume muchos recursos del sistema de computo.

6. ¿Cuáles son las ventajas/desventajas (técnicas), del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

Esta pregunta fue abierta, es decir, que no hubo alternativas para escoger. Aquí las empresas e instituciones encuestadas describieron las ventajas y desventajas técnicas del algoritmo de cifrado de datos que usan: AES y RC4.

Cuadro 25. Ventajas/desventajas (técnicas) del algoritmo AES

Instituciones	AES	
	Ventajas	Desventajas
SRI	Fácil de configurar	Es el protocolo mayormente atacado. No implementa mejoras
Sub. de Educ.	Control de usuarios, Integridad segura, datos seguros	texto de cifrado de mayor longitud
Coord. del MIES	Mas seguridad	
IESS	Encriptamiento de la Información a traves del canal	Encriptamiento simétrico
TELE-RED	Encriptación de dispositivo de origen y destino	Autenticación demora mas de dos segundos

Elaborado por: María Belén Gómez

Cuadro 26. Ventajas/desventajas (técnicas), del algoritmo RC4

Instituciones	RC4	
	Ventajas	Desventajas
MSP	Seguridad de transmisión	Problemas con cobertura
Claro	Comunicación encriptada	Varias configuraciones para usuarios

Elaborado por: María Belén Gómez

7. ¿Cuáles son los beneficios del algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por las WLAN?

Esta pregunta al igual que la anterior fue abierta. Aquí las empresas e instituciones encuestadas describieron los beneficios del algoritmo de cifrado de datos que usan: AES y RC4.

Cuadro 27. Beneficios del algoritmo AES

Instituciones	Beneficios
SRI	Seguridad para las redes abiertas
Sub. de Educ.	Es facil de implementar
Coord. del MIES	Que puede ser administrable
IESS	Incremento de seguridad sobre accesos no deseados Protección sobre ataques de fuerza bruta Control de acceso a los recursos y servicios de red
TELE-RED	Cuando scanea el espectro no se puede visualizar las claves

Elaborado por: María Belén Gómez

Cuadro 28. Beneficios del algoritmo RC4

Instituciones	Beneficios
MSP	Evita accesos o ataques de red
Claro	Única Optima

Elaborado por: María Belén Gómez

4.1.6 Implementación de soluciones de cifrado simétrico en una WLAN

La seguridad es una de las principales inquietudes de las empresas que desean implementar redes inalámbricas. En la actualidad las redes inalámbricas incorporan funciones integras de seguridad de tal forma que las empresas pueden aprovechar con confianza todas las ventajas que ofrecen estas redes.

Como se ha visto en este Capítulo para proporcionar seguridad a las redes inalámbricas, existen tres soluciones disponibles: WPA (WiFi Protected Access), WPA2 (WiFi Protected Access 2) y VPN(Virtual Private Network), WEP está en desuso porque es vulnerable. La solución de seguridad que se elija depende del tipo de LAN inalámbrica a que se está obteniendo acceso y del nivel de cifrado de datos que se requiere.

4.1.6.1 Implementación de WPA y WPA2

WPA (WiFi Protected Access) y WPA2 (WiFi Protected Access 2) son estándares de seguridad de la Wi-Fi Alliance para WLAN de pequeñas, medianas y grandes empresas, pequeñas oficinas y para el hogar, estos estándares proporcionan autenticación bilateral para verificar a usuarios individuales, cifrado de datos y protegen la WLAN de ataques pasivos y activos. WPA proporciona cifrado de datos de tipo empresarial y WPA2 proporciona cifrado de datos de tipo gubernamental. En la actualidad WPA y WPA2 vienen incorporados a los puntos de acceso inalámbricos y a los dispositivos de clientes certificados.

A continuación se detalla los elementos que se requiere para implementar esta solución.

