ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS Y DESCRIPCIÓN DE LA GESTIÓN DE LA SEGURIDAD EN AMBIENTES UMTS Y DESARROLLO DE HERRAMIENTA DIDÁCTICA"

TESINA DE SEMINARIO

Previa obtención del título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES
INGENIERO EN TELEMÁTICA

Presentado por:
NICOLE SAMANTHA VALVERDE PALMA
IVAN FERNANDO FAREZ TAPIA

GUAYAQUIL-ECUADOR
2014

AGRADECIMIENTO

Mi principal agradecimiento Ing. Washington Medina, mi tutor en este proyecto, que brindó su apoyo a mejorar poco a poco el contenido y el desarrollo de la aplicación web.

Un agradecimiento a la señorita Nicole Valverde, mi compañera de proyecto, persona que se ha dedicado en gran esfuerzo a concluir el informe junto conmigo.

Iván Fernando Farez Tapia

AGRADECIMIENTO

Agradezco a Dios por guiar mis pasos en el camino correcto. A mis padres que han estado conmigo dándome su amor y guía, a mis hermanos y familia por brindarme su cariño.

A mi compañero Iván Farez Tapia por estar presente en cada paso del desarrollo del proyecto de graduación.

A mi tutor Ing. Washington Medina por darnos la oportunidad de participar en su seminario y darnos ese sueño de graduarnos.

A mis amigos que han estado presentes en todo momento de mi carrera.

Nicole Samantha Valverde Palma

DEDICATORIA

Principalmente a Dios, el ser que me ha dado fortaleza en todo este proceso desde que ingresé a la universidad; por ello, con todo mi corazón.

Igualmente le dedico esta tesis a mi madre que ha sabido formarme con buenos valores y virtudes. A mis hermanos que han estado apoyándome siempre y que han sido fundamentales para culminar mi carrera de pregrado y en general a toda mi familia, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos en la vida.

Iván Fernando Farez Tapia

DEDICATORIA

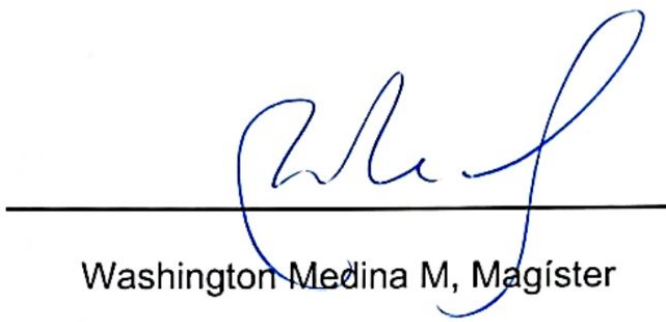
Dedico principalmente mi trabajo a Dios, por iluminarme para poder finalizar una gran etapa estudiantil.

Dedico a mis padres Marcos y Carlota, a mis hermanos Lorena y Omar, a mi abuelita Cristina por darme su cariño incondicional.

A mis amigos por estar presentes en cada paso y momento de mi vida.

Nicole Samantha Valverde Palma

TRIBUNAL DE SUSTENTACIÓN



Washington Medina M, Magíster

PROFESOR DE SEMINARIO DE GRADUACIÓN

Sara Ríos Orellana, Magíster

PROFERSORA DELEGADA POR LA UNIDAD ACADÉMICA

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este informe, nos corresponde exclusivamente, y el patrimonio intelectual del mismo a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Nicole Samantha Valverde Palma

Iván Fernando Farez Tapia

RESUMEN

El presente trabajo de investigación nos provee una visión general del funcionamiento de la seguridad en redes UMTS.

En el capítulo 1 de éste documento, se da una breve introducción sobre la evolución de la tecnología celular móvil hasta su actualidad, el tipo de modulación utilizada en las distintas etapas del desarrollo de la tecnología de las redes. Además de una introducción a la red UMTS, su organización, estructura y características.

En el capítulo 2 se detalla la evolución del tipo de modulación desde TDMA a WCDMA con la técnica DS-CDMA. Se detalla sobre la arquitectura de la red de segunda generación GSM con sus diferentes elementos que lo conforman, su tipo de seguridad, pilar indispensable para el desarrollo y fortalecimiento de las redes UMTS, también detallando el tipo de arquitectura para la seguridad en ambientes conmutados por paquetes que soportan servicios IP.

En el capítulo 3 entra en más detalle sobre sus tipos de cifrado respectivos, los tipos de algoritmos utilizados en redes UMTS como el KASUMI, utilizada en los algoritmos de integridad y confidencialidad, así como generación de claves en función del módulo KGCORE, utilizado en diversos algoritmos para facilitar su

implementación dentro del sistema y desarrollo de futuras mejoras en el ámbito de la seguridad de claves.

En el capítulo 4 se describe los algoritmos de autenticación y generación de claves para el acceso y autenticación a la red, aplicados dentro de los equipos de los usuarios, los centros de Autenticación, bases de datos de los usuarios locales como visitantes, así como el tipo de versiones de los algoritmos de integridad y confidencialidad para el correcto establecimiento de la conexión. También explica los algoritmos para la interacción y exitosa autenticación de los usuarios que se encuentren en dos redes distintas, como GSM y UMTS.

En el capítulo 5 se describe el desarrollo y la arquitectura de la aplicación web, se explica detalladamente los requerimientos funcionales y no funcionales, además de los casos de uso dependiendo de cada uno de los usuarios.

ÍNDICE GENERAL

ABREVIATURAS

2PC	Two-PhaseCommit
3GPP	3rd Generation Partnership Project
A3	Algoritmo de autenticación A3
A5	Algoritmo de encriptación de datos
A5/1	Algoritmo de cifrado de flujo para comunicación en interfaz aire de GSM
A5/2	Algoritmo de cifrado de flujo devoz de GSM
A5/3	Algoritmo de bloques basado en el algoritmo KASUMI
A8	Algoritmo de generación de claves aleatorias
ACID	Atomicity, Consistency, Isolation and Durability
ACK	Mensaje de confirmación de sesión o acción
AES	Advanced Encryption Standard
AH	Authentication Header
AK	Anonymity Key
Algoritmo f8	Algoritmo de confidencialidad f8 por flujo de transmisión
Algoritmo f9	Algoritmo de control de integridad f9 por bloques

AMF	Authentication Management Field
AMPS	Advanced Mobile Phone System
API	Application Programming Interface
API ORM	API Object Relational Mapping
ARIB	Association of Radio Industries and Businesses
Atom	Fichero en formato XML para redifusión web
AuC	Authentication Centre
AUTN	Función de autenticación del Usuario
BEARER	Parámetro de entrada algoritmo de confidencialidad
BS o BTS	Base Station o Base Transceiver Station
BSC	Base Station Controller
BSD	Berkeley Software Distribution
BSS	Base Station Subsystem
BYE	Petición de finalización de la sesión
Bytecode	Código Byte
C o C++	Lenguaje de programación
CANCEL	Mensaje de denegación de sesión o acción
CBC	Cipher Block Chaining

CBC-MAC	Cipher Block Chaining Message Authentication Code
CCSA	China Communications Standards Association
CDMA	Code División Múltiple Access
CEPT	Conference of European Posts and Telegraphs
CIPHERTEXT	Texto cifrado usado como parámetro de salida f8
CK	Clave de cifrado del algoritmo f8
CN	Core Network
COMP128	Algoritmo de autenticación GSM
COUNT-C	Parámetro de entrada algoritmo de confidencialidad
COUNT-I	Parámetro de entrada algoritmo de integridad
CS	Circuit Switching
CSCF	Call Session Control Functions
CSRF	Cross Site Request Forgery
D-AMPS	Digital AMPS
Datafiles	Archivo de datos asociado a una Tablespace
DES	Data Encryption Standard
DIRECTION	Parámetro de entrada algoritmos de confidencialidad e integridad

Django	Framework web Python de alto nivel que fomenta el rápido desarrollo y el diseño limpio y pragmático
DRY	Don't Repeat Yourself
DS-CDMA	Direct Sequence CDMA
EDGE	Enhanced Data Rates for GSM Evolution
EIR	Equipment Identity Register
ESP	Encapsulation Security Payload
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiple Access
FRESH	Parámetro de entrada algoritmo de integridad
GEA3	Encryption Algorithm for GPRS 3
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Services Switching Center
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HFN	Hyper Frame Number
HLR	Home Location Register
HSS	Home Subscriber Server

I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IK	Clave de integridad del algoritmo f9
IKE	IP Multimedia CN Subsystem
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia CN Subsystem
IMS AKA	IMS Authentication and Key Agreement
IMSI	IMS Identity
IMT-2000	ITU global standard for international mobile telecommunications 2000
INVITE	Petición de acuerdo de inicio de alguna sesión
IPsec	IP Security Protocol
ISDN	Integrated Services for Digital Network
ITU	The International Telecommunication Union
Java	Lenguaje de programación
KAC	Key Administration Centre
KASUMI	Algoritmo de cifrado de bloques basado en los algoritmos f8 y f9
KGCORE	Core Keystream Generator
Kc	Key ciphers

KEYSTREAM	Parámetro de salida algoritmos de secuencia de claves f8
IKE	Internet Key Exchange
Ki	Individual Key
LENGTH	Parámetro de entrada algoritmo de confidencialidad
MAC	Medium Access Control
MAC o XMAC-I o	Message Authentication Code
MAC-I	Message Authentication Code - Integrity
MAPsec	Mobile Application Part Security
MCC	Mobile Country Code
ME	Movil Equipment
MESSAGE	Parámetro de entrada algoritmo de integridad
Middleware	Software intermedio de soporte a una aplicación para interactuar con otras aplicaciones
MILENAGE	Conjunto de algoritmos de autenticación y generación de claves
MISTY	Algoritmo de cifrado de bloque, base para el diseño de KASUMI
MNC	Mobile Network Code

MSC	Mobile Switching Center
MSC/VLR	Mobile Switching Center/ Visitor Location Register
MSIN	Mobile Suscriber Identification Number
MySQL	Base de datos para transacciones en línea
NE	Network Element
NSS	Network and Switching Subsystem
OFB	Output Feedback
OK	Mensaje de aceptación de invitación a iniciar la sesión
Online/Hot Backups	Respaldo en línea
OP	Valor utilizado en el conjunto de algoritmos MILENAGE
OPTION	Petición de opciones del usuario que establece la sesión sin inicialarla previamente
Oracle	Consolidación en nubes de bases de datos y sistemas de ingeniería
P-CSCF	Proxy CSCF
PIN	Personal Identification Number
PITR	Point In Time Recovery
PLAINTEXT	Texto claro usado como parámetro de entrada f8

PostgreSQL	Sistema de gestión de bases de datos
PS	Packet Switching
PSTN	Public Switched Telephone Network
Python	Lenguaje de programación
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RAND	Generador del valor de desafío
REDO	Archivo de registro de recuperación
REGISTER	Petición de registro de los usuarios para comunicación SIP
RFCs	Request for Comments
Rijndael	algoritmo de cifrado en bloque
RLC	Radio Link Control
RLC AM	RLC Acknowledged Mode
RLC TM	RLC Transparent Mode
RLC UM	RLC Unacknowledged Mode
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
RSS	Really Simple Syndication

RTP	Real-time Transport Protocol
SA	Security Association
S-CSCF	Serving CSCF
SCP	Service Control Point
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initation Protocol
Socket	Interfaz de programación de aplicaciones API para la familia TCP/IP
SPD	Session Description Protocol
SQLite3	Librería de software que implementa una base de datos SQL
SQN	Sequence Number
SR - Hot Standby	Streaming replication - Hot Standby
SRES, RES o XRES	Expected Result
SRNC	Services RNC
Tabletspace	Lugar de almacenamiento de datos
TCP/IP	Transmission Control Protocol/Internet Protocol
TSG	Grupo de Especificaciones Técnicas

TTA	Telecommunications Technology Association of Korea
UA	User Agent
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UMTS	Universal Mobile Telecommunication System
Unicolde	Código Único
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Acces
UTRA/FDD	Universal Terrestrial Radio Access/Frequency-Division Duplexing
UTRA/TDD	Universal Terrestrial Radio Access/ Time Division Duplex
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
WAL	Write-Ahead Log
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access

XOR	OR exclusivo

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de investigación nos provee una visión general del funcionamiento de la seguridad en redes UMTS, conociendo su historia antes de su creación y con la ayuda de la aplicación web llegar con más detalle a todos los usuarios.

Desde el principio de la historia la comunicación ha sido una necesidad para el ser humano, ya sea con su comunidad como con sus vecinos; sin embargo, no toda la información que se desea transmitir debe ser accesible para todos, por lo que se evidenció en las estrategias militares, descubrimientos científicos de cualquier naturaleza. Es entonces, cuando se comenzó a intercambiar información confidencial dirigida a grupos específicos, y restringida para el resto de la población. Estos mecanismos de seguridad constituían entre otras opciones, una estrategia defensiva de las naciones, ya que la falta de confidencialidad en la información los ponía en desventaja con sus enemigos o rivales en el campo de la investigación y desarrollo. Como ejemplo podemos citar lo que ocurría en épocas de guerra, donde se practicaba distintas formas de “esconder” o “codificar” el mensaje enviado para que solo pueda ser interpretado por el remitente, de tal forma que si el mensajero era interceptado, la información que portaba con él no

corría peligro si caía en manos del enemigo. En la antigüedad ya se usaba éste tipo de comunicación: los romanos utilizaron un sistema de sustitución conocido como César, porque se cree que Julio César lo empleó, siendo uno de los sistemas más conocidos de la antigüedad, en él, las letras del mensaje original eran reemplazadas por otras ubicadas unas posiciones más adelante en el alfabeto (por lo general se desplazaba 3 posiciones). Al final, se tenía un texto incomprensible para la persona que no sabía qué tipo de codificación se había usado, y no se descifraban los planes del imperio romano. Como otro ejemplo podemos citar la Historia de la II Guerra Mundial, en 1942 un hombre llamado Philip Johnston ideó un código que creía que sería indescifrable para los japoneses, en el lenguaje navajo, para encriptar la información del movimiento de tropas, utilizando como “locutores” a indios Navajos entrenados para ser los extremos del enlace de sus comunicaciones por radio (Prieto L.).

En la evolución de las comunicaciones, se llega al desarrollo de la telefonía fija, del Internet y de la telefonía móvil, los mismos que a través de la tecnología actual, cumplen con la necesidad de que la información se transmita sin ser descifrada en el trayecto y sin barreras, permitiendo ingresar al mundo globalizado. Este constituye un gran paso en la era de las telecomunicaciones, y permiten a cada país interconectarse con el resto del mundo, haciendo que millones de personas se encuentren en contacto con demás personas alrededor del mundo, enviando

o recibiendo datos a través de la red, muchas veces de carácter confidencial. Esta necesidad continúa en aumento, y ha motivado a que se incremente la demanda además de exigencia de mejores servicios, tanto en infraestructura como en seguridad a los operadores de su región, evolucionando la manera de comunicarnos y de compartir información en la red.

CAPÍTULO 1

INTRODUCCION A UMTS

1.1. Introducción a la seguridad en telecomunicaciones

Desde sus inicios, la seguridad de la información ha constituido un factor importante de preocupación a nivel empresarial y también del usuario de este servicio; pues cuando la comunicación era solamente alámbrica, (hace unos pocos años atrás) el temor de las empresas era la posibilidad del espionaje empresarial, personal o de otro tipo, a través de este medio. Aunque la comunicación ha estado evolucionando considerablemente a través del tiempo, el uso de redes unidas entre sí por cables conectados a un terminal, aún ofrecen la garantía de que su configuración permanece fija

durante cualquier operación, y la transmisión de datos y voz viaja a través de ella sin problemas, pero no asegura su confidencialidad e integridad frente a atacantes en la mitad (man in the middle), que desean escuchar la comunicación o hurtar datos con fines maliciosos “pinchando” los terminales con otro cable conectado a él. En la actualidad, en redes telefónicas alámbricas, existe aún riesgo en el “pinchazos” de llamadas (Niemi V., Nyberg K., 2003)

1.2. Historia de la telefonía Móvil

En caso de los teléfonos móviles, comenzó con la aparición de la primera generación (1G) a finales de los años 70, caracterizado por su tecnología analógica. Aunque tuvo mucha acogida, al tener mayor cantidad de usuarios, su calidad de servicio se degradaba además de ser poco segura. Se crea el sistema AMPS (Advanced Mobile Phone System), El Sistema Telefónico Móvil Avanzado considerado de primera generación, implementado en el año de 1978 en Estados Unidos, en el que dividen el espacio aéreo geográfico en celdas (de ahí el nombre de telefonía celular o cells) con la capacidad de alternar entre dichas celdas entre radiobases sin perder la conexión pero transmitiendo a diferentes frecuencias, con el fin de evitar interferencias, operando en la banda de 800 MHz. El sistema usa 832 canales simples de enlace ascendente y el mismo número de canales para

enlace descendente, teniendo en total 832 canales dobles. Cada uno de ellos con un ancho de banda de 30 KHz, algunos de los canales son usados, aparte de la comunicación entre usuarios, para el control y administración de los enlaces.

La primera técnica de comunicación inalámbrica que se implementó dentro de la primera generación 1G fue la FDMA (Frequency Division Multiple Access), en el que el espectro es dividido en canales, haciendo que las llamadas sean separadas a frecuencias iguales; es decir, a mayor cantidad de abonados, mayor cantidad de frecuencias dispuestas dentro del espectro, reservando ese canal durante la llamada.

Por su gran demanda por parte de los abonados, al ser una idea exitosa aunque tecnológicamente limitante; puesto que durante la sesión de una llamada, el canal que se le asigna a dicha MS es sólo utilizada por él, ocupando un espacio considerable dentro del enlace, además que al ser señal análoga los hace suceptible a la interferencia. Por estas deficiencias se decidió que era tiempo de incrementar la capacidad dentro del ancho de banda del espectro asignado convirtiendo la señal analógica a la digital. Entonces a inicios de los años 90 se despliega el sistema Digital AMPS (D-AMPS), conocidos ya como sistemas móviles de segunda generación (2G), o TDMA, técnica usada por algunos sistemas de telefonía móvil como el IS-

54 (incluyendo mensajes de texto cortos o SMS) y el IS-136. D-AMPS utiliza canales AMPS que se encuentran existentes, permitiendo una transición suave de la era analógica a la digital. El protocolo que usa dicha técnica es el IS-54, que divide cada canal en tres ranuras de tiempo, comprimiendo los datos de voz de manera digital, y por ende, aumentando la capacidad de llamadas dentro de la misma celda. Mientras el otro estándar (IS-136) es una mejora del IS-54 en la parte de mensajería celular y algunas aplicaciones de datos (Lara J., 2006).

Con la aparición de las redes de segunda generación (2G), había aumentado requerimiento de una alta disponibilidad de enlace para la creciente demanda por parte de los usuarios, llevando al desarrollo de dos sistemas de manera simultánea, TDMA y CDMA.

TDMA fracciona el canal de transmisión en intervalos de tiempo para la transferencia y compresión de datos usando todo el ancho de banda disponible hasta su término, logrando de esta manera subdividir el enlace, con la finalidad de que varios usuarios utilicen el mismo canal de manera simultánea sin interferir entre sí por un tiempo determinado además de permitir mayor capacidad que un sistema analógico con la misma cantidad de canales debido a su compresión digital.

En cambio la tecnología CDMA (Code División Múltiple Access), resuelve la transmisión en un único canal de comunicación y gestiona varias transmisiones al mismo instante, haciendo que todos los usuarios compartan la misma frecuencia; es decir, transmite en todo el ancho de banda que dispone, a diferencia de los sistemas FDMA y TDMA, con el único problema de producir mayor interferencia.

CDMA se caracteriza por sus bandas que son divididas en canales de RF, donde cada canal consiste de un par de frecuencias (Transmisión y Recepción) con 1,25 MHz de ancho de banda; por lo que en teoría podría existir hasta 10 canales de RF en una Banda de 12,5 MHz. En la realidad, ésta cifra es menor pues esta banda se encuentra dividida con la red AMPS, lo que lleva a establecer una banda de guarda (Amaterazú, 2003).

Con el surgimiento de este sistema, se creó el estándar IS-95, o conocido como CDMAOne, diseñado para transmitir voz, datos y señalización de llamadas, en las que todas las estaciones transmiten en la misma banda de frecuencia. La diferencia es la separación entre usuarios, la cual se realiza usando códigos ortogonales que se eliminan al ser multiplicados entre sí. Al final del enlace, la información se recupera en la estación móvil (MS) usando el mismo código que se usó en la estación base.

El estándar definido para el sistema TDMA es el IS-54, con un ancho de banda de 30 KHz de AMPS en cada uno de sus enlaces. Cada canal de voz soporta un frame de TDMA, es decir, seis ranuras de tiempo (time slots) para una comunicación que soportan 3 canales de tráfico full-rate o 6 canales de tráfico half-rate; es decir, tres usuarios pueden compartir el radio canal al mismo tiempo o seis usuarios máximo puedan compartir el radio canal respectivamente dependiendo del rango. La señalización del canal de tráfico es similar al estándar IS-136, herencia del sistema predecesor AMPS o D-AMPS que comparte los mismos canales físicos para poder desplazarse dentro de AMPS y coexistir con ambos estándares (Amaterazú C., 2003).

Con todo el avance aún había problemas como el de no disponer de un mismo teléfono móvil para estar en diferentes regiones o aún más alejado, en diferentes países (Roaming) para la libre circulación. Ante esto, aparece la tecnología GSM (Global System for Mobile Communication), la cual presta servicios de voz de calidad superior y transmisión rápida de datos usando la técnica de TDMA citada anteriormente, con la diferencia que se encuentra dividida en ocho ranuras de tiempo (en lugar de seis como se dijo antes), razón por la cual GSM puede soportar un mayor número de suscriptores por canal de voz. La razón de su popularidad es sin duda el mayor esparcimiento de 200 KHz en lugar de 30 KHZ como se utilizaba en redes AMPS.

GSM se convirtió en la más larga red móvil 2G con su sistema de seguridad de confidencialidad, autenticación del usuario y encriptación de los datos de señalización y llamadas, fue el impulso para el desarrollo de las funciones de seguridad para las generaciones posteriores. Denominada estándar de segunda generación ya que las comunicaciones se producen de un modo completamente digital, a diferencia de la primera generación. Realmente el sistema GSM comenzó en el año de 1989, como un grupo de estudio para el desarrollo de un sistema telefónico móvil para una red celular conocido como Groupe Special Mobile creado por la CEPT (Conference of European Posts and Telegraphs) y ahora Global System for Mobile Communications, pero debido a algunas modificaciones en las especificaciones, retraso en los acuerdos de pruebas de certificaciones y desarrollo de equipos que soporten el sistema digital, no fue hasta el año de 1992 que aparecieron en el mercado los primeros teléfonos móviles incorporados con sistemas GSM extendiéndose rápidamente por todo el mundo por su calidad de servicio y características de roaming entre los países participantes (Lara J., 2006, pág. 7).

Una de las características significativas es de permitir una velocidad máxima de 9,6 Kbps para transmisiones de voz, mensajes SMS o multimedia MMS en la banda de frecuencia de 900 MHz y 1800 MHz con el método TDMA.

En materia de seguridad usa tarjeta para cada usuario para autenticación de la llamada y confidencialidad por medio de números de serie en cada móvil (García R., 2012).

Con el avance de la investigación se amplía la tecnología 2G, partiendo del sistema GSM, a la llamada tecnología 2.5G, la cual añade mejores capacidades de transmisión de datos, por medio de paquetes, mejorando la infraestructura de red existente. Una de las tecnologías diseñadas a partir de GSM encaminadas a la generación 2.5G es el GPRS (General Packet Radio System), mejorando su velocidad en la transferencia de datos (de hasta 144 Kbps) y su conexión permanente, ya que no ocupa los recursos de la red mientras no se encuentre intercambiando datos pero siempre se encuentra "online", aplicaciones para móviles usando el protocolo WAP (Wireless Application Protocol).

Otro protocolo creado a la vez fue el estándar EDGE (Enhanced Data Rates for GSM Evolution) o generación 2.75G, y como se observa es la evolución de GSM/GPRS pensado para la transición hacia los sistemas inalámbricos de tercera generación, basado en conmutación por paquetes para conexión a internet, soporte de servicios en tiempo real tal como videoconferencia, mensajería instantánea, entre otros más. Obtiene transmisiones de datos

con velocidades de 176 Kbps, similares al servicio que ofrece una red de tercera generación.

Así perfeccionándose para llegar a la tecnología de tercera generación 3G, implementada a inicios del nuevo milenio en los países europeos y un poco después en Estados Unidos, encaminada al acceso de manera inalámbrica a Internet con velocidades de transferencia de hasta 384 Kbps para usuarios en movimiento o velocidades de 2Mbps en usuarios estacionarios, mayor seguridad en el enlace y demás. Para luego avanzar hacia la cuarta generación 4G, mejorando la calidad de servicio en la transmisión y recepción a altísimas tasas de velocidades y seguridad del flujo de datos completamente mejorada ya implementada dentro del país recientemente por la operadora estatal.

1.3. Introducción a la red UMTS

UMTS (Universal Mobile Telecommunication System), estándar europeo de tercera generación que es una mejora al antiguo sistema GSM, ya que utiliza muchos conceptos de dicha tecnología. UMTS ha sido diseñada para ser dinámica y flexible ya que se pueden interconectar distintos dispositivos. UMTS se creó en base a ser estándar con el objetivo de poder adaptar varios servicios dentro de la misma red.

Una de sus características que supera a la antigua tecnología de segunda generación es que la tasa de bits para transmisión (en teoría) llega a 2 Mbps, lo que permite la transmisión en tiempo real de audio y video, además de permitir que se trabaje con otras aplicaciones IP con el fin de que su calidad de voz sea equiparable o superior con la red de telefonía fija. Otra diferencia considerable es su tipo de modulación, GSM es basado en TDMA mientras que UMTS se basa en WCDMA (Wideband Code Division Multiple Access) de espectro extendido, es decir, que los usuarios transmiten simultáneamente sus datos y llamadas sobre varias frecuencias al mismo tiempo con el mismo ancho de banda puesto no hay separación de frecuencia, además de ser espectro extendido en su banda base en la salida de su origen para esparcir la señal en todo el ancho de banda por seguridad, entretanto los usuarios TDMA usan un canal fijo para cada transmisión durante un intervalo de tiempo.

UMTS está siendo desarrollado por 3GPP (3rd Generation Partnership Project), un proyecto común en el que colaboran varias empresas alrededor del mundo: ETSI (Europa), ARIB (Asociación de Industrias y Empresas de Radiocomunicaciones) ARIB/TIC (Japón), ANSI T-1 (USA), TTA (Asociación de Tecnología de Telecomunicaciones de Korea), CCSA (China Communications Standards Association). Su principal objetivo de su

cooperación fue de estandarizar los sistemas de comunicaciones celulares. La primera versión de UMTS surgió en el año de 1999 en la que se establecía una evolución desde redes GSM. ITU (Unión Internacional de Telecomunicaciones) es la encargada de establecer el estándar para que todas las redes 3G sean compatibles orientado a proporcionar un servicio orientado a paquetes (Niemi V., Nyberg K., 2003).

Esta red se caracteriza por capacidad de conexión WCDMA y su alta velocidad de transmisión de bits (de hasta 2 Mbps), hace posible que nuevos servicios se puedan implementar dentro de la red logrando abrir nuevos mercados en ella. Muchas aplicaciones de video, juegos en línea ahora son portátiles (son soportados en los teléfonos móviles) gracias a UMTS, sin dejar atrás la ampliación del nuevo mercado para la capacidad de mensajería instantánea que incorporan estos equipos actualmente.

UMTS ha sido creado para un sistema de comunicación global, esto incluye componentes terrestres, sistemas alámbricos, inalámbricos, y sistemas satelitales. También es capaz de interactuar con sistemas de Segunda Generación (2G), permitiendo una suave transición hacia los sistemas de tercera generación; por lo que aún el sistema GSM es importante y continúa trabajando en paralelo con UMTS por algún tiempo. Sin embargo, utilizan diferentes bandas de frecuencia: UMTS trabaja en las bandas de 1920 –

1980 y 2110 – 2170 MHz para enlaces de subida y de bajada con duplexacion FDD, WCDMA, con una longitud de 5 MHz de canal y separación entre ellas de 200 KHz. Bandas de 1900 – 1920 y 2010 – 2025 MHz para duplexacion TDD, CDMA con longitud y separación de canal similares. Finalmente bandas de 1980 – 2010 y 2170 – 2200 MHz para enlaces de subida y bajada satelitales (Proaño T, Rodríguez E., , 2007).

Este sistema UMTS integra todos los servicios ofrecidos por las distintas tecnologías precedentes y redes actuales, incluyendo Internet. El sistema UMTS se compone de 3 grandes bloques que se los describirá en su momento:

- Red central o núcleo de red (Core Network, CN)
- Red de acceso de radio (Radio Access Network ,RAN ó UTRAN)
- Terminales móviles (User Equipment, UE) (López J., 2005)

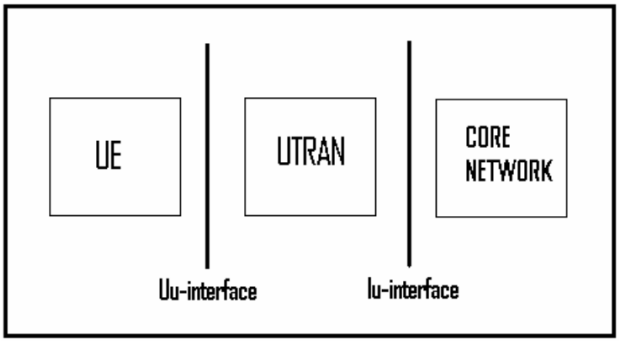


Figura 1.1: Arquitectura de la red UMTS.

