ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"Diseño de un software criptográfico de seguridad para las comunicaciones navales"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN COMPUTACION

Presentada por:

Javier Fabricio Flores Barahona

GUAYAQUIL - ECUADOR

AÑO

2000

AGRADECIMIENTO

A Dios por su inmensa sabiduría y su constante bendición.

A María Fernanda y Daniel por su comprensión, paciencia y amor.

A mis padres por su fortaleza.

A mis hermanos por su confianza.

A mis instructores por su guía, amistad y enseñanza.

A mis compañeros y amigos por su desinteresada colaboración y apoyo.

DEDICATORIA

El trabajo demandado por la presente investigación se lo dedico a quienes han marcado cada una de las etapas de mi vida.

A mis padres, a mi esposa y a mis hijos

TRIBUNAL DE GRADUACION

Ing. Carlos Monsalve Arteaga.
SUBDECANO DE LA FIEC

Ing. Carlos Jordán Villamar
DIRECTOR DE TESIS

Ing. Sergio Flores Macías
MIEMBRO DEL JURADO

Ing. Boris Ramos Sánchez
MIEMBRO DEL JURADO

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

Javier Flores Barahona

RESUMEN

El presente trabajo despliega el diseño de un sistema criptográfico de seguridad para las comunicaciones navales y la implementación de su prototipo inmerso en la red de la Dirección General del Material, ajustándose a las normas emitidas por la Dirección de Informática de la Armada y a las regulaciones dictadas en todo el mundo por la ***ITAR*** para este tipo de aplicaciones.

El sistema criptográfico permite la calificación y/o encriptación de la documentación administrativa de la ***DIGMAT*** para su posterior transferencia interna o hacia el exterior de la red o del país; además permite el envío de mensajes emergentes seguros usando una interfaz rápida y amigable. El manejo de la documentación la calificación está limitada por criptografía simétrica existente en la librería del algoritmo ***Twofish***, mientras que la criptografía asimétrica mediante ***PGP*** se constituye en el paso que asegura la completa codificación del archivo. Por otra parte, para el envío de los mensajes emergentes contamos con criptografía plana propia del prototipo o con codificación de ***PGP***.

El diseño del prototipo se complementa con la adecuación de un camino más amigable hacia Exchange e Internet Explorer, además de permitir el manejo local de las cuentas de administrador y de usuario. Al desarrollar la tesis, el primer capítulo es un resumen de las capacidades tecnológicas existentes en la Armada, en el segundo capítulo expongo un extracto de toda la teoría criptográfica que debemos tener presente y en el último capítulo se detalla la construcción del prototipo. Las pruebas de codificación, transferencia y decodificación de los archivos dentro de la red de ***DIGMAT***, por ***Internet***, por teléfono y por radio se han cumplido satisfactoriamente considerando las limitaciones del prototipo del presente proyecto, proyectándose como la base de una verdadera alternativa de cambio para los sistemas de seguridad existentes.

Fundamentalmente la investigación realizada se ha centrado en el uso de recursos criptográficos existentes y por ello debo concluir que, fruto del trabajo realizado, lo importante es comprender que el problema fundamental no consiste en cuanta tecnología usemos para implementar seguridad sino en como usar la tecnología de la que disponemos.

GLOSARIO

TERMINO	***SIGNIFICADO***
CANOPUS	Proyecto encargado de la automatización de todos los procesos transaccionales y gerenciales que fluyen en toda la DIGMAT.
CEINDE	Centro de Investigación y Desarrollo Naval. Centro encargado de desarrollar soluciones a problemas técnicos existentes en los repartos navales y canalizados a través de la DIGMAT.
CEPROD	Centro de Procesamiento de Datos de DIGMAT. Centro encargado del manejo de los recursos informáticos dentro de la DIGMAT. Actualmente están cumpliendo las útlimas fases del proyecto Canopus.
DATOTEK	Compañía proveedora de sistemas de comunicación seguros. Actual distribuidor de equipos criptográficos a la Armada del Ecuador.
DIGMAT	Dirección General del Material de la Armada. Entidad encargada del mantenimiento y reparación de todos los sistemas electromecánicos de las unidades navales.

DINFOR	Dirección de Informática de la Armada. Entidad encargada del manejo, provisión y administración de los recursos informáticos en los repartos navales
ESDESU / CENTAC	Escuela de Superficie. Anteriormente llamada Centro Táctico Naval, es la encargada del mantenimiento del sistema de Comando y Control de las unidades navales.
INTERNET	Red de redes. Centro de múltiples recursos disponibles a nivel mundial.
ITAR	Normas que regulan el tráfico de armamento a nivel internacional en los EE.UU. Los sistemas criptográficos son considerados dentro de su clasificación.
PGP	Pretty good privacy. Sistema criptográfico desarrollado para brindar una “privacidad bastante buena” al tráfico de la información dentro de una red LAN/WAN o en Internet
NBS	Oficina Nacional de estándares.
NIST	Instituto Nacional de estándares y tecnología. Anteriormente llamado NBS, responsable de los estándares de criptografía.
TWOFISH	Algoritmo criptográfico simétrico y de longitud variable. Es uno de los cinco finalistas en el concurso que selecciona el nuevo estándar de criptografía (***AES***).
VPN’s	Redes privadas virtuales. Intranets creadas usando como camino el Internet.

INDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

ANEXO A

ANEXO C

INDICE DE TABLAS

INDICE GENERAL

INTRODUCCION

En los últimos 10 años, el impacto que la Tecnología de Información ha producido en el mundo, en cualquier tipo de empresa, estrato social o nivel cultural; ha significado en muchos casos un giro sustancial en sus métodos y políticas de planificación, producción y administración; constituyéndose quizás en la razón sin-equanon de la adquisición de nuevos paradigmas y doctrinas que serán pilar fundamental de nuestra presencia en el ámbito mundial.

Siendo parte de un amplio plan de desarrollo informático, existe el proyecto de implantación de seguridad criptográfica en la Armada, este plan se compone de las siguientes fases:

- **FASE I.** Desarrollo del sistema de criptografía y calificación de archivos para el Edificio de *DIGMAT*.
- **FASE II.** Adecuación del software para transferencia de archivos calificados con otros repartos vía e-mail y estudio de sistemas de

comunicación navales para enlace y transferencia de archivos criptografiados y calificados entre buques. Pruebas de enlace.

- **FASE III.** Implementación del software para transferencia de archivos en los buques.
- **FASE IV.** Diseño e implementación de la Red Privada Virtual de Datos y del Sistema de Elaboración, Diseminación y Distribución de Claves para la Armada del Ecuador por parte de la Dirección de Informática de la Armada

El desarrollo de la presente tesis de grado involucra la primera fase del proyecto y sienta las bases de las siguientes fases para que, cuando se asigne presupuesto al proyecto, sean estas implementadas.

CAPITULO 1

1. PLANTEAMIENTO DEL PROBLEMA

Las comunicaciones entre los diferentes repartos operativos y administrativos de la Armada del Ecuador, se están integrando a través de diferentes redes, las cuales utilizan procesadores y computadoras personales para el desarrollo de los diferentes elementos de información. La información que se transmite tiene diferentes grados de calificación, por lo que es necesario buscar una herramienta propia para proteger la información calificada, considerando conveniente el diseño e implementación de un software criptográfico que cumpla con los requerimientos de seguridad y confiabilidad de la institución.

1.1. Objetivo.

Desarrollar un sistema de criptografía de alta seguridad y que sea versátil para poder integrarlo a las diferentes redes informáticas y de comunicaciones de las diferentes unidades y repartos tanto operativos como administrativos. Eliminar la dependencia tecnológica y el problema logístico que representa la generación ya discontinuada de las máquinas criptográficas actuales. El proyecto concibe el diseño de un software que se integre a nuestro sistema de comunicaciones navales, tanto en redes informáticas como vía microondas, incorporado a través de una computadora personal y un módem, generando un código de cifrado de datos tal que pueda ser decodificado únicamente por el destinatario y de acuerdo con el nivel de calificación correspondiente.

1.2. Tareas involucradas en la Tesis

El proyecto debe cumplir con los siguientes puntos:

- Desarrollo del sistema de criptografía y calificación de documentación administrativa para el Edificio de ***DIGMAT*.**
- Adecuación del software para transferencia de archivos calificados con otros repartos vía e-mail y estudio de sistemas de comunicación navales para enlace y transferencia de archivos criptografiados y calificados entre buques. Pruebas de enlace.

Para este desarrollo se han tomado las siguientes consideraciones previa aprobación:

- El diseño total ha sido desarrollado en Microsoft Visual Basic 6.0 bajo sistema operativo Windows 95/98
- La transferencia de archivos dentro de la red de datos de ***DIGMAT*** se la implementó usando un enlace externo a Microsoft Exchange 5.0, corriendo en un servidor particular de comunicaciones e impresión.
- La calificación de la documentación administrativa usa una librería del algoritmo Twofish manejado por el suscrito al nivel de llaves, considerando todas las limitaciones emitidas por la ***ITAR*.**

- La criptografía se implementó externamente con ***PGP*** versión 6.5.3i de acuerdo a lo dispuesto por la planificación anual de la ***DINFOR*****.**
- Para la transferencia remota de archivos calificados y criptografiados punto a punto, cuando se use la línea telefónica se la realizará vía Internet y, cuando no se disponga de ese medio, por ejemplo en la transferencia entre buques, existen varias alternativas de conexión bajo ***VPNs***, por satélite, por radio, etc., alternativas que están siendo estudiadas por el ente regulador (***DINFOR***). Una alternativa probada para la conexión es la provista por los equipos de comunicaciones ***Harris*** detallado en el Anexo A.

1.3. Análisis del flujo de información actual

El flujo que la información recorre dentro de los repartos navales normalmente sigue pasos preestablecidos de acuerdo a normas y directivas promulgadas en la Institución. Para tener una idea clara de la forma en que un documento sale y llega a su destinatario me

valdré del gráfico indicando a continuación que actividad se desarrolla en cada estación:

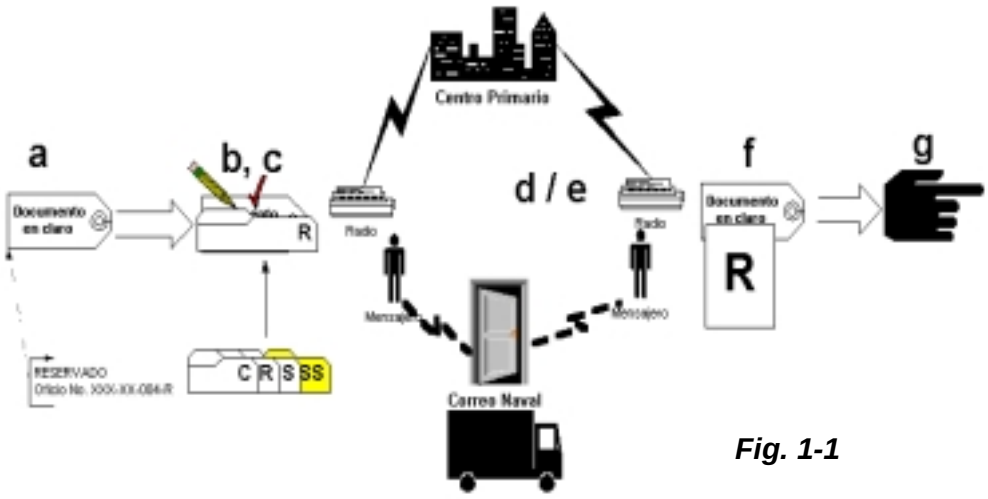


Fig. 1-1

a. El documento recibe una calificación y una numeración.
b. De acuerdo al tipo de calificación el documento es cubierto con una tapa de cartulina distinta: Amarilla (Secretísimo - SS), Roja (Secreto - S), Azul (Reservado - R), Verde (Confidencial - C), sin tapa (Ordinario - O).
c. En esa condición recibe la firma de la autoridad respectiva y solo entonces la tramitación del documento puede ser canalizada. Si el documento tiene una calificación distinta a la Ordinaria debe ser cubierto con una hoja oscura, envuelto en un sobre sellado

con la calificación correspondiente, todo dentro del sobre con el destinatario. En la portada del sobre además de los datos del destinatario deben constar el número del oficio y en la parte posterior el sello del reparto emisor.

d. Cuando el documento es transmitido por los equipos existentes se lo dirige a un centro primario de transmisión y este se encarga de enviarlo al destinatario. La autenticación en cada transmisión existe en la verificación telefónica de la hora y el nombre del emisor.

e. Si el documento es enviado físicamente, es tramitado vía correo naval, el mensajero del reparto lleva los oficios previamente registrados en un libretín al correo, en donde quien los recibe debe colocar su firma, nombre y grado en forma legible responsabilizándose de su envío, el destinatario debe enviar un mensajero al correo naval de la localidad para que una vez que firme el libretín retire el mensaje y lo traslade al reparto.

f. Una vez en el reparto el personal administrativo debidamente calificado para manejar la calificación del documento, rompe los sobres y coloca la tapa correspondiente para tramitar la información al destinatario.

g. Aquí se cierra el ciclo. Una vez analizado el documento por la autoridad correspondiente del reparto receptor, esta toma las acciones correspondientes y la documentación se entrega a las personas indicadas.

1.4. Análisis de sistemas criptográficos existentes

La seguridad en la transferencia de archivos o mensajes es inherente a una institución militar, en consecuencia el desarrollo del proyecto se constituye en una alternativa con nueva tecnología mas que en una solución, debido a que actualmente existen sistemas propios y extraños que proveen ya seguridad en la información.

En este apartado se dará una visión de los sistemas existentes dentro de la Institución que proveen seguridad encriptada de datos o voz a la transferencia de archivos, texto plano y mensajes en claro, sin detallar las características confidenciales de los mismos.

1.4.1. Sistema Datotek

Es un sistema de transferencia de mensajes criptografiados que existe en la Institución desde mediados de los años 80. Esta familia de máquinas diseñadas especialmente para este propósito, permite enviar mensajes cifrados por teléfono, radio o *TTY*. De acuerdo al modelo estas máquinas pueden almacenar un limitado número de mensajes para su transmisión. La velocidad de transferencia máxima para teléfono es de 1200 *baudios*, para radio VHF es de 300 baudios y para radio HF es de 75 baudios. Además de las máquinas de cifrado, se cuenta con un generador de claves provisto por la misma compañía, las cuales son diseminadas por distintas vías a los usuarios del sistema de todo el país, tanto en tierra como en repartos a flote. En cuanto al cifrado existente en el sistema ***Datotek***, este se compone de dos pasos: primero, en código interno se cambia todos los caracteres ingresados en texto plano a caracteres comprendidos entre la A y la Z, luego esta cadena de

caracteres se codifica con claves de 7 bits usando un método especial de ruedas; esto permite, considerando un alfabeto de 26 caracteres, que se obtengan hasta 5 rondas de cifrado.

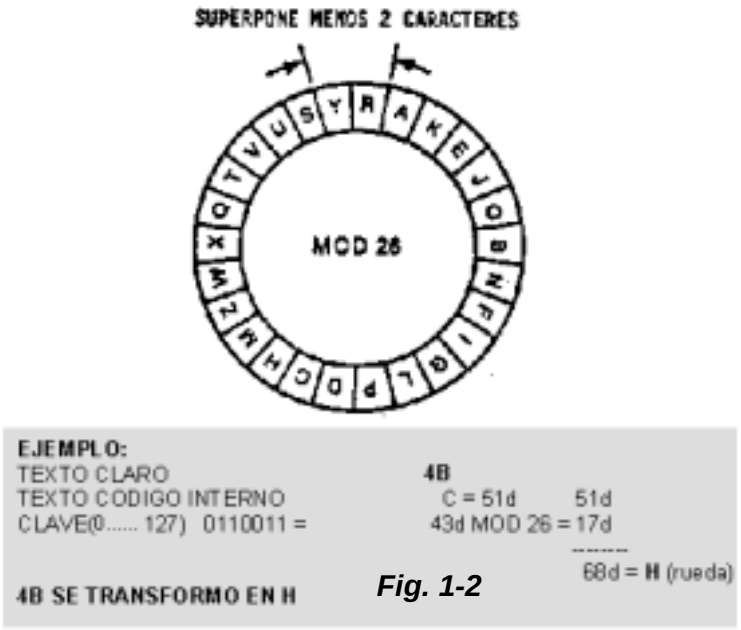


Fig. 1-2

La seguridad del sistema reside no en el “secreto” del algoritmo sino en su diseño complejo desde el punto de vista matemático y en el secreto y el cambio frecuente de las claves que inicializan el algoritmo.

1.4.2. Sistema Cóndor

La *ESDESU* llamada anteriormente *CENTAC* en el año de 1994 conformó un grupo de trabajo que desarrolló un sistema criptográfico denominado “Sistema Cóndor” el cual proveía codificación segura para archivos. Este sistema tiene tres limitantes muy importantes:

- No brinda un entorno amigable al usuario
- El grupo de los desarrolladores no se encuentra ya dentro de la Institución
- No existe documentación que permita mantener o comprender el sistema al 100%

El sistema fue desarrollado bajo C++, y es una fusión de los algoritmos *DES* y un sistema de ruedas similar al usado por la Datotek.