Cuadro 29. Dispositivos para la implementación de WPA y WPA2

Adaptador Wireless PCI d-link de 150 mbps	**Descripción**
	• Adaptador inalámbrico PCI, permite conexiones inalámbricas hasta ISOMbps 802.1 In • Compatible con 802.1 Ib/g/n • Proporciona hasta UMbps para 802.1 Ib, 54Mbpspara 802.llg, ISOMbps para 802. • Soporta WEP, WPA-PersonaKEmpresa, WPA2-Personal //Empresa, WPS • Instalación Plug and Play. Fácil y segura configuración con WPS y Software Quick Setup Wizard. • Antena de 2dBi reemplazable • Soporta WiFi WMM & WMM-PS QoS • Precio: 20,05 (Incluido IVA)
Adaptador USB Wireless Zyxel	**Descripción**
	• Cumple con la norma 802,11 n • Compatible con 802,11 b / g • Inalámbrico Velocidad de transferencia de datos • Transmisión: 150Mbps • Recepción: 150 Mbps • Wi-Fi Multimedia (WMM) • Seguridad inalámbrica • WEP, WPA (WPA-PSK), WPA2 (WPA2-PSK), 802.1x • WPS hardware botón WPS software de funciones • Soft AP compatibilidad con el modo • Wirless peer-to-peer de soporte de conexión • Un botón WPS con Link / Act LED • Un puerto USB 1.1/2.0 • Precio: 26,88 (Incluido IVA)

Router 2 antenas wifi y 4 LAN de red D-Link	Descripción
	**Estándares** • IEEE 802. lln(draft 2.0) • IEEE 802.llg/b • IEEE 802.3 • IEEE 802.3u **Wireless Signal Rales** • 802.11b: 1/2/5.5/11 Mbps • 802.1 lg: 6/9/12/18/24/36/48/54Mbps • 802.11n: 30/60/90/120/180/240/270/300Mbps **Seguridad** • WEP 64/128-Bit Data Encryption (Sofo en 802.11B/G) • Wi-Fi Protected Access (WPA/ WPA2) • (TíCIP, MIC, IV Expansión, Shared Kcy Authcntication) • 802. Ix • WPS (Wi-Fi Protected Setup) • Push Butíon • PIN **Firewall** • Network Address Translation (NAT) • Stateíul Packet Inspection (SPI) • WN pass-through • Muki-session PPP/L2TP/IPSec • TP/Mac Address Filtering • URL Filtering • Scheduling • Domain Btocking • Soporte 1 DMZ **Requerimientos Mínimos del sistema** • Computador con: • Windows® Vista, Windows® XP SP2, Windows® 2000 SP4, o Mac OS® X (v10.4) • Internet Explorer 6 Firefox v.5 o superior • Tarjeta de Red Ethernet • Para acceso a Internet: • Cable or DSL Modem • Subscripción a un Proveedor de Internet (ISP) **Precio** 49,10 (Incluido IVA)

Fuente: www.compudisc.net

Elaborado por: María Belén Gómez

En el siguiente cuadro se muestran los costos de implementar una red local inalámbrica de 10 computadoras con protocolo de cifrado de datos WPA o WPA2. No se consideran los costos de configuración para implementar esta solución, puesto que la configuración es muy sencilla.

Cuadro 30. Costos para implementar WPA y WPA2

Cant.	Detalle	P. Unit.	P. Total
10	Adaptador USB Wireless Zyxel	24,00	240,00
1	Router 2 antenas wifi y 4 LAN de red D-Link	43,84	43,84
	Subtotal		283,84
	IVA 12%		34,06
	Total		317,90

Fuente: www.compudisc.net

Elaborado por: María Belén Gómez

4.1.6.2 Implementación de VPN

VPN proporciona eficiente seguridad para los usuarios que acceden a la WLAN. Con VPN, los usuarios crean un túnel seguro entre 2 ó más puntos de la red mediante el cifrado, incluso si los datos son transmitidos a través de redes públicas inseguras como Internet

Las empresas pueden utilizar redes privadas virtuales (VPN) para conectar de manera segura oficinas y usuarios remotos por medio de accesos económicos a internet dados por terceros. Las VPN dan el mayor nivel de seguridad posible por medio de seguridad IP(IPsec) cifrada o túneles VPN SSL.