Fuente: (López J., 2005, pág. 2)

1.4. Introduccion a 3G Partnership Project (3GPP)

El desarrollo de la red GSM fue un gran avance para la tecnología, existen grandes ventajas de un sistema robusto y bien estructurado como éste, lo que hacía pensar que ya no se necesitaría de un nuevo sistema de comunicaciones móviles al menos por algunos años. Debido a eso el desarrollo de UMTS ha sido en paso lento e inicialmente de manera teórica con el objetivo de implementarla paulatinamente mientras continúa en uso la red anterior y la nueva de forma paralela. En el lado de seguridad, muchas técnicas de cifrado se han propuesto para aumentar la seguridad UMTS; sin embargo en los inicio de ésta tecnología no fue posible decidir entre diferentes propuestas y opciones por las limitaciones impuestas por la arquitectura del sistema de ese entonces.

Por estos inconvenientes se necesitaba de alguna organización que se encargue de poner en marcha y agilice los planes de actualización de la tecnología móvil, lo que dio origen al Proyecto asociación de tercera generación (3GPP), organización de grupos, creado principalmente para diseñar un protocolo para un sistema global de telecomunicaciones de tercera generación 3G en dispositivos basados principalmente en GSM,

dentro del marco del proyecto internacional de telecomunicaciones móviles 2000 de la Unión Internacional de Telecomunicaciones ITU.

3GPP une seis organizaciones de desarrollo de estándares de telecomunicaciones (ARIB, ATIS, CCSA, ETSI, TTA, TTC) conocidos como "socios de la organización" de varios países. Los cuatro grupos de Especificaciones Técnicas más importantes de 3GPP son: Redes de acceso de radio (RAN), Servicio y aspectos del sistema (SA), Núcleo de Red y terminales (CT), Redes de Acceso Radio GSM/ EDGE (GERAN). Los cuales son los encargados de diseñar la red de tercera generación, cada una con una función específica dentro de la organización.

El propósito principal del proyecto 3GPP (3rd Generation Partnership Project) es de actualizar las especificaciones técnicas del estándar WCDMA de IMT-2000, pilar fundamental del sistema UMTS para el acceso a una gran variedad de servicios de telecomunicaciones basadas en las redes de telecomunicaciones fijas. Una de las decisiones tomadas fue la de incluir el modelo del SIM con mejoras e innovaciones también al nuevo sistema por el tema de seguridad, ya que es un método que ofrece autenticación, confidencialidad en las llamadas y transmisión de datos para el UE. Otra mejora significativa es la compatibilidad de servicios IMT-2000 con las redes fijas y aumento de las capacidades de sus sistemas, debido a que este

servicio se sigue ampliando dependiendo de las tendencias de demanda expectativas de los usuarios y tecnología.

Otro propósito del grupo es de buscar seguridad en la comunicación entre los elementos de la red, ya sean pertenecientes a una misma red o de redes diferentes, logrando que por medio de éstos estándares se permita a los diferentes operadores, que administran las redes, la comunicación entre ellos (interconexión mediante acuerdos que los beneficien a las partes) y de esta forma obtener una gran variedad de elementos de red de distintos proveedores que estén unidos entre sí sobre la misma plataforma facilitando la interconexión entre las distintas operadoras (Unión Internacional de Telecomunicaciones, Sector de Radiocomunicaiones, 2003).

Con respecto a la red UMTS, uno de los objetivos del grupo 3GPP estuvo encaminado a conectar la red UTRAN con el CN de GSM/GPRS, haciendo que la MSC (Mobile Switching Center), elemento en la arquitectura GSM, sea parte fundamental, ya que es usado tanto por el sistema GSM como por UMTS; es decir, que los elementos que realizan la conmutación de paquetes como RNS (Radio Network Subsystem) presente en UTRAN del sistema UMTS se puedan conectar con el mismo MSC con la estación base de GSM, componentes descritos más adelante (Niemi V., Nyberg K., 2003, págs. 15, 17).

1.4.1. Introducción de señalización entre operadores

Una de las especificaciones de seguridad del grupo 3GPP es de asegurar la comunicación entre los elementos de la red y que estos cambios sean transparentes al equipo usuario; es decir, que estos elementos de red puedan comunicarse entre ellos así pertenezcan o no a la misma red administrativa. En el último caso (comunicación entre redes) requiere de soluciones estándar para que cada par de operadores acepten una solución común para el “Roaming”, además de tener una gran variedad de elementos de red de diferentes proveedores para su uso.

La seguridad para este tipo de comunicación se ha basado en el sistema de señalización usado para las redes móviles fue el SS7 (Signaling System 7) o Sistema de Señalización por canal común número 7, encargado del intercambio de información. En SS7 existe un solo canal donde viaja información de señalización de varios canales de voz, entre dos elementos de la red o equipos mediante mensajes SS7. SS7 trabaja independiente de la red que da servicio de comunicación, y la red de transporte de comunicación se ocupa de la inicialización de la llamada, su enrutamiento, inclusive en el mantenimiento de la red y constituye el soporte de servicios para

redes inteligentes (IN). A pesar de ser un sistema seguro ya que es difícil crear o adulterar los mensajes SS7 externamente, se desea cambiar a tecnología basadas en Protocolos de internet (IP); que traería varios beneficios por el tipo de empaquetamiento, movilidad a través de la red y demás ventajas, aunque también esto conllevaría a una gran variedad de intrusiones a la red y manipulación de la información; por lo que se debería conocer esta nueva tecnología que se desea implementar. (Niemi V., Nyberg K., 2003)

1.4.2. Arquitectura de Red 3GPP

En esta sección se dará una breve descripción a la arquitectura 3GPP, anteriormente se habló de su historia y conceptos básicos; en esta parte se dará una descripción de los elementos de la arquitectura 3GPP.

En la figura 1.2 se muestra los elementos más importantes en la arquitectura 3GPP. Esta arquitectura se presenta en tres partes principales:

Desde el punto de vista del usuario, la parte con que interactúa con él directamente es el terminal o también llamada Equipo de Usuario (UE). Éste terminal tiene una conexión de radio a nivel local a una

red de acceso de radio (RAN), que además se encuentra conectada a la Red Central (CN).

Además de definir estos elementos de la red, también define las interfaces entre ellas para su comunicación, como los protocolos que se ejecutan entre el UE y la red de acceso, también protocolos entre UE y CN, además de otros elementos de la red. Otro punto que acotar es que la Red Central, encargada de los aspectos globales del sistema, contiene dos dominios de conmutación necesarios para el control y conmutación del abonado. Estos dominios son la conmutación de paquetes (PS) y conmutación de circuitos (CS). El primero descrito es una evolución del dominio de GPRS, que permitió en el avance de la tecnología celular; mientras que el segundo es una evolución de la red GSM tradicional. Actualmente las encapsulación de los datos es en paquetes y fragmentada para su fácil transferencia en la red. Dado que la CN hereda elementos de la arquitectura 2G, es frecuente ver estaciones base GSM y UMTS coexistiendo dentro de una misma red móvil (Niemi V., Nyberg K., 2003, pág. 14).

Este nuevo conjunto de servicios, el GPRS (General Packet Radio Services) fue desarrollado por el grupo ETSI, añadido a los servicios

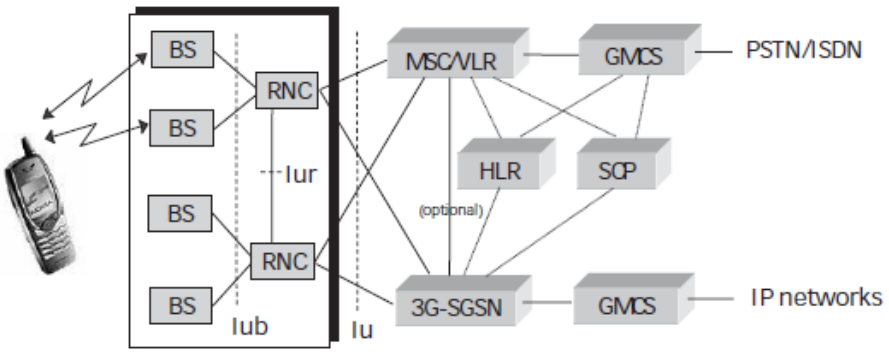
de GSM, el mismo que agrega conmutación de paquetes en todos los niveles de la red para transmitir datos e información de señalización de forma eficiente para poder optimizar el uso de la red y recursos de radio. Además da autenticación, confidencialidad de la identidad del usuario y de su información. Ofrece diferentes tipos de restricciones de acceso a los usuarios del sistema GPRS, manteniendo una brecha entre el subsistema de radio y de red con la finalidad de que el subsistema de red pueda usar diferentes tecnologías de acceso a radio sin realizarle modificaciones a la base instalada en el MSC.

El dominio de conmutación por paquete (PS) es una evolución significativa del dominio GPRS, y los elementos de red más importantes en el dominio PS son el nodo de soporte GPRS (SGSN), el cual es un nodo de servicio GPRS. Como función principal tiene el de dar acceso y seguridad (como el cifrado y autenticación) a los terminales móviles hacia la red de datos que puede ser internet o una red corporativa.

Otro elemento importante es el nodo de soporte de puerta de enlace GPRS (GGSN) que como su nombre lo indica, es una puerta de acceso hacia redes de conmutación PS externas. El dominio PS es

una evolución de la tradicional red de CS GSM con el MSC (o SGSN) como el componente más importante. En el tema de seguridad, las funciones de GPRS son idénticas al de GSM, basados en los mismos algoritmos, criterios y claves, con la diferencia que el algoritmo de cifrado se lo modificó para la transmisión de paquetes de datos; almacenando en el SGSN la información relativa a la seguridad como autenticación del abonado, selección del algoritmo de cifrado y su sincronización que abarca hasta el MS (España M., 2003).

Como se observa en la figura 1.2 de la arquitectura 3GPP, gracias a GPRS la transmisión de paquetes PS es posible, agregándole ésta característica a la red GSM de segunda generación, con el objetivo primordial de proporcionar un alto rendimiento de tasas de datos sin afectar el tráfico de voz minimizando el impacto en el estándar GSM. La arquitectura red GPRS reutiliza los nodos de red GSM como



MSC/VLR, HLR y BSC pero agrega dos elementos para el transporte de paquetes de datos: GGSN y SGSN (In Depth Tutorials & Information)

Figura 1.2: Arquitectura 3GPP.

Fuente: (Niemi V., Nyberg K., 2003, pág. 18)

Para una mejor comprensión del gráfico, en la red local, la información de abonado se mantiene estática en el Registro de Ubicación Local (HLR), que por lo general está integrado con el centro de autenticación (AuC) que contiene los datos de seguridad permanentes relacionados con los suscriptores, generando datos que pueden ser utilizados para las funciones de seguridad en la red de servicio y, especialmente, en el acceso red. También se encuentra el Equipo de Registro de la identidad (EIR), el cual mantiene la identidad (hardware), la información de seguridad del equipo móvil junto con la VLR y el status del equipo. EIR contiene tres listas: la lista Blanca para equipos en correcto funcionamiento, la lista Negra para equipos bloqueados y la lista Gris guarda información sobre equipos sospechosos que están siendo monitoreados.

En el sistema 3GPP se encuentra conformada por dos redes de acceso de radio, una de ella es UTRAN para las redes de tercera generación como UMTS y GERAN para redes de segunda generación o 2.5G como GSM/EDGE y para la mayoría de los propósitos GPRS, con la finalidad de proteger el enlace y ofrecer características de seguridad.

1.4.3. Red de acceso radio terrestre (UTRAN)

UTRAN, (UMTS Terrestrial Radio Access Network) es parte de la arquitectura de 3GPP responsable de la administración del recurso de radiofrecuencia, permite intercambio de datos y de señalización entre el equipo usuario (UE) y la red central (CN) de los sistemas 3GPP. Basada en la tecnología de WCDMA para redes UMTS. Se conecta el UE con la red UTRAN mediante la interfaz Uu, encargada de mantener la conectividad y relaciones entre el enlace, control de cifrado de este canal, protección de la integridad del mensaje, entre otras funciones más (Niemi V., Nyberg K., 2003).

1.4.3.1. Elementos de la red UTRAN

La tecnología UTRAN posee varios elementos, como lo son los Nodo B, que son estaciones bases responsables de la transmisión y recepción entre la estación móvil y una

o más celdas de la red UMTS. También tiene la obligación de reportar las mediciones de interferencia en el enlace ascendente y potencia en el enlace descendente. Otro elemento es el RNC (Radio Network Controller), encargado de controlar y administrar los recursos lógicos de radio de uno a varios nodos B, del proceso de handover local y confidencialidad e integridad, como la asignación de códigos de canalización en el enlace descendente y canales comunes. El RNC se conecta con la CN por medio de la interfaz lu, una de las más importantes, ya que tiene dos diferentes instancias para poder conectarse a dos diferentes elementos de la red: lu-CS para conectar el RNC con la MSC, y lu-PS para conectarse con un SGSN (Serving GPRS Support Node), el cual cumple las funciones de MSC/VLR (Mobile Switching Center/ Visitor Location Register), el de autenticación de identidad y requerimientos de movilidad a través de la red por parte del UE para transmitir la solicitud de datos de autenticación al AuC (Centro de Autenticación) de la red base. Ambos elementos (Nodos

B y RNC) forman conjuntamente el RNS (Radio Network Subsystem).

Otras dos interfaces son la interfaz lub, que se encuentra entre el Nodo B y su RNC, y la interfaz lur, que se encuentra entre dos RNS (Fajardo D., 2004)

La arquitectura de la red UTRAN y el funcionamiento son determinados por las características de la nueva tecnología de acceso de radio basada en WCDMA con sus dos modos UTRA/FDD y UTRA/TDD, las mismas que son usadas para el acceso múltiple además de multiplexación frecuencial, y dependiendo de cuál de los dos se use, varía el modo de dividir el espectro de frecuencia.

El modo FDD (Frequency-Division Duplexing) divide el espectro disponible en canales, correspondientes a distintos rangos de frecuencia, dándoles a los distintos usuarios estos canales para realizar sus comunicaciones sin interferirse entre sí. Utiliza diferentes frecuencias portadoras para enlaces ascendentes (MS hacia BS) y

enlaces descendentes (BS hacia MS). Un máximo de dos espectros de 5 MHz de ancho están atribuidas al modo FDD (López J., 2005)

El modo TDD (Time Division Duplex) utiliza la misma frecuencia portadora para el enlace ascendente y el enlace descendente, multiplexada en el tiempo, permitiendo que los canales de enlace ascendente y enlace descendente de datos se encuentren en el mismo espectro frecuencial, brindando al operador mayor flexibilidad a la hora de dividir el espectro disponible en función de su demanda.

Los modos FDD y TDD, se diferencia por la forma de realizar la transmisión dúplex, en TDD se emplea solo una portadora para todos los usuarios y ambos enlaces, pero dividiéndolas en espacios cortos de tiempo temporales para ambos enlaces, a diferencia FDD que utiliza distintas portadoras para el enlace ascendente y el descendente; pero se prevé facilitar el modo dual FDD/TDD, es decir, que soportará ambas operaciones, tanto FDD como TDD.

El modo TDD es muy adecuado para entornos con altas densidades de tráfico como por ejemplo en las ciudades altamente pobladas, cobertura en interiores, y distribuciones de tráfico asimétricas. TDD facilita el uso eficiente del espectro no apareado y compatible con velocidades de datos de hasta 2 Mbps

Aunque el sistema UMTS ofrece diferentes interfaces aéreas terrestres, se usa el modo UMTS-FDD, ensanchamiento directo W-CDMA, o como se lo conoce UTRA-FDD, la variante más popular para teléfonos móviles, que fue descrito en párrafos anteriores.

1.4.4. Equipo de usuario (UE)

Equipo de usuario o móvil, como su nombre lo indica, es el equipo utilizado por el usuario para lograr una comunicación con una estación base para acceder a los servicios UMTS, siempre y cuando exista cobertura de la señal. Además deben soportar los protocolos y el estándar para los que fueron creados; en este caso, este equipo debería ser capaz de acceder a la red UTRAN a través de la tecnología WCDMA para así poder comunicarse con otro móvil. Estos equipos pueden variar de funcionalidad, tamaño y costo.

La UE se compone de dos partes: el Equipo Móvil (ME) y el módulo de identificación del abonado universal (USIM). La ME es un dispositivo que contiene la funcionalidad de radio y los protocolos que necesita para la comunicación con la estación base. Además estos dispositivos cuentan con la interfaz de usuario y además con muchas otras funcionalidades en la actualidad. El USIM está contenido en una tarjeta inteligente, colocada dentro del equipo móvil. El USIM contiene todos los datos que requiere el operador sobre el cliente o abonado (Fajardo D., 2004).

1.4.5. Red Central (Core Network - CN)

El núcleo del sistema UMTS es la Red Central, siendo una red de tercera generación, utiliza el mismo estándar de red principal como GSM/EDGE, lo que permite una migración sencilla para los operadores GSM existente hacia esta nueva tecnología. Sin embargo, la ruta de migración a UMTS es todavía costosa, debido la obtención de nuevas licencias de espectro, superposición de red UMTS en las torres existentes, adquisición de nuevos productos, desarrollo de nuevas investigaciones para la ampliación de la red a

lugares remotos y demás, a pesar de tener como base las tecnologías que le precedieron.

El CN provee una solución para el tráfico y monitoreo ente redes, medición del flujo de tráfico, control de congestión, una forma en que se descubre la capacidad disponible de la red para una ruta en particular. Se encuentra dividido en un dominio de servicios de conmutación de paquetes PS y conmutación de circuitos CS, implementando uno de los dominios o ambos dominios en los terminales. También realiza transporte de información, tanto de tráfico como de señalización, siendo el cerebro del sistema, puede conectarse a otras redes de comunicaciones como VLR, HLR, Auc, entre otros (López J., 2005).

La Red Central está formada de varios elementos como el MSC (Mobile Services Switching Center), parte fundamental de una red de conmutación de circuitos, éste es usado tanto por el sistema GSM como UMTS, por lo que se pueden interconectar entre ellos por sus diferentes interfaces, gracias al grupo 3GPP que lo hizo posible. El MSC es el encargado de la organización de las llamadas de todos los móviles que se encuentran en su jurisdicción, registro de ubicación, puede operar con otro tipo de redes, administración

del proceso de handover entre sistemas, manejo de los parámetros para la encriptación de los mensajes que pasan a través de ella.

Otro elemento es la SGSN (Serving GPRS Support Node), parte importante de una red basada en conmutación de paquetes. Una de sus funciones es de tener información sobre el IMSI, información de suscripción, información de ubicación, la celda o área en el que el móvil se encuentra registrado, su número VLR, entre otros más, pero éstos son los más significativos.

También hay un GMSC (Gateway Mobile Services Switching Center), es el encargado de encaminar las llamadas fuera de la red móvil; es decir, si algún abonado móvil desea hacer una llamada a alguien fuera de dicha red, ésta petición es enrutada a través del GMSC, así también es para recepciones de llamadas fuera de la red móvil y encaminarlas al apropiado MSC. Otro elemento similar es el GGSN (Gateway GPRS Support Node), responsable de la interconexión entre la red GPRS y redes de paquetes conmutados externas como lo es Internet. Al recibir datos de un usuario específico y revisarlo en su registro de usuarios móviles activos para comprobar si se encuentra activo, reenvía los datos al SGSN que envía al usuario móvil; caso contrario, si no se encuentra activo, los

paquetes son descartados. Otros elementos del CN son HLR, VLR, entre otros similares que se los revisarán en el siguiente capítulo (Fajardo D., 2004).

CAPÍTULO 2

EVOLUCIÓN DE LA SEGURIDAD EN REDES UMTS.

Con la aparición de las redes móviles de tercera generación (3G) se mejoró la multiplexación del espectro desde TDMA a WCDMA, parecido a la técnica CDMA, en la cual los usuarios transmiten en el mismo instante por lo que comparten el mismo ancho de banda, pero se les asigna un código de extendido (spreading codes) para luego poder identificarlos. Una característica de WCDMA usa la técnica de DS-CDMA (Direct Sequence CDMA) que consiste en rechazar las interferencias de banda ancha que se superponen entre ellas con las propiedades de los códigos secuenciales previo a la modulación, debido a que se puede llegar a transmitir al mismo tiempo y frecuencia causando una interferencia mutua (Moshavi Sh., 1996).

Sin embargo, aparte de la accesibilidad al medio, los operadores también necesitan asegurar que la red esté en correcto funcionamiento, teniendo el control de sus funciones por medio de mensajes de control, los cuales son creados por los mismos elementos de la red, y de la comprobación del mismo, para de esta forma asegurar la integridad ante cualquier manipulación externa de dichos mensajes. Pero no solo los operadores son parte de este proceso, los usuarios también desean que sus datos transmitidos a través de la red sean confidenciales, además de conocer los mecanismos de confidencialidad usados para ello, por lo que dichos temas deberían ser relevantes cuando se habla de confidencialidad e integridad dentro de la red.

La red UMTS fue desarrollado a partir de la red GSM, por lo que es indispensable saber el modo que funciona dicha red y el tipo de seguridad que utiliza. Sus interfaces de radio pueden ser diferentes pero algunos sistemas y terminales aún tienen compatibilidades entre sí lo que garantiza interoperabilidad entre sus predecesores 2G como lo es GSM con los sistemas 3G como UMTS, lo que permite interactuar entre las dos plataformas.

2.1. Arquitectura de la red GSM

GSM es un sistema que da servicios de voz de alta calidad, es un estándar de la generación 2G que permite el servicio de transmisión de paquetes a una velocidad de transferencia de 9,6 Kbps (conmutación por circuitos), el

problema con esta red es que se tenía un canal de comunicación asignado la cual permanecía ocupado todo el tiempo; por lo que surgió el servicio GPRS, en el que los paquetes son fragmentados y enviados de esta forma a través de la red teniendo varios canales asignados. Es utilizado para envíos de mensajes cortos (SMS), multimedia (MMS), servicio de acceso a internet y demás. La tecnología GPRS es parte de la comúnmente llamada de generación 2.5G (es la suma de 2G más GPRS y EDGE) ya que es un enlace para la transición hacia la tecnología 3G como es la red UMTS (Lara J., 2006).

Este tipo de red se tiene la siguiente arquitectura:

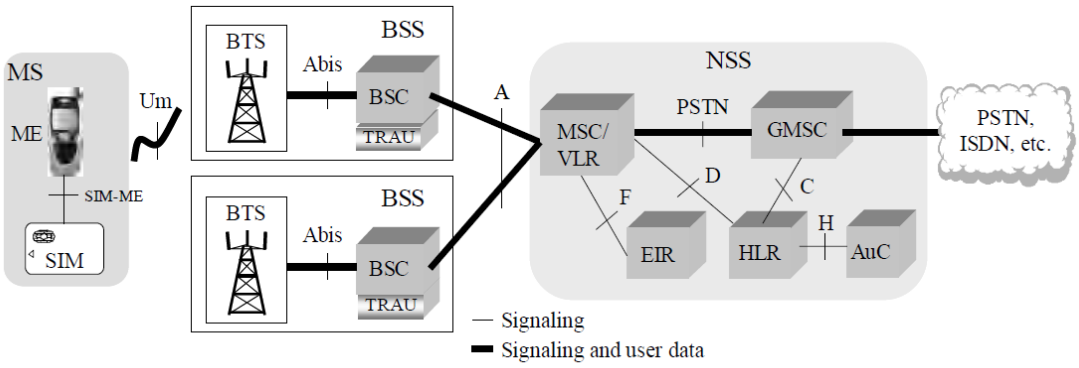


Figura 2.1: Arquitectura de la Red GSM, 2.5G (GPRS + EDGE).

Fuente: (Sanchez J., Thioune M., 2007)

- MS (Mobile Station) o Estación Móvil, que como su nombre lo indica es el equipo terminal, pero también se le puede llamar de esa manera a la tarjeta SIM.
- BTS (Base Transceiver Station o Base Station), son llamados los equipos emisores y transmisores de señales de radio (antenas) que se encuentran en el centro de su celda que es su área de cobertura. Las BTS asumen funciones de capa 1 (Física) entre las comunicaciones entre la MS y la red como codificación del canal, cifrado, generación de ráfagas (burst) entre otras más. Mientras mayor es su densidad de abonados enganchados a ella, menor será el ancho de banda disponible para cada uno de ellos; por lo que en zonas urbanas se encuentran algunas estaciones bases a unos cientos de metros entre sí comparadas con las zonas rurales que pueden cubrir kilómetros.
- BSC (Base Station Controller), encargado del control de varias BS como una central de conmutación de circuitos, además de la gestión de los procesos regulación, de transferencia o traspaso de una BS a otra contigua, denominado handover en inglés.

  En el sistema GSM el tipo de transferencia predominante es el “hard handover”, mientras la MS está en movimiento de una BTS a otra, la conexión inicial termina y su enlace se interrumpe hasta que se conecta a la

siguiente y restablece la comunicación con la BTS siguiente; de este modo solo se utiliza un solo canal de comunicación, lo que lo hace más barato y de fácil implementación con respecto a otro mecanismo que es el “soft handover”, que a diferencia del anterior, ésta mantiene su conexión inicial mientras establece conexión con la nueva BTS ofreciendo continuidad de los servicios pero consumiendo mayor recursos; liberándola después de haber establecido dicha conexión. Aunque es poco utilizada, en WCDMA se usa mayormente este mecanismo.

- BSS (Base Station Subsystem), incluye a dos elementos de la red descritos anteriormente, los BTS y BSC. Los cuales permiten conexión sin cables desde las estaciones móviles a la red por interfaz aire.
- NSS (Network and Switching Subsystem), contiene una o más HLR con su Centro de Autenticación (AuC). Además de contener las bases de datos necesarias para la conmutación de llamadas o conexión MSC conectados al VLR que se describen a continuación:
  - MSC, su función es de conmutar entre BSC y BS dentro de la red, además de gestionar llamadas entre MS. Usualmente se encuentra asociado a un VLR con la finalidad de tomar en cuenta los datos de los usuarios móviles que están en el área que controla el MSC, contenida esta información en una base de datos de los usuarios.

- GMSC (Gateway Mobile Services Switching Center), interconecta dos redes diferentes haciendo que sus protocolos de comunicación se entiendan entre sí, con el fin de garantizar la funcionalidad con redes externas como PSTN, ISDN, entre otras.
- HLR (Home Location Register), es una base de datos estática que contiene información de los subscriptores como las características del servicio que posee dentro de la red e información en cuanto a qué área VLR se encuentra registrado.
- VLR, a diferencia del anterior guarda información temporal de algún usuario mientras esté dentro de la MSC y por ende, usa datos de la HLR de la zona del abonado.
- AuC, es parte fundamental del HLR, se encarga de la autenticidad de los usuarios con sus respectivos resultados (SRES), así como sus claves de cifrado (Kc) de los algoritmos A3 y A8 de los números aleatorios (RAND) generados, además de su clave individual (Ki) almacenado en el HLR.
- EIR (Equipment Identity Register), tiene un registro en una base de datos de los equipos válidos, es decir que no hayan sido robados o sufran daños, y por medio de su IMEI se le permite o deniega el uso de la red. (Sagkob H., 2003)

La tecnología GPRS implementada en la red 2G permite la transmisión de paquetes de datos a una velocidad mayor que la de GSM (de casi 114 Kbps) por intervalos de tiempo, siendo un servicio de conexión permanentemente activa, es decir que no hace uso de recursos de la red mientras no se esté recibiendo ni transmitiendo datos, el cual permite transmisión de datos de una forma más eficiente y menos costosa.

2.2. Seguridad en Red GSM

En el sistema GSM hubo varios ataques activos en contra de la red, con el uso de equipos necesarios para suplantar a un elemento de red (NE), que en varias ocasiones, puede ser un terminal de usuario legítimo que fácilmente puede entrar en los procesos de autentificación mutua entre el usuario y la red. En este ataque al proceso de autentificación de la red entran tres componentes: la red base, la red receptora y el USIM o equipo terminal, compuesto de una tarjeta inteligente. El proceso de comprobación de identidad, de desafío y respuesta, el cual el equipo terminal verifica si la red servidora tiene la autenticación de la red para poder seguir con la comunicación; sin embargo, esto no es suficiente para evitar que algún intruso pueda colarse en la comunicación y tratar de obtener algún beneficio real, por lo que es de suma importancia de hacer uso de otros mecanismos de seguridad que eviten esta molestia.

En la materia de seguridad, GSM también ha ido mejorando pero las estructuras básicas permanecen iguales. Las características principales en el sistema GSM son:

- Autenticación de la identidad del usuario
- Cifrado de la comunicación de radio enlace
- Confidencialidad de los datos de usuario y de señalización
- Uso de identidades temporales

El usuario se identifica por medio del IMSI (International Mobile Subscriber Identity), un código de identificación único para cada dispositivo móvil que se encuentra dentro de la tarjeta SIM (Subscriber Identity Module), el cual está formado por tres campos:

- MCC (Mobile Country Code) o código del país de 3 dígitos
- MNC (Mobile Network Code) o código de la red móvil de 2 ó 3 dígitos, dependiendo del país
- MSIN (Mobile Suscriber Identification Number) o número que contiene la identificación de la estación móvil de 10 dígitos como máximo (Lara J., 2006, págs. 92, 93).