1.4.3. Sistema de mensajes del C3I

El *C3I* que actualmente se encuentra en su segunda fase, dentro de sus módulos mantiene un comando de texto *CEE,* el cual permite envío de mensajes criptografiados de hasta 100 caracteres, para indicar situaciones de emergencia a bordo de los buques de la Armada que cuentan con este sistema. Para lograrlo se ha realizado una interface con el Sistema *FALCON* de los equipos de radio HF Harris, en donde el sistema *FALCON* es el que realmente provee el envío de los mensajes.

INTERACCION	1	AEREA	1	---------- 50 char
		SUBMARINA	2	---------- 50 char
		SUPERFICIE	3	INFORMACION
		AEREA	4	AMPLIATORIA

AMENAZA	2	AEREA	1	---------- 50 char
		SUBMARINA	2	---------- 50 char
		SUPERFICIE	3	INFORMACION
		MISIL	4	AMPLIATORIA
		TORPEDO	5	
SITUACION A/B	3	INCENDIO	1	---------- 50 char
		HOMBRE AL AGUA	2	---------- 50 char
		COLISION	3	INFORMACION
		PERDIDA DE GOBIERNO	4	AMPLIATORIA

EJEMPLO

EL MENSAJE: 3 4 COSTA DE MANTA

SIGNIFICARA: TENEMOS A/B PERDIDA DE GOBIERNO FRENTE A LA COSTA DE MANTA

Tabla 1-1

En este capítulo he tratado de introducir al lector en la situación actual de seguridad en la que nos encontramos, donde resumiendo podemos ver que contamos con los siguientes sistemas:

- Sistema Datotek
- Sistema Cóndor

- Sistema de mensajes del C3I

Estos sistemas si bien están siendo utilizados en menor o mayor grado; con excepción del último, carecen del mínimo soporte técnico indispensable en cuanto a la tecnología criptográfica utilizada; entendiéndolo mejor, contamos con personal especializado en el equipo pero no contamos con personal especializado en el sistema de codificación y, si a esta problemática agregamos que la compañía proveedora de los equipos Datotek cerró sus puertas, estamos a un paso de que nuestra información pueda ser obtenida libremente. El prototipo diseñado es propuesto como una solución inicial al problema, en el futuro, depende del apoyo humano y económico para que este se perfile como el nuevo sistema criptográfico para las comunicaciones navales.

CAPITULO 2

2. CRIPTOLOGIA Y SEGURIDAD INFORMÁTICA

2.1. Generalidades.

Los avances tecnológicos e informáticos de los últimos veinte años convergen y actualmente han logrado convertirse en el pilar fundamental de la “globalización de los mercados”, de la cual todos dependemos en mayor o menor grado.

Por ello al valorar los activos de una empresa además de los objetos físicos, suma de capitales, producción e infraestructura; añadiremos el valor de la información. Como parte de los activos,

cada día es mas importante mantener la seguridad de la información, pero también los riesgos son cada vez mayores. Muchas veces el valor añadido de la empresa puede ser la información que maneja.

Debemos aprovechar, el tiempo de paz, para proveer a la Institución de políticas y sistemas de seguridad para el manejo de la información renovados y que se implementen acorde al desarrollo tecnológico mundial.

2.2. Riesgos de Seguridad.

El uso de un sistema informático involucra niveles de seguridad que permitan manejar de una manera eficaz las tareas de administración, proceso y gestión tanto de usuarios como de administradores. Al considerar un potencial humano heterogéneo en un alto porcentaje, existen riesgos al manejar la información que los podemos clasificar en tres tipos:

- Errores involuntarios de personas y/o máquinas
- Desastres naturales
- Ataques voluntarios

El índice de errores involuntarios puede disminuir si proveemos al usuario de la debida capacitación en el sistema, ayuda y un mantenimiento adecuado al equipo informático; los desastres naturales son impredecibles en tanto que el tercer riesgo viene a ser motivo de nuestra preocupación y el justificativo del proyecto.

2.2.1. Amenazas a la Seguridad.

Para que exista seguridad entre computadoras o dentro de una *LAN/WAN*, *Intranet/Extranet* debemos tener claro que esta labor implica a tres exigencias básicas:

- ***Secreto.*** Requiere que la información sea accesible para lectura solo para usuarios autorizados.
- ***Integridad.*** Requiere que los recursos o la información sean modificados solamente por entes autorizados.

- ***Disponibilidad.*** Requiere que los recursos estén disponibles solamente a los entes autorizados

2.2.2. Ataques a la Seguridad.

Debemos considerar como ataque a toda acción que afecte el estado de la información inicial. Cuando analizamos el término ***estado*** este se refiere a las múltiples instancias que puedo obtener de un conjunto de datos en un determinado período de tiempo. Existen cuatro categorías generales de ataques:

- ***Denegación de servicio.*** Cuando requiere que la información sea accesible para lectura solo para usuarios autorizados.
- ***Interceptación.*** Cuando personas no autorizadas acceden a información que pueden utilizarla para dañar a la Institución.

- ***Modificación.*** Cuando personas no autorizadas logran accesar a la información y la modifican en perjuicio de otros.
- ***Fabricación.*** Cuando personas no autorizadas insertan objetos falsos en el sistema.

Estos ataques activos (denegación de servicio, modificación, fabricación) presentan características opuestas a los ataques pasivos (interceptación). Mientras un ataque pasivo no es detectable con facilidad existen medidas disponibles para prevenirlo; en cambio, para un ataque activo debemos contar con la debida protección física/lógica constante de todos los recursos y vías de transmisión.

2.2.3. Servicios de Seguridad.

Para proteger la información debemos utilizar los servicios de seguridad. Estos se clasifican según su utilidad:

- ***Autenticación.*** Asegura que el usuario y la información son auténticos.
- ***Control de Accesos.*** Protege la información contra accesos no deseados, tanto físicos como lógicos.
- ***Confidencialidad.*** Oculta los datos a observaciones no deseadas.
- ***Integridad.*** Comprueba que la información no ha sido modificada
- ***No repudio.*** Evita que una persona autorizada sea rechazada al acceder a una información.
- ***Disponibilidad.*** Asegura la disponibilidad de todos los recursos.

La tabla indica que ataques protegen los servicios anteriores:

		ATAQUES			
		Denegación de servicio	Interceptación	Modificación	Fabricación
SERVICIOS	Autenticación		**X**	**X**	**X**
	Control de accesos		**X**	**X**	**X**
	Confidencialidad		**X**		**X**
	Integridad			**X**	**X**
	No repudio	**X**			
	Disponibilidad	**X**			

Tabla 2-1

2.2.4. Mecanismos de Implementación.

Podemos implementar un servicio de seguridad a una capa específica o al sistema en general. Los generales son:

- ***Funcionalidad de confianza.*** El sistema de seguridad está libre de ataques.
- ***Etiquetas.*** Clasifica la información por niveles e seguridad.
- ***Auditorías.*** Almacena las acciones realizadas sobre el sistema.
- ***Detección de eventos.*** Detecta movimientos peligrosos dentro del sistema.
- ***Recuperación de desastres.*** Todas las políticas para recuperar la información después de haber recibido un ataque con éxito: backups, mirrors, etc.

- ***Políticas de personal.*** Normativas sobre las actuaciones del personal

Los mecanismos específicos son:

- ***Cifrado.*** Se transforman los datos para que solo sean inteligibles a los usuarios autorizados.
- ***Firma digital.*** A la información se le añaden unos datos que únicamente puede generar un determinado usuario, además no permiten la modificación de la información por otros usuarios.
- ***Control de accesos.*** No permiten el acceso físico o lógico a la información a usuarios no autorizados.
- ***Integridad de datos.*** Añaden datos a la información que detectan si esta ha sido modificada.
- ***Tráfico de relleno.*** Inyectan tráfico sin información en las redes para confundir a los observadores de la red.
- ***Control de encaminamiento.*** Se utilizan los sistemas de encaminamiento para proteger la información.

▪ ***Notorización.*** Una tercera persona física o jurídica confirma la seguridad de procedencia e integridad de los datos.

La tabla siguiente relaciona los mecanismos específicos con los servicios de seguridad:

		ATAQUES					
		Autenticación	Control de accesos	Confidencialidad	Integridad	No repudio	Disponibilidad
MECANISMOS	Cifrado	**X**		**X**	**X**		
	Firma Digital	**X**			**X**	**X**	
	Integridad				**X**	**X**	**X**
	Control de accesos		**X**				**X**
	Tráfico de relleno			**X**			
	Encaminamiento			**X**			
	Notorización					**X**	

Tabla 2-2

Los mecanismos de cifrado, firma digital, control de accesos e integridad utilizan criptología para su implementación.

2.3. Principios de Criptología.

La palabra Criptografía, conforme el Diccionario de la Real Academia, proviene del griego κρυτοσ (kripto) que significa oculto y γραπηοϖ (graphos) que significa escritura, su definición es: Arte de escribir con clave secreta o de un modo enigmático.

La criptografía ha llegado a constituirse en un conglomerado de técnicas que tratan sobre la protección de la información; entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Teoría de números y la Complejidad algorítmica.

La Criptología agrupa tanto a la criptografía como a la técnica utilizada para romper esta protección, el criptoanálisis.

2.3.1. Primalidad y aleatoriedad.

Podemos asegurar que estos dos términos son la base del fundamento matemático de la criptografía, dentro de la presente fase del proyecto no se cuenta con la debida asesoría para atacar este problema, debido a ello se describirá este tema sin mayores complicaciones.

Como veremos existen algoritmos criptográficos de llave pública y simétricos de uso cotidiano que se fundamentan en la intratabilidad de los logaritmos discretos ya que no existen algoritmos analíticos eficaces que sean capaces de calcular en tiempo razonable logaritmos de esta naturaleza, además esta demostrado que si se puede calcular un logaritmo entonces se puede factorizar el número fácilmente. Estos algoritmos deben cumplir la

propiedad de que en su módulo n sea un número muy grande con pocos factores (usualmente dos), estos funcionan si se conocen n y sus factores se mantienen en secreto; habitualmente para obtener n se calcula primero dos números primos muy grandes que después se multiplican. La factorización es el problema inverso a la multiplicación: dado n, se trata de buscar un grupo de números tal que su producto total de cómo resultado n y cada uno de estos factores a su vez sea un número primo. Al igual que con el problema del algoritmo discreto tampoco existe un algoritmo eficiente para efectuar este tipo de cálculo, siempre y cuando los factores de n hayan sido escogidos correctamente, esto nos permite confiar que así el criptoanalista logre descifrar n no pueda obtener sus factores y en consecuencia no pueda obtener las llaves de desencriptamiento de nuestro mensaje cifrado. Como hemos dicho que no existen algoritmos eficientes de factorización para números grandes, para poder comprobar si un número es o no primo existen algoritmos probabilísticos que solucionan este problema con un alto

grado de certeza. Si al desarrollar un algoritmo criptográfico consideramos este precedente y con un buen método de generación de números primos grandes logramos cimentarlo, podemos estar seguro que hemos construido algo sólido y confiable.

Debemos mencionar también el termino aleatoriedad debido a que, los algoritmos de clave pública suelen ser empleados junto con algoritmos de clave privada, en donde la generación de las claves además de usar primos grandes debe ser aleatoria ya que no debe existir dependencia de ningún tipo entre una clave generada y otra. Para obtener una aleatoriedad criptográficamente aceptable existen mecanismos que cuantifican señales obtenidas por medios analógicos (lectura de velocidad de unidades de disco, lectura de sonido de tarjetas de audio, captura del movimiento del mouse, etc.) para luego ser procesadas en el PC. Para evitar que esta semilla sea

detectada por el criptoanalista esta debe ser completamente impredecible.

2.3.2. Criptosistemas

Un conocimiento esencial que debemos incluir como uno de los pilares de este proyecto es el referido a los criptosistemas. Criptosistema es un conjunto de valores (M,C,K,E,D) donde:

- ***M*** representa al mensaje en texto claro o plano que debe ser enviado
- ***C*** representa al mensaje cifrado
- ***K*** representa a las claves que se pueden usar dentro del criptosistema
- ***E*** es el conjunto de transformaciones de cifrado que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor posible de K.

▪ ***D*** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema debe cumplir la siguiente condición: $D_k(E_k(M)) = M$ explicándolo, si tenemos un mensaje M, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos nuevamente el mensaje M.

En general los criptosistemas actuales utilizan algoritmo público y claves secretas, donde el nivel de seguridad es el mismo, los algoritmos públicos se pueden fabricar en cadena, tanto en chips de hardware como en aplicaciones de software proveyendo un desarrollo mas barato, los algoritmos públicos están mas probados, ya que toda la comunidad científica puede trabajar sobre ellos buscando fallos o agujeros y además, es mas seguro transmitir una clave que todo el funcionamiento de un algoritmo. Considerando el tipo de clave existe dos tipos fundamentales de criptosistemas:

▪ ***Criptosistemas simétricos o de clave privada.*** Son los sistemas de criptografía más antiguos, se utilizan desde los tiempos de Julio Cesar hasta la actualidad. Son aquellos que emplean la misma clave k tanto para cifrar como para descifrar la información.

Fig. 2-1

Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos como transmitir la clave de forma segura. Me permito referirme a los algoritmos simétricos más utilizados ofreciendo un resumen de sus características generales:

- **DES (Data Encryption Standard).** Inventado por *IBM* en 1971 basado en todas las teorías existentes sobre Criptografía, inicialmente se llamó *LUCIFER* y funcionaba con claves simétricas de 128 bits, en 1973 el National Bureau of Standard (*NBS*) de los Estados Unidos de Norteamérica convocó un concurso para elegir un estándar de encriptación para la seguridad de los documentos oficiales, el cual fue ganado por una versión mejorada del hasta ese entonces *LUCIFER*, pasando a llamarse *DES*, desde entonces este algoritmo se ha constituido en el estándar de criptografía del *NIST* hasta nuestros tiempos. La versión implementada con hardware entró a formar parte de los estándares de la Organización Internacional de Estándares (*ISO*) con el nombre de *DEA* (Algoritmo de Encriptación de Datos). A partir de 1999 el *NIST* abrió el concurso para adoptar el nuevo algoritmo estándar. El algoritmo *DES* encripta bloques de 64 bits con una clave de 56 bits mas 8 de paridad, la desencriptación es similar.

Como inconvenientes del algoritmo encontramos que: no puede ser usado fuera de los EEUU sin un permiso del Departamento de Estado de ese país, la clave es corta, existe un nuevo sistema de criptoanálisis (diferencial) capaz de romper el DES teniendo suficientes muestras. En cuanto a sus ventajas podemos mencionar que es el mas extendido en el mundo, es el más barato, el más probado y, en 20 años nunca ha sido roto con un sistema práctico de criptoanálisis.

- **TripleDES (TDES).** Con el fin de evitar el problema de la clave corta y continuar utilizando el DES apareció el triple DES, que utiliza una clave de 128 bits y es compatible con el DES. Se utiliza una clave de 128 bits (16 de paridad y 112 de clave), se aplican 64 bits a los dos DES y los otros 64 bits al DES inverso (ANTIDES) que se realiza entre los otros dos.

Si la clave de 128 bits está formada por dos claves iguales de 64 bits el sistema se comporta como un DES simple, matemáticamente: $E_k(D_k(E_k(M))) = E_k(M)$.

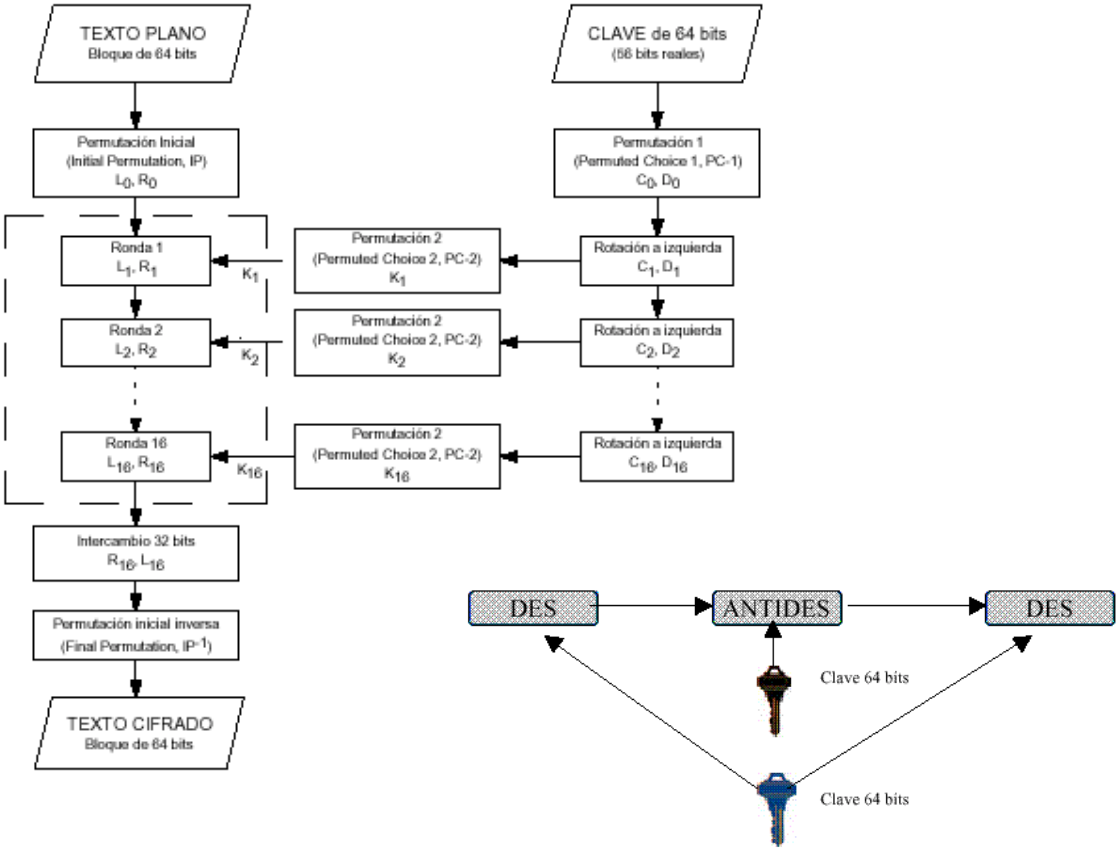


Fig. 2-2

- **IDEA (Algoritmo de encriptación de datos internacional).** En 1990 Lai y Massey del Instituto Federal de tecnología suizo inventaron un nuevo algoritmo denominado IDEA. En 1992 se publicó la segunda versión resistente a ataques de criptología diferencial, este algoritmo está libre de restricciones y permisos nacionales y es de libre distribución por Internet; esto lo ha popularizado y actualmente se lo utiliza en sistemas UNIX, en aplicaciones como PGP, etc. El algoritmo trabaja con bloques de texto de 64 bits y una clave de 128 bits. Siempre opera con números de 16 bits utilizando operaciones como XOR, suma de enteros o multiplicación de enteros, el algoritmo de desencriptación es similar. Hasta ahora nunca ha sido roto aunque no tiene la confiabilidad que presenta el DES.