Para implementar esta solución se requiere Adaptadores Wireless (Tarjetas de red inalámbricas USB o PCI) como en la solución anterior y de un router VPN, como el que se detalla a continuación:

Cuadro 31. Dispositivo para la implementación de VPN

Firewall VPN Cisco RV110W Wireless-N	Descripción
	• Conectividad inalámbrica 802.11n de alta velocidad • Switch integrado de 4 puertos 10/100 • Firewall comprobado y compatible con normas de acceso y seguridad inalámbrica avanzada • Compatibilidad con calidad de servicio (QoS, Quality of service) para mejorar el tráfico de voz, video y datos • Compatibilidad con redes "virtuales" separadas que le permiten configurar el acceso inalámbrico seguro de usuarios temporales. • Compatibilidad para VPN con seguridad IP (IPsec, IP Security) y Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol), lo cual proporciona conectividad de acceso remoto seguro para computadoras con S.O. Windows y Mac. • Compatibilidad con IPv6, la más reciente tecnología de Protocolo de Internet • Configuración simplificada por medio de un administrador de dispositivos intuitivo con una interfaz basada en un navegador • Precio: 135,52 (Incluido IVA)

Fuente: www.solnetdelecuador.com

Elaborado por: María Belén Gómez

En el siguiente cuadro se muestran los costos de implementar VPN entre dos WLAN. Cada red local inalámbrica está compuesta de 5 computadoras.

Cuadro 32. Costos para implementar VPN

Cant.	Detalle	P. Unit.	P. Total
10	Linksys AE2500-LA Dual-Band Wireless-N 300 Mbps USB Adapter	39,00	390,00
2	Firewall VPN Cisco RV110W Wireless-N	121,00	242,00
1	Instalación y configuración de las dos WLAN	240,00	240,00
	Subtotal		872,00
	IVA 12%		104,64
	Total		976,64

Fuente: www.solnetdelecuador.com

Elaborado por: María Belén Gómez

4.2 Tecnología de cifrado asimétrico

Los algoritmos asimétricos en la práctica solamente son utilizados para el intercambio de claves simétricas, y con este funcionamiento es muy utilizado en los diversos sistemas seguros implementados la red pública Internet como SSL (Secure Sockets Layer) y VPN (Virtual Private Network).

Los costos computacionales para implementarlos son más altos que el de los algoritmos simétricos, por esta razón no se usan para cifrar mucha información. Su principal uso está en la fase inicial de una transmisión de datos, puesto que ayuda a que los dos extremos de la comunicación se autentifiquen e intercambien claves secretas del algoritmo simétrico, que es el que va cifrar la información entre los dos extremos. Entre los algoritmos más conocidos de este tipo están: RSA y Diffie- Hellman.

Características

Los algoritmos asimétricos son muy lentos pero ayudan al intercambio fácil de la clave y también proporciona soporte a la firma digital.

Posee una complejidad de cálculo por lo cual son lentos.

Esta forma de cifrado posee varios estándares disponibles para su utilización y se puede usar en redes cableadas e inalámbricas.

Cifran y descifran con diferentes llaves. Los datos se cifran con una clave pública y se descifran con una clave privada.

Para ser seguros requieren una longitud de clave muy grande en comparación a un algoritmo simétrico. Por ejemplo con una clave de 3.000 bits alcanzaría un nivel de seguridad similar al de un algoritmo simétrico de 128 bits.

4.2.1 Algoritmo Diffie- Hellman

Este algoritmo de cifrado, lleva este nombre por sus creadores: Whitfield Diffie y Martin Hellman. Su importancia se debe sobre todo al hecho de ser el punto de partida para todos los algoritmos asimétricos, puesto que en la práctica sólo es utilizado para el intercambio de claves privadas, y gracias a esta funcionalidad es muy usado en los diversos sistemas

seguros implementados en las redes, como por ejemplo SSL (Secure Socket Layer) y VPN (Virtual Private Network).