Junto con el IMSI hay una clave de identificación individual para cada usuario Ki que son guardadas en la tarjeta SIM y en el AuC, y es autenticada por el usuario mediante “desafíos”.

Una cadena de 128 bits aleatoria es enviado al móvil, la cual es transferida a la tarjeta SIM donde hay un algoritmo de cifrado A3 que permite cifrar los datos y realizar la autenticación del usuario, tomando los datos de la cadena de bits y la clave Ki; con estos datos realiza la comprobación botando un valor de respuesta SRES de 32 bits (respuesta firmada), si es correcta abre el camino para la comunicación, si este no es el caso se cierra la comunicación y se genera un mensaje de fallo en la autenticación (Niemi V., Nyberg K., 2003).

Con los mismos parámetros usados en el cifrado A3, usa una clave unidireccional A8 utilizado para el cifrado de llamadas telefónicas con ayuda del algoritmo A5, dicho algoritmo inicia con una petición del modo de cifrado que se utilizará en el proceso, mismo que da una clave de sesión de salida temporal Kc de 64 bits para cifrar datos entre la estación móvil y la estación base. Con los tres parámetros generados (Kc, SRES y la cadena de bits) puede manejar la seguridad. Son enviados al elemento de red de servicio MSC/VLR o SGSN ya codificados, obteniendo un sistema más robusto contra posibles escuchas ilegales en el enlace.

No hay que olvidar que el cálculo de Kc se lo realiza internamente en la tarjeta SIM y no se lo envía a través de la red, por lo tanto, estos tipos de claves no las revela aumentando la seguridad en el equipo (Niemi V., Nyberg K., 2003).

Los algoritmos A3 y A8 al tener características similares en su funcionalidad, como autenticación en dichas interfaces al visitar redes GSM, se implementan como único algoritmo en lugar del algoritmo COMP128, el que se lo describirá en capítulos más adelante.

2.2.1. Algoritmo de cifrado A5

El algoritmo de cifrado A5 es el que permite cifrar las llamadas (datos de voz) que se estén realizando entre el móvil y las BTS para enviarlos a través de la red de forma segura hasta que ocurra la próxima autenticación usando una secuencia pseudoaleatoria. Toma un contador de 22 bits y una clave Kc de 64 bits, la cual produce dos bloques keystream (flujo de claves) de 114 bits cada una para enlace de subida y de bajada. El proceso se lo observa en la figura 2.2.

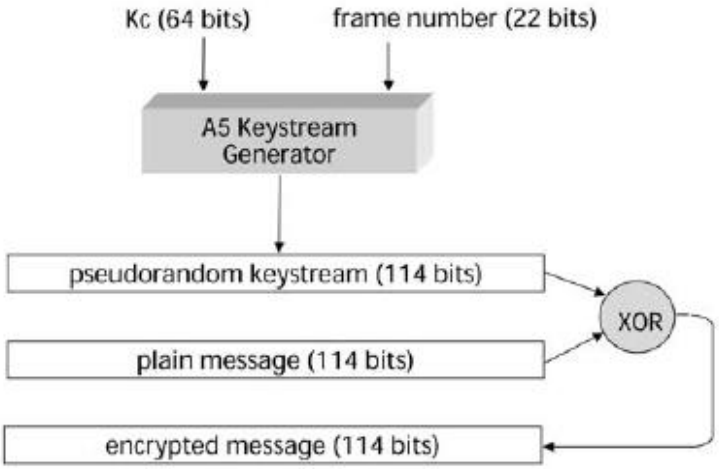


Figura 2.2: Estructura de un cifrado A5 (seguridad GSM)

Fuente: (Niemi V., Nyberg K., 2003, pág. 10)

El generador de claves A5 tiene tres tipos de variantes del algoritmo: A5/1, A5/2 y A5/3.

El primero, el algoritmo A5/1 genera una clave de 64 bits (aunque en general son 54 bits ya que 10 bits siempre son cero) el cual permite cifrar las tramas enviadas entre el terminal y operador mediante la clave de sesión Kc, generado por el algoritmo A8 descrito anteriormente, pero con el pasar del tiempo se ha podido descubrir su clave de una manera “sencilla”: Se intercepta la comunicación cifrada, además de su clave, y se la compara en una base de datos donde se encuentra almacenada todas las posibles combinaciones; una vez encontrado el patrón se puede obtener su clave de cifrado y

por ende descifrar la conversación “en el aire” en tiempo real. Este cifrado de flujo compuesto de tres LFSRs (Linear Feedback Shift Registers) o Registros de Desplazamiento Lineal de Retroalimentación, los registros (R1, R2, R3) de 19, 22 y 23 bits respectivamente, están sincronizados e inicializados en 0; un bit de cada registro determina la sincronización y en cada paso en el que los registros de los cuales los bits se encuentran sincronizados son desplazados.

El segundo, el algoritmo A5/2, es más sencillo que el algoritmo A5/1, no se usa mucho y su cifrado es similar al anterior al igual que su descifrado en tiempo real (Niemi V., Nyberg K., 2003).

El tercero, el algoritmo A5/3, más robusto que sus predecesores, definido en términos de KGCORE es basado en el cifrado de bloques KASUMI (tamaño de bloques de 64 bits) y no en flujo como los anteriores, el cual produce dos cadenas “keystream”, uno para el cifrado y descifrado de enlace de subida y el otro para enlace de bajada. Este algoritmo permite mejoras futuras al estar basado en KASUMI (3G) como el soporte de claves Kc más largas (tamaño de clave de 128 bits) con la finalidad de asegurar la confidencialidad e integridad de la misma (Sankaliya A., Mishra V., Mandloi A., 2011).

El diseño de KASUMI es basado en el algoritmo MISTY, debido a sus características en el tema de seguridad contra varios tipos de ataques e implementación de hardware sencilla. Sin embargo el equipo de diseño de 3GPP consideraba que se necesitaba mejorar su velocidad en los procesos y sea amigable, implementando de ella los algoritmos f8 y f9.

2.3. Tipos de seguridad adicionales usados en redes GSM

Otros tipos de seguridad utilizados en sistemas GSM para la identificación de los equipos móviles, es mediante el IMEI, código no asociado con el usuario o tarjeta SIM, debido a que puede ser puesto en otro terminal móvil diferente.

El IMEI consta de 15 o 17 números que permiten el bloqueo del terminal móvil en caso de hurto y se lo puede solicitar a la operadora en dónde se haya comprado el equipo o por medio de mensajes de texto. Dicha característica puede ser transferida a otras tecnologías, como en redes UMTS y solo puede ser usado en el lado del terminal móvil (Lara J., 2006, pág. 93).

Otro sistema de seguridad GSM es el PIN (Personal Identification Number), medida de prevención en contra del fraude en el servicio telefónico móvil,

conocido únicamente por el usuario y el USIM, de 4 a 8 números de longitud, cuya función es de no permitir el acceso no autorizado a los servicios del móvil como la tarjeta SIM, contactos, al igual al equipo donde se encuentra y se lo habilita cuando no se lo esté usando; sin embargo en el momento de un robo, éste sistema no asegura la confidencialidad de la información debido a que su autenticación ya había sido establecida con anterioridad y el teléfono móvil se encuentra en pleno funcionamiento (Lara J., 2006).

2.4. Arquitectura IMS para asegurar el acceso

Una parte importante del grupo de trabajo 3GPP se encuentra enfocado a la especificación de la IP Multimedia CN Subsystem (IMS). Es un sistema de la capa de aplicación que utiliza PS de dominio, pero está diseñado de tal manera que es independiente de la tecnología de acceso subyacentes como son las redes UTRAN y GERAN, bases para las redes UMTS y empezar a utilizar diversos servicios multimedia mediante IP (Heras D., Pauta H., 2011).

El proyecto 3GPP diseñó este subsistema con independencia de acceso al medio de forma transparente en una red estructurada para soportar tráfico IP llamada IMS, diseñado para una red evolucionada de GSM, de tercera generación.

IMS es una plataforma que permite conectividad sobre infraestructura IP entre los dispositivos que posean una dirección IP única, compatible con IPv6, ya que no tiene escasez de direcciones como es el caso de IPv4. Además de soportar tráfico de voz y datos, como es el caso de GSM, también permite voz sobre IP (voIP), servicios multimedia avanzadas para todo terminal ya sea móvil o fijo que se pueda conectar a la red con alguna dirección IP, y mantenimiento de las sesiones sin importar que haya cambio de red u operadora.

Debido a que es un sistema de la capa de Aplicación para redes que utilicen conmutación por paquetes, como el caso de UMTS, el flujo de datos de control de los sistemas de señalización y los datos multimedia del usuario viajan de forma separadas, usando a GPRS 3G como vía de comunicación dentro del dominio de la red móvil.

La arquitectura IMS es basado en SIP (Session Initation Protocol) desarrollado por IETF, la cual brinda iniciación, mantenimiento, registro y culminación de sesiones IMS, además de especificar la ubicación de sus usuarios conectados. Para proteger la integridad de estos servicios, se usa el protocolo SPD (Session Description Protocol) de IPsec (en especial los mensajes INVITE utilizados para establecer sesiones) entre los extremos

para decidir qué tipos de formatos multimedia entrarán en la sesión como se observa en la figura 2.3.

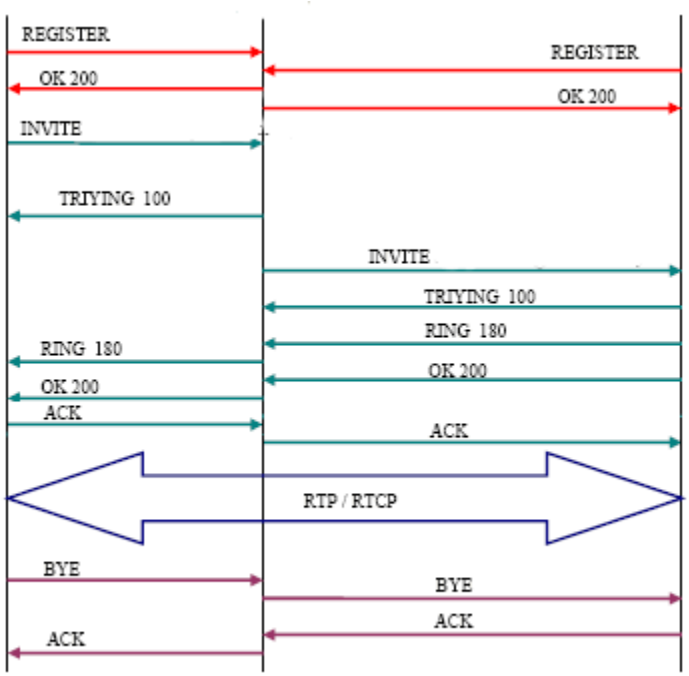


Figura 2.3: Autenticación SIP

Fuente: (Ing. en Telecomunicaciones especializado en Voip, 2011)

Un usuario o Agente de Usuario (UA) inicia la sesión por medio de la petición INVITE, el agente SIP, intermediario de dichas peticiones, ayuda a autenticar los mensajes SIP e intercambiar datos multimedia entre los extremos, así como también enviar peticiones de REGISTER a un servidor de registro SIP, el cual guarda información relacionada con el usuario y su sesión con la finalidad de que otros usuarios lo puedan encontrar, o si ya no

quiere ser encontrado puede borrar su registro. El usuario destino acepta la invitación con el mensaje OK para establecer la llamada e intercambio de datos de voz en tiempo real mediante el protocolo para el transporte de datos RTP (Real-time Transport Protocol) y al terminar el intercambio o la sesión, cualquiera de los usuarios puede enviar el mensaje de BYE. Pero no solo hay estas peticiones, igualmente hay la petición OPTION para conocer las opciones del usuario que establece la sesión sin inicialarla previamente, ACK y CANCEL para confirmar y denegar dichas sesiones respectivamente (Niemi V., Nyberg K., 2003, pág. 87).

2.4.1. Seguridad en IMS

En el tema de seguridad, IMS está edificado sobre el dominio de Conmutación por paquetes (PS), con características de seguridad en redes UMTS como autenticación mutua de acuerdo, protección de integridad, autenticación de cada mensaje SIP mediante distintos mecanismos de seguridad y cifrado entre los terminales del usuario; estas características se ilustran en la figura 2.4.

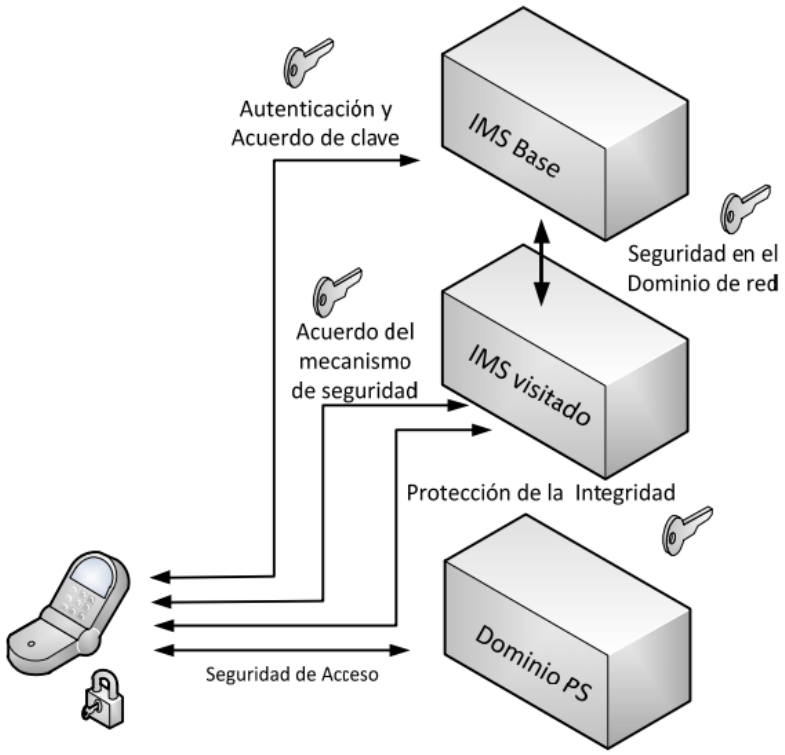


Figura 2.4: Características de Seguridad IMS

Fuente: (Heras D., Pauta H., 2011, pág. 62)

En la arquitectura IMS los elementos principales son los CSCF (Call Session Control Functions), entidades con diversas funciones dentro del subsistema SIP para que el usuario pueda acceder a los servicios IP multimedia. Cuando un usuario desea iniciar el intercambio de datos multimedia con otro, éste envía mensajes de INVITE para el inicio de la sesión como se puede simplificar en la figura 2.5:

El primer nodo de entrada al subsistema IMS desde UE es el Proxy CSCF (P-CSCF) por lo que todo el tráfico da señalización SIP pasa por él. La comunicación se inicia a través de la petición REGISTER para el registro, ésta solicitud es enviada a un nodo intermedio para soportar la operación, Interrogating CSCF (I-CSCF) o interrogante, que determina el siguiente salto de los mensajes SIP (enrutamiento de las peticiones) para realizar la señalización y con ayuda del HSS (Home Subscriber Server), similar al HLR de redes GSM, base de datos significante de IMS que registra la identidad del usuario, parámetros de acceso, así como su clave de seguridad, para poder asignarle un S-CSCF de acuerdo a lo recibido del HSS que entran al servidor (Heras D., Pauta H., 2011).

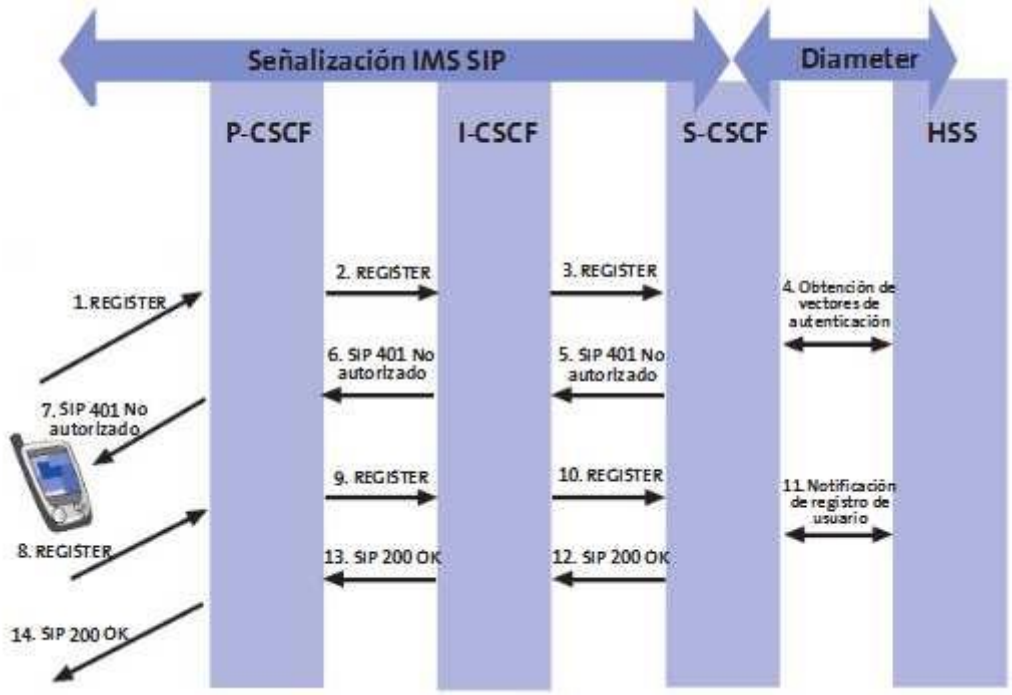


Figura 2.5: Inicio del intercambio multimedia

Fuente: (WordPress, 2012)

El Serving CSCF (S-CSCF) o servidor, que además de enrutar y mantener las sesiones del usuario inicial (UE) lo registra y autentica para determinar que no sea un usuario ya registrado. Para verificar las identidades públicas asignadas, se utiliza el algoritmo de desafío IMS AKA (IMS Authentication and Key Agreement). Una vez que el abonado ha sido verificado y registrado se envía el mensaje OK al UE con el que puede acceder a los servicios IP multimedia que da IMS como videoconferencias entre usuarios IMS de la misma red o distinta, o en este caso particular, tiene el significado de que el

usuario invitado se ha decidido por aceptar el intercambio de datos multimedia, y el usuario que inicio la sesión envía en respuesta un mensaje ACK de respuesta. Al final si desean terminar la sesión se puede enviar peticiones de BYE para su clausura o CANCEL si quieren parar el intercambio de información, y finaliza con la respuesta del destinatario con un mensaje OK. (Niemi V., Nyberg K., 2003, pág. 88).

AKA es un mecanismo de autenticación basado en desafío y respuesta para redes GSM como UMTS, el usuario llega a un acuerdo con el operador de IMS para asignarle a éste una identidad privada de IMS (IMSI) que se almacena en el HSS. Para que el subscriptor pueda usar los servicios IMS y tener una comunicación segura, se encuentran protegida este canal con métodos de seguridad de dominio de red: como se describió anteriormente, después de seleccionar una ruta con ayuda del S-CSF, se envía la petición de REGISTER, toma los vectores de autenticación del HSS, de similar formato que los usados en autenticación de dominios PS y CS, para enviarlo al proxy de CSCF, el cual extrae la clave Ik y envía el equipo usuario los parámetros restantes (RAND y AUTN). Ya en el extremo, en el UE, se comprueba la validez del AUTN para

luego calcular los parámetros Ik y RES. Éste último se le agrega a la nueva solicitud REGISTER para seguir con el proceso de autenticación en el S-CSCF, donde se compara el parámetro RES con el XRES, y si es exitoso se envía un mensaje OK hasta el UE (Heras D., Pauta H., 2011).

De manera general, AKA divide los servicios de autenticación y encriptación en dos fases: La primera es la Generación del Vector de Autenticación, que consiste en un número aleatorio RAND, respuesta esperada XRES, las claves de cifrado Ck y de integridad Ik, generados por el AuC para ser enviado al MSC.

La segunda fase es de Autenticación y Acuerdo de claves, en la que cada extremo hace correr el algoritmo de autenticación y así calcular una respuesta, que es enviada desde el terminal móvil al nodo de autenticación para su comparación. En el caso que se encuentre una igualdad o sean compatibles, dicho terminal es autenticado.

Las redes GSM avanzadas y UMTS utilizan este mecanismo secreto para la autenticación conocido como Autenticación y acuerdo de claves (AKA), llevada a cabo en el módulo USIM. Con la diferencia

que en redes GSM se utiliza AKA para la autenticación del terminal móvil a la red; en cambio, en redes UMTS usas el método de autenticación mutua para proveer seguridad de BS falsas, que son BS que transmiten en un espectro licenciado, sin embargo no pertenecen ni son operados por algún operador móvil (Heras D., Pauta H., 2011).

2.4.2. MAPsec

En el tema de seguridad, en el caso de las redes SS7, utilizan un mecanismo llamado MAPsec, desarrollado por el protocolo MAP (Mobile Application Part), que da integridad y confidencialidad. Este protocolo es utilizado como medio de señalización dentro del CN y está siendo usado en la actualidad en las redes GSM de segunda generación (2G) para brindar seguridad a los mensajes MAP que viajan en la red en la capa de Aplicación para nodos núcleos tanto GSM, UMTS como GPRS brindado servicios móviles integrados seguros. MAP controla los mensajes enviados entre los MSC o Nodo de Soporte GPRS (SGSN) para elementos de tercera generación, y las bases de datos (HLR, VLR, EIR) como apoyo para la autenticación del abonado dentro del centro de Autenticación AuC

como solicitudes de registro de ubicación del visitante, del usuario local, su perfil e información de control o señalización.

Los pasos para la protección de los datos es: Primero se envía un mensaje MAPsec, un mensaje MAP en texto plano que es encriptado, al que también se le incluye un código de autenticación de mensajes (MAC), para ser introducido en un nuevo mensaje MAP. Si el mensaje enviado al elemento de red asociado soporta dicho mensaje, se envía un mensaje de respuesta MAPsec al origen. De no ser este el caso, se retorna un mensaje MAP que indica que el mensaje MAPsec enviado no es reconocido por el destino (Niemi V., 2005).

Los KAC (Key Administration Centre) son los encargados en la negociación de las Asociaciones de Seguridad (SA) de MAPsec (SA fueron creadas inicialmente para IPsec) como claves de cifrado para los mensajes que viajan a través de la red, y de verificar cúal elemento de red tiene la capacidad de soportar MAPsec o no. La información es ingresada en una base de datos de Medidas de Seguridad por medio de SPD, que indica que tipo de mensajes se intercambian (MAPsec o MAP)

La desventaja de un elemento de red no soporte MAPsec es que enviará sus mensajes MAP sin encriptación y añadirá retrasos de dos ciclos del proceso, lo que lleva a cargas adicionales en los procesos de la red de señalización, retrasos en sus operaciones como gestión de llamadas, entre otras. Sin embargo se necesita de un periodo de transición para que todos los elementos de la red soporten MAPsec, mientras tanto se necesita que éste mecanismo pueda comunicarse con elementos que no usan MAPsec.

En este mecanismo existen tres maneras de protección:

- Modo 0, sin protección. El encabezado de seguridad se envía sin cifrar y el mensaje MAP.
- Modo 1, solo protección de integridad, es decir autenticación de mensajes. Aquí se coloca en el encabezado la MAC y el mensaje MAP protegido realizando un cálculo y el resultado se lo coloca en un mensaje MAPsec.
- Modo 2, protección de integridad y confidencialidad de la información o cifrado. Aquí en cambio se coloca el resultado del cálculo la MAC en el encabezado de seguridad y el mensaje MAP cifrado (Niemi V., Nyberg K., 2003).

2.4.3. IPsec

En redes UMTS se utiliza el protocolo IPsec (Protocolo de Seguridad IP), utilizado en la arquitectura 3GPP que brinda integridad y confidencialidad a los datos en las transmisiones de red, similar al protocolo descrito anteriormente, con la diferencia que IPsec es dirigida a las comunicaciones sobre el protocolo de Internet IP, ofreciendo autenticación en las comunicaciones (inicio y al final de sesiones), prevención de ataques de reproducción, confidencialidad e integridad del tráfico IP en flujo de paquetes, rechazando el tráfico alterado. IPsec actúa en la capa de red (capa 3 del modelo OSI) en adelante; es decir, protege protocolos de capa superior como TCP y UDP sin alterar su código.

Estandarizado por la IETF, grupo de trabajo para el desarrollo e ingeniería de protocolos de internet, mediante la creación de documentos técnicos usados para el diseño y gestión de la Internet, documentos llamados RFCs (Request for Comments) o propuestas de libre acceso (RFCs 2401–2412). IPsec da protección a los paquetes IP (Niemi V., Nyberg K., 2003, pág. 81).

Sus componentes fundamentales son:

- Protocolos de seguridad: Encabezado de Autenticación (AH) y Encapsulation Security Payload (ESP).
- Clave de Internet Exchange (IKE) para establecer una Asociación de Seguridad (usado también en MAPsec por su independencia de negociación)
- Algoritmos para autenticación y cifrado
- Asociaciones de Seguridad (SA) permite conexión de los servicios de seguridad para el tráfico entre dichos servicios.

Estos protocolos: AH protege la integridad de los paquetes IP autenticando la cabecera IP del mismo por medio de claves para el cifrado y autenticación en una sola dirección, habiendo un par de AH para asegurar el flujo bidireccional; en cambio ESP es el encargado de la confidencialidad de los paquetes IP y la protección de su integridad, es decir, autenticación de los mensajes por medio del protocolo ESP; y el protocolo IKE Internet Key Exchange negocia en modo seguro para que se puedan utilizar ESP y AH con el fin de intercambiar claves secretas sobre un canal ya sea fiable o no para obtener una comunicación segura. Debido a que entre los dos protocolos de autenticación (AH y ESP) tienen similares funciones (con unas pequeñas diferencias) y se superponen entre sí, seria

redundante hablar de los dos, por eso se explica sobre el funcionamiento de ESP con más detalle.

Existen dos modos de funcionamiento de ESP que se detallan a continuación:

El ESP de modo de Transporte, se cifra toda la porción de dato del paquete IP encapsulado con excepción de la cabecera, añadiendo una nueva cabecera ESP entre la cabecera IP no cifrada y la parte cifrada; se calcula la MAC de toda la información excluyendo a la cabecera IP y se lo agrega al final del paquete. Sin embargo cuando se utiliza la cabecera de autenticación AH las direcciones IP no pueden ser traducidas permaneciendo el enrutamiento intacto. Todo el proceso se lo realiza con el fin de que en el otro extremo puedan llegar dichos paquetes IP sin haber sido alterado en el camino. Para confirmar lo dicho se elimina la cabecera IP y la MAC del final, se le ejecuta un algoritmo utilizando la clave que se encuentra en la cabecera ESP y el resultado se lo compara con la MAC del paquete, si el resultado es positivo se elimina la cabecera ESP y se descifra la parte que resta del paquete. Este tipo de comunicaciones se lo realiza cuando es entre dos puntos finales (point to point). Para aplicarla en redes 3GPP y comunicar dos elementos de red, es

necesario saber las direcciones IP de cada uno y añadir la función de IPsec.