- **RC5.** Inventado por Rivest proviene del RC4 y propiedad de RSA Data Security Inc. Es utilizado por

Nestcape en su sistema de seguridad SSL. Como la mayoría de los algoritmos permite diferentes longitudes de clave, fuer de los EEUU solo se puede exportar, de acuerdo a las últimas normas ITAR, la versión con clave de 40 bits. Funciona como un generador de números aleatorios que se suman al texto mediante una XOR. Permite la configuración de muchos parámetros: número de iteraciones, longitud de clave y tamaño de bloque, esto permite adaptarse a las necesidades de velocidad/seguridad de cada aplicación.

- **AES (Estándar de encriptación avanzado)**. El NIST (anteriormente llamado NBS), debido a que el DES presentaba características que, con el incremento de necesidades y aplicaciones tecnológicas mas versátiles, se volvieron pobres en sus bondades, tales como la clave corta, clave fija, limitaciones legales; en 1997 decidió no volver a utilizarlo y en consecuencia se convocó a concurso para buscar un nuevo sistema estándar, el cual

se llamará AES y su algoritmo AEA (Algoritmo de encriptación avanzado). Hasta junio de 1998 se receptaron los candidatos y luego de la primera ronda se obtuvo los 15 semifinalistas (tabla semifinalistas), actualmente han pasado ya a la segunda ronda 5 finalistas: Mars, RC6, Rijndael, Serpent y Twofish. En Internet no se ha publicado todavía que algoritmo es el nuevo estándar criptográfico.

Nombre del algoritmo	*Creadores del algoritmo*
CAST-256	Entrust Technologies, Inc.
CRYPTON	Future Systems, Inc.
DEAL	Richard Outerbridge, Lars Knudsen
DFC	CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure
E2	NTT - Nippon Telegraph and Telephone Corporation
FROG	TecApro Internacional S.A.
HPC	Rich Schroeppel
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG
MARS	IBM
RC6	RSA Laboratories
RIJNDAEL	Joan Daemen, Vincent Rijmen
SAFER+	Cylink Corporation
SERPENT	Ross Anderson, Eli Biham, Lars Knudsen
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Fig. 2-3

▪ ***Criptosistemas asimétricos o de clave pública.*** Son aquellos que emplean un par de claves (k_p,k_P). k_p se conoce como clave privada y k_P se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de descifrado. Debemos cumplir con la condición de que el conocimiento de la clave pública no permita calcular la clave privada.

Este criptosistema nos permite establecer comunicaciones por canales inseguros (Internet) puesto que únicamente viaja la clave pública, este método es utilizado por PGP, detallado en un capítulo posterior. En la actualidad se utilizan sistemas mixtos simétricos para confidencialidad y asimétricos para distribución de claves simétricas, autenticación y firma digital.

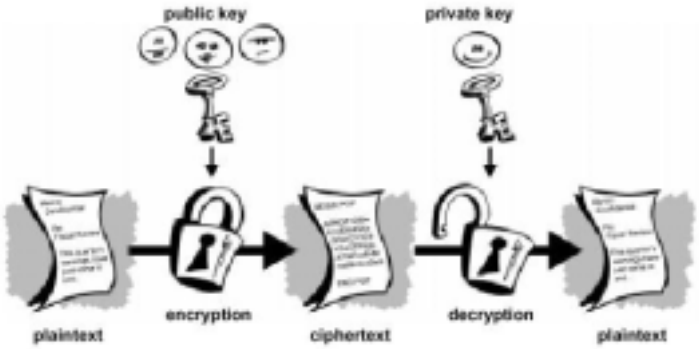


Fig. 2-4

A continuación menciono los algoritmos asimétricos más utilizados ofreciendo un resumen de sus características generales:

- **RSA (Rivest, Shamir y Adlman).** Inventado en 1978 por los autores indicados en su nombre, es el más popular y utilizado de este género, Los creadores patentaron el algoritmo y cuando alcanzó popularidad fundaron la RSA Data Security Inc para su explotación comercial; para poder implementarlo y utilizarlo se deben pagar los correspondientes derechos, pero actualmente encontramos muchas versiones gratuitas en Internet, fuera de los EEUU el uso de este algoritmo solo se encuentra permitido con claves menores o iguales a 512 bits. El RSA utiliza las siguientes claves: públicas, dos números grandes e y n (elegidos por un programa) y privada un número grande d que es consecuencia de los anteriores. El cálculo de estas claves se realiza en secreto en la

máquina depositaria de la privada. En agosto de 1999 la propia compañía consiguió romper un RSA con clave de 512 bits en algo mas de 5 meses con el trabajo conjunto de más de 290 PC's, por ello es aconsejable usar claves de 1024 bits o más lo que resulta paradójico ya que nos encontramos fuera de los límites legales.

- **DSS (Estándar de firma digital).** Es un sistema de firma digital adoptado como estándar por la NIST. Utiliza la función hash SHA y el algoritmo asimétrico DSA (Algoritmo de firma digital). El DSA es un algoritmo asimétrico que únicamente se puede utilizar con firma digital. Utiliza más parámetros que el RSA y así consigue un grado mayor de seguridad (KG, KU, KP, k, s y r).

- **Algoritmo de Diffie-Hellman.** Publicado en 1976 fue el primer algoritmo asimétrico desarrollado, usado para ilustrar la nueva criptografía de clave pública, la seguridad

del algoritmo depende de la dificultad del cálculo de un logaritmo discreto. Junto con el RSA estos algoritmos son utilizados indistintamente por el PGP para la creación de pares de claves (pública y privada).

2.3.3. Certificados de clave pública.

En la criptografía simétrica la transmisión de la clave es un problema importante ya que si se descubre todo el sistema se rompe, la solución adoptada ha sido enviarla con un sistema asimétrico. En estos sistemas la clave privada no se transmite nunca y, por lo tanto es segura; el conocimiento de la clave pública no pone en peligro la seguridad del sistema, pero el problema cuando se recibe una clave pública es saber si la identidad del propietario de esta clave no es falsa, ya que si una persona puede hacerse pasar por otra es capaz de firmar en nombre de otro y realizar transmisiones confidenciales mediante claves de sesión donde la otra persona cree que esta

comunicado con la identidad real. En los certificados de clave pública encontramos la siguiente información:

- Nombre del usuario
- Clave pública del usuario
- Foto del usuario
- Datos e informaciones del usuario
- Firma de una tercera persona de confianza

Actualmente todas las claves públicas se envían en certificados, aceptar o rechazar una clave pública depende de la firma que avala el certificado, todos los programas navegadores y de correo actuales están preparados para recibir certificados, comprobarlos y dar un mensaje al usuario de auténtico o no. Con los certificados el problema de la suplantación de personalidad se ha trasladado de la recepción de claves públicas a la confianza en las claves de terceras personas, para resolver este problema en PGP se han usado los niveles de confianza y también se las tramita con autoridades de

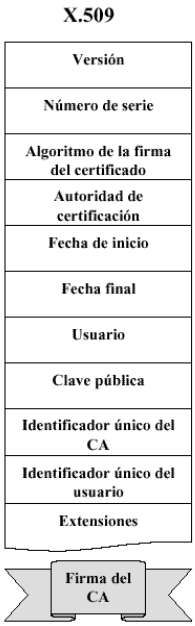
certificación. En PGP se asignan dos niveles de confianza a cada clave pública, la confianza propia otorgada por el mismo usuario o la confianza otorgada por un sistema seguro; este sistema sirve para grupos donde siempre hay enlace, pero tiene como inconveniente que no es práctico para millones de usuarios de Internet y tampoco es confiable en caso de requerimientos judiciales ya que habrá que seguir una larga cadena para verificarlo.

Cuando se presentan estos problemas es necesario acudir a las autoridades de certificación, estas son entidades públicas o privadas cuya función es ofrecer confianza en los certificados que firman, generan claves públicas y certificados para usuarios bajo demanda, además de dar a conocer sus claves públicas para las comprobaciones. Los usuarios se deben identificar personalmente para pedir un certificado a una CA, es un sistema parecido a la cédula de identidad, donde el gobierno, como entidad de confianza, genera un documento que los bancos y las

empresas consideran fiable. Para descentralizar la gestión de los CAs existe una estructura jerárquica a nivel mundial (Gráfico). La CA más conocida es la empresa privada VeriSign, además de las empresas de tarjetas de crédito conocidas a nivel mundial, existe también la capacidad de que empresas grandes puedan crear sus propias CA privadas para su uso interno, esta opción debe considerarse a ser implementada a mediano plazo dentro de nuestra Institución.

2.3.4. Certificados X.509

El formato X.509 para certificados digitales es el mas común y extendido en la actualidad. El estándar de este formato solamente define su sintaxis, por lo que dentro de su implementación no existe dependencia de ningún algoritmo en particular. El estándar X.509 contempla los siguientes campos:



- Versión
- Número de serie
- Identificador del algoritmo empleado para la firma digital
- Nombre del certificador
- Período de validez
- Nombre del usuario
- Clave pública del usuario
- Identificador único del certificador
- Identificador único de sujeto
- Extensiones
- Firma digital de todo lo anterior generada por el certificador

Fig. 2-5

Estas certificadoras mantienen también una estructura jerárquica y normalmente las claves públicas de mas alto nivel existe en medios escritos para su divulgación. Para conseguir un certificado X.509 nosotros debemos identificarnos positivamente con la autoridad de certificación, enviar nuestra clave pública, a continuación recibiremos un nuevo par de llaves generado por el certificador con toda la información ya mencionada y solo entonces nuestra firma tendrá una certificación X.509.

Recientemente se han flexibilizado las regulaciones en la creación de empresas certificadoras, gracias a ello podremos a mediano plazo contar con este requerimiento muy cerca de nosotros y a largo plazo este mecanismo de certificación llegara a ser un estándar en el país.

2.4. Descripción del Algoritmo Twofish

Entre 1972 y 1974 el NBS (Oficina Nacional de estándares), ahora llamado NIST (Instituto Nacional de estándares y tecnologías), emitió el primer requerimiento público para un estándar de encriptación, el resultado de ello fue la aparición del DES y desde allí ha sido uno de los algoritmos más utilizados en diferentes mecanismos de seguridad de datos, tanto en soluciones de hardware como de software.

Debido a su popularidad el DES ha sido también objeto de críticas y de mucha controversia, tales son: posible existencia de puertas traseras, claves simétricas fijas y cortas, etc... Como una solución intermedia a estas seudo debilidades apareció el triple DES y otras variantes.

En 1997 el NIST emitió el nuevo concurso para el AES (Estándar de encriptación avanzado), para ello promulgó los siguientes parámetros del concurso:

- ♠ se deben permitir claves simétricas mayores y de longitud variable
- ♠ se deben utilizar bloques de cifrado de gran tamaño
- ♠ se deben proveer una gran velocidad de cifrado
- ♠ se debe dar la mayor flexibilidad y soporte multiplataforma

2.4.1. Metas de diseño del Twofish

El algoritmo Twofish nació como una evolución de otro algoritmo llamado Blowfish, que trata de cumplir con todos los requerimientos del NIST para el nuevo AES añadiendo un valor agregado. Específicamente, las metas de diseño radican en:

- Un bloque de cifrado simétrico de 128 bits
- Longitud de llaves de 128, 192 y 256 bits
- No existencia de claves débiles
- Eficiencia en múltiples plataformas de hardware y software
- Diseño flexible
- Diseño simple
- Valor agregado: soporte de claves variables de longitudes mayores y menores a 256 bits, alta velocidad de codificación, no contener operaciones que sean

ineficientes en otros procesadores de 8, 16, 32 o 64 bits, no incluir componentes que lo hagan ineficiente al implementarlo en hardware, número variable de rondas de encriptamiento e incluir un horario de claves.

2.4.2. Bloques de construcción del Twofish

En este apartado, sin profundizar en complejidades matemáticas, trataré de describir los bloques que conforman el algoritmo Twofish, del cual he utilizado una librería compilada bajo Visual Basic para la calificación de la documentación naval. Estos bloques son:

2.4.2.1. Redes de Feistel

Una red de feistel es un método general de transformación de cualquier función (usualmente llamada función F) dentro de una permutación. 4 bits de un bloque de texto plano son tomados de dos en dos y son transformados dentro de una permutación; en consecuencia, dos rondas de la red de Feistel es llamada un ciclo de cambio en donde cada bit de el

bloque de texto ha sido transformado por lo menos una vez.

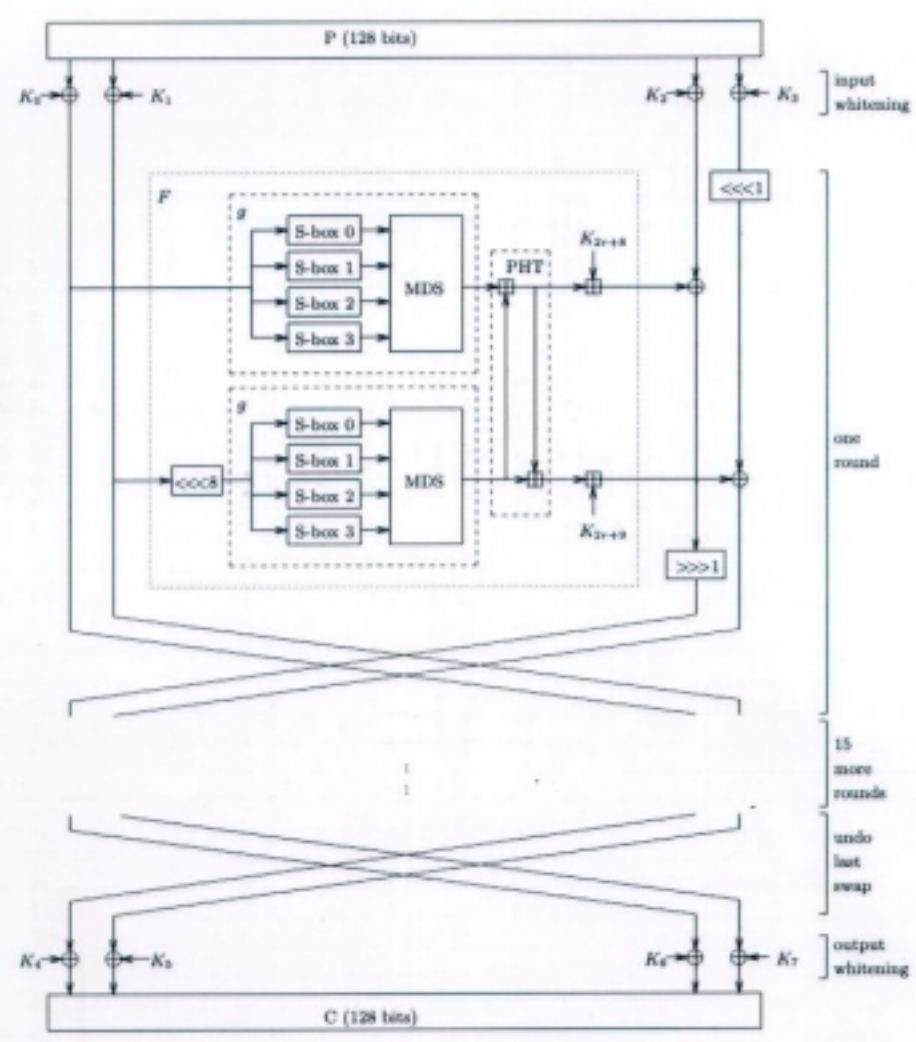


Fig. 2-6

Este mecanismo de transformación de bits de información ha sido utilizado en la mayoría de los nuevos bloques de cifrado existentes, ejemplo de ello lo encontramos en los siguientes algoritmos: FEAL, GOST, Khufu and Kafre, LOKI, CAST-128, Blowfish y RC5. En Twofish se usa una conjunción de una red de Feistel de 16 rondas, o ciclos, con una función F biyectiva.