Este algoritmo sirve para que dos máquinas puedan convenir una misma clave secreta, por medio de un canal inseguro (Por ej. Internet) y enviando solamente dos mensajes. La clave secreta acordada no puede ser descubierta por terceras personas, aunque estas consigan los dos mensajes enviados, por ello la principal aplicación que se le da a este algoritmo es compartir una clave privada entre dos usuarios con la que posteriormente se cifrará las comunicaciones entre ellos.

En la actualidad se sabe que es vulnerable a ataques "de hombre en medio", es decir cuando un atacante se sitúa entre dos máquinas A y B, y acuerda una clave privada con cada una de las máquinas, haciendo pasar por la maquina A ante la máquina B y viceversa. Una vez establecidas las dos claves privadas, el atacante hace de puente entre las dos máquinas, descifrando y cifrando toda la comunicación. Para corregir esta vulnerabilidad, el algoritmo debe ser usado en combinación con algún sistema que autentifique los mensajes.

4.2.2. Algoritmo de cifrado asimétrico RSA

El algoritmo RSA (siglas de sus creadores Rivest, Shamir y Adelman), fue desarrollado en 1977. En la actualidad es el más utilizado de los algoritmos de cifrado asimétrico, y es válido para cifrar y para firmar digitalmente.

Emplea 2 claves: una pública para cifrar el texto claro y otra privada relacionada matemáticamente con la pública para descifrar el texto claro. La clave privada es la única que puede descifrar correctamente el mensaje, por esto la clave privada es la que debe protegerse.

En este algoritmo la clave pública de un usuario se guarda en una entidad confiable que garantiza que la clave es verdaderamente de quien dice ser.

La seguridad de este algoritmo radica en la hipótesis matemática de que no existe una manera eficaz de factorizar números que sean productos de dos números primos de gran tamaño (de 100 ó más dígitos), si estos números primos están ocultos.

La seguridad del algoritmo RSA depende de la longitud de sus claves, normalmente tienen claves entre 1024-2048 bits de longitud. Las claves más grandes aumentan la seguridad del algoritmo pero al mismo tiempo disminuyen su eficiencia y generan más texto cifrado.

Los bloques de texto plano pueden ser de cualquier tamaño, siempre y cuando sean menores que la longitud de la clave, en cambio los bloques de textos cifrados generados son del tamaño de la clave.

Comparado con los algoritmos de cifrado simétrico como el DES, este algoritmo es 100 veces más lento en software y entre 1000 y 10000 veces más lento en hardware.

4.3 Cuadro comparativo de métodos de cifrado de datos

Cuadro 33. Cuadro comparativo de métodos de cifrado de datos

	CIFRADO SIMÉTRICO	CIFRADO ASIMÉTRICO
Ventajas	Método eficiente en grupos muy reducidos de usuarios, puesto que sólo se requiere de una clave compartida No requiere de una Autoridad de Certificación Infraestructura sencilla de implementar	Número de claves reducido, puesto que cada usuario necesita sólo un par de claves Computacionalmente es complejo encontrar la clave privada a partir de la clave pública No se requiere transmitir la clave privada entre las dos partes (emisor y receptor) Ayuda a autenticar a quien use la clave privada
Desventajas	Se requiere compartir la clave privada entre el emisor y el receptor por medios o canales inseguros Si la clave se compromete, toda la información o comunicación se compromete No ayuda a autenticar al emisor, puesto que la misma clave la utilizan dos usuarios Se requiere de un gran número de claves	Costos computacionales muy altos en el proceso de generación de claves Se requiere de una Autoridad de Certificación Se requiere de una infraestructura grande independientemente del número de usuarios. Requiere que la longitud de la clave sea más grande, para proporcionar alta seguridad
Aspectos de Seguridad	Confidencialidad Integridad	Confidencialidad Integridad Autenticidad del emisor No repudio
Aplicación	Cifrado de datos	Cifrado de datos, firma digital e intercambio de claves