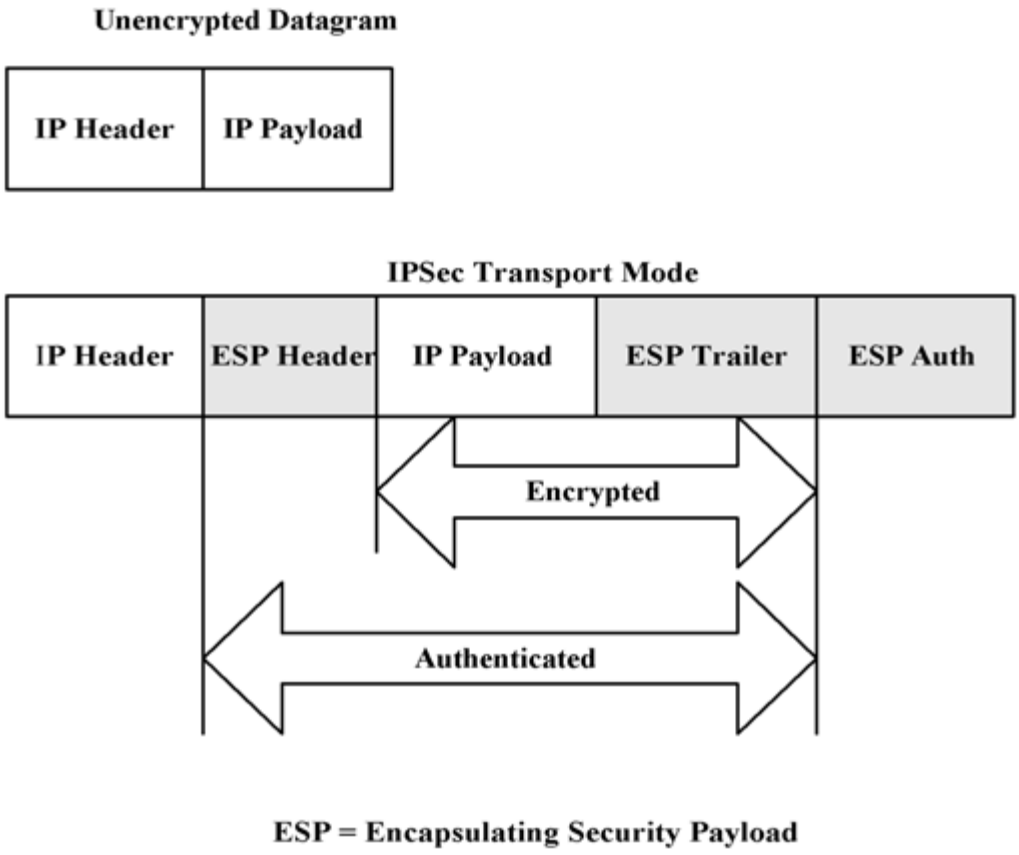


Figura 2.6: Modo transporte ESP de IPsec

Fuente: (Kozierok C., 2004)

El otro tipo de ESP es en modo Túneles, en el que es cifrado completamente el datagrama IP (incluyendo las cabeceras del mensaje) ocultando su tamaño y características externas del tráfico. El procedimiento es similar al modo de transporte, pero con la

diferencia de que la cabecera ESP se la agrega al comienzo para proteger a la cabecera IP original. Este modo es usado para comunicaciones entre dos nodos intermedios, es decir, redes remotas que se encuentran en un canal inseguro (tunneling entre routers, VPN), entre la red y un ordenador o lo contrario, así otorgando implícitamente protección extremo a extremo ya que todo el paquete se encuentra dentro del enlace que está protegida entre las gateways. Por esto es el método preferido en redes UMTS para los mensajes de control del CN entre puertas de enlace de seguridad (Sava R., 2013).

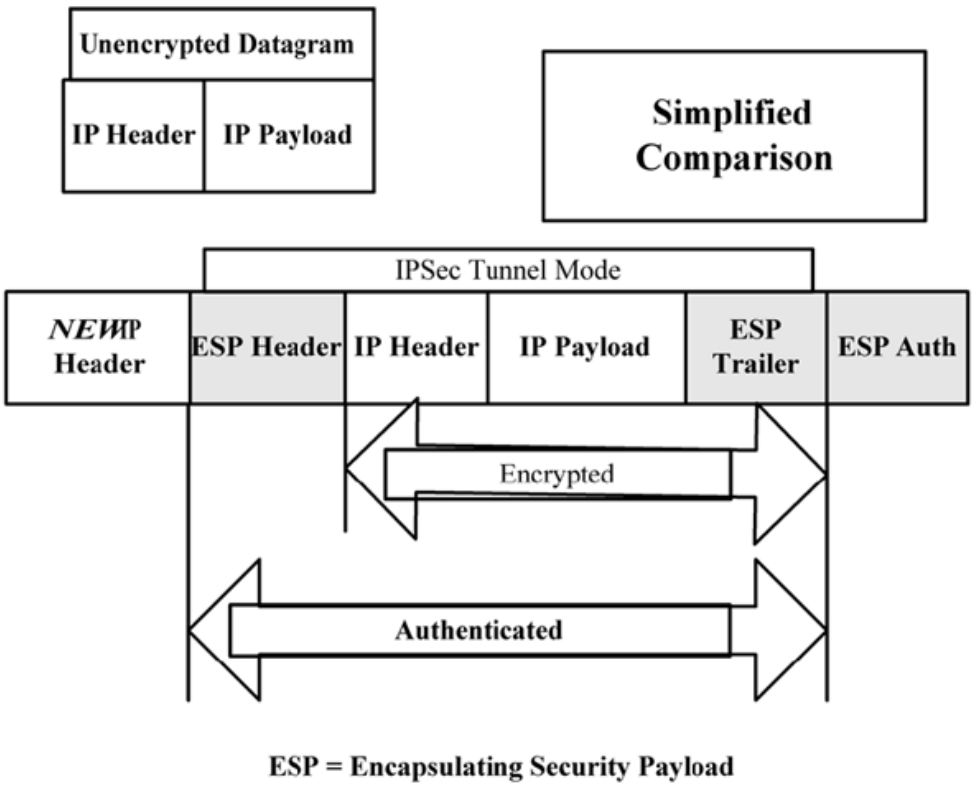


Figura 2.7: Modo túnel ESP de IPsec

Fuente: (Kozierok C., 2004)

IPsec fue diseñado para ofrecer seguridad en las plataformas IPv4 (mecanismo opcional) así como IPv6 (obligatorio), los servicios que incluye son: autenticación de parte del origen de los datos por medio de seguridad en gateways, control de acceso al medio, integridad durante la conexión o fuera de ella, confidencialidad como cifrado del flujo de tráfico, protección contra duplicaciones, entre otras más;

y pueden ser usados por cualquier protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, etc.

Otra componente fundamental para IPsec son las SA, ya que contiene, de manera general, tanto información sobre el algoritmo usado como el tiempo de vida (lifetime) de sus claves de autenticación, hasta un número de secuencia para la protección de ataques de reproducción.

Los dos protocolos descritos anteriormente (AH y ESP) ofrecen seguridad en el tráfico con ayuda de clave criptográfica IKE para los procedimientos de gestión y protocolos; aunque AH provee integridad y ESP provee confidencialidad e integridad para el tráfico, se puede usar una de ellas o ambas para obtener redundancia ya que se superponen. Sin olvidar que estos dos protocolos hacen uso de Asociaciones de Seguridad, que deben realizarse antes de usar los protocolos AH y ESP para asegurar una comunicación segura (por medio de IKE) entre los dos puntos, factor muy importante debido a que contiene información sensible como el algoritmo utilizado, vida útil de las claves, hasta un número de secuencia usado como protección contra ataques de repetición o duplicación de identidad.

El protocolo AH se puede usar cuando no se necesita de confidencialidad o uso de cifrado por alguna restricción dada y únicamente se necesita asegurar la integridad (sin conexión) de los datos del receptor para ayudar a contrarrestar los ataques de denegación de servicios (anti-replay). Otra función del protocolo es el de proteger los campos (autenticación) que tiene la cabecera de un datagrama IP que no sufren cambios en el camino.

En cambio, el protocolo ESP, además de ofrecer integridad como AH, ofrece confidencialidad o encriptación de una parte del paquete IP, pero no significa que su seguridad sea más débil, sino que brinda beneficios importantes con respecto a los intrusos que deseen leer lo que hay dentro del paquete (Boman K., Horn G., Howard P., Niemi V., 2002).

CAPÍTULO 3

CRIPTOGRAFÍA Y ALGORITMOS CRIPTOGRÁFICOS.

En la actualidad, es importante la privacidad de la ubicación del usuario cuando se usa o se tiene el teléfono móvil consigo, ya que si el seguimiento de su ubicación fuera continuo y dinámico se podría convertir en una oportunidad de rastreo, permitiendo a un uso ilegal de dicha información para fines maliciosos como delincuencia y atracos; por lo que la herramienta de seguridad que más se usa por parte de los proveedores de servicios de telecomunicaciones móviles para proteger a sus usuarios es la criptografía.

Sin embargo, no solo la protección de la ubicación del abonado es necesaria, también se debe asegurar que los mensajes enviados por ellos a través del canal sólo sean entendidos por los destinatarios, apareciendo los sistemas de cifrado,

procesos en los que los mensajes pasan por un proceso de encriptación para su posterior envío hacia el destinatario quien lo descifra. No es necesario que el proceso de cifrado/descifrado sea similar, puede depender del sistema que se esté utilizando. Hay que tener en cuenta de que el sistema criptográfico no es necesariamente confidencial; lo que sí se debe mantener en secreto es el valor de los parámetros criptográficos utilizados, así se mantiene la incertidumbre de cuál de todos los parámetros está siendo usado en dicho canal (Niemi V., Nyberg K., 2003).

En redes UMTS, existen dos tipos de cifrados, una es cifrado por bloques (Block Ciphers), el cual utiliza los códigos de autenticación de mensajes para demostrar la integridad del mismo y como método de autenticación de la entidad receptora; y el otro tipo es cifrado de flujo de transmisión (Stream Ciphers), que son utilizados para la voz y los datos.

3.1. Cifrado de flujo de transmisión (Stream Ciphers)

El cifrado de flujo es un algoritmo criptográfico para el control de la confidencialidad, con el objetivo de cifrar un texto plano. De manera similar que en cifrado de bloques, dicho texto se convierte de cadena de datos en una cadena de bits, que luego es combinada con una secuencia de bits de clave (keystream) mediante la operación XOR, que resulta en un flujo de

texto encriptado. El proceso de descifrado que ocurre en el otro extremo, se lo hace de manera inversa, desligando el flujo de texto plano con el flujo de claves, haciendo sus algoritmos de cifrado y descifrado idénticos.

CLAVE K	101001010011010111011101
TEXTO PLANO	010000011010010100100010
TEXTO CIFRADO	111001001001000011111111

Figura 3.10: Cifrado en flujo

Para que pueda funcionar este algoritmo correctamente, se debe inicializar el estado utilizando la clave secreta K y un valor inicial público, las cuales deben estar sincronizados de manera que se genera exactamente el mismo bloque de cadenas de claves (keystream) para el mismo bloque de datos (Niemi V., Nyberg K., 2003, pág. 125).

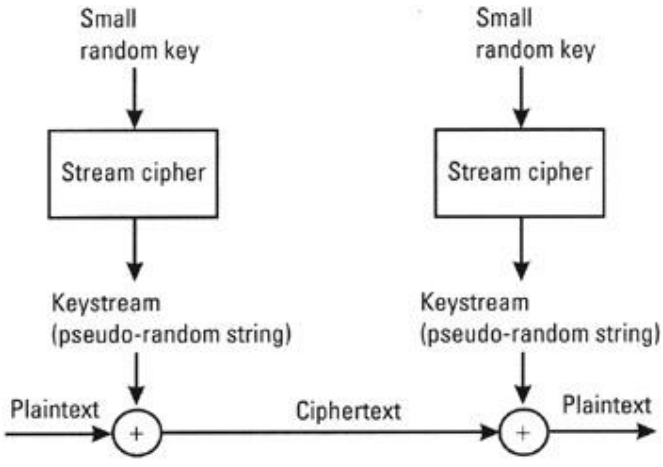


Figura 3.2: Cifrado y descifrado en flujo

Fuente: (Kobara K., 2006)

3.1.1. Algoritmo de confidencialidad f8

Un algoritmo que utiliza éste mecanismo de cifrado de flujo es el algoritmo de confidencialidad f8, utilizado para cifrar y descifrar los bloques de datos (entre 1 a 5114 bits de longitud), en el dispositivo del usuario, a partir de una clave CK previamente calculada durante la autenticación, calcula una secuencia de cifrado para luego realizar una operación XOR entre esta secuencia de bits y los datos originales, obteniendo un bloque de datos cifrados. Estos datos cifrados se envían a la red a través de la interfaz radio. Mientras en el RNC, se realiza una operación XOR entre esta secuencia y el bloque cifrado recibido para así recuperar los datos originales.

Se aplica sobre los canales dedicados entre el UE y el RNC con la identidad temporal de usuario, mientras que la función de cifrado se aplica en el subnivel RLC (Radio Link Control) o MAC (Medium Access Control) de la capa de Enlace de Datos para proteger la confidencialidad de los datos de usuario y datos de señalización que se envían a través del RLC entre el equipo de usuario (UE) y el controlador de red de radio (RNC).

En la capa RLC se realiza el cifrado, mismo usado en la capa MAC, por lo tanto se puede decir que el texto plano es un bloque RLC dentro de la red UTRAN. Los elementos que varían entre los dos son:

- La clave de cifrado CK que el UE aplicará para enviarla al CN, y dependerá del modo de negociación en el que se encuentre. Si está en el dominio CS o en el dominio PS, utilizará la clave CKCS o CKPS para los mensajes de subida (uplink).
- Otro elemento es el parámetro de entrada COUNT-C variante en el tiempo, que dependerá del modo de transmisión y el canal RLC usado:
    - RLC TM, modo transparente, donde pasan todos los datos desde las capas superiores hasta la capa MAC sin agregarle alguna cabecera RLC (el cifrado se lo realiza en la capa inferior).
    - RLC UM Unacknowledged Mode y RLC AM Acknowledged Mode, en cambio segmentan el paquete a un tamaño apropiado en paquetes UM PDU (excluyendo sus cabeceras) y le añaden cabeceras RLC para su verificación y

reemsamblaje del dato original en el extremo receptor (Hajji S., Orhanou G., 2012).

La clave CK se renueva en cada proceso de autenticación, mientras que las señales COUNT-C, BEARER y DIRECTION se pueden considerar como parámetros de inicialización, debido a que se renuevan por cada bloque de cadenas de claves "keystream"; aunque la entrada COUNT –C (32 bits de longitud), señal dependiente del tiempo que se inicializa al establecimiento de la conexión, es enviada en texto claro y es usada además de lo descrito arriba, como parámetro de sincronización para el cifrado de flujo síncrono. Su función es la de contador para evitar la reutilización de una cadena de claves.

Otro parámetro de entrada es el de LENGTH (que varía su longitud de 1 a 20000 bits), que solo afecta a la longitud de cadenas de claves, más no a los bits que se encuentran actualmente en ella. El parámetro BEARER (5 bits de longitud) evita que la misma clave de cifrado pueda ser usada simultáneamente en diferentes portadores de radio asociados con un solo usuario, por lo que su función es de generar la cadena de claves basado en la identidad del portador de radio.

La señal DIRECTION, de longitud de un bit: 0 para enlaces de subida, es decir, mensajes desde UE hasta el RNC; y 1 para enlaces de bajada, desde el RNC al equipo usuario UE. Este bit de dirección evita el uso de la misma cadena de claves para cifrar las transmisiones de enlace de subida y de bajada. Esta característica es nueva en redes UMTS, ya que en redes GSM eran separados por segmentos los enlaces.

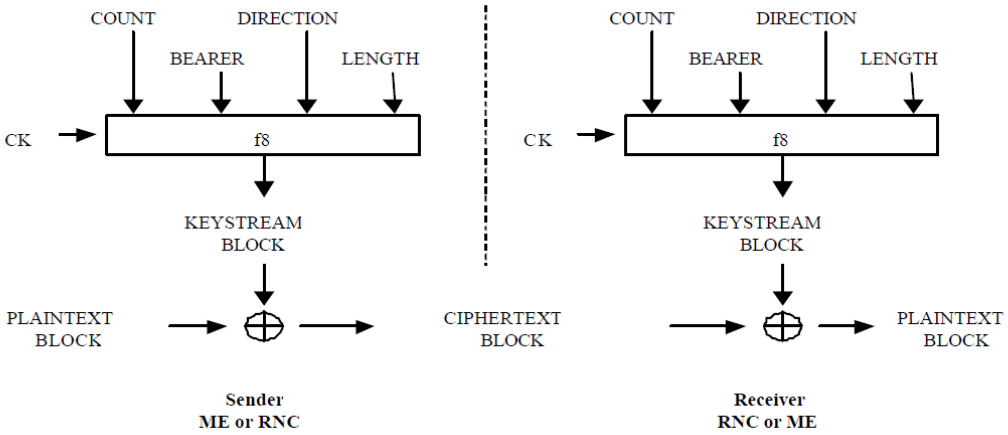


Figura 3.3: Mecanismo de control de confidencialidad UMTS.

Fuente: (Niemi V., Nyberg K., 2003, pág. 137)

Con los parámetros de entrada descritos, se genera el bloque de salida de secuencias de claves (KEYSTREAM), el cual se utiliza para cifrar el bloque de texto claro externo (PLAINTEXT) juntándolos y dando como resultado el bloque de salida de texto cifrado (CIPHERTEXT).

Las ventajas de este tipo de criptografía es su rapidez con respecto al cifrado por bloques y, por ende, menor complejidad de hardware para su implementación. Además de que éste algoritmo puede ser adaptado para que procese el texto plano bit a bit sin propagación de errores, mientras que en el cifrado por bloques requiere un búffer para tener los bloques de texto plano completo (Niemi V., Nyberg K., 2003).

El algoritmo f8 hace uso de un cifrado de bloques KASUMI desarrollado para éste fin por el grupo de trabajo algoritmos 3GPP. KASUMI es una modificación de MISTY1 y ofrece un grado de seguridad alto.

3.2. Cifrado de bloques (Block Ciphers)

El cifrado en bloque transforma un bloque de texto plano de longitud n en un bloque de texto cifrado de igual longitud, que es controlado por una clave secreta de K bits, el cual constituye 2^k transformaciones invertibles. Este tipo de clave es invertible, por lo que para descifrar se puede utilizar la transformación de cifrado inversa. Pero es posible recuperar el texto original

del texto cifrado sin conocimiento de la clave, por lo que el objetivo de este tipo de criptografía es proteger contra dicha amenaza.

El texto en claro es separado en grupos de bits de igual longitud denominados bloques, y a cada bloque se le realiza una transformación XOR con la clave secreta, resultando en bloques de texto cifrado de igual tamaño. De ésta manera se forma el primer bloque de cifrado, donde el bloque de texto cifrado se suma con el segundo bloque de texto plano para luego encriptar su resultado con la clave secreta, y continúa sucesivamente hasta cifrar todos los bloques.

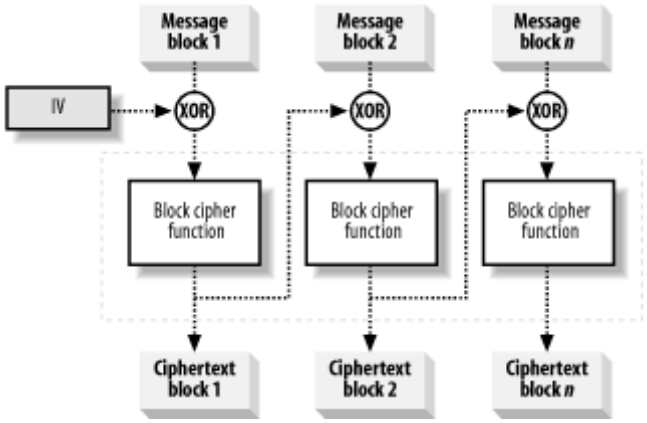


Figura 3.4: Cifrado por bloques

Fuente: (Univeridad Estatal de Tver, 2003)

En algunos casos, los cifrados de bloque incluyen un pequeño número de transformaciones sencillas, permutaciones de bits y pequeñas transformaciones de sustitución llamadas S-boxes o cajas-S, que son la

primera parte de un cifrado de bloques y se va construyendo mediante la repetición de la transformación alrededor de un número adecuado de veces. El objetivo de las permutaciones de bits es de esparcir tanto como sea posible la influencia de cada bit de datos de entrada y cada bit de clave que tiene sobre todo el bloque, mientras que el objetivo principal de las cajas-S es de ocultar como sea posible todas las interrelaciones entre diferentes bits. Un ejemplo de este tipo de encriptación usado en redes UMTS es el bloque de cifrado KASUMI, que se lo describirá más adelante (Niemi V., Nyberg K., 2003, pág. 120).

El estándar de telefonía 3G (3GPP) ha implementado un nuevo esquema de seguridad para asegurar la confidencialidad e integridad de la información, sean datos de señalización o de usuario, información que es enviada por la interfaz radio. Dichos algoritmos fueron creados juntos como nuevos cifrados de bloques, trabajando en conjunto para la protección de la identidad del usuario, de su ubicación, la información que envía a través del enlace, que no haya sido alterada y que provengan del mismo usuario que hace la transferencia:

El algoritmo de control de integridad f9 de cifrado por bloques garantiza la integridad de la información de señalización para el usuario como para la red y su estructura es de cifrado por bloques, mientras que una de las

funciones principales del algoritmo de cifrado de flujo f8 es la de evitar que la identidad de algún usuario que recibe determinados servicios pueda extraerse de la conexión en la que se encuentra como también de su ubicación (González A., 2010).

3.2.1. Algoritmo de integridad f9

Dado que el control de la información de señalización transmitida entre la estación móvil y la red es tan importante, su integridad debe ser protegida. El mecanismo que lleva a cabo esta función de seguridad se basa en un algoritmo de integridad f9 implementado tanto en la estación móvil como en el módulo de la UTRAN más cerca de la red de núcleo, es decir, el RNC. Consiste, de manera general, en la generación de un MAC (Message Authentication Code) por mensaje.

Para verificar el origen e integridad de los mensajes recibidos, el receptor calcula el MAC-I y compara con el recibido con el mensaje de señalización, descartando los que tengan un código MAC diferente. Este checksum se lo realiza con el algoritmo de integridad UMTS f9, el cual usa una clave IK de 128 bits durante el procedimiento de autenticación. La figura 3.5 muestra el cálculo de la MAC-I usando f9 con otros parámetros de entrada.

El procedimiento de señalización de verificación de integridad de los datos en la dirección de enlace ascendente como descendente consta de cuatro pasos:

1. El algoritmo f9 en el equipo de usuario calcula un código de autenticación de mensaje de 32 bits para la integridad de los datos de señalización (MAC-I) con respecto a sus parámetros de entrada y los datos de señalización (MESSAGE).
2. Con el MAC-I calculado, es adjuntada a la información de señalización y son enviados a través del interfaz de radio desde el equipo de usuario al RNC.
3. El RNC calcula un valor de código de autenticación de mensaje esperado de MAC (XMAC-I) de la misma forma que se hizo en la primera parte con el equipo usuario para recibir los datos de señalización y el MAC-I. La integridad de la información de señalización se determina comparando el MAC-I y el XMAC-I del emisor y receptor.
4. El receptor solo acepta la MAC si los valores comparados son iguales.

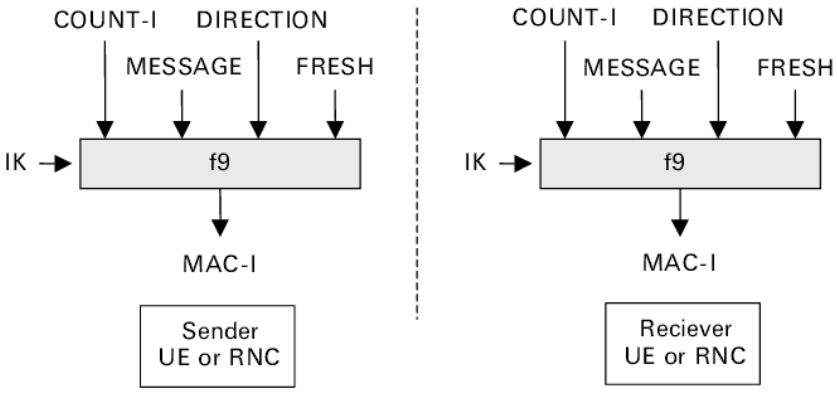


Figura 3.5: Algoritmo de cifrado f9.

Fuente: (Niemi V., Nyberg K., 2003, pág. 155)

Recordar que MAC-I, la letra I es de integridad de los datos de señalización en un mensaje de señalización.

La señal de entrada IK, de longitud de 128 bits, es una clave criptográfica generada nuevamente en cada proceso de autenticación. Los parámetros COUNT-I, FRESH y DIRECTION son considerados parámetros de entrada, que también se inicializan para cada mensaje que es autenticado.

El parámetro COUNT-I (32 bits de longitud), similar al COUNT-C del algoritmo f8 en la manera que se inicializa, ayuda a proteger contra la re-producción durante una conexión, debido a que su valor se incrementa en 1 por cada mensaje de entrada. Éste se divide en dos

partes: el HFN (Hyper Frame Number), parte más significativa, mientras que el RRC (Radio Resource Control) y el número de secuencia (SQN) son considerados la parte menos significativa para éste parámetro. Sin embargo, la capa RRC maneja la parte principal del control de señalización como establecimiento, mantenimiento de una conexión RRC entre el UTRAN y el UE, control de las funciones del algoritmo de protección de la integridad así como sus mensajes de señalización, presentación de informes de medición y soporte para funciones de posicionamiento del UE, entre otras más (Holma H., Toskala A., 2010).

El valor inicial del HFN es enviado por el usuario a la red estableciendo la conexión, y el mismo usuario almacena la parte más significativa del HFN de la conexión anterior y lo incrementa para la nueva conexión, asegurando, por parte del usuario, que el valor de COUNT-I sea reutilizado y use la misma clave IK.

El valor de FRESH (longitud de 32 bits), escogida por el RNC y transmitida al UE, se introduce en el algoritmo para asegurar que la parte de la red del usuario no esté re-produciendo antiguas MAC-Is, haciendo que la misma clave Ik puede ser utilizado para varias conexiones consecutivas y volver a reproducir mensajes de señalización

RRC de conexiones anteriores manteniéndose constante sobre una conexión sin repetirse al igual que COUNT-I.

El dato de señalización del MESSAGE de aproximadamente de 20000 bits de longitud, anteriormente de 5114 bits como límite superior, lo más probables es que no se alcance el límite mencionado como parámetro de entrada de datos en esta algoritmo. Aunque en documentos recientes, menciona sobre la longitud de la cadena de claves para el algoritmo f8 como 20000 bits de tope, en el algoritmo f9 no se pone un límite para la longitud del mensaje de entrada.

El bit de DIRECTION es usada para los mensajes de enlace ascendente y enlace descendente, es decir desde el UE hacia el RNC (bit 0) y de manera inversa (bit 1) respectivamente (Niemi V., Nyberg K., 2003).

3.2.1.1. Estructura del algoritmo de integridad f9

Dentro de la estructura del algoritmo f9 se puede observar que utiliza la clave de integridad IK compartida, además de tener una serie de módulos de bloque de cifrado KASUMI interconectados en una variante del Cipher Block Chaining (CBC).

El algoritmo se puede observar en la Figura 3.6, donde combina las salidas de 64 bits de todos los bloques de cifrado mediante el uso de operaciones XOR, aplicando al final, el algoritmo KASUMI a todas estas sumatorias. De esta manera se obtiene el valor MAC-I de 32 bits de la salida de 64 bits del proceso descrito.

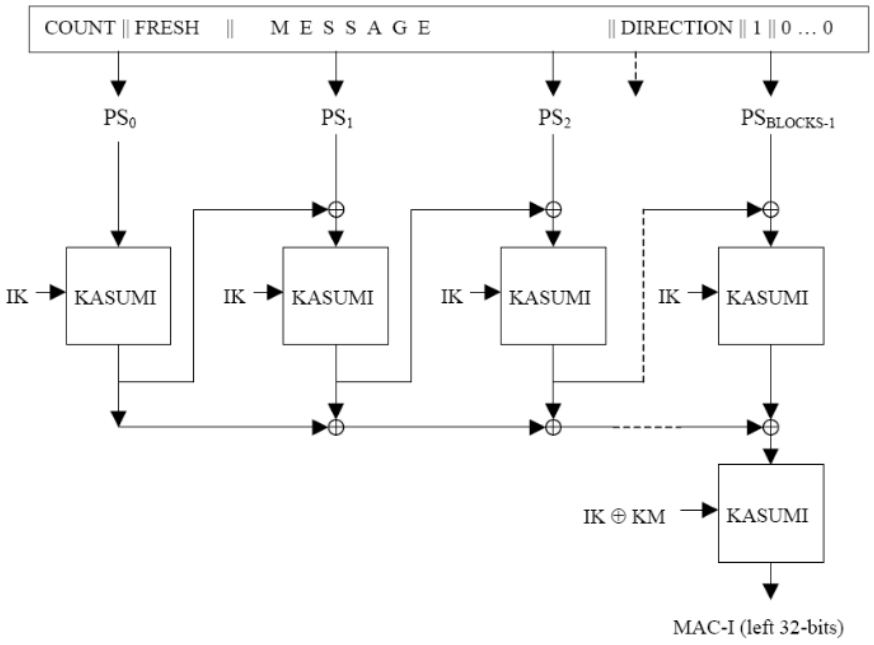


Figura 3.6

Figura 3.6:Estructura del algoritmo de integridad f9.

Fuente: (Balderas T., Cumplido R., 2004, pág. 16)

3.3. Antecedente al algoritmo de cifrado KASUMI

La versión final del algoritmo de cifrado de bloques se conoce como KASUMI, que en japonés significa "nebuloso, oscuro, confuso". KASUMI, también llamado A5/3, es una unidad de cifrado por bloques utilizada en algoritmos de confidencialidad f8, e integridad f9 anteriormente descritos para Telefonía móvil 3GPP.

La unidad de cifrado KASUMI fue diseñado por el grupo SAGE (Security Algorithms Group of Experts) que forma parte del organismo de estándares europeos ETSI (Instituto Europeo de Estándares de Telecomunicación). La finalidad de este grupo es de diseñar y formular la especificación de los algoritmos de confidencialidad e integridad estándar; para ello ETSI creó un proyecto específico, llamado el Grupo de Trabajo de SAGE para los algoritmos de 3GPP (SAGE TF 3GPP) para dicho propósito. SAGE redacta documentos que definen los servicios de seguridad que los algoritmos criptográficos deben dar para la seguridad de las redes UMTS, además de las interfaces técnicas, como parámetros de entrada y salida, requisitos de rendimiento y seguridad generales para éstas redes de tercera generación.