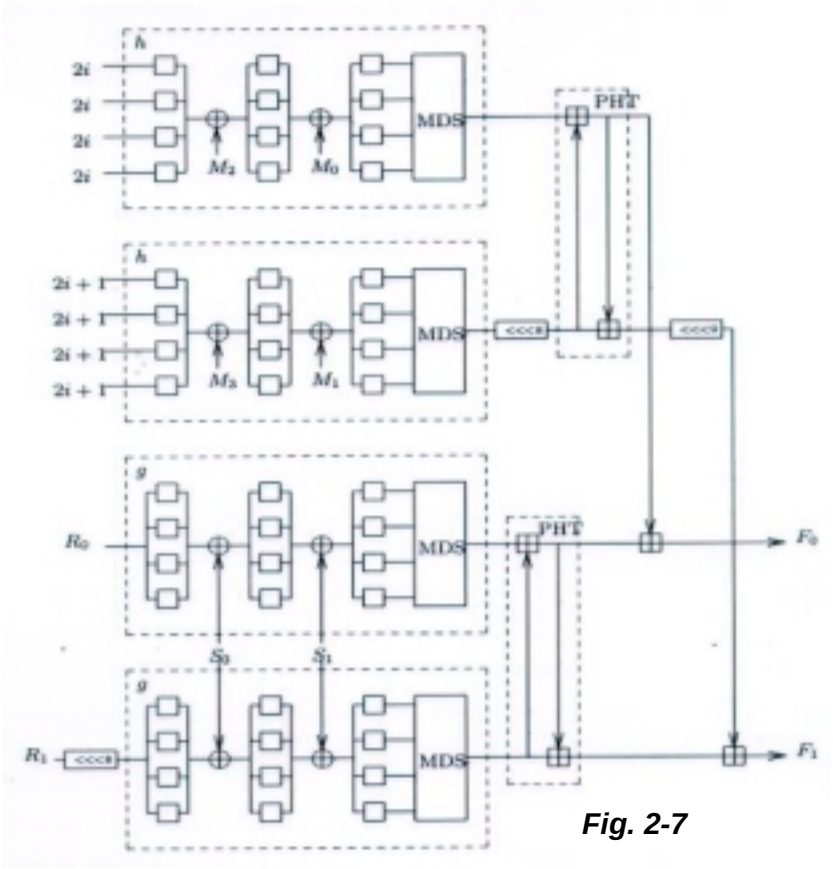


Fig. 2-7

2.4.2.2. Cajas – S

Una caja-s es una operación de sustitución no linear manejada por tablas usada también en la mayoría de los bloques de cifrado. Estas varían tanto en su cantidad de entradas como en su cantidad de salidas., y pueden ser creadas randómica o algoritmicamente. Las cajas-s fueron usadas en Lucifer, en DES y posteriormente en la mayoría de algoritmos de encriptación. Twofish usa cuatro diferentes cajas-s, biyectivas y dependientes de la clave de 8x8 bits en su implementación. Estas cajas-s son cosntruídas usando dos permutaciones fijas de 8x8 bits y material de clave.

2.4.2.3. Matrices MDS

Estas matrices fueron prouestas por primera vez en 1995 por Serge Vaudenay, publicada en el algoritmo de cifrado no publicado Manta (1996) y utilizado en Twofish con una simple matriz de 4x4 sobre GF.

2.4.2.4. Transformadas Pseudo-Hadamard

Estas son simples operaciones de mezcla que corren rápidamente por software. Dadas dos entradas, a y b, la PHT de 32 bits usada en Twofish, es definida como:

$a' = a + b \bmod 32$

$b' = a + 2b \bmod 32$

2.4.2.5. Blanqueamiento

El uso de operaciones XOR con material de clave antes de la primera ronda y después de la última ronda de Twofish, incrementa sustancialmente la dificultad del criptoanalista de buscar los restos o huellas del cifrado. Twofish usa este blanqueamiento con subclaves de 128 bits, y estas subclaves no son usadas para el cifrado.

2.4.2.6. Horario de clave

Esta técnica ayuda a definir que bits de la clave pueden ser usados dentro de las rondas de cifrado. Twofish usa

gran cantidad de material de clave y con ello provee un complicado horario de clave.

El rendimiento del algoritmo en sistemas Pentium o Mac cumple con las especificaciones del concurso para el nuevo AES, esto se detalla a continuacion:

Processor	Language	Keying Option	Code Size	Clocks to Key			Clocks to Encrypt		
				128-bit	192-bit	256-bit	128-bit	192-bit	256-bit
Pentium Pro/II	Assembly	Compiled	8900	12700	15400	18100	285	285	285
Pentium Pro/II	Assembly	Full	8450	7800	10700	13500	315	315	315
Pentium Pro/II	Assembly	Partial	10700	4900	7600	10500	460	460	460
Pentium Pro/II	Assembly	Minimal	13600	2400	5300	8200	720	720	720
Pentium Pro/II	Assembly	Zero	9100	1250	1600	2000	860	1130	1420
Pentium Pro/II	MS C	Full	11200	8000	11200	15700	600	600	600
Pentium Pro/II	MS C	Partial	13200	7100	9700	14100	800	800	800
Pentium Pro/II	MS C	Minimal	16600	3000	7800	12200	1130	1130	1130
Pentium Pro/II	MS C	Zero	10500	2450	3200	4000	1310	1750	2200
Pentium Pro/II	Borland C	Full	14100	10300	13600	18800	640	640	640
Pentium Pro/II	Borland C	Partial	14300	9500	11200	16600	840	840	840
Pentium Pro/II	Borland C	Minimal	17300	4600	10300	15300	1160	1160	1160
Pentium Pro/II	Borland C	Zero	10100	3200	4200	4800	1910	2670	3470
Pentium	Assembly	Compiled	8900	24600	26800	28800	290	290	290
Pentium	Assembly	Full	8200	11300	14100	16000	315	315	315
Pentium	Assembly	Partial	10300	5500	7800	9800	430	430	430
Pentium	Assembly	Minimal	12600	3700	5900	7900	740	740	740
Pentium	Assembly	Zero	8700	1800	2100	2600	1000	1300	1600
Pentium	MS C	Full	11800	11900	15100	21500	630	630	630
Pentium	MS C	Partial	14100	9200	13400	19800	900	900	900
Pentium	MS C	Minimal	17800	3800	11100	16900	1460	1460	1460
Pentium	MS C	Zero	11300	2800	3900	4900	1740	2260	2760
Pentium	Borland C	Full	12700	14200	18100	26100	870	870	870
Pentium	Borland C	Partial	14200	11200	16500	24100	1100	1100	1100
Pentium	Borland C	Minimal	17500	4700	12100	19200	1860	1860	1860
Pentium	Borland C	Zero	11800	3700	4900	6100	2150	2730	3270
UltraSPARC	C	Full		16600	21600	24900	750	750	750
UltraSPARC	C	Partial		8300	13300	19900	930	930	930
UltraSPARC	C	Minimal		3300	11600	16600	1200	1200	1200
UltraSPARC	C	Zero		1700	3300	5000	1450	1680	1870
PowerPC 750	C	Full		12200	17100	22200	590	590	590
PowerPC 750	C	Partial		7800	12200	17300	780	780	780
PowerPC 750	C	Minimal		2900	9100	14200	1280	1280	1280
PowerPC 750	C	Zero		2500	3600	4900	1030	1580	2040
68040	C	Full	16700	53000	63500	96700	3500	3500	3500
68040	C	Partial	18100	36700	47500	78500	4900	4900	4900
68040	C	Minimal	23300	11000	40000	71800	8150	8150	8150
68040	C	Zero	16200	9800	13300	17000	6800	8600	10400

Fig. 2-8

El corazón de Twofish lo conforma la función g, en ella se procesan los bloques de las cajas-s mas las matrices MDS utilizando dos bits de cuatro cada caja-s, la proxima tomarán los otros dos y se completará una ronda. Este complejo diseño matemático que puede ser implementado por software o hardware nos provee quizás el agoritmo simétrico más potente jamás inventado y que, con justa razón, está próximo a ser declarado como el nuevo estándar de criptografía. Resumiendo mi investigación con este pequeño anexo, espero haber justificado el uso de la librería de este algoritmo, provista por el Ing. Jesper Soedeberg (Alermania) para ser usada en el prototipo, en la rutina de calificación y descalificación de archivos. Si bien dentro de este capítulo hemos revisado varios aspectos relacionados tanto con la criptografía como con la seguridad informática en la que debemos terminar, estas líneas no son mas que un puñado de arena de todo el conocimiento que debemos tener firme en nuestras mentes para obtener un desarrollo criptográfico propio y confiable.

CAPITULO 3

3. CONSTRUCCIÓN DEL PROTOTIPO

3.1. Análisis

La tesis desarrollada además de presentar el problema existente al no contar con un sistema desarrollado internamente y estando en el límite de una obsolescencia tecnológica al desaparecer la empresa proveedora del sistema criptográfico en uso dentro de las unidades navales, también se ha querido brindar un marco teórico suficiente que justifique el desarrollo del presente prototipo como una posible solución al problema detallado. Basándome fundamentalmente en una investigación aplicada, usando recursos existentes a nivel mundial, se quiere cubrir los siguientes requisitos:

- Calificación
- Encriptación y,
- Transferencia de archivos

Con la presente implementación no se ha pretendido analizar las características operacionales, en cambio si se han analizado y atacado las características funcionales necesarias que puedan satisfacer los requisitos ya indicados.

3.1.1. Especificaciones de los requisitos

Existen requisitos básicos que el software desarrollado debe cumplir, con ellos podremos desarrollar una solución razonable para el problema existente en la Institución. El prototipo implementado cumplirá con las siguientes actividades directas e indirectas para la red de DIGMAT:

- Calificación de archivos con cinco niveles de *criptografía* (5 llaves de diferente longitud) usando el algoritmo Twofish. Los niveles usados con su correspondiente longitud de clave son:

- Ordinario (196 bits)
- Confidencial (388 bits)
- Reservado (580 bits)
- Secreto(772 bits)
- Secretísimo(964 bits)

Es conveniente indicar que la clave a usarse es variable completamente y que las longitudes utilizadas pueden ser ampliamente utilizadas, como está demostrado, además, considerando que la calificación es de uso interno a la Institución y está siendo utilizada bajo un sistema propio las longitudes de clave utilizadas no se constituyen en una violación de las normas ITAR.

- Criptografía de documentos con PGP. La planificación del control y distribución de claves públicas está dentro de la planificación de la DINFOR, el cual será centralizado por lo menos en dos puntos de la Intranet Naval próxima a construirse.
- Envío de mensajes emergentes codificados mediante el Control Winpopup. En cuanto esta opción es un adicional a los requerimientos planteados ya que esta actividad también

puede hacerse por el Winpopup de Win95/98 mas PGP, he utilizado un shareware dentro del prototipo el cual será reemplazado por un Control Active X final cuando exista el prototipo sea aprobado y los fondos asignados.

- Transferencia de los archivos criptografiados y/o calificados en la red de DIGMAT usando Exchange 5.0. Existe ya un uso constante y diario de esta herramienta dentro de la red de DIGMAT por mas de seis meses; ya que, mediante este medio se publica diariamente el periódico del Edificio y se envían los mensajes de dominio particular o público sin presentarse problemas.
- Administración de usuarios y claves de acceso. En el prototipo se anexa una tabla de Access básica que administra el user, la contraseña y el tipo de usuario que ingresa localmente al sistema.

El uso adecuado de estas funciones proveerá al documento en texto claro de las siguientes características de seguridad adicionales:

- Cifrado del documento seguro y confiable gracias al uso del PGP y de su política de manejo de llaves (uso del *llavero*)
- Doble *cifrado* al usar la librería del algoritmo *Twofish* para la calificación del documento previamente *encriptado*. Esta *seudocalificación* es tan óptima en su desempeño que, aunque las seguridades del PGP fuesen rotas o el documento no haya sido *encriptado* con PGP, obtenemos un alto nivel de codificación del archivo y en consecuencia su transferencia será completamente segura.
- *Transferencia* de mensajes cifrados emergentes dentro de la red de *DIGMAT* mediante una alternativa de Winpopup.
- Enlace a Microsoft Exchange 5.0 para la trasferencia de los archivos *codificados*

- Recolección de los archivos *codificados* para que puedan ser enviados por diferentes medios de transmisión: radio, satélite, teléfono, etc.

3.1.2. Diagramas de Flujo de Datos

Una vez delimitadas las actividades que se cumplirán con el prototipo es conveniente parametrizar los requisitos que se cumplirán en cada una de estas actividades, para esto, a continuación detallare los respectivos diagramas de flujo de datos indicando todas las subactividades que ayudaran a la completa satisfacción del requisito involucrado.

3.1.2.1. Flujo de datos general

Se requiere construir un prototipo que permita cumplir con 4 actividades especificas:

1. Codificación de documentos (calificación / encriptación). Figura 3-2.
2. Envío de mensajes emergentes codificados. Figura 3-3.
3. Control de usuarios. Figura 3-4.
4. Búsqueda de ayuda. Figura 3-5.

Este sistema para cumplir estas actividades se ayudará de aplicaciones complementarias, de una base de datos y del Web. Tendremos un flujo de datos como el que se muestra a continuación:

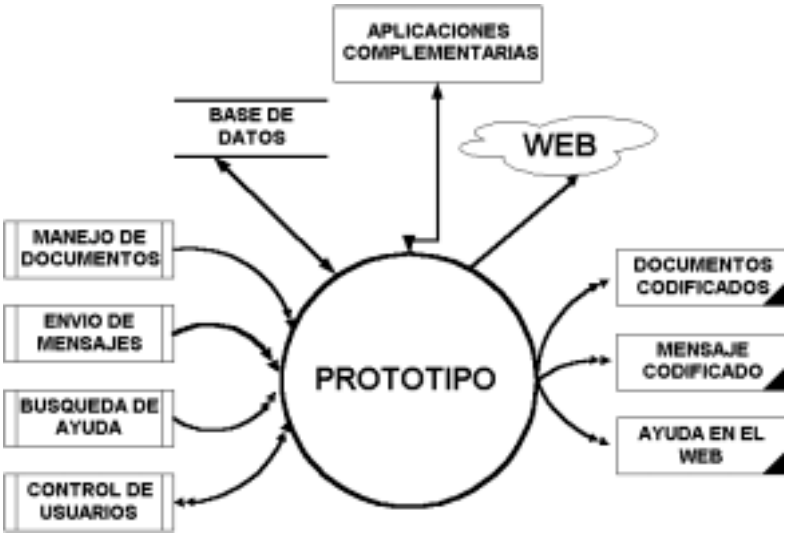


Fig. 3-1

Las entradas del sistema serán: los documentos en texto plano, los mensajes, la petición de ayuda y las necesidades de los usuarios; mientras que una vez procesada esta información obtendremos: los documentos debidamente codificados, los mensajes enviados con seguridad y la información precisa

obtenida desde el sitio Web de apoyo a los proyectos del Centro de Investigaciones (será construido el próximo año). Esta visión global del sistema nos permite desglosar cada una de sus actividades.

3.1.2.2. Codificación de Documentos

Esta actividad se constituye en el requisito fundamental del sistema desarrollado; para nosotros poder codificar el documento debemos tener presente que este puede ser encriptado, encriptado y calificado o solamente calificado antes de ser transferido al destinatario por cualquier medio de comunicación, para ello, previamente el usuario debe ser validado en la base de datos local. En el diagrama de flujo de datos la entrada se constituye en el documento ingresado y la salida se será el documento codificado y guardado en la carpeta predeterminada, podemos definirlo con el siguiente diagrama:

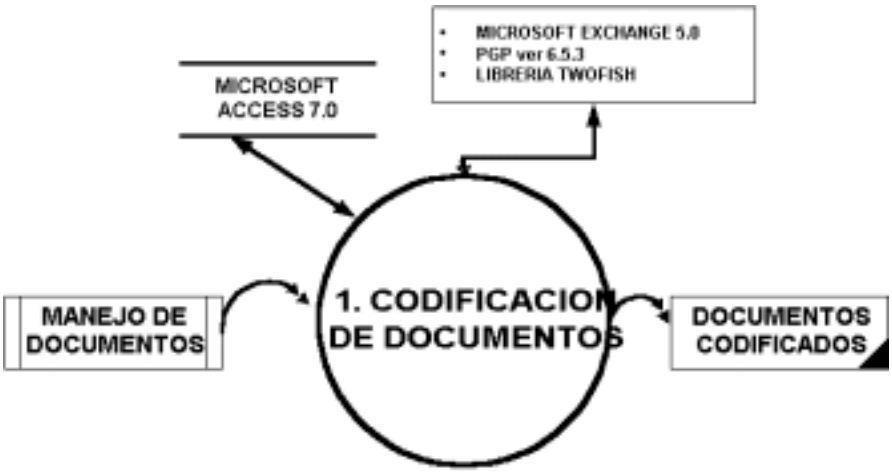


Fig. 3-2

Dentro de esta actividad el flujo corre de la siguiente manera:

- Previo al ingreso debe existir la adecuada validación del usuario. Esto lo hacemos comparando el user y el password del usuario con los datos almacenados en la base de datos local.
- Una vez que ingreso al sistema codifico el documento con código interno y con ayuda de aplicaciones adicionales como el PGP y la librería del Twofish.
- Cuando ya se generó el documento codificado, este es guardado para ser transferido por la red de DIGMAT usando Exchange.