Elaborado por: María Belén Gómez

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Objetivos específicos	Conclusiones
Mejorar la seguridad disminuyendo la vulnerabilidad ante amenazas de acceso no autorizado a la información.	Las redes inalámbricas usan medios inseguros para la transmisión de datos y esto influye mucho en la seguridad de la información que se transmite. Con la finalidad de ofrecer seguridad en las redes inalámbricas se desarrollaron diversos protocolos de cifrado de datos, entre los que se puede mencionar: WEP, WPA, WPA2, IPSec, los cuales tratan de proporcionar la misma seguridad que la de un cable, a la información que circula por la red. Estos protocolos mejoran la seguridad porque cubren cuatro aspectos fundamentales de las comunicaciones seguras que son: Asegurar que los datos privados transmitidos en una red no sean revelados a personas no autorizadas (confidencialidad); garantizar la autenticidad del mensaje (autentificación); garantizar que la información que se transmite no sea alterada por personas no autorizadas (integridad); y evitar que el emisor o el receptor nieguen la transmisión de una información (no repudio). Lo anterior lo corrobora un estudio realizado a importantes empresas e instituciones del país como son: SRI, Subsecretaría de Educación Coordinación Zonal 8, Coordinación Zonal 8 del MIES, Ministerio de Salud Pública, IESS, TELE-RED y Claro. El 86% de estas instituciones y empresas, afirmaron que el algoritmo de cifrado de datos que utiliza la solución de seguridad más usada por sus redes inalámbricas les ofrece un alto nivel de seguridad. Todas estas instituciones y empresas utilizan como solución WPA2 a excepción del MSP que utiliza WEP y Claro que utiliza VPN.

Establecer costo-beneficio del cifrado de datos.	Como se vio anteriormente para proporcionar seguridad a las redes inalámbricas, existen tres soluciones disponibles: WPA (WiFi Protected Access), WPA2 (WiFi Protected Access 2) y VPN(Virtual Private Network), WEP está en desuso porque es vulnerable. La solución de seguridad que se elija depende del tipo de LAN inalámbrica a que se está obteniendo acceso y del nivel de cifrado de datos que se requiere. WPA (WiFi Protected Access) y WPA2 (WiFi Protected Access 2) son estándares de seguridad para WLAN de pequeñas, medianas y grandes empresas, pequeñas oficinas y para el hogar, para su implementación se requiere de adaptadores de red inalámbricos USB o PCI y de un router inalámbrico cuyos costos en el mercado no son muy altos. Según la investigación de campo realizada para montar una red inalámbrica de 10 computadoras con ésta solución de seguridad se requiere de $317,90 y su instalación y configuración es fácil. En cambio VPN está dirigida a empresas que desean conectar de manera segura oficinas y usuarios remotos por medio de accesos económicos a internet dados por terceros. Las VPN dan el mayor nivel de seguridad posible por medio de seguridad IP(IPsec) cifrada o túneles VPN SSL, para su implementación al igual que la solución de seguridad anterior se requiere de adaptadores de red inalámbricos USB o PCI y de un router VPN inalámbrico cuyo costo es muy elevado. Según la investigación de campo realizada, para montar una VPN compuesta de dos WLAN, donde cada WLAN está compuesta de 5 computadoras se requiere de una inversión de $976,64 incluyendo los costos de instalación y configuración de las dos WLAN, puesto que montar ésta solución de seguridad es más compleja y se requiere de personal muy capacitado. Según la encuesta realizada a las instituciones y empresas mencionadas anteriormente los beneficios de implementar WPA y WPA2 son: seguridad para las redes abiertas, fácil de implementar, puede ser administrable, incremento de