El grupo realizó algunos cambios en este tema; por ejemplo, modificó el algoritmo de integridad f9 para fortalecerlo, de manera que los enlaces ascendente y descendente sean separados criptográficamente con la adición de un bit de dirección para las entradas, además de aumentar el tamaño en bits de salida de la MAC de 24 a 32 para estar a la par con los estándares actuales, la seguridad y los recursos de ancho de banda limitado por la interfaz aérea (Niemi V., Nyberg K., 2003).

3.3.1. Algoritmo MISTY-1

El algoritmo de cifrado por bloque KASUMI, fue desarrollado a partir del algoritmo MISTY-1, por lo que antes de ahondar en la estructura del algoritmo KASUMI, primero se debe saber un poco más sobre el algoritmo que le precedía, MISTY-1.

El grupo SAGE tomó la decisión de tomar el algoritmo de cifrado MISTY-1, en sus versiones tempranas, como punto de partida para elaborar algoritmos de cifrado de flujo que no estén basados en algún algoritmo criptográfico que haya existido hasta ese entonces, utilizando cifrado de bloque para acelerar los procesos de diseño y evaluación.

MISTY-1 es cifrado de bloques de 64 bits con una clave de 128 bits, y un número variable de rondas. Creado por Mitsuru Matsui de Mitsubishi Electrical Corporation, se pudo corroborar que dicho cifrado era seguro contra el criptoanálisis diferencial y lineal: el primero trata sobre la localización de las relaciones entre el texto plano, el texto cifrado resultante del sistema y la clave, con ayuda de la operación XOR (método diferencial) que se realiza entre los bloques de texto plano y poder así, durante o después del cifrado, predecir el resultado; mientras que el método lineal analiza la predicción de las combinaciones lineales de los bits de texto sin formato. Se puede observar que, de estos dos métodos, el criptoanálisis lineal es más potente cuando se aplica el Estándar de cifrado de datos DES (Data Encryption Standard).

DES es un método para cifrar información de bloques de 64 bits por medio de operaciones básicas, permutación y sustitución, usando una clave de 56 bits (sumando 8 para paridad, en total son 64 bits) para modificar la transformación. Tiene 19 etapas diferentes de las cuales 16 etapas son idénticas en el proceso, denominada así rondas de la red Feistel, el cual asegura que el

cifrado y descifrado sea similar, con la diferencia que las subclaves de valor K (con longitud de 56 bits y diferentes en cada vuelta) sean aplicadas de manera inversa al descifrar. Las tres etapas restantes: la primera y la última son una transposición del texto plano, con la diferencia que en el último es exactamente la inversa de la primera; y la penúltima etapa realiza un intercambio de los 32 bits de la derecha y de la izquierda.

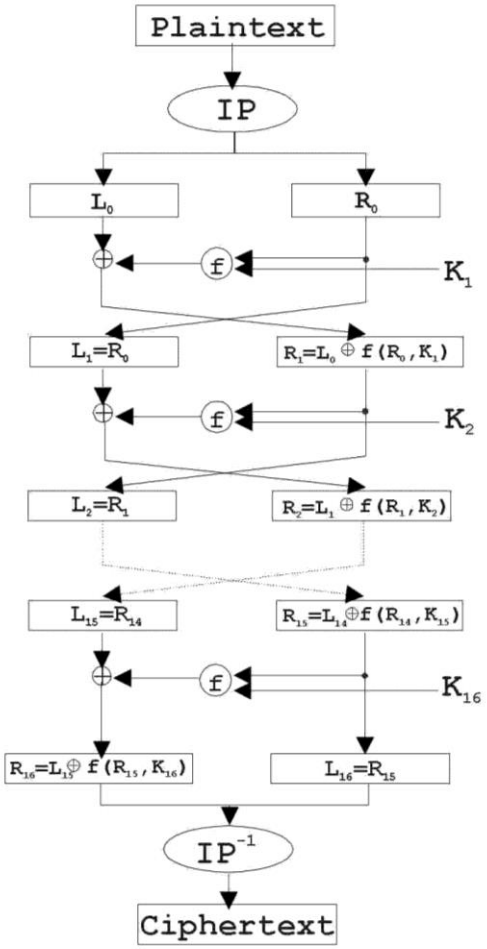


Figura 3.7: Estructura DES (16 rondas)

Fuente: (Salomon D., 2003)

Este procedimiento, sumado al criptoanálisis lineal, y al tener una gran cantidad de datos más fiables es el resultado al obtener los bits de clave. Para contrarrestar estos ataques, en la actualidad (en algunos casos) se recomienda su uso.

Una de las motivaciones para el diseño e implementación de MISTY fue el de oponerse al criptoanálisis lineal y diferencial, aparte de ser práctico así tenga una complejidad computacional elevada. Por lo que para perfeccionar el algoritmo, Matsui tuvo la idea de una estructura anidada de cifrados de bloques con la adición de una función diferencial resistente utilizando la estructura DES (duplicando la longitud de los bloques), obteniendo como resultado un sistema de cifrado robusta teniendo así mayor previsibilidad para combinaciones lineales y diferenciales (Niemi V., Nyberg K., 2003, págs. 172-174).

Con el tiempo se crearon dos versiones: MISTY-1 y MISTY-2 posteriormente, pero se había notado que MISTY-1 tenía alguna ventajas con respecto a MISTY-2 por sus propiedades pseudoaleatorias, con lo que el grupo SAGE podría haber seleccionado MISTY-1 para futuras investigaciones (Matsui M., 1997). MISTY-1 fue considerado como el mejor motor de cifrado para los algoritmos de encriptación y confidencialidad por 3GPP, por su modo OFB estándar para el algoritmo de confidencialidad (bloques de cifrado operan como cifrado en flujo) y el modo

CBC-MAC (Cipher Block Chaining Message Authentication Code) para el algoritmo de integridad.

CBC-MAC es una técnica para la construcción de un código de autenticación a partir de un bloque de cifrado. El mensaje es encriptado con algún algoritmo de cifrado de bloque en modo CBC, el cual cada bloque de texto plano se realiza una operación XOR con el bloque de texto cifrado antes de ser encriptado; haciendo que cada bloque de texto cifrado dependa de algún bloque de texto plano procesado hasta ese momento. Así, se crea una cadena de bloques con todo el mensaje encriptado, haciendo, de manera general, que cada bloque dependa de la encriptación del bloque previo, pero para hacer el mensaje único, debe haber un vector de iniciación en la primera parte para el cálculo del primer bloque de texto cifrado.

La finalidad de este proceso es de asegurar la integridad del texto original, ya que si ocurre algún cambio en cualquiera de los bits de texto plano, habrá un cambio significativo en él o los bloques de cifrado al final, con la finalidad que no se pueda predecir sin antes conocer la clave del cifrado de bloques, o el texto sin formato inicial, aparte del vector de iniciación.

Una desventaja del CBC es en sí su tipo de cifrado, de modo secuencial; es decir, que el mensaje de texto plano es procesado a la par con el bloque de cifrado, y si se realiza algún cambio en el mensaje original, ésta afectará a los siguientes bloques de texto cifrado que se crean, alargando el proceso haciendo lentecer el sistema. Si bien CBC-MAC es seguro para mensajes que tienen una longitud constante, no se puede decir lo mismo para mensajes de longitud variable arbitraria, por lo que sería otro problema para éste algoritmo (Hong D., Kang J., Preneel B., Ryu H., 2003, pág. 4).

Dado que muchos de los ataques de MISTY1 también pueden ser relevantes para 3GPP KASUMI, y lo contrario (como el criptoanálisis lineal y diferencial), el extenso análisis y desarrollo que han hecho los investigadores sobre MISTY1 también ha consolidado la posición de KASUMI como un seguro algoritmo criptográfico.

3.4. Estructura del algoritmo KASUMI

El algoritmo de cifrado KASUMI, de bloques de salidas de 64 bits con claves de 128 bits, presenta una estructura de Feistel por su antecesor MISTY, comprendido en ocho rondas, el cual la entrada de texto sin

formato es la entrada a la primera ronda; la codificación y decodificación son parecidas pero con claves K diferentes (KLi, KOi y KIi) en cada ronda i, con una función diferente. Posee ocho rondas de procesamiento, incluyendo el texto plano como entrada de la primera ronda y el texto cifrado luego de la vuelta final, donde cada ronda calcula una función diferente por cada subfunción:

Función FO, llamadas redes internas donde cada una tiene tres rondas que hace uso de la la subfuncion FI y las subclaves KOi y KIi.

Función FL, consta de una entrada de 32 bits y la subclave KLi que es dividida en dos subclaves más de 16 bits (KLi1 y KLi2)

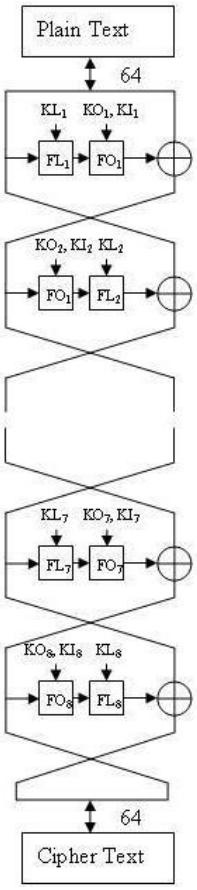


Figura 3.8: Cifrado por bloques KASUMI

Fuente: (Gardezi A., 2006)

En la estructura en cada iteración separa el bloque de un mensaje en dos partes o funciones de 32 bits: una derecha (FO) y otra izquierda (FI), conmutando éstas partes con una función unidireccional, por un número reiterado de veces. Sin olvidar que el orden de las subfunciones depende del número de iteración, es decir, en rondas pares se aplica primero la función FO mientras que en las impares la

función FI es asignado primero. Esta estructura de red fue usada por MISTY1, y al igual que a ella, procesa la mitad de los bits del bloque dejando el resto sin alterar durante una vuelta, y así continua en las siguientes rondas, otorgándole un alto grado de seguridad debido a su complejidad elevada en su desarrollo (Dunkelman O., Keller N:).

Aunque KASUMI fue diseñada a partir de MISTY1, hubo unos cambios significativos, sobretodo en la generación de claves, ya que el programa de claves de MISTY1 tenía un desarrollo complejo, con un tiempo de procesamiento relativamente largo debido a que las sub-claves vuelven a calcularse cuando se cambia la clave de cifrado. Dado que las claves de cifrado en el sistema UMTS se renuevan en cada proceso de autenticación (brindado un alto grado de seguridad de los datos), la finalidad es de hacer del proceso de cálculo sea lo más rápido posible en el nuevo algoritmo de cifrado y otras modificaciones por algunas irregularidades no deseadas en su cifrado.

Otra diferencia es que a pesar de que MITSY1 utilice la función de descifrado DES, también hicieron unos cambios al algoritmo de cifrado KASUMI como las últimas rondas de sus funciones de cifrado: en KASUMI las mitades de los datos no se intercambian, mientras que en DES si lo hacen; aun así, sus transformaciones de cifrado y descifrado

son similares, pero al no intercambiarse los datos tiene una cierta ventaja para la aplicación (Matsui M., pág. 2).

Como se mencionó anteriormente, el grupo 3GPP actualmente tiene la responsabilidad del mantenimiento del grupo de especificaciones para GSM y GPRS, incluidos el algoritmo A5/3, para la transmisión de voz vía GSM o EDGE desde el usuario hasta la antena de la BS, y GEA3 utilizado en GPRS para brindar seguridad en el trayecto radio, el trayecto más vulnerable, evitando que información sensible pueda ser interceptada por personas ajenas con fines maliciosos.

A5/3 y GEA3, algoritmos de encriptación para UMTS y GPRS respectivamente, son cifradores de flujo que usan el algoritmo KASUMI en el modo de OFB (Output Feedback) para la generación pseudo aleatoria de claves, además de construirse bajo un módulo de función llamado KGCORE, también basado en el cifrado de bloques KASUMI (Niemi V., Nyberg K., 2003).

3.5. Módulo KGCORE para generación de claves

KGCORE (Core Keystream Generator) asigna varias entradas, de los algoritmos de cifrado, a las entradas del módulo para la generación de bits de clave de flujo (keystream) a la salida con el propósito de generar

keystream en términos de la función núcleo KGCORE para la fácil implementación de diversos algoritmos y futuras mejoras como el soporte de una clave Kc de mayor longitud.

Su estructura es idéntica a la del algoritmo de cifrado de flujo f8: así como en f8, el conjunto de bloques KASUMI están conectados en modo OFB, donde los datos de retroalimentación son modificados por un valor estático y un contador de 64 bits. KGCORE tiene siete parámetros como entrada (CA, CB, CC, CD, CE, CK y CL) con longitudes variables, y una salida (CO)

Tabla I Entradas KGCORE

Parámetros	Descripción
CA	8 bits CA[0]…CA[7]
CB	5 bits CB[0]…CB[4]
CC	32 bits CC[0]…CC[31]
CD	1 bit CD[0]
CE	16 bits CE[0]…CE[15]
CK	128 bits CK[0]…CK[127]
CL	Entero rango 1…2^{19} especificando el número de bits de salida para producir

Tabla II Salida KGCORE

Parámetros	Descripción
CO	CL bits CO[0]…CO[CL-1]

Los algoritmos A5/3 y GEA3 se definen mediante la asignación de sus entradas a las entradas del módulo KGCORE, y las salidas del algoritmo a la salida del mismo.

3.5.1. Algoritmo A5/3

El algoritmo A5/3, usado en ambientes EDGE y GPRS, toma una clave CK de 64 bits de longitud y un contador COUNT de 22 bits (parámetros de entrada) que produce dos bloques de 114 bits (BLOCK1 y BLOCK2) para cifrar los datos de usuario, de señalización sobre la interfaz aérea, es decir, para el servicio de radio para paquetes GPRS de GSM. Este bloque se divide entonces en dos bloques para el enlace ascendente y enlace descendente de cifrado y descifrado. Se lo puede observar en la figura a continuación, el cual muestra los parámetros de entrada,

de salida y la información que pasa al bloque de función KGCORE.

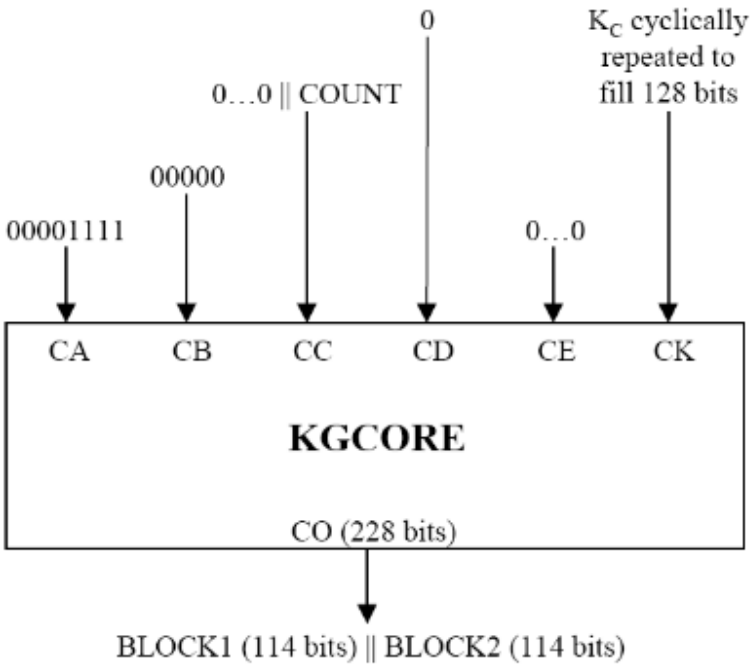


Figura 3.9: Algoritmo de cifrado de flujo A5/3.

Elaborado por: (Balderas T., Cumplido R., 2004, pág. 32)

3.5.2. Algoritmo GEA3

El algoritmo GEA3 para GPRS (definido en términos de KGCORE al igual que A5/3), donde las transferencias de enlace ascendente y descendente son independientes, haciendo que el cifrado para el enlace ascendente y el enlace descendente sean

completamente independientes entre sí. A comparación con el algoritmo A5/3, donde “keystreams” para ambos tipos de enlaces son generados a partir de la misma entrada del bloque de cifrado.

Una característica particular, es que la estación móvil (MS) que admite solamente un “time slot” de comunicación GPRS, similar al cifrado A5/3, también puede tener un MS que admite comunicación GPRS sobre el número máximo de ocho “time slots” en ambas direcciones.

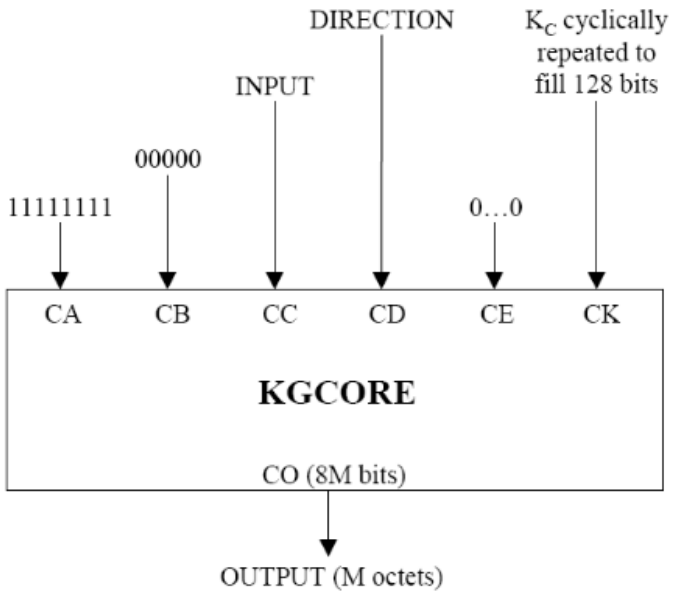


Figura 3.10: Algoritmo de cifrado de flujo GEA3.

Elaborado por: (Balderas T., Cumplido R., 2004, pág. 33)

Este cifrado genera un bloque de secuencia de claves de M octetos pero puede variar pero sin exceder de 216, es decir 65.536. Otra característica es que la producción del parámetro de salida CO del KGCORE tiene una longitud, en bits, de ocho veces el valor del entero de M; es decir, que puede aceptar bloques pequeños de datos (25 a 50 octetos) o paquetes largos (500-1.000 octetos). Sin olvidar que GEA3 está abierto a posibles mejoras futuras para apoyar una clave de cifrado Kc más larga que la actual.

Más adelante se muestra una pequeña comparación de los dos algoritmos recientes, sobre sus parámetros de entradas y su parámetro de salida respectivos, describiéndolos de manera general, enfatizando sus diferencias:

Tabla III A5/3 y GEA3 en términos de KGCORE

	GSM A5/3	GEA3
CA	00001111	11111111
CB	00000	00000
CC	0…0 ‖COUNT	INPUT
CD	0	DIRECTION
CE	00…0	00…0
CK	Kc repetido para llenar los 128 bits	Kc repetido para llenar los 128 bits
CO	BLOCK1 ‖ BLOCK2	OUTPUT

Fuente: (Niemi V., Nyberg K., 2003, pág. 163)

Para el grupo 3GPP solamente la función de encriptación de KASUMI debe ser definida, ya que en el modo de funcionamiento de f8 y f9, la función del núcleo solo se calcula en una dirección, aún la función de núcleo (kernel function) sea un cifrado de bloques, el proceso de descifrado no se utiliza; sin embargo sería posible derivar la función de descifrado a partir de la de cifrado pero no es necesario en el contexto 3GPP. Esto aclararía la diferencia entre la función DES y la función de cifrado KASUMI.

El objetivo de estos algoritmos de cifrado es que las MS puedan tener libre restricciones al uso de los servicios de la red para permitir la libre circulación de los terminales 3G, mientras los equipos de red que incorporan estos algoritmos puedan operar bajos estas restricciones velando por la seguridad del tráfico y de la identidad del usuario.

CAPÍTULO 4

ALGORITMOS DE AUTENTICACIÓN Y GENERACIÓN DE CLAVES

Para los operadores móviles, no es necesario que los algoritmos de autenticación y generación de claves para el sistema UMTS, usados para el acceso a la red y autenticación de origen sean estandarizadas; es decir, que ellos pueden elegir los algoritmos a su conveniencia que se aplicarán en los Centros de Autenticación del Operador (AuC) y en los USIM de los dispositivos móviles de los suscriptores del mismo operador. Ésta acotación supondría que no sería necesario que haya interoperabilidad entre los operadores, sin embargo, para que haya comunicación entre las diferentes aplicaciones, USIM y el AuC, es necesario un algoritmo estándar para la interoperabilidad, característica indispensable que debe brindar un servicio móvil de tercera generación.

4.1. Algoritmos de Autenticación de claves

El sistema AKA de UMTS tiene diferentes tipos de algoritmos criptográficos para realizar varias tareas de seguridad. En total ocho funciones diferentes son usados, aunque dos de éstas (f5 y f5*) son opcionales; y solo son necesarios si el número de sincronización queda oculto, ya que éste número permite que diferentes instancias de autenticación se relacionen entre sí, revelando la identidad del usuario.

Se definen las ocho funciones criptográficas del proceso de autenticación del sistema UMTS:

- f0, función de generación de desafío aleatoria
- f1, función de autenticación de red
- f1*, función de autenticación de mensajes de re-sincronización
- f2, función de autenticación de usuario (AUTN)
- f3, clave de cifrado (CK) función de derivación
- f4, integridad de claves (IK) función de derivación
- f5, clave de anonimato (AK de 64 bits) función de derivación para el funcionamiento normal (opcional)
- f5*, clave de derivación de AK para la re-sincronización (opcional)

Las funciones de los algoritmos f0 a f5 son utilizadas únicamente para la autenticación de la entidad mutua entre la tarjeta SIM y el AuC, derivando las claves para proteger al usuario, señalizando los datos transmitidos a través del enlace de acceso de radio y ocultando el número de secuencia (SQN de 48 bits), que es ordenado de forma ascendente para verificar que no han sido utilizado antes, otorgando total confidencialidad de identidad del usuario. Las funciones f1 al f5, f1* y f5* están localizadas en las AuC y el USIM, mientras que la función f0 solo se las asigna al Auc.

4.1.1. Descripción de las funciones de los algoritmos de autenticación de claves

Todas estas funciones trabajan con dos parámetros de entrada que son la clave maestra K de cada una y el número aleatorio RAND (también de 128 bits), una cadena de bits aleatoria de 128 bits guardado en la USIM, que se crea al mismo instante que el de la SQN. La diferencia con la función f1 es que recibe otros dos parámetros adicionales que son el número de secuencia SQN y el campo de gestión de autenticación AMF de 16 bits de longitud.

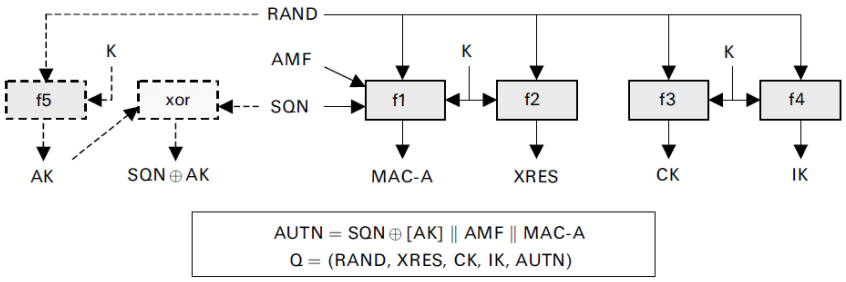
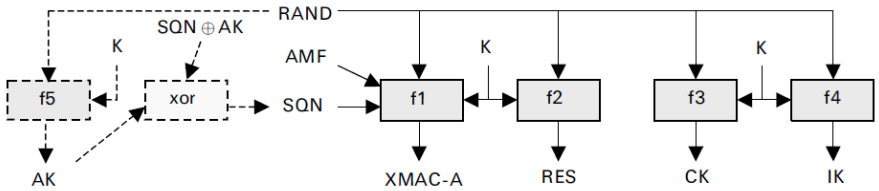


Figura 4.1: Generación de los vectores de autenticación en el AuC

Fuente: (Niemi V., Nyberg K., 2003, pág. 203)

Figura 4.2: Generación de los vectores de autenticación en el USIM



Fuente: (Niemi V., Nyberg K., 2003, pág. 204)

Para la autenticación del USIM usa las funciones f1 al f5, pero en este caso f5 se debe calcular antes que f1 debido a que ésta función es la encargada de que el SQN se mantenga oculto. Cada función descrita a continuación:

La función f0 se encarga de la “generación del desafío aleatoria”, es decir que al ser una función pseudoaleatoria, genera números al azar además de mapear el estado interno del valor RAND generado.

La función f1 se encarga de la autenticación de la red, una función MAC que toma la clave K del suscriptor y le asignan los datos SQN, RAND, AMF para generar un código de autenticación de mensajes (MAC) para la autenticación (MAC-A o XMAC-A). Con lo último se puede deducir haciendo el proceso contrario, con el conocimiento de RAND, SQN, AMF y MAC-A (AuC) o XMAC-A (USIM), la clave K.

La función f1* se encarga de la autenticación de mensajes de re-sincronización, una función MAC que toma la clave K del suscriptor y asigna los datos SQN, RAND, AMF* que es el valor por defecto para AMF usado en re-sincronización, para generar un código de autenticación de mensajes (MAC) para la sincronización (MAC-S o XMAC-S). De manera similar a la función anterior, se podría obtener el valor de la clave K con el conocimiento de RAND, SN, AMF* y MAC-S (XMAC-S).

La función f2 se encarga de la autenticación del usuario, una función MAC que toma la clave K del suscriptor y asigna el valor de desafío RAND para generar una respuesta esperada RES (USIM) o XRES (AuC). También se puede obtener el valor de K con el conocimiento de RAND y RES (o XRES).

La función f3 se encarga de la derivación de claves CK, que toma la clave K del suscriptor y el valor aleatorio de desafío RAND como entradas, generando la clave de cifrado CK como salida. Asimismo se puede obtener la clave K del conocimiento de RAND y CK.

La función f4 se encarga de la derivación de claves IK, que toma la clave K del suscriptor y el valor aleatorio de desafío RAND como entrada, generando la clave de integridad (IK) como salida. De la misma forma se podría obtener la clave K a partir de RAND e IK.

La función f5 se encarga de la derivación de claves AK para el funcionamiento normal, que toma la clave K del suscriptor y el valor aleatorio de desafío RAND como entrada, generando la clave de anonimato (AK) como salida. De igual manera que en las funciones anteriores, se podría obtener la clave K a partir de RAND e AK (Niemi V., Nyberg K., 2003, págs. 221, 222).

Tabla IV *Descripción de los elementos de los vectores de autenticación*

Parámetro	Longitud	Descripción

MAC-A y XMAC-A	64 bits	Códigos de mensajes de autenticación de la red al usuario Para la autenticación de la integridad de los datos y el origen de los datos de RAND, SQN y AMF. Autenticación de la entidad de la red hacia el usuario.
MAC-S y XMAC-S	64 bits	Autentica la integridad de los datos y el origen de los datos de RAND, SQN y AMF. Provee autenticación del origen de datos debido a algún fallo en la información durante la sincronización. Enviado del USIM al AuC
RES y XRES	32 a 128 bits	Entidad de autenticación del usuario a la red. Enviado del USIM al AuC
CK e IK	128 bits	Clave de cifrado

		Los bits más significativos deben llevar efectiva información clave mientras que los menos significativos son puestos en 0
AK	48 bits	Igual longitud al SQN Opcional Clave de anonimato del usuario

Fuente: (Herazo G., Flórez H., 2009)

4.2. Proceso para autenticación y acuerdo de claves

El objetivo de este proceso es el de autenticar al usuario y establecer un nuevo par de claves de integridad y cifrado entre el VLR y el USIM de usuario. Para obtener la autenticación mutua entre el usuario y la red con el conocimiento de una clave secreta K solo para el USIM y el AuC del abonado, el VLR/SGSN manda una petición al AuC, éste en respuesta envía una cadena ordenada de n vectores de vuelta al origen. Estos vectores son las funciones criptográficas que contienen en ellas: un numero aleatorio RAND, una clave de cifrado CK, una respuesta esperado XRES, una clave de integridad IK y un vector de autenticación AUTN, representando cada una de la funciones f1-f5, que sirven para una correcta autenticación y acuerdo de claves entre el VLR/SGSN y el USIM.