- En el caso de haber recibido un documento codificado el sistema opera para descodificarlo usando los mismos medios ya descritos y lo guarda para su distribución.

Esta actividad puede ser dividida en varios subgrupos:

1.1 Codificación de documentos

1.1.1 Calificación de documentos

1.1.2 Encriptación de documentos

1.2 Decodificación de documentos

1.2.1 Descalificación de documentos

1.2.2 Desencriptación de documentos

1.3 Transferencia de documentos

Para cada uno de ellos vamos a tener un DFD particular, su descripción la mostramos en las siguientes páginas.

Codificación de Documentos

Para poder codificar el documento debemos contar con las entradas de: documento en texto claro, PGP y el algoritmo Twofish, esto nos proporciona como salida el documento debidamente codificado y listo para ser transferido por cualquier medio.

Fig. 3-3

Calificación de documentos

Para poder calificar el documento he utilizado la librería del algoritmo de Twofish previamente compilada para usarla con una variación en la longitud de las llaves de acuerdo al grado de calificación preestablecido. El documento tiene 5 grados de

calificación y la longitud de cada una de sus llaves es de una longitud proporcionalmente mayor. Los grados de calificación definidos con su longitud de clave son:

- Ordinario (196 bits)
- Confidencial (388 bits)
- Reservado (580 bits)
- Secreto(772 bits)
- Secretísimo(964 bits)

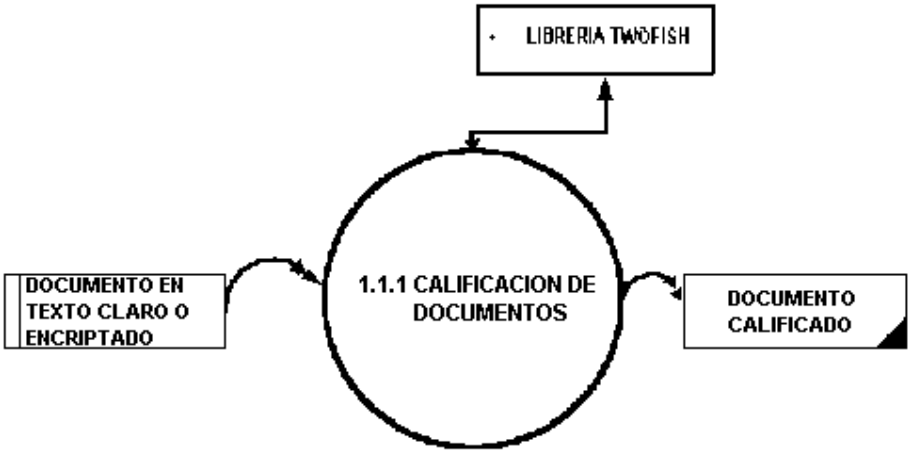


Fig. 3-4

El flujo de entrada se constituye en el documento en texto claro o previamente encriptado con PGP, más la codificación con

Twofish, y el flujo de salida es el documento calificado y guardado en la carpeta Crypto / Calificados del disco C.

Encriptación de documentos

Para brindar una seguridad mas al documento se lo puede encriptar con PGP. En las PC de pruebas se ha instalado el PGP version 6.5.3 freeware, se han generado el par de claves de usuario tanto con RSA como con Diffie-Heffmann; el intercambio de llaves se lo ha hecho manualmente por la red interna y se han obtenido documentos seguros previos a la calificación

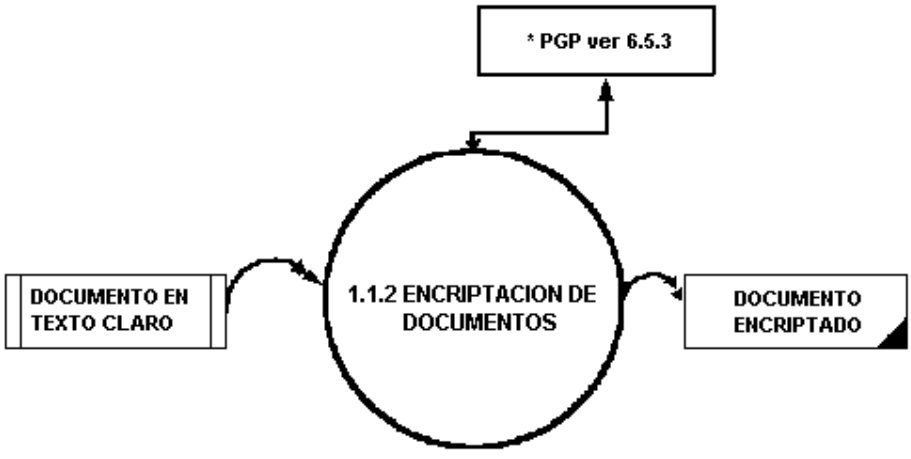


Fig. 3-5

El flujo de entrada se constituye en el documento en texto claro más la aplicación de PGP, y el flujo de salida es el documento encriptado y guardado en la carpeta Crypto / Criptografiados del disco C.

Decodificación de Documentos

Para poder decodificar el documento debemos contar con las entradas de: documento codificado, PGP y el algoritmo Twofish, esto nos proporciona como salida el documento debidamente decodificado y listo para ser transferido por cualquier medio.

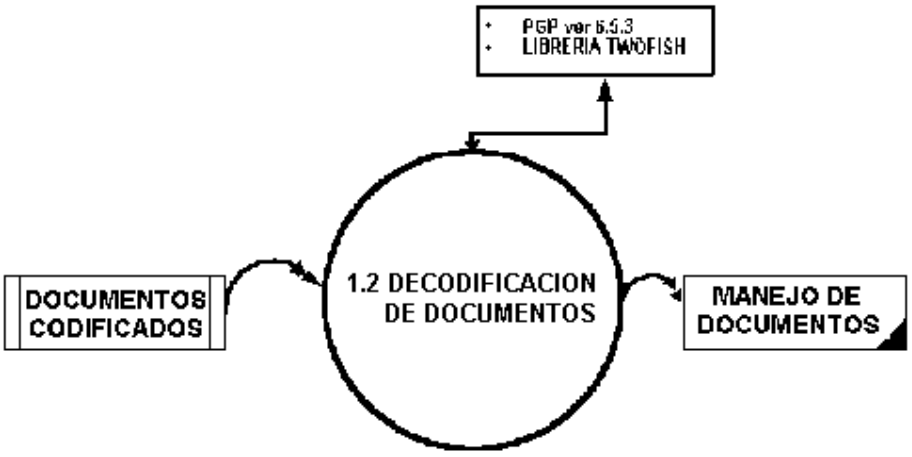


Fig. 3-6

Descalificación de documentos

Para poder descalificar el documento he utilizado la librería del algoritmo de Twofish previamente compilada para usarla con una variación en la longitud de las llaves de acuerdo al grado de calificación preestablecido. El documento tiene 5 grados de descalificación automática y cada llave utilizada es igual a la usada en la calificación.

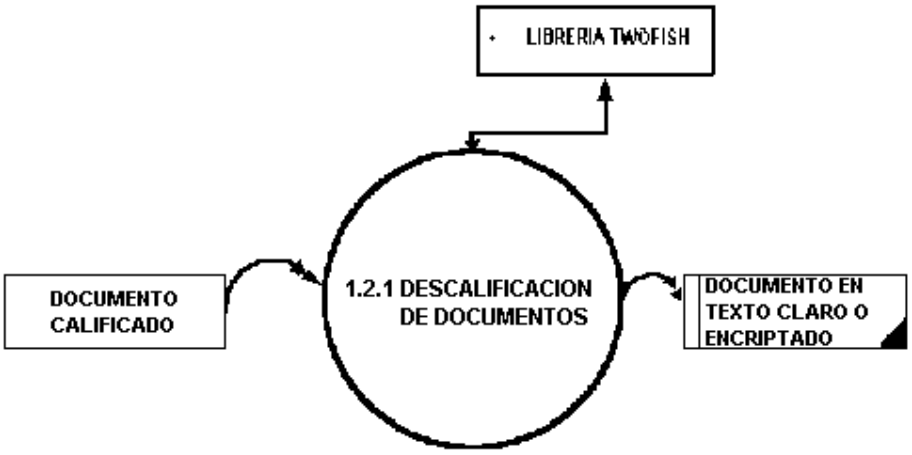


Fig. 3-7

El flujo de entrada se constituye en el documento calificado más la codificación con Twofish, y el flujo de salida es el documento

en texto claro y guardado en la carpeta Crypto / Descalificados del disco C.

Desencriptación de documentos

Una vez que se descalifica el documento este puede estar en texto claro y ya no necesita ningún paso más o puede estar encriptado con PGP, entonces nosotros podemos llamar al PGP desde nuestro programa y desencriptarlo siempre y cuando seamos el o los usuarios seleccionados para abrir el documento, para entenderlo mejor , si es que en la encriptación fue usada nuestra llave pública podremos desencriptar el documento, en caso contrario no.

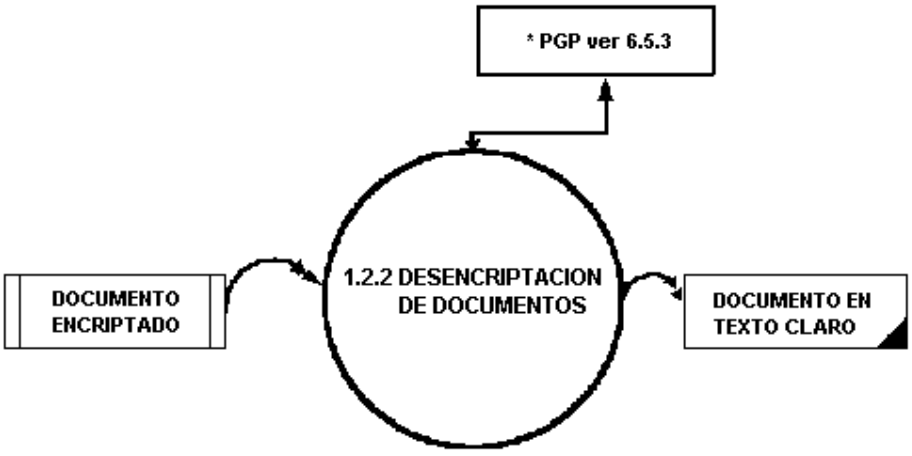


Fig. 3-8

El flujo de entrada se constituye en el documento encriptado más la aplicación de PGP, y el flujo de salida es el documento en claro y guardado en la carpeta Crypto / Criptografiados del disco C.

Transferencia de archivos

Para la transferencia de archivos se encuentra instalado y operando por mas de seis meses un servidor de comunicaciones con Microsoft Exchange instalado, esta aplicación da servicio a todos los puntos de la red de DIGMAT, el sistema llama a la carpeta de direcciones de Exchange y allí con funciones propias de la aplicación podemos anexar el documento codificado o en texto claro de acuerdo a nuestras necesidades

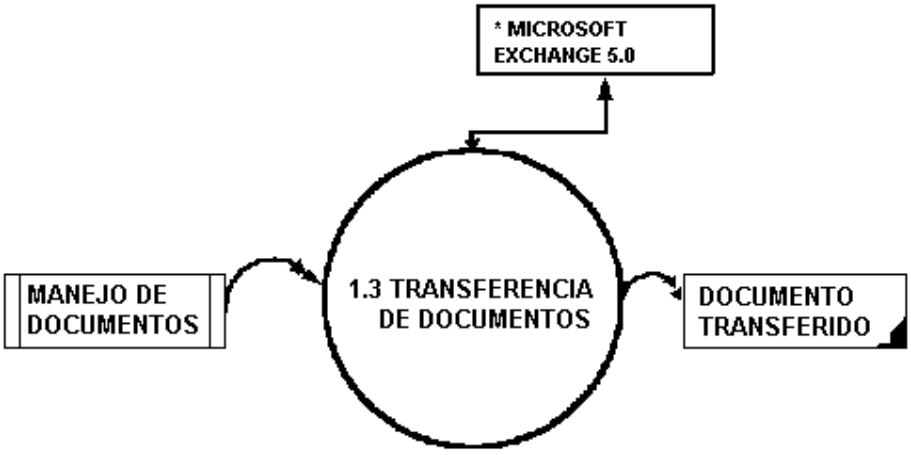


Fig. 3-9

3.1.2.3. Mensajes Emergentes

Esta actividad se constituye en un complemento que permite enviar mensajes rápidos y seguros a través de la red de DIGMAT. Usando un componente shareware para Visual Basic he querido colocar un ambiente semejante al Winpopup de Windows. Para la codificación se utiliza un código interno de codificación básica y lineal sobre el texto. Si existiese un requerimiento mayor en tiempo de uso o en capacidad de encriptación entonces podemos cerrar nuestro módulo y usar el Winpopup de Windows más PGP.

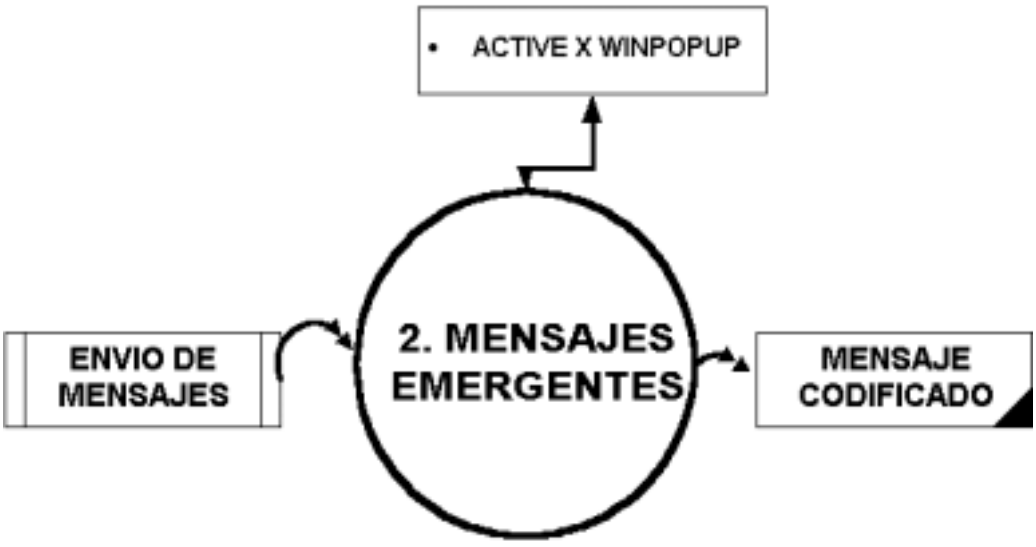


Fig. 3-10

Dentro de esta actividad el flujo corre de la siguiente manera:

- Ingresa el mensaje al sistema
- El mensaje es codificado
- El mensaje es enviado
- En la recepción, el mensaje recibido es decodificado
- Se toma conocimiento del mensaje

Debido a que la longitud de la acción es relativamente baja no he considerado la subdivisión de la misma.

3.1.2.4. Control de usuarios

Fue necesario brindar una seguridad de inicio del sistema. Para el prototipo se diseño una tabla básica en Microsoft Access principalmente para mostrar la funcionalidad de esta actividad. El control de usuarios es local y en el pueden ingresar tanto administradores como usuarios normales, claro está que, cada uno tiene diferentes privilegios.

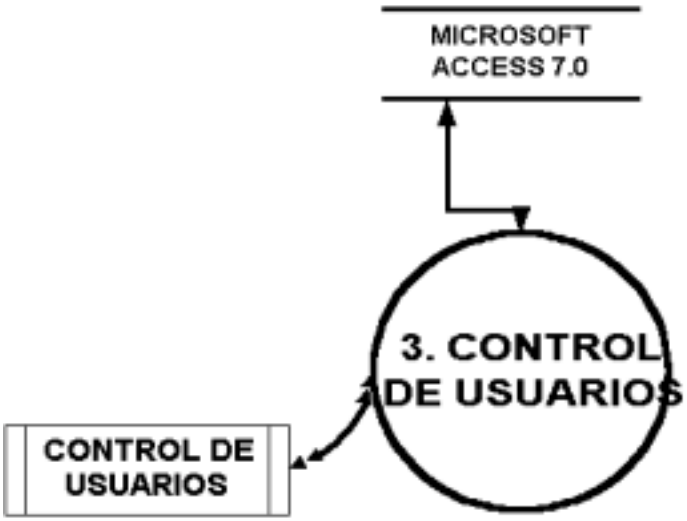


Fig. 3-11

El usuario puede ingresar al sistema y de acuerdo a su clave puede optar por las funciones de administrador o de simple usuario, por ello, fue conveniente dividir esta acción en las siguientes:

3.1. Opciones del Administrador

3.2 Opciones del Usuario

Opciones del Administrador

Una vez que el administrador ingresa al módulo este esta en la capacidad de ingresar un nuevo usuario o eliminar un usuario existente. Como flujo de entrada se receptarán el user y password y los datos del usuario a ser ingresado o eliminado,

mientras que como flujo de salida tendremos la base de datos actualizada.