	seguridad sobre accesos no deseados, protección de ataques de fuerza bruta, control de acceso a los recursos y servicios de red, entre otros. Y los beneficios de implementar VPN son: evita accesos o ataques a la red, es óptima y única.
Realizar un estudio que determine la carga de procesamiento que demanda el cifrado de datos y su comportamiento en el ciclo de transmisión.	Para realizar el estudio se encuestó a profesionales del área de sistemas (Especialista en Informática, Jefe de Unidad TIC, Analista Senior TIC´s, Coordinador servicios informáticos, Director de Sistemas, Ingeniero en Network SIS) de las instituciones y empresas antes mencionadas ubicadas en la ciudad de Guayaquil, las cuales poseen muchas WLAN dentro de su infraestructura de redes. De acuerdo al estudio, Servicio Rentas Internas, Subsecretaría de Educación Coordinación Zonal 8, Coordinación Zonal 8 del MIES, IESS y TELE-RED y Claro que representan el 86% de las instituciones y empresas encuestadas afirmaron que los algoritmos AES y RC4 les ofrecen una alta velocidad de transmisión de un archivo. La mayoría de estas empresas utilizan AES a excepción de Claro que utiliza el algoritmo de flujo RC4 implementado en VPN, el cual es muy usado en las conversaciones de telefonía celular, donde la voz se digitaliza, es decir, se convierte a un flujo de bits. En cuanto a la carga de procesamiento que demanda el cifrado de datos, según el estudio el 100% de las empresas e instituciones encuestadas respondieron que es baja la carga adicional asociada con el cifrado y descifrado de datos que tiene que soportar el sistema de computo con el algoritmo de cifrado de datos, lo que significa que con ninguno de los 2 algoritmos que utilizan (AES o RC4) estas entidades consume muchos recursos del sistema de computo.

Recomendaciones

Objetivos específicos	Recomendaciones
Mejorar la seguridad disminuyendo la vulnerabilidad ante amenazas de acceso no autorizado a la información.	El Ministerio de Salud Pública debería dejar de utilizar la solución de seguridad WEP, puesto que este protocolo de cifrado no es muy fuerte y tiene muchas vulnerabilidades, ya que no es tan difícil obtener la contraseña de cifrado. Debería utilizar WPA2 que es compatible con WPA y utiliza el algoritmo AES para el cifrado de datos, esta solución proporciona un alto nivel de seguridad y es de bajo costo de implementación. WPA2 puede habilitarse en 2 versiones: WPA2 Personal que protege de acceso no autorizado a la red usando una contraseña determinada y WPA2 Enterprise que verifica a los usuarios de la red a través de un servidor. También puede optar por la solución VPN, que es otra solución fuerte que existe en la actualidad para redes inalámbricas, pero su costo de implementación es más alto.
Establecer costo-beneficio del cifrado de datos.	Al implementar la solución WPA o WPA2 se puede utilizar adaptadores de red inalámbricos del tipo USB que son de fácil instalación en comparación con los PCI, los cuales requieren de conocimientos técnicos para su instalación. La diferencia en costo no es muy alta en comparación con los PCI. Si se va a implementar la solución VPN, hay que asesorarse con socios comerciales de empresas líderes a nivel mundial en soluciones de redes, como por ejemplo CISCO. Estos socios se encuentran ubicados en las principales ciudades del país y ofrecen servicios de: diseño e implementación de VPN para entornos empresariales; venta, asesoramiento, instalación y configuración de equipos de redes; mantenimiento preventivo y correctivos de equipos de red, entre otros.

	Al implementar cualquiera de las soluciones de cifrado antes mencionada, es necesario saber que por más mecanismos de seguridad implementados, las redes inalámbricas no son 100% seguras. Por ejemplo un atacante podría usar un inhibidor de señales inalámbricas como las que tienen los bancos y podría hacer que la red inalámbrica deje de funcionar.
Realizar un estudio que determine la carga de procesamiento que demanda el cifrado de datos y su comportamiento en el ciclo de transmisión.	Se recomienda utilizar el algoritmo AES implementado en WPA2 y el algoritmo RC4 implementado en VPN, ya que de acuerdo al estudio realizado a las instituciones y empresas que tienen implementadas soluciones de seguridad en sus WLAN, determinó que estos algoritmos ofrecen una alta velocidad de transmisión de la información y una baja carga adicional relacionada con el proceso de cifrado y descifrado de datos para el sistema de computo. Al implementarlos procurar la versión del algoritmo con la longitud de clave más grande que exista, puesto que este es el factor más importante y que lo hace más seguro.