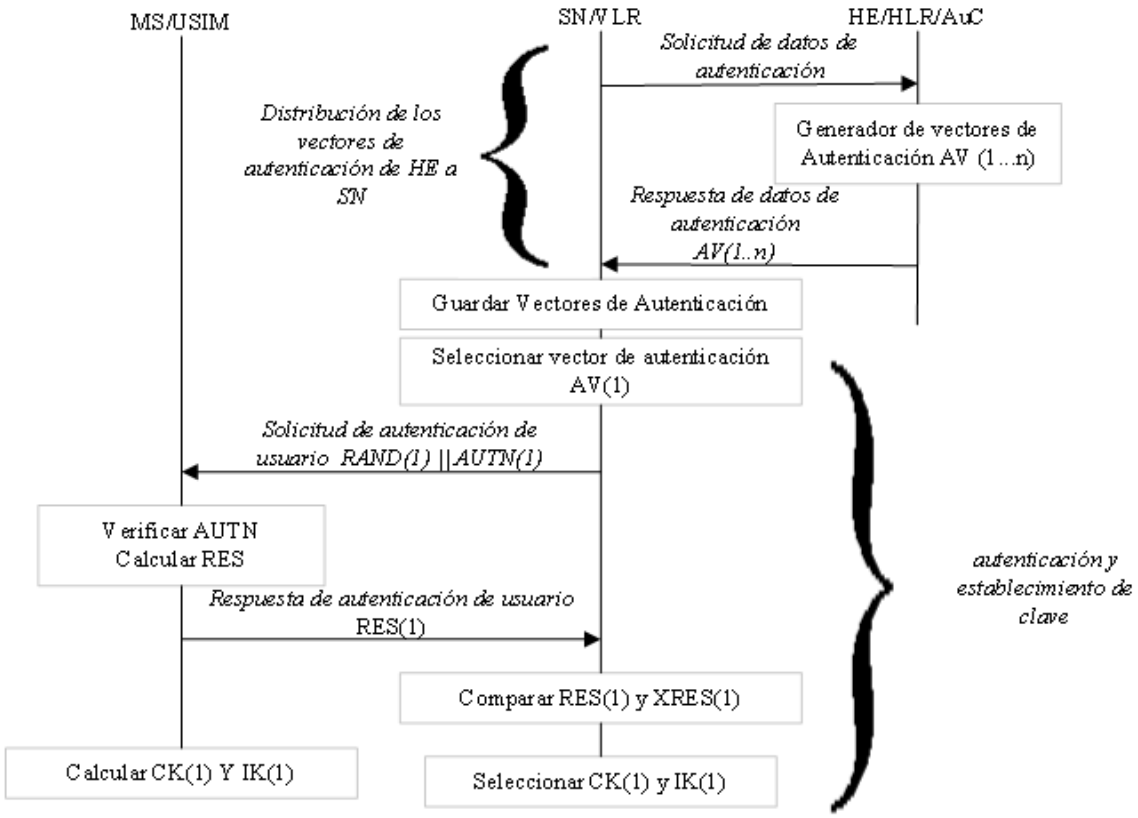


Figura 4.3: Proceso de autenticación y acuerdo de claves en redes UMTS

Fuente: (Salvela J., 2000)

El HLR/AuC genera un número aleatorio RAND con ayuda de la función f0 que calcula la MAC para MAC-A, la salida XRES de la función f2, la clave CK de la función f3 y la clave IK de la función f4; le agrega el símbolo de autenticación AUTN que contiene el SQN, AMF y el MAC-A, con lo que forma el "quinteto" Q = (RAND, XRES, CK, IK, AUTN), llamado también como "Vector de autenticación" o "Autenticación múltiple". En el caso de que la SQN esté oculto, el HLR/AuC puede calcular esta clave AK de la función f5

(de manera opcional), con lo que la función de autenticación del usuario (AUTN) contendría los mismos elementos aunque el SQN se le sumaría la clave AK.

Se puede decir que el VLR primero inicia la autenticación y de acuerdo a las claves selecciona el siguiente vector de autenticación de la cadena, enviando al móvil del usuario los parametr4o RAND y AUTN. En ese momento que recibe dichos parámetros, el USIM recupera el SQN oculto si es que estuviese oculto, y valida el AUTN recibido, y si es correcto genera una respuesta RES que es enviada de vuelta al VLR con las claves CK e IK calculados con los otros vectores. El VLR compara la respuesta esperada RES o XRES y si es afirmativa, éste considera el proceso finalizado con éxito; con lo que las claves IK y CK se envían desde las dos aplicaciones (VLR y el USIM) hacia las entidades que ejecutan las funciones de integridad y confidencialidad o cifrado.

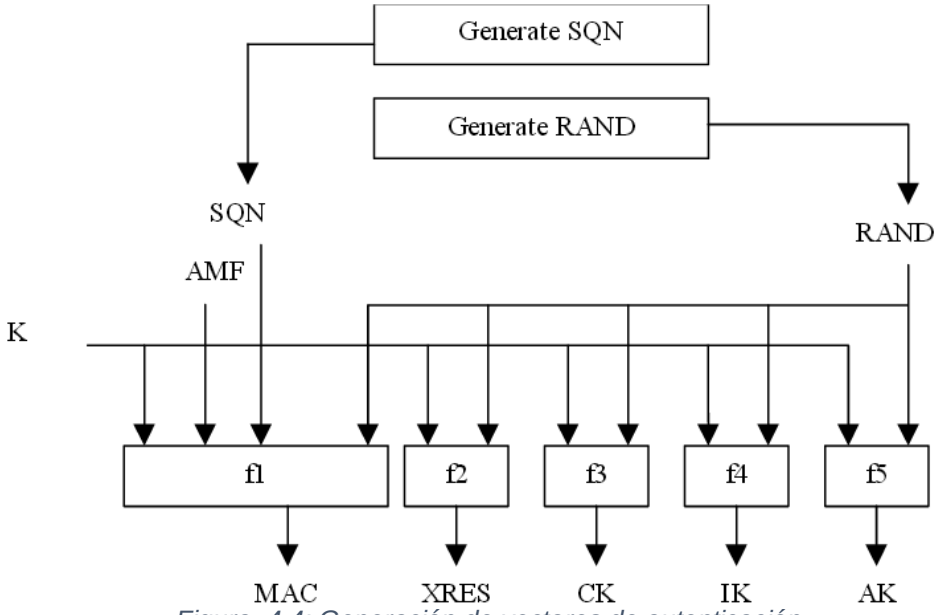


Figura 4.4: Generación de vectores de autenticación.

Fuente: (González A., 2010, pág. 54)

Pueden ocurrir casos en el que la conexión con el AuC no esté disponible en ese momento, para éste inconveniente, el VLR/SGSN permite la utilización de las claves CK e IK previamente calculadas para otorgar de manera segura al usuario una conexión sin la necesidad de autenticación y acuerdo de claves. Otro escenario es cuando hay un error de sincronización, el USIM genera una petición de re-sincronización calculando la MAC-S, y en ese momento, se cambia a AUTS con los elementos SQN y MAC-S; y en el caso que tuviera el SQN oculto, se le agregaría a ésta la clave AK para enviársela de vuelta al AuC, para que éste compruebe si el MAC-S incluido en el AUTS es igual al valor calculado XMAC-S para poder continuar con el

proceso de autenticación y eliminar los antiguos vectores de sincronización para ese usuario (González A., 2010, págs. 56, 57).

4.3. Establecimiento de conexión

Una vez que el VLR conoce la identidad del usuario móvil y que las claves IK y CK están guardadas, son llevadas al RNC cuando éste lo requiera. Las claves de dominio CS y PS se almacenan en el USIM y se actualizan para la siguiente autenticación del dominio respectivo. En el caso de que durante el proceso de autenticación se dé en una conexión PS o CS, la nueva clave de confidencialidad e integridad se usará tanto en el RNC como en el equipo usuario (UE), formando parte de la negociación de seguridad del proceso de autenticación.

Cuando una MS quiere establecer alguna conexión con la red, debe indicarle sobre su USIM y los algoritmos de integridad y cifrado que soporta, sin olvidar, que también ésta información puede estar protegida por medio de la función de integridad descrita anteriormente. En el otro ambiente, en el que la MS no tenga en común alguna de las versiones del algoritmo de integridad UMTS (UIA), la conexión acabará en ese momento. Pero de existir al menos una de las versiones UIA en común, la red, a la que la MS desea conectarse, seleccionará una de ellas para aplicar la conexión. En el caso extremo en el

que la MS y la red no tienen versiones comunes de UIA; y sin embargo, dicha red puede utilizar una conexión no protegida, podrá usar este modo para conectarse a la red.

Pero no solo dependerá de las preferencias de integridad y los requerimientos de suscripción de la red como del MS, también se compararán sus preferencias de cifrado y de esa manera observar si tienen versiones del algoritmo de encriptación de UMTS (UEA): En el caso que no tengan versiones UEA comunes, ni la estación móvil esté preparada para utilizar una conexión no cifrada, se finalizará dicha conexión. Al igual que los algoritmos de integridad, de existir entre ellas una versión UEA común, la red optará por una de ellas para la conexión; y de no tener versiones UEA comunes, pero sí puede usar una conexión no cifrada, se seleccionará este modo. Al final para ambos dominios (PS y CS), las preferencias y requerimientos para el modo de cifrado e integridad deben ser iguales, y así el nodo CN determina los UIAs y UEAs permitidas.

Para poder continuar con el establecimiento de la conexión, luego de haber hecho la petición inicial de conexión para establecer el modo de seguridad se necesita que la identificación por identidad, autenticación y acuerdo de claves ya se haya procesado. Una vez que se completa esta fase, la CN inicia el algoritmo de integridad y de confidencialidad enviando el mensaje

de RANAP (Radio Access Network Adaptation Protocol), encargado de proveer servicios de señalización entre UTRAN y CN, un protocolo de adaptación a la red del acceso de radio, al RNC de servicios (SRNC) donde decide qué algoritmos de seguridad se puede usar de la lista de algoritmos permitidos, genera un número aleatorio FRESH con el que inicia el proceso de integridad; y como se lo describió antes, de no soportar ningún UIA se rechaza el modo de seguridad. Luego el SRNC calcula la MAC-I y lo agrega al mensaje de “Security control command” con la clave IK a usar al MS con el objetivo de compararlas con las enviadas al inicio de todo el proceso; calcula la XMAC-I con el UIA escogido y lo compara con el MAC-I recibido, guardando el contador COUNT-I y FRESH.

La MS recibe el mensaje y genera un MAC-I para enviarle de regreso al SRNC, el cual calcula una XMAC-I y lo compara con el MAC-I recibido; y finaliza la comunicación el SRNC con el mensaje de RANAP de “Security mode complete” hacia la red central (CN). Así termina el establecimiento de la conexión para que la MS pueda estar dentro de la red (González A., 2010, págs. 62, 63).

4.4. Algoritmo MILENAGE

Para la realización del cálculo del vector de autenticación se usan cinco funciones, denotadas por f1, f2, f3, f4, f5, y la elección de cualquiera es específica del operador, debido a que solo se usan en las AuC y las tarjetas SIM. Pero para lograr interoperabilidad entre el AuC y las distintas implementaciones del USIM podría requerir un esfuerzo extra; por lo que facilitaría el proceso si se utilizara un algoritmo estándar.

En la tecnología 3G, para evitar el inconveniente, el grupo 3GPP crearon un conjunto de algoritmos de autenticación y generación de claves (AKA) denominado MILENAGE, encaminado hacia los operadores que no desean proveer alguno de su propiedad, ya que el diseño e implementación de algún algoritmo de cifrado es complejo además de costoso y no se encuentra al alcance de todas las operadoras. MILENAGE está basado en el algoritmo de cifrado en bloque Rijndael. Se escogió este algoritmo como base debido a que es un fuerte algoritmo de cifrado; ya que en la época, fue ganador del concurso de AES (Estándar de cifrado avanzado, sucesor del ya caduco DES) por ser un fuerte candidato para adecuarlo al entorno 3GPP, que permite proteger la información sensible de los usuarios. Más adelante describimos su funcionalidad (Niemi V., Nyberg K., 2003, págs. 223-232).

4.4.1. Algoritmo Rijndael

El algoritmo Rijndael es un sistema simétrico de cifrado por bloques, es decir, utiliza la misma clave para el proceso de cifrado y descifrado, operando a nivel de byte con nivel de registros de 32 bits. Su margen de seguridad es un poco complicado de medir, ya que el número de rondas cambia de acuerdo al tamaño de la clave, siempre múltiplo de cuatro bytes, por lo que las longitudes por defecto son de 128 (AES-128), 192 (AES-192) y 256 bits (AES-256). Al igual que la longitud de la clave, hace uso de bloques de información de longitud variables (múltiplo de cuatro bytes), siendo el de 128 bits (16 bytes) el tamaño mínimo.

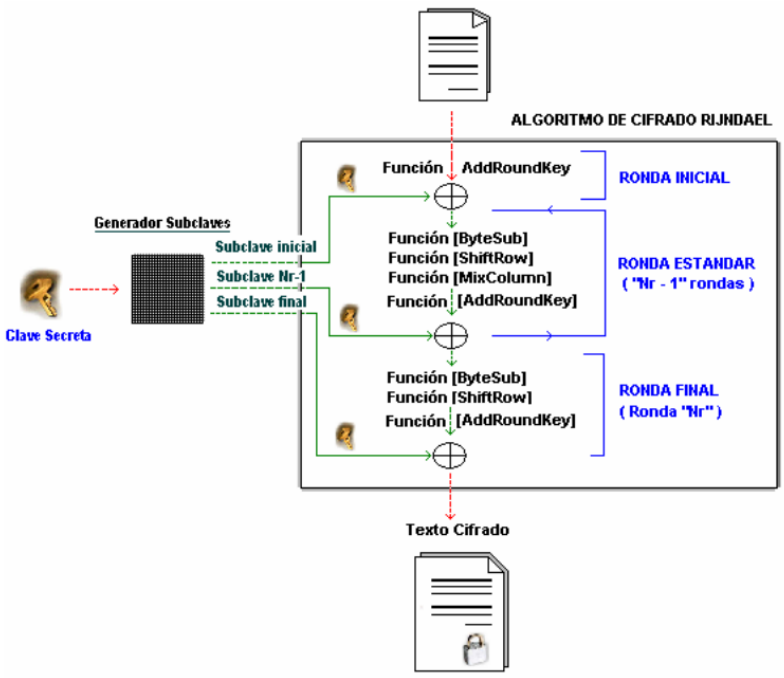


Figura 4.5: Estructura del algoritmo Rijndael

Fuente: (Muñoz A., 2004, pág. 22)

Su estructura está conformada por un conjunto de rondas de cuatro funciones matemáticas diferentes e invertibles aplicadas para producir una información encriptada. Este algoritmo no posee una estructura Feistel, a diferencia de muchos algoritmos simétricos, por lo que puede producir una mayor dispersión de la información cifrada con un número menor de vueltas o de funciones matemáticas; básicamente, trata todos los bits por cada ronda y en cada vuelta les agrega funciones invertibles o capas.

La información que es generada por cada función matemática es solo una respuesta intermedia o Estado, representada por una matriz rectangular de bytes de 4 filas y n columnas, estando n en función del tamaño del bloque usado en bits; asimismo la clave se representa de manera similar al Estado, por una matriz rectangular de 4 filas y m columnas, en función del tamaño de la clave en bits.

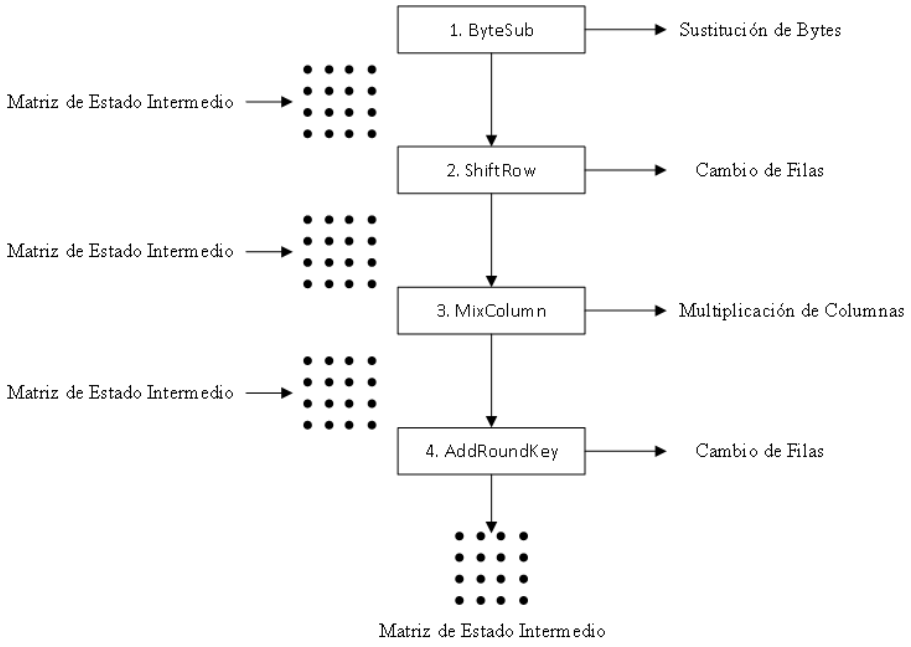


Figura 4.6: Estados del algoritmo Rijndael

Fuente: (Pinzón B., 2011)

Ya establecido los parámetros iniciales, el bloque a cifrar o descifrar se traslada sobre la matriz Estado byte a byte así como los bytes de la clave en la matriz de clave. La matriz de Estado pasa por cuatro procesos por ronda, las cuales son:

Función ByteSub, consiste en una sustitución no lineal que es aplicado a cada byte de la matriz de Estado, generando un nuevo byte.

Función ShiftRow y MixColum, que permiten una alta difusión de la información por las diferentes iteraciones. La función ShiftRow rota

a la izquierda los bytes de las filas de la matriz Estado de la transformación anterior; mientras que la función MixColum mezcla los bytes de una misma columna de la misma matriz.

Función AddRoundKey, el cual realiza la operación XOR con la subclave de cada ronda, siendo las subclaves la esencia de éste algoritmo, y la matriz de Estado que viene del proceso anterior (Muñoz A., 2004).

El bloque resultante de estos tres procesos, es la nueva matriz de Estado o bloque de salida, si se encuentra en la última iteración. La seguridad del algoritmo solo depende de la clave utilizada, que usa diferentes subclaves para el cifrado y descifrado, dependiendo únicamente de la clave de usuario. Para generar las claves el procedimiento es igual para el cifrado y descifrado, con la diferencia que en el proceso de descifrado se escogen bytes de la lista de claves desde el final hasta llegar al inicial, es decir, desde la última subclave que se usó para cifrar, es la primera para descifrar. La cita a continuación explica mejor sobre el algoritmo Rijndael comparando con la estructura Feistel:

“Dos vueltas de Rijndael producen una difusión completa, en el sentido de que, cada bit del estado depende de todos los bits de las dos vueltas anteriores, es decir, un cambio en un bit del Estado es similar a cambiar la mitad de los bits del Estado después de dos vueltas. La alta difusión de una vuelta de Rijndael es gracias a su estructura uniforme que opera con todos los bits del Estado. Para cifradores de tipo Feistel, una vuelta sólo opera con la mitad de los bits de estado y una difusión completa se obtiene en el mejor de los casos después de tres vueltas y en la práctica cuatro o más” (Muñoz A., 2004, pág. 41).

Por todos estos factores, este algoritmo fue escogido el algoritmo estándar de la AES y como base a implementarse en el algoritmo MILENAGE para la autenticación y acuerdo de claves: por tener un muy buen desempeño tanto en hardware como en software, requisitos muy bajos de memoria (al no usar la estructura Feistel en el proceso de cifrado) con excelente rendimiento lo hace adecuado para espacios pequeños, y su versión del bloque de 128 bits de clave.

4.4.2. Estructura del algoritmo MILENAGE

Al implementarse el algoritmo escogido por la AES, el algoritmo Rijndael, debe tomarse en consideración que las entradas y salidas de este algoritmo se definen como cadenas de bytes, al igual que la cadena de claves y salida. Es decir, la cadena de 128 bits se lo trata como cadena de bytes tomando los primeros ocho bits como el primer byte, los otros ocho bits como el segundo byte y así sucesivamente.

Su construcción hace uso del algoritmo de cifrado de 128 bits como función de núcleo (Kernel function), además de un campo de configuración adicional, parámetro asignado por el operador. También se recomienda, como función del núcleo, el uso de la AES específica, aunque el operador podría optar por otro tipo de cifrado de bloques, siempre y cuando cumpla con los requerimientos para los parámetros de la interfaz.

El conjunto de algoritmos da a conocer dos opciones principales para la personalización del algoritmo: OP de libre selección, un campo de 128 bits para configuración del algoritmo que es parte de las funciones f1, f1*, f2, f3, f4, f5 y f5*, y la otra opción es la función del núcleo extraíble (removable kernel function) para protección

contra ataques del canal lateral, abriendo una opción de personalización para configurar a su elección.

Su arquitectura es tan flexible, que permite a los operadores definir y gestionar su propio valor para OP, valor que será utilizado en cada módulo USIM de sus suscriptores. Dada su importancia en el proceso de autenticación, 3GPP decidió colocar un valor intermedio no invertible llamándolo OPc, dependiente de cada abonado, almacenando dentro de ella el valor de OP y la clave secreta K (OPc = OP + Ek(OP)), haciendo más difícil a algún atacante deducir el valor de OP aún teniendo un gran número de OPc y claves K. Sin embargo, no será necesario que se guarde éste valor dentro de la tarjeta USIM, ya que si se ve comprometida, el valor de OP aún estaría a salvo y en secreto. Aunque se recomienda que éste valor se mantenga en secreto, el algoritmo MILENAGE está diseñado, de modo tal, que aún sabiendo el valor de OP en el criptoanálisis, la plataforma sigue siendo segura gracias a éste algoritmo; es decir, que el cifrado de la OP proporciona un nivel adicional de seguridad, siendo un obstáculo más en la trayectoria del atacante.

La función del núcleo, la principal fuerza criptográfica de MILENAGE, debe tener un cifrado de bloques robusto de tamaño de

128 bits y de igual longitud para la clave, para satisfacer la asunción de que una fuerte función de encriptación de cifrado de bloque es utilizada como función de núcleo en el conjunto de algoritmos MILENAGE. Para probar su estructura, el grupo 3GPP evaluó la seguridad y la independencia de los modos de funcionamiento del algoritmo con las diferentes funciones (f1-f5*) de forma individual haciendo cumplir que ningún ataque, que tome menos que 2^{128} cálculos, pueda recuperar cualquier información sobre el valor de la clave K o predecir cualquiera de su salidas aún se tenga el conocimiento del valor de RAND, AMF o el valor de OP.

Aunque, luego de algunos criptoanálisis por parte de algunos investigadores (como Courtois y Pieprzyk), las opiniones acerca su tiempo de vida como algoritmo estándar podría reducirse a lo previsto originalmente, debido a su aplicación y el modo de protección contra ataques de canal lateral. Los investigadores hacen uso de sistemas de ecuaciones algebraicas mejor definidas que el bloque de cifrado Rijndael pueda manejar.

Y no solo eso, también se ha podido descubrir (por otros investigadores como Murphy y Robsaw) la relación entre el texto plano, la clave y el texto cifrado por medio de un sistema de

ecuaciones cuadráticas de grado uno o dos, comprometiendo el proceso que utiliza al algoritmo base Rijndael para el conjunto de algoritmos MILENAGE.

Sin embargo, hay varias opiniones en cuanto a la eficiencia de estos ataques y estiman que la complejidad de romper el cifrado AES es tan bajo que, las vulnerabilidades descubiertas no proyectan ninguna amenaza; y que la seguridad teórica de la función de núcleo del conjunto de algoritmos depende más bien de la fortaleza del bloque de cifrados de 128 bits (Nyberg K., 2004, pág. 9).

4.5. Compatibilidad con A3/A8

La red GSM utiliza dos algoritmos relacionados, A3 y A8, para autenticar al suscriptor (A3) y para generar una clave de cifrado (A8). Al igual que las funciones de autenticación UMTS (f1-f5), los algoritmos A3/A8 son específicos de los operadores e implementados en la tarjeta SIM independiente del hardware o la operadora. Esto quiere decir que si un terminal UMTS visita una red que sólo admite la autenticación y cifrado GSM, el terminal debe autenticarse utilizando la interfaz A3/A8 para su conversión (las entradas de f1-f5 para salidas A3/A8) y lo contrario cuando desea entrar

a una red 3G: se utilizan las reglas de conversión para las entradas A3/A8 a las salidas f1-f5.

Estas reglas de conversión también se pueden utilizar junto con los algoritmos MILENAGE para aplicarse en tarjetas SIM GSM, en lugar de confiar en algoritmos propietarios como COMP128, conocido por su nivel inferior en el tema de seguridad, ya que debido a sus deficiencias, la red ha sido víctima de clonación de tarjetas SIM: ésta técnica de clonación SIM consiste en duplicar la identidad del SIM para realizar llamadas o usar algún otro servicio por pagar de la tarjeta clonada. En el auge de la tecnología GSM, debido a las pobres características de seguridad, la copia de los datos del usuario era más común de lo que es actualmente. Ahora que la propia tarjeta SIM realiza operaciones de seguridad de sus datos y tiene protocolos que verifican su legitimidad, la clonación es más difícil de realizarla.

La red GSM como la red UMTS permite únicamente a un usuario SIM acceder a su red, por lo que si en un momento el atacante y el usuario víctima del robo de identidad o clonación tratan de acceder a la red desde distintos lugares, las redes se darán cuenta de la existencia de duplicación de usuario y procederá a deshabilitar la cuenta afectada. Una deficiencia del algoritmo es de tener una clave de 64 bits (10 de ellos están establecidos en

cero, es decir 54 bits de clave) mostrando ser un algoritmo de privacidad más débil de lo que las documentaciones hablan de él (Gutérrez J., 2003).

El algoritmo A3 envía como parámetro de entrada el número aleatorio RAND (desafío de 128 bits) que da como respuesta el parámetro para la autenticación SRES (64 bits de longitud) con ayuda de una clave Ki de 128 bits para enviarla al VLR. El otro algoritmo (A8), que se encuentra dentro del módulo de identidad del usuario, toma el parámetro de entrada y con la clave Ki produce una clave nueva Kc de 64 bits. Se necesita de tres parámetros para la conversión: RAND, SRES y Kc. El sistema GSM también usa este algoritmo para la autenticación y generación de claves de cifrado, y al no ser un algoritmo estándar, los operadores son libres de elegirlo y desarrollarlo a su manera. Cuando un usuario GSM se encuentra conectado a la UTRAN, su autenticación es por la tarjeta SIM, por lo que las claves de cifrado e integridad CK e IK (de UMTS) de 128 bits son originados de la clave de cifrado Kc de GSM usando algunas conversiones.

En resumen, el algoritmo A3 se utiliza para la autenticación del usuario a la red mientras que el otro algoritmo A8 se usa para generar la clave de sesión Kc y la clave SRES. Estos parámetros van hacia la red con la que se quiere autenticar después de que dicha red haya enviado el desafío para el reconocimiento del usuario. Después de su autenticación por parte del

usuario, puede ordenar al móvil comenzar la encriptación usando la clave de sesión Kc para tener una transferencia de voz y datos segura.

La clave Ki se establece de antemano entre el SIM y el AuC y es almacenada en la tarjeta SIM; para después que el AuC genere un vector de autenticación, con ayuda de la clave compartida Ki. Este vector de autenticación, que es descargado en un servidor, guarda dentro de ella un número de desafío RAND, un resultado SRES esperado y una clave de sesión Kc para el cifrado. Dentro del servidor se crea una solicitud de autenticación con el desafío RAND para ser entregada al cliente; lo que él

produce una respuesta de autenticación SRES con el Ki y el RAND y enviada de vuelta al servidor. Se compara, en el servidor, la respuesta de autenticación SRES con la respuesta esperada; y si el resultado de la comparación es exitoso quiere decir que el usuario se ha autenticado satisfactoriamente. Sin olvidar que la clave de la sesión Kc es usado para la protección más estricta entre el cliente y el servidor (Wallis B., 2008, págs. 4, 5).

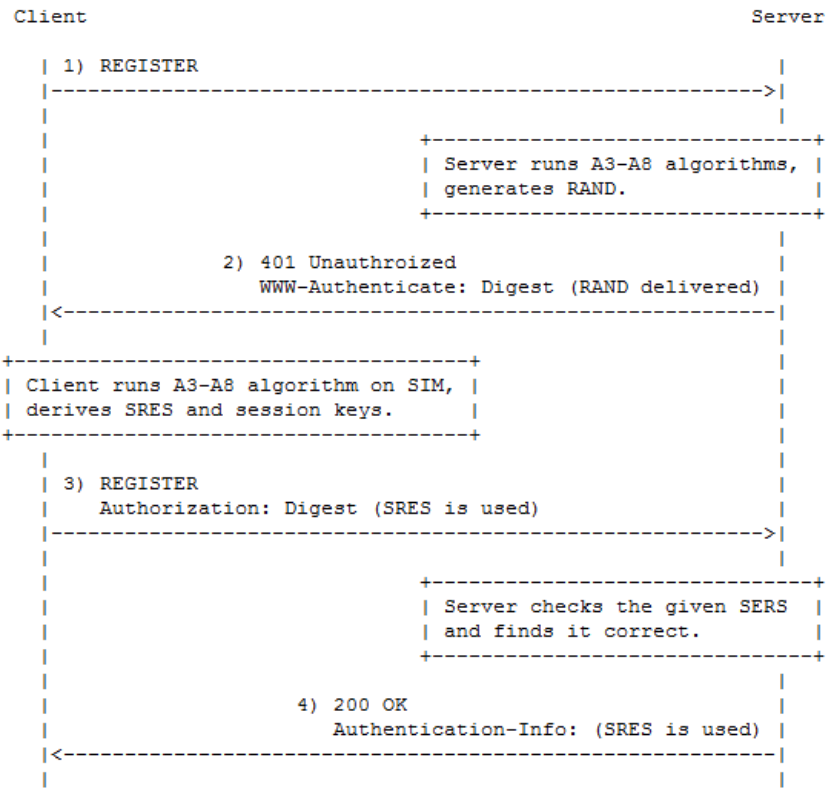


Figura 4.7: Comunicación entre el Cliente y Servidor para una autenticación exitosa

Fuente: (Wallis B., 2008, pág. 7)

En la figura 4.7 describe un flujo de mensajes que describe un proceso de los algoritmos A3-A8 en la autenticación de una solicitud SIP, es decir, la solicitud de REGISTRO SIP detallado en párrafos anteriores.