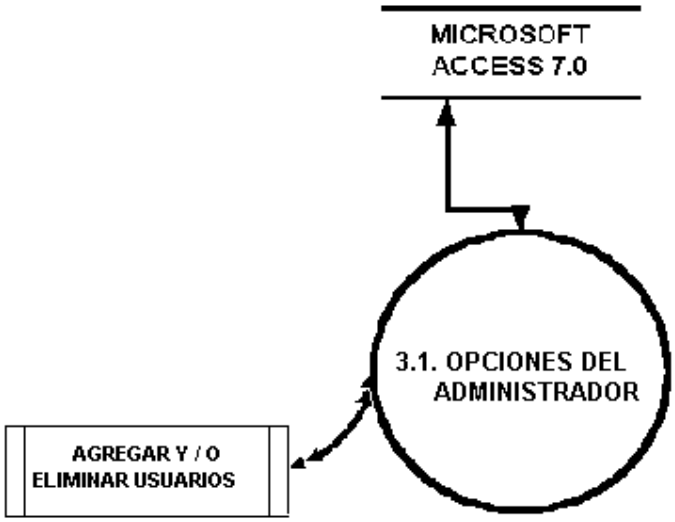


Fig. 3-12

Opciones del Usuario

Una vez que un usuario ingresa al módulo tiene la opción de modificar su password, esta necesidad se puede presentar por cualquier razón que nos haga pensar que la seguridad de nuestro password ha sido violada.

Como flujo de entrada se receptarán el user, password viejo y password nuevo, mientras que como flujo de salida también tendremos la base actualizada.

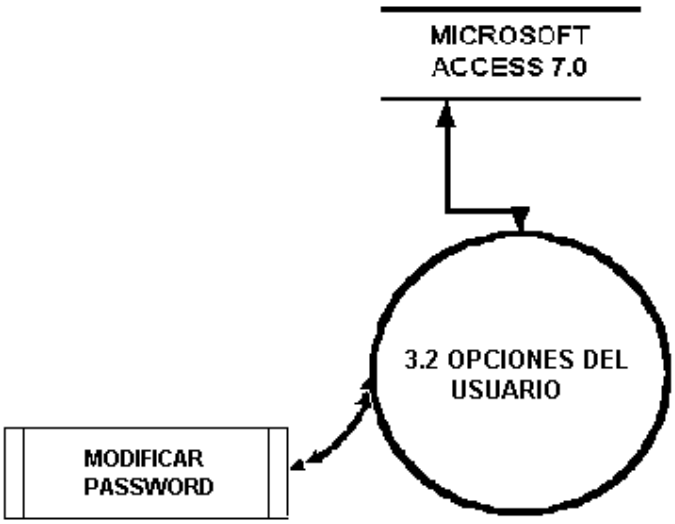


Fig. 3-13

3.1.2.5. Búsqueda de ayuda

Esta actividad a pesar de ser un adicional al objetivo buscado, no puede dejarse de lado. En esta opción nosotros podremos enlazarnos al sitio Web de soporte de proyectos y obtendremos información general del proyecto.

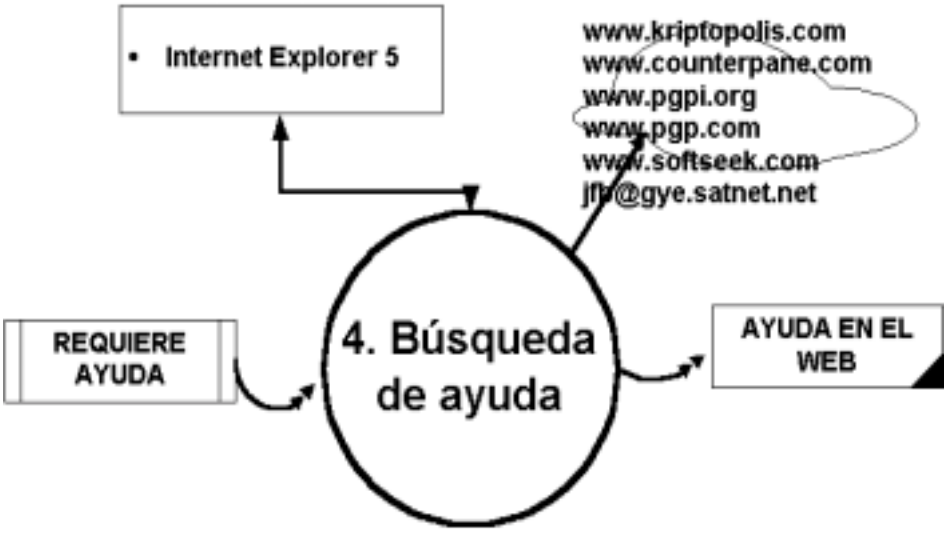


Fig. 3-14

Está propuesto la construcción a mediano plazo de un sitio Web de soporte informativo y técnico con el que el Centro de Investigaciones podrá estar presente para brindar ayuda de primera mano a todos los repartos en donde se han implementado los diversos proyectos desarrollados. Entonces brindar el enlace directo a este sitio directamente dentro del prototipo ha sido considerado como unan actividad que no puede quedar fuera de él. Como flujo de entrada tendrá la dirección o las direcciones de soporte y como flujo de salida tendrá la

información requerida, ya sean manuales, consejos, control de fallas, enlaces de interés, investigaciones adicionales, etc.

3.2. Diseño

El diseño del presente *software* se compone básicamente de 2 actividades:

- Diseño arquitectónico del prototipo
- Diseño funcional del prototipo

Como el diseño funcional tiene mas la orientación al desarrollo propiamente dicho, este aquí será obviado y se reforzará mas tarde la construcción del prototipo.

En cuanto al diseño arquitectónico del prototipo, primeramente detallaré los módulos principales de los que se compone, su nivel de participación en cuanto a la codificación y luego se bosquejará los formularios que se utilizarán en cada uno de los módulos del sistema.

3.2.1. Descripción de módulos

Una vez que hemos analizado la forma en como el flujo de los datos participa en el prototipo, hemos revisado las aplicaciones que se encuentran vinculadas; y, hemos diagramado como queremos presentar las diferentes opciones, es conveniente comenzar con la descripción de cada módulo de acción que forma parte del mismo. Dentro de este acápite vamos a describir los siguientes:

- ♠ Módulo de calificación de archivos
- ♠ Módulo de mensajes emergentes
- ♠ Módulo de manejo de cuentas internas
- ♠ Módulo de enlace a aplicaciones
- ♠ Módulo de ayuda
- ♠ Implementaciones futuras

3.2.1.1. Módulo de calificación de archivos.

Permite calificar el documento que fue previamente encriptado o no con PGP, tenemos cinco niveles de calificación: O (Ordinaria), R(Reservada), C(Confidencial), S (Secreta) y SS (Secretísimo) los cuales son manejados con diferente longitud de llave. La llave puede ser modificada de acuerdo a políticas que deben ser promulgadas por la DINFOR tanto para estas como para el manejo de las llaves públicas del PGP.

Este módulo fue construido utilizando una librería del algoritmo Twofish, en donde las claves hexadecimales de acuerdo a su calificación pueden tener un orden máximo de: O (O), R(Reservada), C(Confidencial), S (Secreta) y SS (Secretísimo).

3.2.1.2. Módulo de mensajes emergentes.

Permite el envío de mensajes rápidos y codificados similar al Winpopup con la diferencia que puedo optar por aplicar al texto

una codificación lineal propia o por PGP, y asegurar el tráfico emergente interno a la red.

3.2.1.3. Módulo de manejo de cuentas internas.

Nos ayuda a administrar localmente los usuarios y la seguridad del password de cada persona involucrada en el sistema. Se encuentra implementado usando una tabla de Access para almacenarlos, pero en el futuro estos deben ser administrados remotamente en un servidor seguro que provea actualizaciones periódicas tanto de estos usuarios como de las llaves simétricas y asimétricas usadas por cada reparto naval.

3.2.1.4. Módulo de enlace a aplicaciones.

En el prototipo enlazo dos aplicaciones: PGP y Exchange, la primera, encripta los documentos y la segunda los transmite en la red de DIGMAT.

3.2.1.5. Módulo de ayuda.

A mediano plazo se implementará un sitio de ayuda en línea para brindar soporte a todos los proyectos que maneja el Centro de Investigaciones de la Armada, en el prototipo se ha incluido un formulario navegador de Web en donde se direccionará el sitio indicado.

3.2.1.6. Módulo de implementaciones futuras.

En el anexo A se describen las facilidades de los equipos de radio HARRIS, ya utilizados en la Armada con propósitos similares, como una posible solución al enlace remoto necesario para enlazar a los buques, así mismo se describe las ventajas y posibilidades de uso de equipos de seguridad biométrica y de tarjetas criptográficas, todas estas opciones se podrán implementar siempre que exista el tiempo y los recursos necesarios.

Los módulos detallados se enlazan como se indica a continuación:

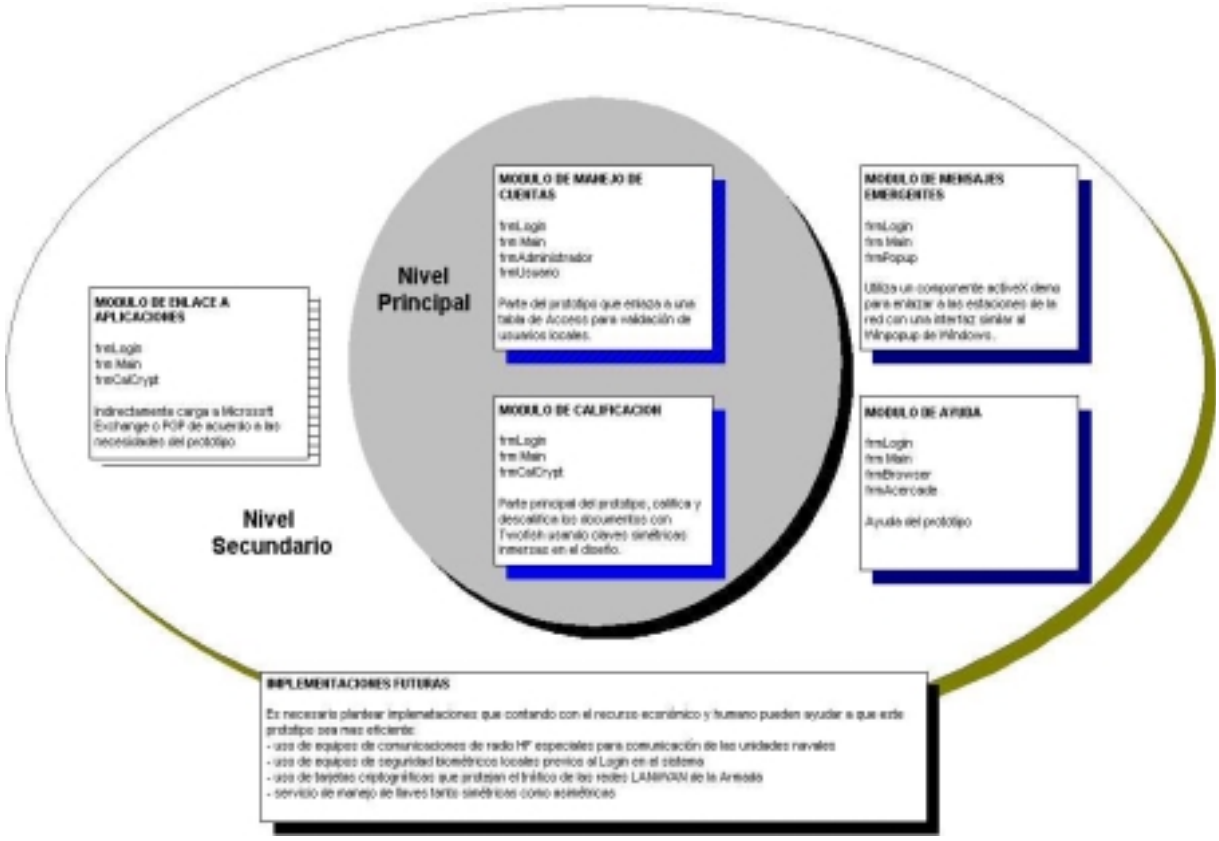


Fig. 3-15

El nivel principal encierra a todos los formularios que codifican directamente la información y controlan a los usuarios, mientras que el nivel secundario tiene relación con el enlace a las aplicaciones que actúan indirectamente junto al prototipo (Exchange y PGP).

3.2.2. Descripción de los formularios

Las formas utilizadas para el entorno utilizando el lenguaje escogido (Visual Basic 6.0) son el reflejo de las necesidades indicadas en los DFDs, agrupadas todas estas en el menú general. El menú de inicio de sesión y el menú general son los principales (Ver Figura 3-16, Figura 3-17).

Fig. 3-16

Fig. 3-17

En el nivel principal del menú tenemos 4 operaciones posibles: Archivo, Opciones, Cuentas y Ayuda. En Archivo se encuentra la suboperación que nos permite salir de la aplicación, en Opciones podemos seleccionar si vamos a manejar archivos o vamos a enviar algún mensaje emergente, en Cuentas podemos ingresar como Administrador local o como Usuario del sistema, finalmente en Ayuda podemos ingresar a una pantalla de Internet Explorer y obtener información del prototipo.

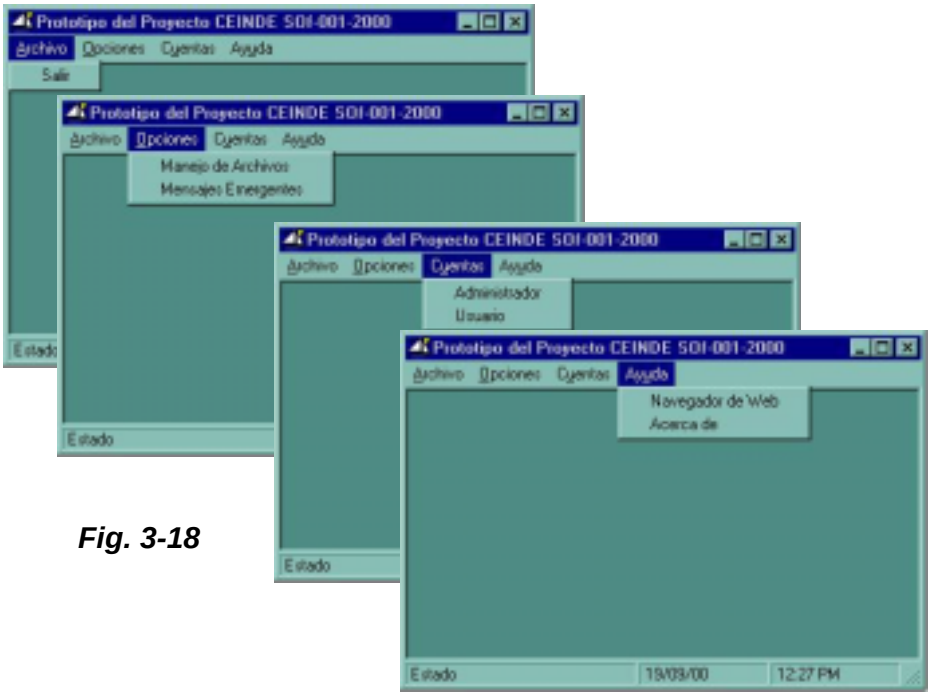


Fig. 3-18

En cuanto a Manejo de Archivos se refiere, en esta interfaz contamos con varias actividades posibles, las dos principales son el manejo de Archivos Salientes y el manejo de Archivos Entrantes, en ambas situaciones contamos con el enlace que llama tanto a PGP como Exchange para poder encriptar o desencriptar el archivo y para poder enviar el documento por la red. En la lengüeta de Archivos entrantes podemos buscar el archivo previamente encriptado o no y calificarlo físicamente con la asignación de un nuevo nombre y lógicamente usando el algoritmo Twofish con una llave propia para cada tipo de calificación, en cuanto a esta tenemos 5 requerimientos básicos de calificación de un documento: Ordinario, Confidencial, Reservado, Secreto y Secretísimo. Cuando recibimos un archivo codificado podemos descalificarlo y guardarlo en la carpeta correspondiente. Para este trabajo se ha definido la siguiente organización de archivos:

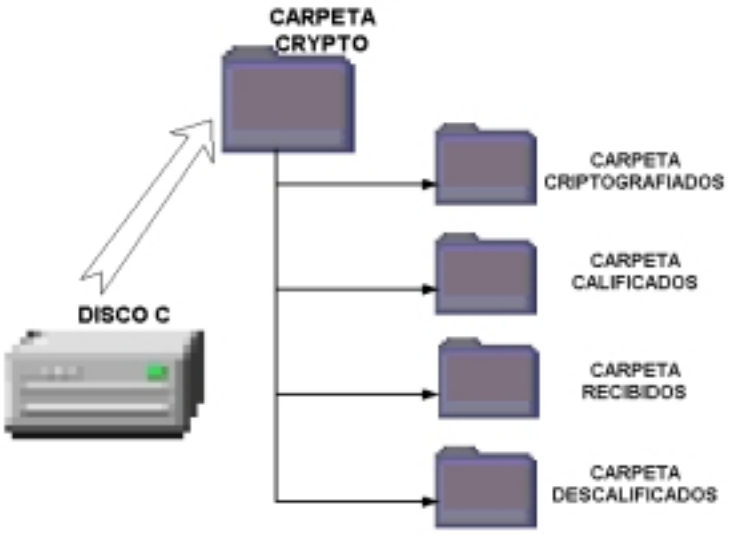


Fig. 3-19

Al utilizar el manejo de archivos salientes podemos buscar el archivo criptografiado en la carpeta indicada y si no usamos un archivo en texto claro podemos buscarlo en cualquier carpeta; este archivo calificado se guardará en la carpeta Calificados listo para ser enviado por cualquier medio.