BIBLIOGRAFÍA

Atelin, Philippe., Dordoigne, José. *Redes Informáticas: Conceptos fundamentales*. Barcelona, Ediciones ENI, 2006.

Gil, Pablo. Pomares, Jorge. Candelas, Francisco. *Redes y transmisión de datos*. España, Univesidad de alicante. 2010

Mouteira, Ruben. *Instalación de redes informáticas de ordenadores*. Ideas propias, 2004

Sampalo, María. Leyva, Esteban. Garzón, María. Prieto, José. *Informática.* España: MAD. S.L. 2003

Tanenbaum, Andrew. *Redes de computadoras. México,* Prentice Hall, 2003

Seoane, Eloy. *Estrategia para la implantación de nuevas tecnologías en Pymes*. España, Ideas propias, 2005

Fernández, Santiago. *La Criptografía Clásica*. Sigma No. 24. 2004.

Mathon, Philippe. *Windows Server 2003: servicios de Red TCP/IP*. Barcelona, ENI, 2004

Sánchez, Luis. *Informática II*. México, Pearson Educación, 2007

Savitch, Walter. *Resolución de problemas con C++: el objetivo de la programación*. México, Prentice Hall, 2006

Stallings, William. Fundamentos de seguridad en redes: aplicaciones y estándares. Madrid, Pearson Educación S.A., 2004

WEBGRAFÍA

Pes, Carlos. Redes Cliente/Servidor e Igual a Igual. http://www.carlospes.com/curso_de_informatica_basica/04_02_redes_cliente_servidor_e_igual_a_igual.php. Acceso: el 3 de mayo de 2013

Araúz, Ibell., Guerra, Katherine., Serracín, Karoll., Tristán, Adilia. Topología de malla. Fuente: http://topo-malla.blogspot.com/. Acceso: el 3 de mayo de 2013

Cárdenas, Lina. Programación orientada a objetos. http://programaciooao.blogspot.com/2011/05/byte-bit.html. Acceso: el 3 de mayo de 2013

Banco de Guayaquil. EasyLogin. https://bancavirtual.bankguay.com/nuevabancavirtual/EasyLogin/wflogin.aspx. Acceso: el 5 de mayo de 2013

Scribd. *Historia de las redes de computadoras*. http://es.scribd.com/doc/50158399/HISTORIA-DE-LAS-REDES-DE-COMPUTADORAS. Acceso: el 3 de mayo de 2013

Wikipedia. *Transmisión de datos* http://es.wikipedia.org/wiki/Transmisi%C3%B3n_de_datos. Acceso el 3 de mayo de 2013

Silcom. Silcom. http://www.silcom.com.pe/soluciones_seguridad_redes.html. Acceso: el 5 de mayo de 2013

Rincón Astur. Memorias de un aprendiz de PHP. http://www.rinconastur.com/php/php19.php. Acceso: el 10 de mayo de 2013

Trendnet. Trendnet/Products/Tew-711BR. http://www.trendnet.com/langsp/products/proddetail.asp?prod=225_TEW-711BR&cat=173. Acceso: el 10 de mayo de 2013

Sánchez, Jorge. Descripción del algoritmo DES. http://www.tierradelazaro.com/public/libros/des.pdf. Acceso: el 15 de mayo de 2013

Rennella, Michael., Erazo, Juan., Muñoz, Luis. Antología del algoritmo de cifrado AES. http://www.fup.edu.co/investigacion/fupcric/images/pdf/aes.pdf. Acceso: el 15 de mayo de 2013

http://www-ma2.upc.es/~cripto/Q1-02-03/wep.pdf. Acceso: el 15 de mayo de 2013

IPSD. IPSD-Soluciones Inalámbricas. http://www.ipsd.cl/net_red2.html. Acceso: el 17 de mayo de 2013

Compudisc. Redes. www.compudisc.net. Acceso: el 1 de Agosto de 2013