El sistema de seguridad de GSM constituyó un punto de partida para el desarrollo de las funciones de seguridad de las generaciones siguientes. Su objetivo inicial fue el de garantizar la correcta facturación de las llamadas telefónicas utilizando diversos mecanismos de autenticación seguros, ya sea por medio de la clave secreta almacenada en el SIM o protegiendo el enlace por dónde va el mensaje y proteger la autenticación del abonado.

Con ésta revisión general se puede concluir que la red GSM tiene muchas fallas en el tema de seguridad, siendo una debilidad que puede ser ventajoso para ser utilizado por algún atacante externo a ella que desee causar daño al usuario o la red misma. Una de ellas es el misterio en la arquitectura de los algoritmos criptográficos, además de tener una débil protección de la integridad de los datos sobre la interfaz aérea.

Por tal motivo, fue de vital importancia mejorar la seguridad de extremo a extremo para satisfacer con la necesidad de tener un sistema que vaya acorde con la demanda mundial de servicios móviles rápidos. Sin embargo,

no hay que olvidar que el sistema GSM fue el punto de partida para el desarrollo de las funciones de seguridad, de futuras aplicaciones y tecnologías para tecnologías de tercera generación como lo es UMTS y sus posteriores.

En un principio era relativamente fácil hacerse pasar por un usuario legítimo de la red GSM si no se aplica algún mecanismo de autenticación; y en el caso de este sistema se innovó en una tarjeta SIM en el que, dentro de ella, se realiza la autenticación del abonado para poder entrar a la red y poder utilizar sus servicios dentro de ella. Aunque si funciona este tipo de autentificación en la práctica, el sistema de seguridad GSM está lejos de ser perfecto, debido a que la arquitectura de seguridad es demasiado simple para satisfacer las crecientes necesidades de los diferentes servicios que ofrece y desarrolla. Además, en el momento de desarrollo de dichas aplicaciones de seguridad (ya hace algunos años atrás) no estaban previsibles algunos ataques en contra de la red como falsas BS, avanzadas herramientas de criptoanálisis para el ataque, entre otras más.

En cambio en las redes UMTS, por medio de algoritmos criptográficos se protege la autenticación del abonado, aparte de la autenticación en la tarjeta SIM antes mencionada. Es decir, se adoptó la misma arquitectura básica de los sistemas celulares de segunda generación, pero se realizaron varias

mejoras y cambios a la misma con el fin de satisfacer las exigencias de los sistemas de telecomunicaciones nuevas, para asegurar no sólo la comunicación de voz, sino también una creciente variedad de otros servicios.

Por estos antecedentes, UMTS es una ya una tecnología que se encuentra posicionada, contando con millones de usuarios a nivel mundial y continúa en aumento, además de poseer una gran cantidad de equipos para su operación, está evolucionando, desarrollándose y muchas compañías proveedoras de servicios móviles siguen impulsándola, mejorando sus protocolos de seguridad y ofreciendo un mejor servicio a sus usuarios.

CAPÍTULO 5

DESARROLLO DE LA APLICACIÓN WEB

5.1. Introducción

Para el diseño de la herramienta didáctica se ha utilizado una aplicación web, un medio por el que cualquier usuario con acceso a internet puede acceder, además de ser netamente dinámica explicando detalladamente algunos temas de la seguridad en UMTS y el proceso en el cual se genera cada uno de los temas a tratar.

Una de las ventajas de presentar una aplicación web es que los estudiantes podrán tener un extenso material, además de la visualización de los diferentes temas en lo que se refiere a la seguridad en redes UMTS, sus

procesos de autenticación, arquitectura, información sobre las redes precedentes a ella, historia y evolución de las redes móviles hacia la tercera generación 3G.

El sistema se llama “LUS”, acrónimo de “Learning UMTS Security” (Aprendizaje de la seguridad UMTS), dirigido a los estudiantes, para que puedan interactuar con la aplicación y al mismo tiempo tener un contenido de explicación. Uno de los atributos de la aplicación web en comparación con un video es su contenido y el modo de visualización, como el de seleccionar el tema a su preferencia, la lectura del tema en particular al ritmo deseado, además de tener un diseño amigable con el usuario.

En “LUS” los visitantes se pueden registrar, leer el contenido del sistema, realizar pequeñas revisiones del capítulo si desean llamadas “Lecciones”, observar su puntuación de las lecciones, enviar sugerencias para hacer de la aplicación un sistema más interactivo y con variedad de opciones al gusto de los usuarios en la opción del menú “Acerca de”.

En la aplicación se ha utilizado herramientas de programación web robustas además de flexibles detalladas a continuación.

Para la programación en el servidor hemos utilizado Python, ya que existe un registro de usuarios, formularios en las revisiones y manejo de base de datos.

5.2. Lenguaje de Programación:

Python es un lenguaje de programación flexible, de fácil entendimiento y multiparadigma, es decir, no obliga a los programadores a adoptar un estilo particular de programación, permite varios estilos: programación orientada a objetos, programación imperativa y programación funcional.

Python es un lenguaje de programación creado por Guido van Rossum a principios de los años 90 cuyo nombre está inspirado en el grupo de cómicos ingleses “Monty Python”.

Figura 5.1: Logo del lenguaje de programación Python

Fuente: (Python Software Foundation, 2001 - 2014)

Python es una herramienta tan poderosa que puedes usar en desarrollo web, para escribir interfaces gráficas de usuario (GUI) de escritorio, crear

juegos relativamente con gran facilidad y claridad de código (Aguilar L., 1996).

Una característica importante de Python es la resolución dinámica de nombres; es decir, lo que enlaza un método y un nombre de variable durante la ejecución del programa.

Otro objetivo del diseño del lenguaje es la facilidad de extensión. Python puede incluirse en aplicaciones que necesitan una interfaz programable.

Las siguientes características de Python son:

- Alto nivel, es decir que leer y escribir código en Python es realmente fácil y de sencillo aprendizaje.
- Lenguaje interpretado: Un lenguaje interpretado o de script es aquel que se ejecuta utilizando un programa intermedio llamado intérprete, en lugar de compilar el código a lenguaje máquina que pueda comprender y ejecutar directamente una computadora lo que generalmente hacen los lenguajes compilados.

  La ventaja de los lenguajes compilados es que su ejecución es más rápida ya que se ejecutan directamente. Sin embargo los lenguajes interpretados son más flexibles y más portables, ya que sólo se

necesita tener instalado el intérprete y cualquier programa en Python podría ejecutarse.

Python tiene, no obstante, muchas de las características de los lenguajes compilados, por lo que se podría decir que es semi interpretado. En Python, el código se traduce a un pseudo código máquina intermedio llamado bytecode la primera vez que se ejecuta, esto genera archivos .pyc o .pyo (bytecode optimizado), estos son los que se ejecutarán en sucesivas ocasiones por eso se lo llama semi interpretado.

- Orientado a objetos: La orientación a objetos es un paradigma de programación en el que los conceptos del mundo real relevantes para nuestro problema se trasladan a clases y objetos en nuestro programa. La ejecución del programa consiste en una serie de interacciones entre los objetos.

  Python también permite la programación imperativa, programación funcional y programación orientada a aspectos.

- Fuertemente Tipado: Las variables se la declaran de un solo tipo y no se puede cambiar su tipo durante la ejecución al menos que se haga una conversión, es necesario declarar de forma explícita dicha

variable al nuevo tipo previamente. Es decir, si tenemos una variable que contiene un texto (variable de tipo cadena) no podremos tratarla como un número o como otro tipo cualquiera que sea sin antes cambiarla de tipo. En otros lenguajes el tipo de la variable cambiaría para adaptarse al comportamiento esperado, aunque esto es más propenso a errores.

- Multiplataforma: Python está disponible en multitud de plataformas (UNIX, Solaris, Linux, DOS, Windows, OS/2, Mac OS, etc.), por lo que si no utilizamos librerías externas específicas de cada plataforma nuestro programa podrá correr en todos estos sistemas sin grandes cambios (González R., 2007).

5.3. Framework

Para la creación de una aplicación web de manera fácil, ordenada y segura generalmente los programadores utilizamos herramientas de desarrollo para no tener que volver a “reinventar la rueda”, es decir no tener que volver a escribir funciones para tareas de sistemas ya creadas. Para esto utilizaremos un framework web.

Un framework es una plataforma para el desarrollo de aplicaciones de software. Proporciona una base estructurada sobre la que los

desarrolladores de software pueden crear programas. Por ejemplo, un “framework” puede incluir clases predefinidas y funciones que se pueden usar para procesar la entrada, gestionar los dispositivos de hardware, interactuar con el software del sistema, trabajar con las peticiones web, en caso de una aplicación web, manejar sesiones, y muchos otros procedimientos más lo que simplificaría el proceso de desarrollo en gran medida.

La principal función de los frameworks web, es aliviar el exceso de funciones y procedimientos ya definidos que se asocian con actividades comunes usadas en desarrollos web como las descritas anteriormente.

Existen el mercado una variedad de frameworks web para Python y para otros lenguajes de programación, se ha escogido Django Framework por su facilidad y gran alcance en aplicaciones web.

5.4. Django

De acuerdo su página web, Django es un framework web Python de alto nivel que fomenta el rápido desarrollo, un diseño limpio y pragmático, debido a que tiene un núcleo bastante robusto con múltiples librerías que ahorran de manera significativa el trabajo.

“Django fue desarrollado por una operación en línea-noticias, lo cual fue diseñado para manejar dos retos: los plazos intensivos de una sala de redacción y los estrictos requisitos de los desarrolladores web con experiencia que lo escribieron. Permite construir de alto rendimiento, aplicaciones web elegantes rápidamente” (Django Software Foundation, 2005 - 2014).

Figura 5.29: Logo del Framework web Django

Fuente: (Django Software Foundation, 2005 - 2014)

El objetivo principal de Django es facilitar la creación de sitios web complejos, pone énfasis en el re-uso de código, la importación de componentes y conectividad, el desarrollo rápido de código y el principio “no te repitas” (DRY, por sus siglas en inglés “don't repeat yourself”). Python es usado en todas las partes del framework, incluso en configuraciones, archivos, y en los modelos de datos lo que hace más fácil de codificar y configurar.

La distribución principal de Django también permite unir aplicaciones que proporcionan un sistema de comentarios, herramientas para sindicar contenido via RSS, aplicaciones integradas para el manejo de los modelos de la base de datos, "páginas planas" que permiten gestionar páginas de contenido sin necesidad de escribir controladores o vistas para esas páginas, aplicación que gestiona servidor ftp para compartir archivos y un sistema de redirección de URLs muy potente y simplicista.

Otras características de gran importancia de Django son:

- Un mapeador objeto-relacional para el manejo de la base de datos.
- Una API de base de datos robusta, la cual permite de manera sencilla realizar consultas a la base de datos sin necesidad de aprender el lenguaje o el comportamiento de la base de datos que se esté usando, si es que la base de datos esta soportada en esta API.
- Un sistema incorporado de "vistas genéricas" que ahorra tener que escribir la lógica de ciertas tareas comunes ahorrando tiempo y esfuerzo.
- Un sistema extensible de plantillas basado en etiquetas, con herencia de plantillas, lo que le da una gran ventaja al no tener que reescribir código.
- Un despachador de URLs basado en expresiones regulares.

- Un sistema "middleware", aplicaciones intermedias, para desarrollar características adicionales; por ejemplo, la distribución principal de Django incluye componentes middleware que proporcionan cacheo, protección CSRF, soporte de sesiones, etc.
- Soporte de internacionalización, incluyendo traducciones incorporadas de la interfaz de administración y en los mensajes de errores de programación.
- Documentación incorporada accesible a través de la aplicación administrativa, además de documentación versionada en la web que se puede acceder a través de su página web.
- Django soporta múltiples bases de datos pero como recomendada es PostgreSQL, también son soportadas MySQL, SQLite 3 y Oracle. Se encuentra en desarrollo un adaptador para Microsoft SQL Server para Python. Una vez creados los “modelos”, Django proporciona una abstracción de la base de datos a través de su API ORM que permite crear, recuperar, actualizar y borrar objetos. También es posible que el usuario ejecute sus propias consultas SQL directamente mediante funciones de conexión a la base. En el modelo de datos de Django, una clase representa un registro de una tabla en la base de datos y

las instancias de esta serán las filas en la tabla (Django Software Foundation, 2005 - 2014).

5.5. Base de Datos

PostgreSQL es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia de software libre BSD (Berkeley Software Distribution), con menos restricciones, y con su código fuente disponible libremente. Sistema de gestión de bases de datos de código abierto más potente del emporio, y sus últimas versiones no poseen comparación a otras bases de datos comerciales en cuanto a eficiencia (Martinez R., 2009 - 2013).

Figura305.3: Logo del administrador de base de datos PostgreSQL

Fuente: (PosgreSQL-es, 1996 - 2014)

PostgreSQL utiliza un modelo cliente/servidor, el cual el servidor está en espera a alguna petición del cliente , además de usar multiprocesos en vez de multihilos para asegurar la estabilidad del sistema; es decir, un fallo en

uno de los procesos no afectará el resto y el sistema continuará funcionando normalmente.

Postgres es un sistema de base de datos muy potente y versátil que maneja una gran cantidad de datos para poder distribuirlos en diferentes instancias de base, como por ejemplo, Postgres usa "foreign tables" (tablas extranjeras), tiene la facilidad de acceder a una base de datos distinta de la que se encuentra, dándole una gran ventaja para mantener los datos distribuidos.

A continuación se muestra la figura 5.4 donde se muestra el funcionamiento de postgres:

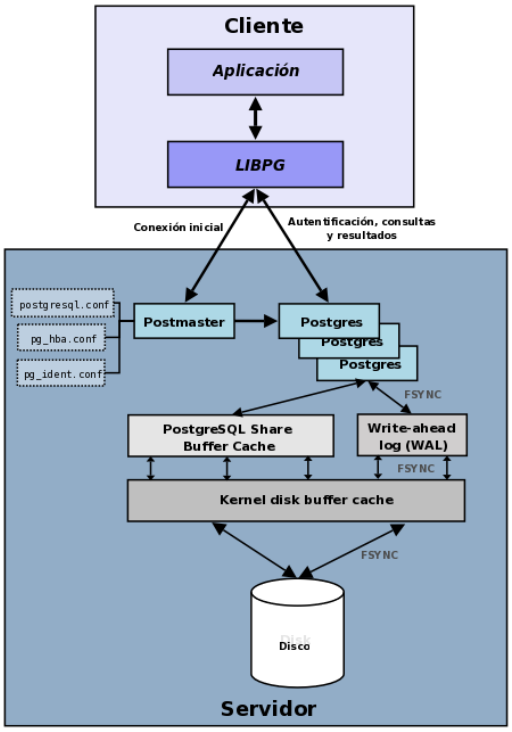


Figura 5.4: Arquitectura de Postgres

Fuente: (Martinez R., 2009 - 2013)

La aplicación cliente es un software que se utiliza para la conexión con PostgreSQL como administrador de bases de datos. La conexión puede ser vía TCP/IP o en sockets locales.

El postmasters un proceso principal del motor de base de datos PostgreSQL encargado de escuchar por un puerto/socket conexiones entrantes de clientes y se encarga de manejarlas. También crea los procesos hijos que

se encargaran de autenticar estas peticiones, gestionar las consultas y mandar los resultados a las aplicaciones clientes.

Los ficheros de configuración son tres ficheros principales de configuración que utiliza PostgreSQL los cuales son:

- postgresql.conf,
- pg_hba.conf y
- pg_ident.conf

Dichos archivos de configuración permiten brindar seguridad a Postgres, como bloquear ip's, permitiendo solo las ip's que se haya ingresado, y muchas otras opciones para hacer de la aplicación más segura.

Existen también los llamados "procesos hijos" que son los que se encargan de autenticar a los clientes, gestionar consultas y mandar los resultados a las aplicaciones a los clientes.

La memoria compartida usada por PostgreSQL, PostgreSQL share buffer cache, sirve para almacenar datos en memoria caché de rápido acceso.

El WAL (Write-Ahead Log), componente del sistema encargado en la integridad de los datos (recuperación de tipo REDO).

El Kernel disk buffer cache, es simplemente la memoria caché del disco del sistema operativo.

El disco, elemento físico del servidor donde se almacenan los datos y toda la información necesaria para que PostgreSQL funcione de la forma correcta.

La última serie de producción del sistema es la 9.3 y, debido a sus características técnicas la hacen una de las bases de datos más potentes y robustos del mercado, incluso comparada en cierta parte a la base de datos consolidada Oracle. Su desarrollo comenzó hace más de 16 años, y durante ese tiempo, la estabilidad, potencia, robustez, facilidad de administración e implementación de estándares han sido características que han impulsado su creciente desarrollo. PostgreSQL funciona muy bien con grandes cantidades de datos y con una alta concurrencia de usuarios accediendo a la vez al sistema. Algunas características de postgreSQL son:

Una base de datos 100% ACID (Atomicity, Consistency, Isolation and Durability), un grupo de rasgos para de esta manera una secuencia de instrucciones sean consideradas como una sucesión:

- La primera sigla significa Atomicidad, es una de las peculiaridades de postgreSQL, asegurando la operación sea exitosa al realizarla o no, y

por lo tanto ante un fallo del sistema no pueden existir transacciones o sucesiones a medias.

- La palabra Consistencia (de la sigla C) se refiere a que PostgraSQL garantiza que sólo se empieza aquello que se puede terminar, por lo que se ejecutan aquellas operaciones que no van a romper las reglas y directrices de integridad de la base de datos.
- Aislamiento significa que postgreSQL asegura que una operación no puede afectar a otros procesos corriendo en paralelo, logrando que la realización de dos transacciones sobre la misma información sea transparente.
- La última sigla significa Durabilidad, propiedad que confirma que una vez realizada una transacción, ésta persistirá y los datos sobrevivirán en todo el procedimiento.

5.5.1. Integridad referencial

Para la protección de la integridad se usa Tablespace, una unidad lógica que denota el espacio de almacenamiento de datos dentro de una base de datos constituidos por uno o más archivos de datos Datafiles. Además es un fichero físico en el disco, un nombre que posee un grupo de propiedades de almacenamiento que se aplican

a los objetos (tablas, secuencias, entre otras) creadas en la base de datos bajo el Tablespace indicado (tablas, secuencias, etc.).

Transacciones anidadas, es una transacción de base de datos que se inicia con una instrucción en el marco de una operación o transacción ya iniciada sin tener la obligación de haber finalizado la anterior.

Streaming Replication - Hot Standby, espera para consultas de solo lectura. Utilizado para conmutación por error de base de datos y balanceo de carga.

2PC (Two-PhaseCommit), algoritmo que permite que los nodos tengan un acuerdo para comprometerse a una transacción, encaminado al caso de fallos en los nodos o en la red.

La recuperación de punto en el tiempo (PITR) es una característica de PostgreSQL, capaz de visualizar una tabla de base de datos, además de sus datos, a pesar de ser una fecha pasada.

Copias de seguridad en caliente (Online/Hot Backups), como su nombre lo indica, realiza una copia de solo lectura de la base de datos mientras se encuentre activa.

Capacidad de guardar en Unicode, estándar de codificación de caracteres creado para optimizar la transmisión y visualización de textos de múltiples lenguajes especificando un identificador numérico por cada carácter.

Multi-VersionConcurrency Control (MVCC), es un método para control de acceso utilizado para proporcionar acceso concurrente a los datos.

Multiples métodos de autentificación, los más utilizados es el MD5.

Acceso encriptado via SSL y licencia BSD.

PostgreSQL se encuentra disponible para Linux y UNIX en todas sus variantes (AIX, BSD, HP-UX, SGI IRIX, Mac OS X, Solaris, Tru64) y Windows 32/64bit.

Funciones/procedimientos almacenados en numerosos lenguajes de programación, entre otros PL/pgSQL, PL/Perl, PL/Python y PL/Tcl.

Bloques anónimos de código de procedimientos (sentencias DO).

Numerosos tipos de datos y posibilidad de definir nuevos tipos. Además de los tipos estándares en cualquier base de datos,

tenemos disponibles, entre otros, tipos geométricos, de direcciones de red, de cadenas binarias, UUID, XML, matrices, etc

Soporta el almacenamiento de objetos binarios grandes (gráficos, videos, sonido)

APIs para programar en C/C++, Java, .Net, Perl, Python, Ruby, Tcl, ODBC, PHP, Lisp, Scheme, Qt y muchos otros.

Todas éstas características dan mucha libertad a los programadores, en el momento de realizar su trabajo y realizarla de una manera más personalizada de acuerdo con las exigencias del cliente.

5.6. Análisis del sistema

El sistema descrito en este documento es una herramienta didáctica que permite a los usuarios registrarse en el sistema y seguir un curso interactivo en línea orientado a la seguridad en UMTS. Haciendo que el aprendizaje de los usuarios sea mediante una herramienta en la que la mayoría pueda acceder y esta es mediante una página web. Existen algunas limitaciones del sistema por cuestiones de tiempo, ya que se le podrían agregar más funcionalidades como videos, foros y herramientas para que los usuarios aprendan con más facilidad.

5.7. Requisitos funcionales:

- El usuario se podrá registrar en el sistema mediante datos básicos un usuario, correo y una contraseña con la que pueda ingresar al sistema.
- El usuario va a poder elegir libremente los temas a estudiar en la sección de capítulos donde va a encontrar todo el contenido del curso.
- El usuario va a tener la oportunidad de probar sus conocimientos mediante un módulo de lecciones donde se le evaluará, con la finalidad de reforzar su aprendizaje.
- Brindar un módulo donde el usuario tendrá acceso directo a contenido gratuito online donde pueda leer más sobre el tema a tratar.

5.8. Requisitos no funcionales

- La disponibilidad del sistema depende de si el usuario tiene o no conexión a internet.
- El sistema al ser web está orientado a que se puede acceder mediante cualquier dispositivo que cuente con un explorador de internet.
- La disponibilidad del sistema dependería de terceros ya que estaría en un hosting alquilado, y se depende de ese proveedor para la disponibilidad.

5.9. Casos de Uso:

En el sistema existen tres tipos de usuarios, el usuario registrado, el usuario sin registrar y el administrador.

El administrador cuenta con las opciones siguientes:

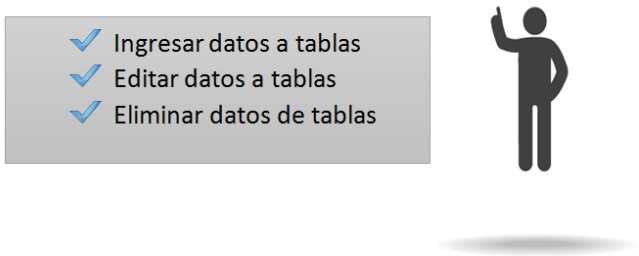


Figura 5.5: Rol del usuario Administrador

Para el rol de administrador se le permite realizar tareas de mantenimiento de las tablas de la base de datos del sistema, además que el administrador del sistema tiene libre acceso, es decir, también tiene permitido las acciones que tiene el rol estudiante. Las acciones del administrador son:

- Ingresar datos en tablas: El administrador del sistema ingresará los datos básicos para que funcione correctamente la aplicación.
- Editar datos en tablas: Para motivos de mantenimiento existe esta función para que cualquier cambio en el contenido sea fácilmente editado.
- Eliminar datos en tablas: Opción que permite al administrador eliminar datos del sistema.

El usuario registrado cuenta con las siguientes funciones:

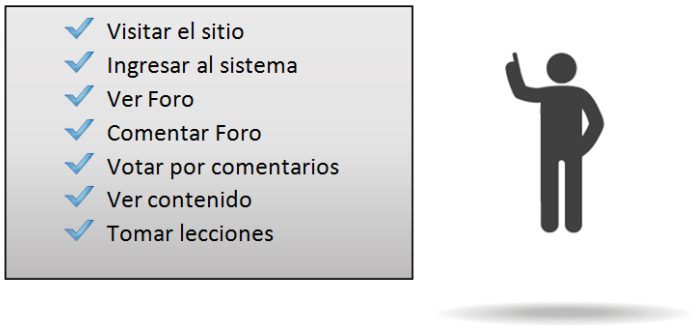


Figura 5.6: Rol del usuario registrado

- Visitar el sitio: Permite visitar el sitio del sistema web.
- Ingresar al sistema: Permite al usuario ingresar al sistema y poder acceder al contenido en línea.
- Ver Foro: Permite al usuario revisar el foro que se encuentra alojado en el sitio.
- Comentar foro: Permite al usuario comentar cualquier foro que desee.
- Votar por comentarios: Permite al usuario votar por la respuesta más acertada según su criterio en el foro.
- Ver contenido: Se refiere a todo el contenido que pueda acceder desde el sistema.

- Tomar lecciones: Permite al usuario autoevaluarse e ir conociendo como va su avance con lo aprendido en el sistema.

El usuario no registrado cuenta con las siguientes funciones:

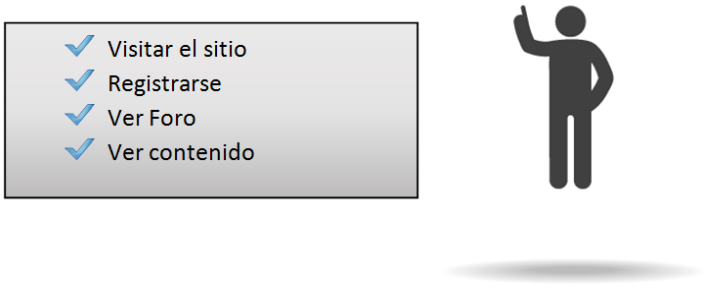


Figura 5.7: Rol del usuario no registrado

- Visitar el sitio: Permite visitar el sitio del sistema web.
- Registrase: Permite al usuario registrarse en el sistema con sus datos.
- Ver Foro: Permite al usuario revisar el foro que se encuentra alojado en el sitio.
- Comentar foro: Permite al usuario comentar cualquier foro que desee.
- Votar por comentarios: Permite al usuario votar por la respuesta más acertada según su criterio en el foro.
- Ver contenido: Se refiere a todo el contenido que pueda acceder desde el sistema.

5.10. Estructura de la Aplicación Web

LUS está definido bajo la modalidad MVC (modelo, vista, controlador) en Django MVT (“model, view, template”, modelo, vista, plantilla), el cual separa los datos y la lógica de negocio de la interfaz de la aplicación y el módulo encargado de gestionar los eventos y las comunicaciones entre los usuarios. Este método es muy efectivo en sistemas de gran tamaño y alcance y mantiene una estructura ordenada de la aplicación.

Principalmente el proyecto se encuentra dividido en cuatro pequeños paquetes o módulos, las cuales son administración: “administrador”, “lus”, “módulos” y “librerías”.

En el módulo de “administración” se encuentra todo lo relacionado a mantenimiento de la información de la aplicación, lo referente a mantenimiento de las tablas de la base de datos. Se usa una herramienta de Django la cual, con solo darle algunos parámetros da directamente la administración de las tablas de la base de dato, además aquí de definir algunas constantes del sistema, las cuales se van a utilizar en todo el código del sistema.

En el módulo LUS, aquí se definen los parámetros de configuración del sistema, por ejemplo el usuario y contraseña de la base de datos, se insertan

las aplicaciones que van a ser usadas en el sistema, la configuración del correo electrónico, si se desean enviar correos a los usuarios, zona horaria. Se pueden configurar algunos parámetros de seguridad, como es el dominio que va a escuchar la aplicación, se activan algunos módulos de Django para la seguridad como por ejemplo en “CsrfViewMiddleware”, que es el que nos protege contra los ataques CSRF (“Cross-site request forgery”) la explicación detallada de este tipo de ataques lo podemos encontrar en su página web oficial. En resumen este módulo es para configuraciones generales del servidor, de seguridad y de conexiones del sistema (Creative Commons 3.0 License, 2014).

El otro “módulo”, llamado así ya que se crean las funciones principales del sistema, en éste módulo se crean las funciones de escucha de peticiones de usuario, por ejemplo cuando el usuario haga una petición de algún recurso del sistema como por ejemplo cuando desee ingresar a leer un capítulo o simplemente ingresar al sistema. Maneja la completa interacción entre el usuario y el sistema y es el encargado de ofrecer al usuario todos los recursos requeridos, ayudándose de los módulos restantes.

El módulo librerías se tiene una serie de funciones internas que ayudan a los módulos principales del sistema, aquí es donde alojan los paquetes de procesos que facilitan la lectura del código en los módulos. Estas funciones

hacen el código más legible al programador además ayuda a la reutilización de código y agiliza los cambios que se le quiera hacer al sistema en un futuro, ya que sólo se harían cambios a dichas funciones y no a la estructura de código en nuestro programa.