Fig. 3-20

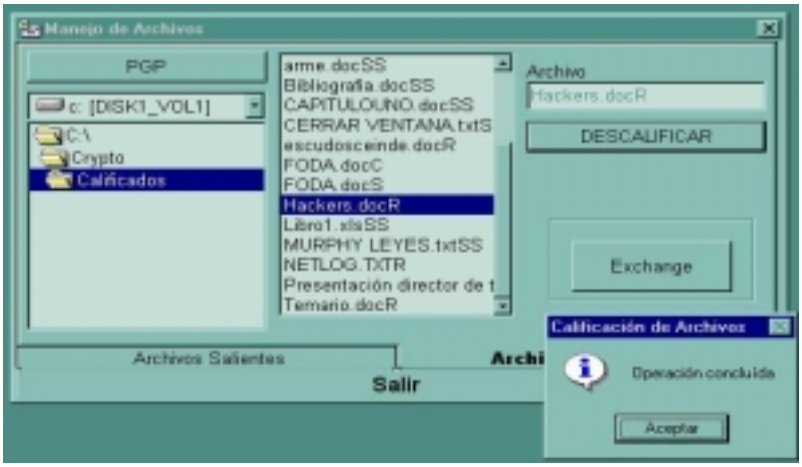


Fig. 3-21

Así mismo cuando recibimos un archivo lo debemos guardar en la carpeta Recibidos y cuando procedemos a descalificarlo se guardara en la carpeta Descalificados listo para ser leído, tramitado, distribuido o desencriptado.

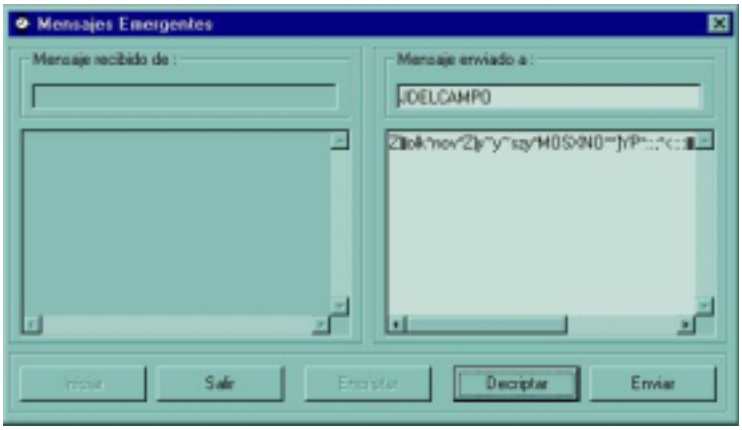


Fig. 3-22

Para los mensajes emergentes el prototipo cuenta con una interfaz similar a la utilidad Winpopup que viene con Windows 95/98. Esta pantalla permite enviar mensajes dentro de la red de DIGMAT que previamente pueden ser encriptados, para esta labor, considerando que la información dentro de estos mensajes solo será meramente administrativa, se utilizó codificación simple y lineal del mensaje. Eventualmente, en caso de requerir mayor seguridad podemos utilizar PGP para una encriptación más fuerte del mensaje.

Fig. 3-23

Para el manejo local de las cuentas de usuario de cada reparto, podemos editar la base de datos, ya sea como

administradores o usuarios. El administrador puede ingresar a la base y tiene la facilidad de modificar, eliminar o añadir usuarios.

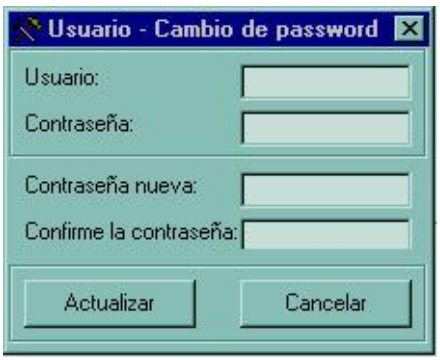


Fig. 3-24

El usuario solamente tiene la potestad de modificar su password cada vez que presienta que se han violado sus seguridades.

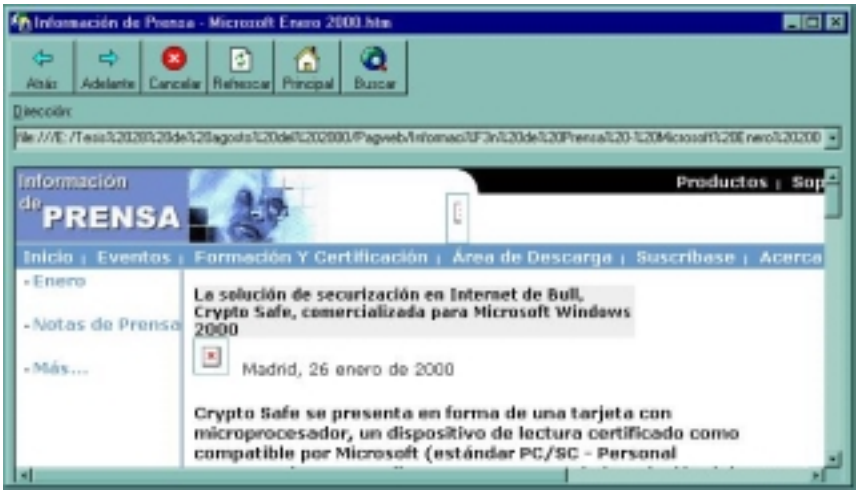


Fig. 3-25

El navegador de web existente en la ayuda permite consultar cualquier información necesaria en el momento, posteriormente podremos vincular a esta pantalla, el sitio en línea de soporte del presente proyecto.

Finalmente en la pantalla Acerca de encontramos información general del prototipo y un enlace de correo electrónico del autor.

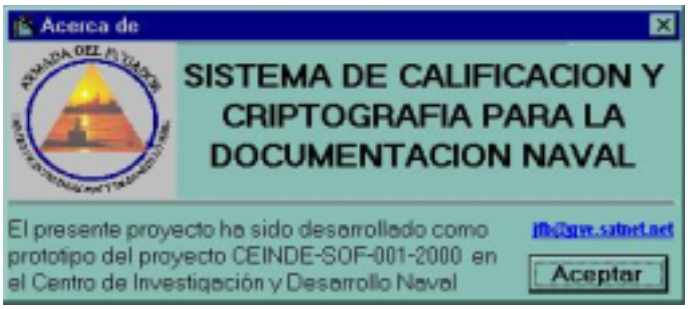


Fig. 3-26

3.3. Construcción del Prototipo

El concepto del presente trabajo radica en proveer un sistema seguro y confiable para la transferencia de documentos administrativos a través de la red de DIGMAT y posteriormente a

los demás repartos navales, entonces es conveniente que, los recursos de software usados en el proyecto y los recursos de hardware proyectados que son componentes necesarios del proyecto, sean descritos en cuanto a su funcionalidad, manejabilidad y seguridad que estos proveen.

En el anexo A se presenta un panorama mucho más claro de cómo complementan directa o indirectamente al sistema criptográfico en desarrollo el uso de los siguientes recursos de hardware y software:

- **Software:**
  - Microsoft Visual Basic 6.0 Edición Empresarial
  - Microsoft Exchange 5.0
  - Pretty Good Privacy (PGP)
  - Universal Data Terminal (UDT)
  - Controles Active X prediseñados

- **Hardware:**
  - Equipos de radio Harris RF-6710 y RF-6750
  - Sistemas biométricos
  - Tarjetas criptográficas

Después de habernos empapado de cómo trabajan los sistemas criptográficos existentes en la Institución, de haber comenzado a obtener conocimientos básicos de criptología y seguridad informática y de saber cómo aplicaciones existentes pueden ayudarnos a cumplir con nuestro objetivo, es tiempo de condensar y analizar esta información, utilizar e integrar los medios, incluirlos en el entorno y, con todo esto, colocar nuestro grano de arena en la implementación de mecanismos de seguridad de alta tecnología en la Armada del Ecuador.

Basándonos en los módulos y formularios ya detallados es necesario detallar ¿qué queremos hacer? Paso a paso dentro de los mismos. Para conseguir esto utilizaré un lenguaje normal que indique todas las tareas que se podrán realizar. Posteriormente

en los anexos B y C se incluye mayor información con un detalle del código utilizado y el manual del usuario del prototipo desarrollado.

3.3.1. Inicio de sesión

Cada vez que se inicie una nueva sesión del prototipo diseñado se mostrará una interfaz en donde se llevarán a cabo las siguientes actividades:

- Ingresar user
- Ingresar password
- Validar user y password
- En caso de error, presentar mensaje y permitir nuevo ingreso
- Permitir el ingreso al sistema
- Permitir abandonar el sistema

3.3.2. Menú Principal

Esta interfaz reúne todos los enlaces a las acciones que ejecuta el prototipo, es decir, desde aquí nosotros podremos aprovechar todas las facilidades que el sistema nos provee. Dentro de este se cumplirán las siguientes acciones:

- Acceso a la codificación y manejo de los documentos
- Acceso a la utilidad de mensajes emergentes
- Acceso a las cuentas como Administrador
- Acceso a las cuentas como Usuario
- Acceso a la ayuda en el Web
- En caso de error, presentar mensaje informativo
- Salir del sistema

3.3.3. Codificación y manejo de documentos

Esta parte quizás es la que encierra las tareas o acciones fundamentales del prototipo, he tratado de describirlas cronológicamente, aunque pueden obviarse o cambiar de lugar determinadas acciones.

- Búsqueda del archivo que será calificado o transferido
- Llamada a PGP
- Selección de la clave
- Calificación del archivo
- Descalificación del archivo
- Llamada a la libreta de direcciones de Microsoft Exchange
- En caso de error, presentar mensaje informativo
- Salir del sistema

3.3.4. Envío de mensajes emergentes

Este formulario permitirá al usuario enviar mensajes codificados a través de la red, se utiliza encriptación lineal propia del prototipo, aunque también podemos utilizar la codificación del PGP, de acuerdo a nuestras necesidades. El conjunto de tareas que podemos cumplir aquí son las siguientes:

- Conexión del sistema de mensajes
- Encriptación de la información a ser enviada
- Desencriptación del texto recibido
- Envío y recepción de los mensajes

3.3.5. Opciones del Administrador

Dentro de esta actividad el administrador local del sistema, se encuentre en un reparto en tierra o a flote, puede cumplir con las siguientes tareas:

- Creación de nuevos usuarios
- Eliminación de usuarios existentes
- Salir del sistema

3.3.6. Opciones del Usuario

Dentro de esta actividad el usuario local del sistema puede cumplir con las siguientes tareas:

- Modificar su password
- Salir del sistema

3.3.7. Navegador de Web

En esta pantalla, el usuario del prototipo podrá cumplir con las siguientes tareas:

- Enlace a sitios de soporte del prototipo
- Enlace a sitios de soporte de otros proyectos

- Enlace a sitios relacionados con la criptografía
- Enlace a sitios relacionados con la tecnología

Hasta este punto, la construcción del prototipo ya contaría con la suficiente información para ser implementado, si es requerido ya se mencionó que el código utilizado para definir todas estas actividades se encuentra en el Anexo B.

3.4. Pruebas realizadas

3.4.1. Descripción de las pruebas

El prototipo ha sido implementado con el fin de satisfacer las necesidades básicas del proyecto contemplado; por ello he trabajado en las pruebas respectivas atacando tres frentes diferentes:

- **El software desarrollado.** Básicamente la calificación y el manejo de usuarios se la hace de una manera sencilla, el

envío y recepción de los mensajes emergentes está limitado a las restricciones de la licencia del control que lo maneja; se han hecho las pruebas en máquinas Pentium II con 64 Mb de *RAM* y no se han presentado inconvenientes, al contrario en máquinas Pentium I con 16 Mb de *RAM* se presentaron problemas de falta de memoria en el momento de compilar la librería del algoritmo Twofish. Considerando las pruebas realizadas y las especificaciones de pruebas del algoritmo obtenidas en *Internet*, es aconsejable utilizar máquinas de por lo menos 32 Mb de RAM con procesadores Pentium MMX o superiores para obtener un desempeño adecuado del diseño realizado.

- **La transferencia de archivos dentro de la red de *DIGMAT* y de forma remota.** En la red *LAN* existente la transferencia realizada mediante Exchange 5.0, en el cual debemos anexar el archivo codificado por el prototipo, no ha presentado mayores inconvenientes.

- **El uso del *PGP***. Para beneficio de todos esta utilidad de seguridad es de fácil uso y amigable al usuario, nos permite encriptar texto, archivos y en la versión comercial permite la encriptación del disco duro completo, el llavero del que dispone nos facilita el manejo de llaves tanto para la codificación y decodificación de los archivos como en la validación, autenticación y revocación de las claves de los usuarios con quienes vamos a intercambiar la información.

3.4.2. Casos específicos

3.4.2.1. Transferencia de Archivos por diversos medios

La transferencia de información calificada por Internet obtuvo un promedio de 50 kb por minuto, para esta prueba se utilizó una máquina Clon Pentium II de 466 Mhz, 32 Mb de RAM, tarjeta de fax/módem de 56kbps tecnología V.90, y la aplicación utilizada fue Outlook Express 5.

La velocidad de transferencia medida se tomó en la trasmisión efectuada entre la cuenta propia del reparto (Telconet) y una cuenta pública de Hotmail. Se realizaron 5 pruebas de transferencia de diferente tamaño de acuerdo al siguiente detalle:

Enlace	**Tiempo (minutos)**	**Tamaño del archivo (kb)**	**Velocidad promedio**
Telco - Hotmail	5	240	48
Hotmail - Telco	75	3200	42.67
Hotmail - Telco	4	210	52.5
Telco - Hotmail	23	1240	53.9
Hotmail - Telco	11	560	50.91
Velocidad de transferencia promedio			***49.6 kb/min***

Tabla 3-1

Para la transferencia punto a punto usando la red telefónica pública esta velocidad llegó a obtener un promedio de 87 kb/min. Para las pruebas utilicé dos máquinas Pentium MMX de 166 Mhz, 32 Mb de RAM y los puntos se ubicaron en la Base Naval Sur con una tarjeta de fax/módem de 56 kbps y en Entre

Ríos con una tarjeta de fax/módem de 33.6 kbps, usando líneas telefónicas de centrales digitales (48 y 83 respectivamente). El software utilizado fue Supervoice para Windows 95. Los resultados parciales fueron los siguientes:

Enlace	Tiempo (minutos)	Tamaño del archivo (kb)	Velocidad promedio
ER – BASUIL	16	1240	77.5
BASUIL – ER	2	200	100
ER – BASUIL	24	2210	92.08
BASUIL – ER	4	285	71.25
BASUIL – ER	7	670	95.71
Velocidad de transferencia promedio			***87.31 kb/min***

Tabla 3-2

En la transferencia por radio HF las pruebas realizadas se tomaron dos puntos estratégicos del Comando del Teatro de Operaciones que contaban con el equipo adecuado (detallado en el Anexo A). Se utilizó la interfaz UDT (Universal Data Terminal) diseñada para las tarjetas RF-6710. El resultado de estas pruebas alcanzó una velocidad media de transferencia de

37 kb por minuto con una efectividad del 100% al enviar archivos de hasta 2Mb, las cuales se detallan a continuación:

Enlace	Tiempo (minutos)	Tamaño del archivo (kb)	Velocidad promedio
Pto1 – Pto 2	3	124	41.33
Pto 2 – Pto 1	41	1500	36.59
Pto1 – Pto 2	falla	3400	no
Pto 2 – Pto 1	58	1950	33.62
Pto1 – Pto 2	40	1420	35.5
Velocidad de transferencia promedio			***36.76 kb/min***

Tabla 3-3

3.4.2.2. Calificación de Archivos.

Para esta prueba se tomaron 3 documentos: 1 imagen en formato JPG, un documento de Word y un documento previamente encriptado con PGP; a continuación, se presenta la información extraída del documento original y extractos de la información calificada.

Imagen JPG

Calificado Confidencial

è/]|T*Ú\æ$°#[hFÇ ‘•×:¡uÌ° ¦Þ8ÖÔäA°±@

Calificado Secreto

½ß„O10ý'>p]-’ß©Ð…¿R½»Yè oªü

Calificado Secretísimo

è/]|T*Ú\æ$°#[hFÇ ‘•×:¡uÌ°

Documento de word

Este es un documento de prueba de encriptación y calificación de los documentos en el prototipo diseñado

Calificado Confidencial

W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!W¹ U©CWÆ$C+Ã m™!