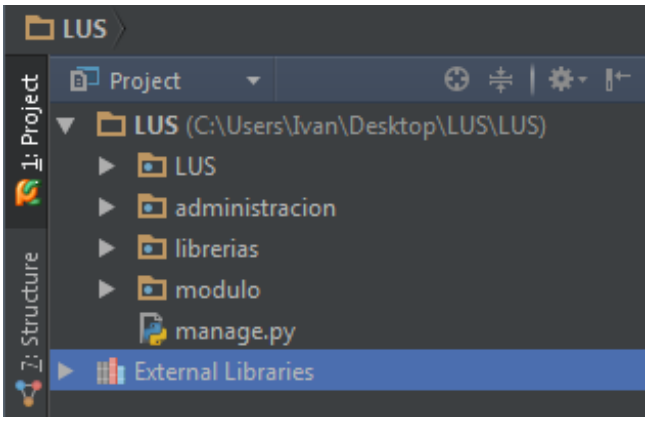


Figura 5.8: Estructura de LUS

5.10.1. Estructura de los módulos

Cada uno de los módulos a excepción del módulo “LUS” posee los siguientes archivos en común los cuales son models.py, urls.py, views.py.

En el archivo models.py encontramos la declaración de clases de objetos, las cuales representan tablas en la base de datos.

En el archivo urls.py contiene como dice su nombre las URL (“uniform resource locator”, localizador uniforme de recursos), las cuales son direcciones lógicas que apuntan a recursos del sistema.

El archivo views.py se encuentran las “vistas” o “controladores”, según el modelo vista controlador, ya explicado con anterioridad.

5.11. Diseño del sistema:

El diseño de nuestro sistema está enfocado a ser de fácil uso para el usuario, hemos tomado como referencia algunos sistemas online de cursos para tener una idea más clara de cómo mostrar nuestra idea.

La figura 5.10.1 muestra la pantalla principal del sistema, la cual vemos un menú principal, un banner, y un explicativo de lo que hace nuestro pequeño sistema.

Figura 5.9: Pantalla principal del sistema

En la figura 5.9 se puede observar algunas opciones como son: inicio, contenido, lecciones, foro, acerca de descritos con más detalle adelante:

En la opción de iniciar sesión es para que los usuarios registrados puedan ingresar al sistema, y así poder acceder a las opciones que son solo para usuarios registrados, las cuales son lecciones, comentar foro y votar en foro.

Figura 5.10: Pantalla de Ingreso al sistema

En la opción de registro, sirve para que los nuevos usuarios se puedan registrar al sistema, llenando un pequeño formulario con datos básicos del usuario, como un nombre, un apellido, sexo, usuario, contraseña y un correo electrónico.

Así quedarán registrados en el sistema y podrán acceder a las opciones de los usuarios registrados.

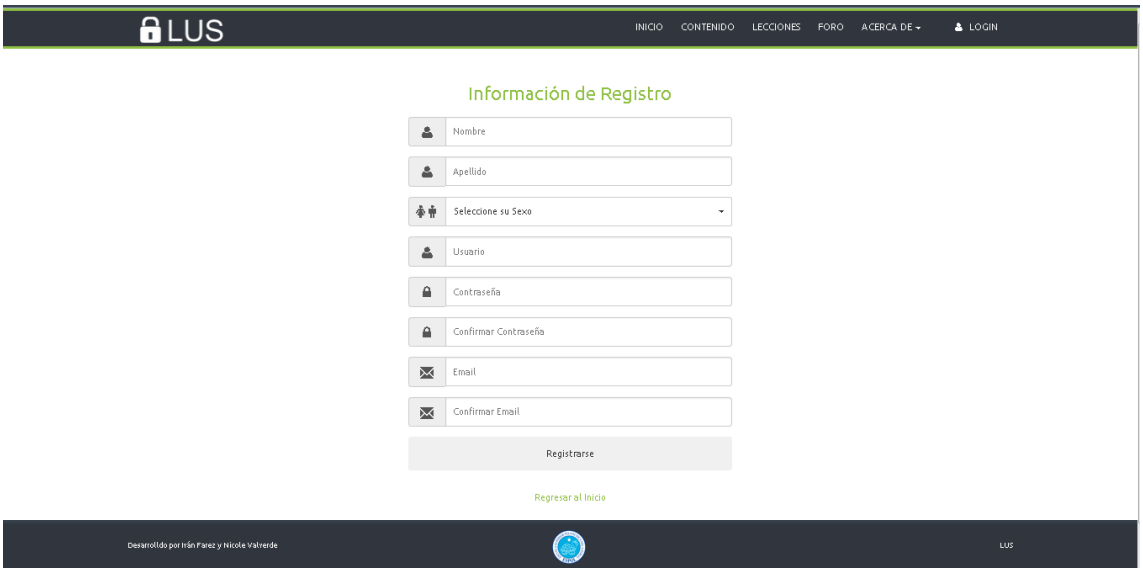


Figura 5.11: Pantalla de registro al sistema

En el menú se encuentra la pestaña de contenido donde se obtendrá todo el material del curso en línea separado por capítulos para que las personas elijan que temas en específico quieren aprender.

La opción de lecciones podrán obtener la lista de las lecciones que tenemos y la podrán tomar todos los usuarios que se encuentren registrados en el sistema.

En la figura 5.12 se puede observar la lista de las lecciones que tiene el sistema, se puede entrar a cada lección con solo dar clic en la opción “Tomar Lección” en la parte inferior izquierda de cada lección.

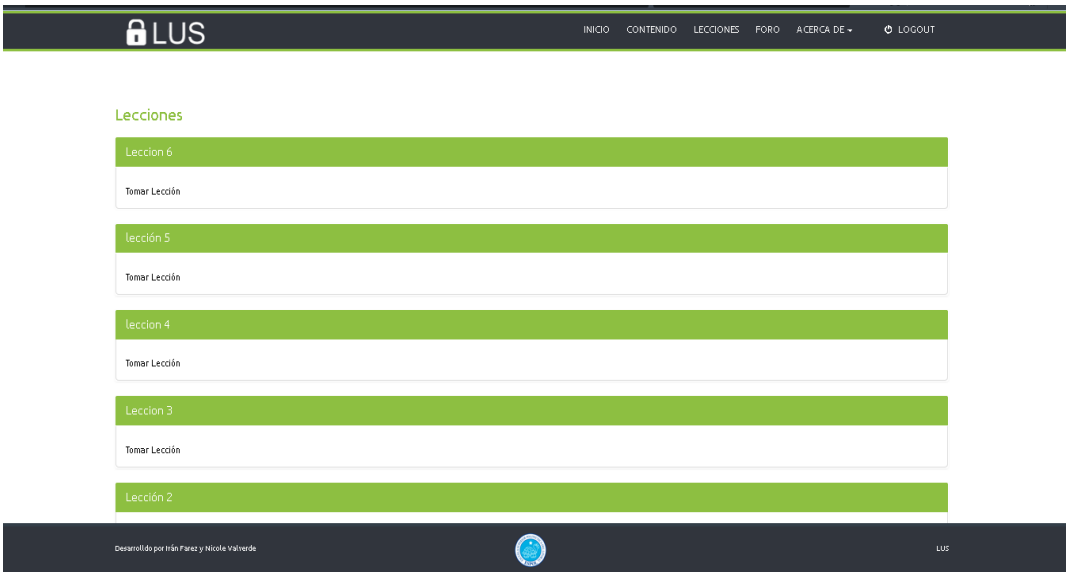


Figura 5.12: Pantalla de la lista de lecciones

En la figura 5.13 se puede observar como es la mecánica de la lección, preguntas objetivas, es decir, solo hay que seleccionar la o las respuestas correctas en cada pregunta, haciéndole más fácil responder a la lección.

Cada usuario pude tomar estas lecciones sin límite de tiempo, para no forjar presiones en los usuarios, solo pueden ir tomar la lección sin preocuparse por el tiempo.

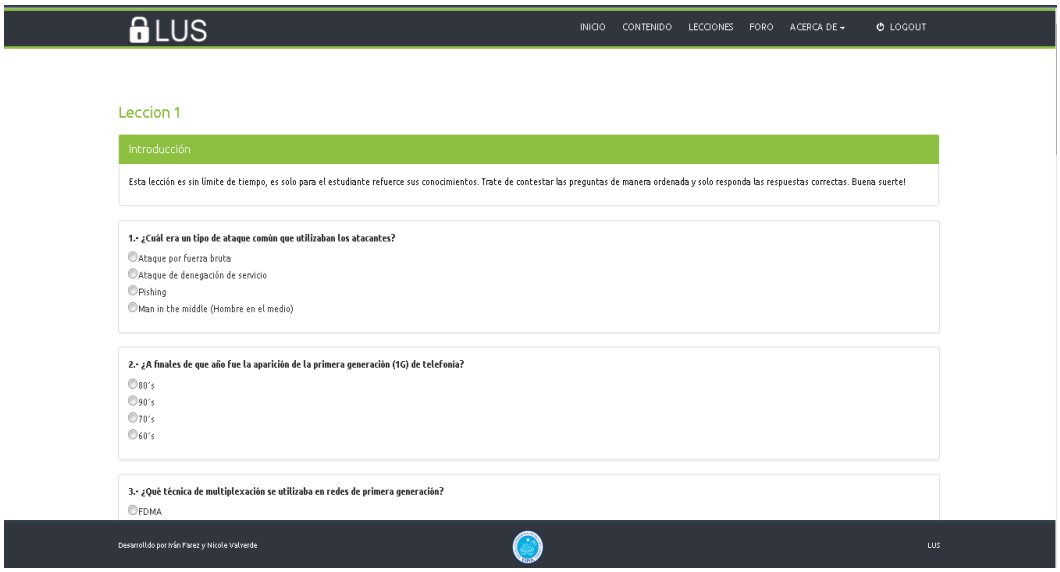


Figura 5.13: Pantalla de lección del sistema

En la figura 5.14 se muestra que cuando algún usuario haya terminado con su lección podrá revisar sus aciertos y fallos en la lección así como unas tablas de resultados.

Se le mostrará en cada pregunta correcta un ícono con un visto, y si esta errada se le mostrará un ícono de error, si es el caso de que no contestó o contestó mal una pregunta le saldrá un aviso de cuál era la respuesta correcta.

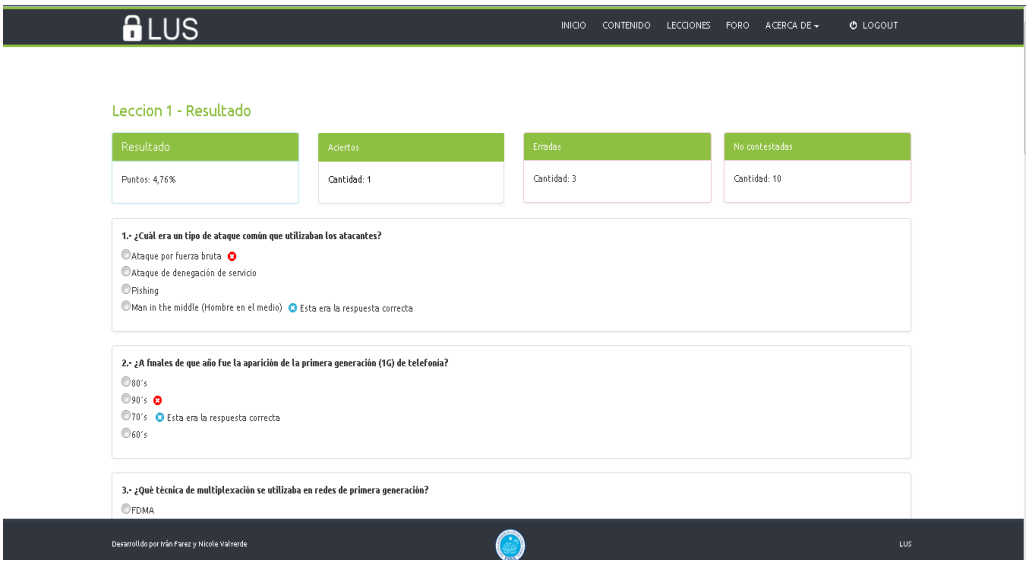


Figura 5.14: Lección calificada por el sistema

En la opción de Foro se encuentran los temas que los usuarios hayan subido al sistema y que sean de interés para los demás usuarios. Como se ve en la figura 5.15, presenta una lista de todos los artículos subidos al foro, paginados para que no le salga una lista extensa.

Se podrá ingresar a revisar el foro tan solo dando clic en el enlace de “Ver más”, se ingresará a la pantalla del foro, si es un usuario registrado, entonces podrá comentar y dar votos a otros usuarios que hayan comentado, caso contrario solo podrá observar el foro.

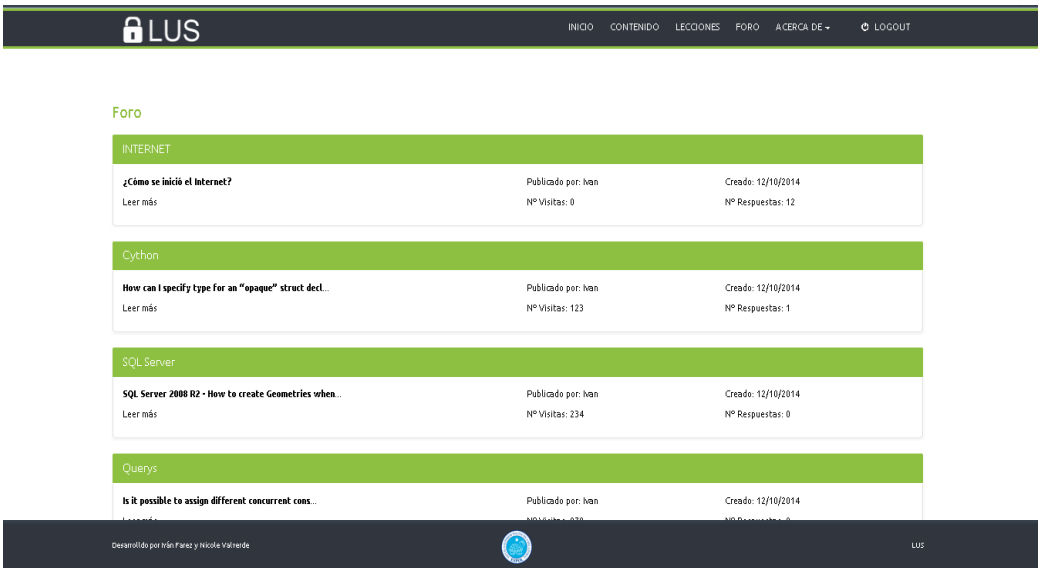


Figura 5.15: Página principal del Foro

Como se muestra en la figura 5.16 se tiene el artículo a tratar en el foro, la pregunta de un usuario, los comentarios del mismo y se ha añadido la opción de comentar en el foro, así como también la opción de dar su voto a dicho comentario. Para hacerlo más dinámica y amigable con el usuario.

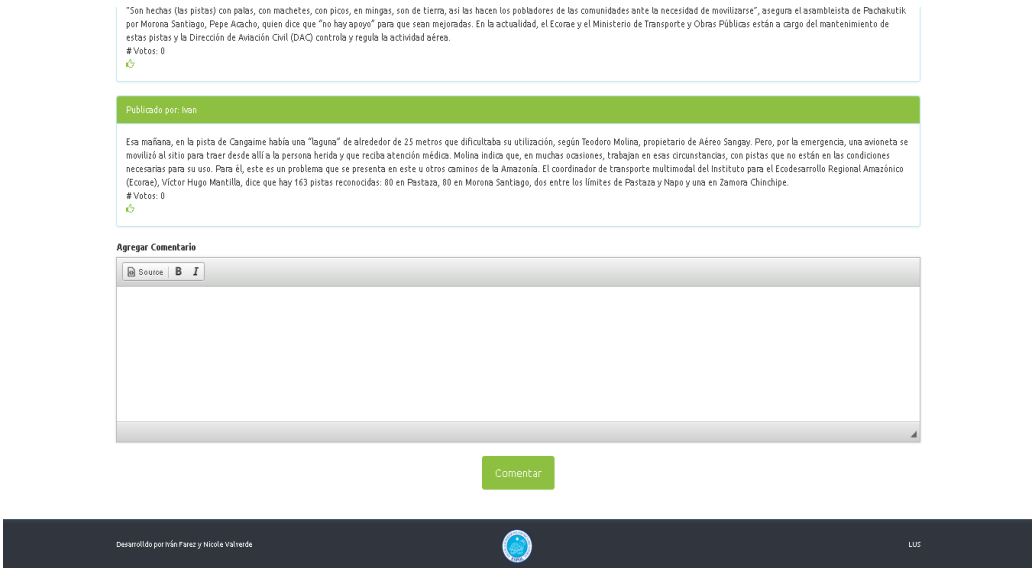


Figura 5.16: Artículo del Foro con la opción a comentar

En la pestaña “Acerca De” de la página principal de Lus, se muestra información de los creadores del sistema y para poder contactar, de tal manera, las personas puedan enviar sus quejas o sugerencias para así poder mejorar el sistema y brindar un servicio que sea de mayor agrado a la gente, además que explique en ella el análisis sobre la seguridad en ambientes UMTS, de tercera generación.

CONCLUSIONES

1. A partir del desarrollo de GPRS, extensión de GSM, red denominada 2.5G, los datos son transmitidos por medio de paquetes (PS) perfeccionándose hacia la redes 3G como UMTS completamente conmutadas por paquetes para la transferencia de audio y video en tiempo real (video llamadas, mensajería instantánea móvil, entre otras) con modulación WCDMA, de espectro extendido, para las señales banda base con la finalidad de que se dificulte la intercepción de las señales dispersas en todo el ancho de banda, además que pueda resistir a los ruidos e interferencia del medio.

2. El uso de los algoritmos de cifrado por bloques para la integridad f9 y cifrado de flujo para la confidencialidad f8 son de mucha importancia para la protección de los datos mientras los datos viajan en el enlace entre la red y el

usuario evitando suplantación de identidad durante la conexión mediante claves de cifrado que se renuevan en cada proceso de autenticación.

3. El protocolo MAPsec es efectivo para la protección de los mensajes MAP de señalización dentro del CN, ya que aseguran la identidad del usuario local como visitante y alguna información sensible referente a su perfil y características que viajen en el enlace. Mientras el protocolo IPsec es encaminada al tráfico IP, de su integridad y confidencialidad, ya sea en enlaces punto a punto o entre redes remotas por medio de sus modos de funcionamientos AH, ESP de transporte y modo túnel respectivamente.

4. La negociación de los vectores de autenticación realizada entre el AuC y VLR/SGSN es un paso fundamental previo al intercambio de información e inicio de la comunicación entre el usuario (USIM) y el VLR/SGSN, puesto se envían en ellas las funciones criptográficas necesarias para el proceso de verificación, y si es exitosa, las claves generadas CK e IK sean enviadas para así continuar con el procedimiento de proveer integridad y confidencialidad del enlace de tercera generación.

5. El algoritmo de cifrado KASUMI es usado en los algoritmos de confidencialidad f8 y de integridad f9, elaborado en base al algoritmo de cifrado MISTY-1 para proteger las comunicaciones en el intervalo aéreo entre el móvil y la BS. Mientras MILENAGE es un conjunto de algoritmos de autenticación y generación de claves estándar para lograr interoperabilidad segura y confiable entre el AuC con las diferentes implementaciones de la tarjeta SIM basado en el algoritmo de cifrado en bloque Rijndael.

6. La implementación de un sistema web como herramienta didáctica constituye un aporte para el aprendizaje de los procesos de seguridad en redes 3G como lo es UMTS con toda la información de respaldo que garantiza el acceso a la misma en todo momento.

RECOMENDACIONES

1. Se podría extender el alcance del sistema web con opciones de talleres o proyectos con la finalidad que el aprendizaje del usuario sea más dinámico e interactivo.

2. El sistema podría adaptarse para alojar más de un tema a tratar para que haya diversidad de contenido.

3. Para mayor entendimiento del proceso de seguridad en las redes UMTS de tercera generación podrían visitar el sitio web de la aplicación, además de revisar las citas bibliográficas donde se puede encontrar el contenido con más detalle.

4. Un punto importante en consideración es de realizar estudios para medir la fortaleza del algoritmo KASUMI dentro de alguna operadora, así como de sus claves Kc, debido a que ésta es base fundamental para los demás mecanismos de cifrado y confidencialidad del mensaje.

5. No confundir confidencialidad con integridad de los datos, ya que confidencialidad es el modo en que los datos viajan en el enlace, entretanto integridad es la estructura interna del mismo; por lo que el algoritmo f8 se lo utiliza para el cifrado y descifrado del flujo de datos del usuario, mientras el algoritmo f9 es encargado de proteger la integridad de la información transmitida en el enlace.

6. El algoritmo A3/A8 es importante ya que permite la comunicación entre dos plataformas móviles distintas, como GSM y UMTS, por medio de la autenticación de los usuarios usando la interfaz A3/A8 y reglas de conversión, para así tener interoperabilidad en el proceso de traspaso de tecnología móvil de segunda a tercera generación.

BIBLIOGRAFÍA

[1] In Depth Tutorials & Information. (s.f.). Traffic on 2G Networks. Obtenido de what-when-how: http://what-when-how.com/qos-enabled-networks/case-study-ip-ran-and-mobile-backhaul-qos-part-1/

[2] Python Software Foundation. (2001 - 2014). python. Obtenido de The python logo: https://www.python.org/community/logos/

[3] Aguilar L. (1996). Programacón Orientada a Objetos Primera Edición. Santa Fé, México: McGraw-Hill.

[4] Amaterazú C. (2003). Operación deuna radio base celular cuando coexisten GSM & IS-54, IS-136. Puebla, México: Universidad de las Américas.

[5] Balderas T., Cumplido R. (2004). Security Architecture in UMTS Third Generation Cellular Networks. Puebla, México: Coordinación de Ciencias Computacionales INAOE.

[6] Boman K., Horn G., Howard P., Niemi V. (2002). UMTS Security. Finland: Electronics & Communication Engineering Journal.

[7] Creative Commons 3.0 License. (20 de Septiembre de 2014). Owasp. Obtenido de Cross-Site Request Forgery (CSRF): https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

[8] Django Software Foundation. (2005 - 2014). django. Obtenido de Meet django: https://www.djangoproject.com/

[9] Dunkelman O., Keller N:. (s.f.). An Improved Impossible Differential Attack on MISTY1. Jerusalem, Israel: Einsein Institute of Mathematics, Hebrew University.

[10] España M. (2003). GPRS (General Packet Radio Service). En E. M., Servicios Avanzados de Telecomunicación (págs. 154, 155). España: Díaz de Santos S.A.

[11] Fajardo D. (2004). "Estructura de la red UMTS", Simulación de tramas de WCDMA. Cholula, Puebla, México: Universidad de las Américas Puebla.

[12] García R. (2012). Sistemas de Radiocomunicaciones. En M. S. García R., Instalaciones de Radiocomunicaciones (pág. 34). España: Paraninfo.

[13]Gardezi A. (2006). Security in Wireless Cellular Networks. Washington: Washington University in St. Louis.

[14]González A. (2010). Modelos de Seguridad para móviles. Madrid: Universidad Carlos III.

[15]González R. (2007). Python para todos. España: Creative Commons Reconocimiento 2.5.

[16]Gutérrez J. (2003). La tarjeta inteligente usada en el sistema GSM - COMP128. En T. J. Gutiérrez J., Protocolos Criptográficos y Seguridad en Redes (págs. 56, 57). Cantabria, España: Servicio de Publicaciones de la Universidad de Cantabria.

[17]Hajji S., Orhanou G. (2012). Confidentiality in yhe UMTS Radio Access Network. Rabat, Maroc: Université Mohammed V Agdal, Faculte des Sciences.

[18]Heras D., Pauta H. (2011). Estudio del Arte en redes UMTS/3G con el Subsistema IMS. Cuenca: Universidad Politécnica Salesiana Sede Cuenca.

[19]Herazo G., Flórez H. (2009). Seguridad en UMTS: Independencia entre conmutación de circuitos y de paquetes. Colombia: Investigación y Desarrollo.

[20]Holma H., Toskala A. (2010). WCDMA for UMTS - HSPA evolution and LTE fifth Edition. United Kingdom: John Wiley & Sons Ltd.

[21]Hong D., Kang J., Preneel B., Ryu H. (2003). A concrete Security Analysis for 3GPP-MAC. Korea: International Assciation for Cryptology Research.

[22]Ing. en Telecomunicaciones especializado en Voip. (2011). Voip Foro. Obtenido de Ejemplo Comunicaión SIP: http://www.voipforo.com/SIP/SIPejemplo.php

[23]Kobara K. (2006). IHS GlobalSpec. Obtenido de Stream Ciphers: http://www.globalspec.com/reference/81191/203279/2-6-stream-ciphers

[24]Kozierok C. (15 de Noviembre de 2004). CertiGuide for Security. Obtenido de IPSec Transport and Tunnel Modes : http://www.certiguide.com/secplus/cg_sp_IPSecTransportandTunnelModes.htm

[25]Lara J. (2006). Conceptos Básicos de Telefonía Celular. Pachuca de Soto, Hidalgo: Instituto de Ciencias Básicas e Ingeniería, Universidad Autónoma del Estado de Hidalgo.

[26]López J. (2005). Simulación de tramas de comunicación para UMTS. Puebla, México: Universidad de las Américas.

[27]Martinez R. (2009 - 2013). PostgreSQL-es. Obtenido de Sobre PostgreSQL-es: http://www.postgresql.org.es/sobre_postgresql

[28]Matsui M. (1997). New Block Encryption Algorithm MISTY. En B. E., Lecture Notes in Computer Science, Fast Software Encryption (págs. 54, 59). Haifa, Israel: Springer-Verlag Berlin Heidelberg.

[29]Matsui M. (s.f.). New Block Encryption Algorithm MISTY. Kanagawa, Japan: Information Technology R&D Center, Mitsubishi Electric Corporation.

[30]Moshavi Sh. (1996). Multi-User Detection for DS-CDMA Communications. New Jersey: IEEE Communications Magazine.

[31]Muñoz A. (2004). Algoritmo Criptográfico Rijndael. Madrid: Seguridad Europea para EEUU.

[32]Niemi V. (2005). Security in the UMTS Enviroment. En A. A. Kaaranen H., UMTS Networks: Architecture, Mobility and Services (Second Edition) (pág. 274). England: John Wiley & Sons, Ltd.

[33]Niemi V., Nyberg K. (2003). UMTS Security. Finland: John Wiley & Sons, Ltd.

[34]Nyberg K. (2004). Cryptographic Algorithms for UMTS. Jyvaskyla: ECCOMAS.

[35]Palm Inc. (2012). Asistencia de Palm. Obtenido de Bandas y frecuencias de red para dispositivos GSM/UMTS: http://kb.hpwebos.com/wps/portal/kb/common/article/65931_es.html

[36]Pinzón B. (2011). Protección y Seguridad. SlidePlayer.

[37]PosgreSQL-es. (1996 - 2014). PostgreSQL. Obtenido de The PostgreSQL Global Development Group: http://www.postgresql.org/

[38]Prieto L. (s.f.). Segunda Guerra Mundial. Obtenido de Los indios navajos en la Segunda Guerra Mundial: http://segundaguerramundial.es/indios-navajos-segunda-guerra-mundial/

[39]Proaño T, Rodríguez E., . (2007). Análisis comparativo del servicio de internet móvil brindado a través de 3G (UMTS) versus la opción brindada por el anexo "e" del estándar IEEE 802.16 (WIMAX MÓVIL). Quito, Ecuador: Escuela Politécnica Nacional.

[40]Sagkob H. (2003). the basics: Principles of GSM and Influences on GPRS. En S. H. Heine G., GPRS: gateway to third generation mobile networks (págs. 1-6). Norwood: Artech House, Inc.

[41]Salomon D. (2003). Data Privacy and Security. California State University, Northridge: Springer.

[42]Salvela J. (2000). Access Security in Third Generation Mobile Networks. Finland: Technology Research Center .

[43]Sanchez J., Thioune M. (2007). Universal Mobile Telecommunications System. London: ISTE Ltd.

[44]Sankaliya A., Mishra V., Mandloi A. (2011). Implementatio of Criptographic Algorithms for GSM Cellular Standard. Gujarat, India: Ganpat University Journal of Engineering & Technology.

[45]Sava R. (1 de Octubre de 2013). IPsec y certificados. Obtenido de Slideshare: http://www.slideshare.net/ricardosava/ipsec-y-certificados-26744145

[46]Unión Internacional de Telecomunicaciones, Sector de Radiocomunicaiones. (Junio de 2003). International Telecomunication Union. Obtenido de ITU global standard for international mobile telecommunications ´IMT-Advanced´: http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1645-0-200306-I!!PDF-S.pdf

[47]Univeridad Estatal de Tver. (2003). Metodológica Centro informatización del proceso educativo. Obtenido de Ciphers modes: https://www.google.com.ec/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&docid=44yvLQ5fvK__UM&tbnid=XUkqAC7MQcoZTM:&ved=0CAEQjxw&url=http%3A%2F%2Fedc.tversu.ru%2Felib%2Finf%2F0087%2F0596004427_prognetsec-chp-14-sect-2.html&ei=TNL-U_O1LcTGggT4vI

[48]Wallis B. (4 de February de 2008). Hypertext Transfer Protocol (HTTP) Digest Authentication using Global System for Mobile Communications (GSM) A3 and A8. Obtenido de IETF.org: http://tools.ietf.org/html/draft-ietf-http-digest-auth-a3a8-01#page-5

[49] WordPress. (Mayo de 2012). Edadmóvil. Obtenido de Funcionamiento IMS: http://edadmovil.wordpress.com/casos-de-desarrollo/implementacion-ims/funcionamiento-ims/