Calificado Reservado

lÐ âô¨²Øy•¥<¤óè +éO¤Jj 6â îæ[ØúñÈ ³&O'É§ßåÝp &Òßû\ÁlØ1ÂÜ ©pä; ¢T%™Ñ°ñ- <q8†Z-ÅßÃµb>Ö { ”fÇ'É Â¶*—ó PÑ ›o í^, – 8göô!ÊúÎX íøÝú7î{ eèÇR-WÍœÁDu

Calificado Secreto

Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜ Åð OwßOÎ±9ÃXGÝ˜

Documento de word previamente encriptado con PGP

8ˆVKsáýd´´ Í®Iò”ó¹H¤|ÔRÔYj ÅÔ›¨³®vîY4ñøœl=&bØß
Cc #j£>!seg< 5†v*o——
ohI±gNC©¬)&¤¡ ›h]ìnwQì •FÚ<Ñ ÍÆ³¹kùMrøÉÇ Ûí¬
íM§zÐbN–
íÉ r =Ò› z _Pû F\ÀPWwX` ÉÊ9rË@Ÿ˜_Ÿeœ=c•
aÙ?r'ìH?oÒBŸaàb bé›S'º:èhÛ6Ï–@Zõcº

Calificado Ordinario

Ág D2¯/÷‰/ ï õ²â£«Pv eÔhw['~³ø4÷"} lN9: øQ—
ò?xJt ¾É ‰3è5õ /-ÑWÓj_ïõšœ&i8À?¶ mO™³
{¢+K)Ô¡iN L?¢G -¼ê t. iw •ºÔÌ%Æ…:¼Û Šç0Î
¼

Calificado Confidencial

ïü- ûó-ï-Ä2FT…Ñ6Htþ‰ ê¡Ð#õ.(LÎ°4>sèò¡
-ƒ‰FæcââB>~Âäf‰c u C ŸtÖ,unc lg_
Ã#X…ÝÍ$Y¹\ÂA¦ôÏÃXY/ûä
qºGÛéÌ•LZ#1ãSæ¤Æ% NV¿œ# £I[{=æ4/ Ò~£ØÓ
ŒþD‰ï,yÙ¨ù

Calificado Reservado

*ïü- ûó-ï-Ä2FT…Ñ6Htþ‰ ê¡Ð#õ.(LÎ°4>sèò¡
-ƒ‰FæcââÅB>~Âäf‰c u C ŸtÖ,unc lg_
Ã#X…ÝÍ$Y¹\ÂA¦ôÏÃXY/ûä
qºGÛéÌ•LZ#1ãSæ¤Æ% NV¿œ# £I[{=æ4/ Ò~£ØÓ
ŒþD‰ï,yÙ¨ù

Estos documentos al ser descalificados con la misma clave inicialmente utilizada en cada caso producen como resultado el documento original cumpliéndose el ciclo de calificación deseado.

A pesar de que los enlaces a las aplicaciones son sencillos, cumplen con el objetivo planteado, siguen un proceso similar al proceso manual actual y proveen niveles de seguridad adecuados para la transferencia de la documentación calificada a través de la red de DIGMAT y/o a través de cualquier otro medio de transmisión existente.

Es oportuno destacar que los conocimientos criptográficos en el país son muy limitados, por ello es conveniente sugerir que la criptografía y

la seguridad en redes sean incluidas en el pénsum del estudiante de nivel superior; a sabiendas de que, un manejo apropiado de estos recursos es fundamental tanto para las instituciones militares y gubernamentales como para los negocios electrónicos de cualquier magnitud.

Este proyecto se ha constituído, en el prototipo de la transferencia de archivos calificados; y se espera que, una vez concluídas todas las fases del macro proyecto que lo conjuga, se dotará a la Institución, de un sistema confiable, fácil de usar y principalmente **seguro** para las comunicaciones navales.

Al finalizar este informe, no queda mas que exponerlo al análisis y a la aprobación de la Escuela Superior Politécnica del Litoral y de la Armada del Ecuador; esperando que el trabajo demandado en estos meses de constante investigación, justifique el tiempo y el esfuerzo invertido.

CONCLUSIONES

- La solución criptográfica existente para la transferencia de documentación naval ha llegado al punto de su obsolescencia logística debido a que se compone de equipos de más de 15 años de servicio y además, la empresa proveedora ha sido cerrada.
- El prototipo realizado es parte de las primeras acciones realizadas en la Armada para actualizar tecnológicamente el sistema de seguridad en la transferencia de datos existente.
- El uso continuo dentro de la red de DIGMAT del software desarrollado proveerá de un mayor grado de seguridad para la documentación naval, así mismo será un termómetro de su eficiencia para su posterior implementación en los demás repartos navales.
- El uso de nuevas doctrinas de seguridad junto con el software desarrollado mejorará la calidad de la información procesada.

RECOMENDACIONES

- Es recomendable que los organismos encargados impulsen las siguientes fases para así llegar a una solución de seguridad actual, integral y acorde tecnológicamente a los objetivos planteados.
- Es necesario que la Dirección de Informática de la Armada provea el empuje necesario para el desarrollo de las siguientes fases del proyecto, conforme las palabras citadas de Bruce Schneier "***diseñar el sistema por completo de manera que todas las medidas de seguridad, incluyendo la criptografía, funcionen juntas***"
- Sugiero el uso de los equipos Harris de conexión remota RF-6750W y RF-6710W para proveer a las fragatas de la Escuadra Naval de puntos de red inalámbricos dentro de la red de DIGMAT, constituyéndose este enlace en el prototipo de comunicaciones remotas futuras.
- Recomiendo mantener, aumentar y promocionar el valor agregado a la información obtenida para conseguir paso a paso, los fondos y el personal necesario para el completo desarrollo del proyecto de Seguridad Naval.

ANEXO A

Aplicaciones de Hardware y Software utilizadas

En este apartado se detallan todas las aplicaciones adicionales que son utilizadas por el prototipo, tanto para criptografía como para transferencia de los archivos codificados internamente en la red de DIGMAT como remotamente hacia otros repartos o unidades navales en tierra o en la mar. Además se detallan aplicaciones de seguridad que deben ser consideradas a mediano plazo, tales como la utilización de equipos biométricos para incrementar las seguridades locales y el uso de tarjetas de red criptográficas para incrementar la seguridad en el tráfico de la red.

Microsoft Visual Basic 6.0 Edición Empresarial

Entorno visual de programación, parte del paquete Visual Studio de la compañía Microsoft Corporation ha sido utilizado como software de enlace y desarrollo por los siguientes motivos:

- El sistema Canopus de la red de DIGMAT ha sido desarrollado con la misma herramienta.

- Es un entorno de programación mucho más amigable tanto para el programador como para el usuario.
- Es compatible con el algoritmo Twofish para Visual Basic, del cual obtenemos la librería de calificación de los documentos.

Como un complemento temporal al prototipo dentro de la programación se ha usado un control Active X que trabaja similar al Winpopup de Windows 95/98, tiene los limitantes de la licencia, pero actualmente esta siendo usado como prueba para la transferencia de mensajes emergentes requerida.

Microsoft Exchange 5.0

El servicio de mensajería de Exchange está siendo probado en la red de DIGMAT por mas de 6 meses, por este medio se transmiten mensajes oficiales, el periódico del Reparto y los mensajes personales o de algún grupo de trabajo en particular. La presente aplicación ha sido instalada en un servidor que solo es utilizado para mensajería e impresiones, por lo que brinda un excelente rendimiento dentro de la red. El prototipo desarrollado enlaza a esta aplicación permitiendo el envío y la recepción, a través de la red, de los documentos encriptados y calificados.

Esta proyectado el cambio a un mediano plazo del sistema operativo de los servidores a Linux, esto no representa un problema ya que el prototipo

solamente deberá direccionarse a la nueva aplicación de mensajería que se implemente y continuará su funcionamiento transparentemente.

PGP

La aplicación PGP se trata de un proyecto iniciado a principios de los años 90 por Phill Zimmerman quien lo desarrolló para llenar el vació que existía en esos tiempos debido a la total ausencia de herramientas sencillas, potentes y baratas que acercaran la criptografía seria al usuario común.

Actualmente se ha convertido en uno de los mecanismos más populares y fiables para mantener la seguridad y la privacidad en las comunicaciones, especialmente a través del correo electrónico, tanto para pequeños usuarios como para grandes empresas. Hasta la fecha la política de distribución de PGP ha consistido en permitir su uso gratuito para usos no comerciales y en publicar el código fuente en su integridad, con el objetivo de satisfacer a los desconfiados y a los curiosos; esta aplicación se ha convertido ya en un estándar internacional (RFC 2440), ello a dado como consecuencia la aparición de múltiples productos y variaciones de PGP, herramientas para encriptar discos duros, tráfico sobre TCP/IP, etc., estas utilidades las encontramos en la versión que hemos utilizado junto con el prototipo pero en su versión comercial.

Fundamentos y estructura del PGP

PGP maneja dos conceptos básicos en su funcionamiento: el uso de criptografía asimétrica y uso del llavero Cuando usamos criptografía asimétrica debemos tener la llave pública de todos nuestros interlocutores además de nuestra llave privada propia, para manejar esta información tenemos el llavero el cual es el único fichero en el que se pueden efectuar operaciones de extracción e inserción de claves de manera sencilla, y que además proporciona un mecanismo de identificación y autentificación de llaves completo y simple de utilizar, esta facilidad en la gestión de claves es una de las causas fundamentales que han hecho a PGP tan popular. PGP para codificar un mensaje sigue los siguientes pasos:

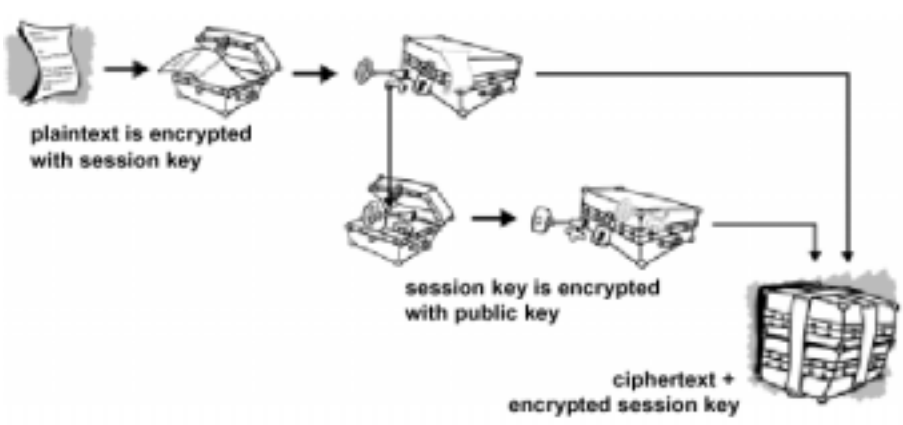


Fig. A-1

- Primero cifra el mensaje empleando *un algoritmo simétrico* con una *clave de sesión* generada aleatoriamente

- Después codifica la clave haciendo uso de la llave pública del destinatario extraída del llavero existente. Existe la posibilidad de enviar el mensaje a mas de un destinatario que se encuentre dentro de nuestro llavero.
- Si queremos firmar el mensaje codificado debemos ingresar a continuación nuestro código secreto con el que generamos nuestra llave privada, entonces el algoritmo de firma digital DSA cumple con esta acción.

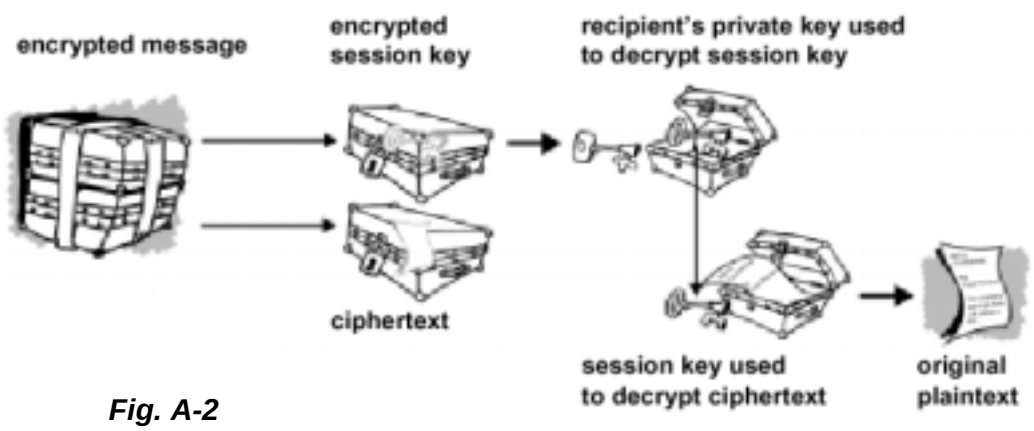


Fig. A-2

Para decodificar un mensaje llegado para nosotros debemos ingresar nuestro código secreto y abriremos el mensaje en claro. La seguridad del PGP radica en la sabia administración de muchos aspectos, tales como:

- Siempre que queremos hacer uso de nuestra clave privada en la computadora que usemos debemos ingresar nuestra contraseña, por ello si el llavero de nuestras llaves privadas es interceptado por cualquier medio necesariamente deben calcular nuestro código secreto. Si esto sucediera nosotros podemos revocar nuestras claves y generar otras.

- Debemos escoger contraseñas adecuadas, estas deben ser memorizadas, suficientemente complejas, carecer de significado, fáciles de recordar y modificadas con frecuencia para garantizar la seguridad de los mensajes generados con esta aplicación.

- Nuestros llaveros de claves públicas y privadas debemos protegerlos y respaldarlos previendo eventualidades de hardware y/o violaciones de seguridad de cualquier tipo.

- Emitir la revocación de nuestras claves inmediatamente después de haber recibido un ataque informático.

- Cuando vayamos a firmar o validar una clave, debemos estar completamente seguros de la autenticidad del interlocutor, es la única manera en la que puede funcionar nuestra red de confianza y mantenerla libre de claves falsas.

La rápida popularidad del PGP y la disponibilidad de su código fuente ha hecho posible la proliferación de variantes más complejas como por ejemplo el *PGPg* que opera con claves de mayor longitud o el *GNU-PG* que se basa únicamente en algoritmos de libre distribución.

Vulnerabilidades del PGP

Esta utilidad nos brindará un gran rendimiento siempre y cuando se la emplee correctamente, su uso inadecuado lo volvería obsoleto en cuanto a

brindar seguridad de datos; al usar PGP es conveniente tener en cuenta las siguientes recomendaciones:

- Escoger contraseñas adecuadas.
- Proteger adecuadamente los archivos sensibles
- Emitir revocaciones de nuestras claves al generarlas y guardarlas en un lugar seguro
- Firmar solo las claves de cuya autenticidad estemos seguros.

Según la información existente en cuanto a rendimiento y confiabilidad del PGP hasta ahora se podía decir que el PGP era invulnerable; sin embargo, en agosto del presente año el alemán Ralph Senderek publicó un documentado trabajo acerca de debilidades descubiertas en las nuevas versiones de PGP (5.x y posteriores). El problema afecta a todas las claves DH y RSA que usan el formato de autofirma v4. creado cuando PGP pasó a manos de la empresa Network Associates. Esta vulnerabilidad del PGP puede ser aprovechada por el criptoanalista solamente si se cumplen condiciones específicas en el entorno atacado, de todas formas es recomendable actualizar a versiones de PGP libres de esta falla (deben estar por salir) además de aplicar siempre que se requiera las recomendaciones detalladas recientemente. En caso de que este ataque sea perpetrado en nuestra red, el prototipo provee una seguridad adicional a la información cuando el archivo encriptado con PGP es diversamente calificado con un algoritmo simétrico distinto y con claves propias de la Institución.

Equipos Harris

Actualmente los equipos de comunicaciones por radio HF de la empresa Harris se encuentran instalados en varias unidades a flote y repartos en tierra de la Armada del Ecuador. Estos equipos proveen muchas características especiales en cuanto a la seguridad y confiabilidad que debe existir en el enlace. Los equipos existentes permiten la transmisión de voz encriptada y la transmisión de líneas de texto de hasta 100 caracteres, una vez que se han enganchado dos usuarios estos pueden usar funciones de enlace en frecuencias múltiples evitando la interceptación de la señal por parte del enemigo e incluso pueden recibir señales de posicionamiento global (GPS) con fines estratégicos.

Dentro de las opciones adicionales al equipo estándar existente, con el debido financiamiento podemos incluir aplicaciones tales como el UDT RF-6710 o el WG RF-6750 detallados anteriormente; y poder proveer de un punto de acceso vía HF/VHF a nuestra red a los buques de la Escuadra Naval. A continuación detallo dos aplicaciones que provee la misma empresa para explotar todas las capacidades de estos equipos de radio.

UDT RF-6710

El terminal universal de datos RF-6710 se basa en un terminal de datos para computadora que automáticamente permite transmisión de mensajes de

texto, archivos, facsímil e imágenes de alta resolución libres de errores a alta velocidad, sobre circuitos de radio HF, VHF y UHF. El UDT trabaja sobre Win95/98 y contiene además del software la tarjeta PERC (controlador de radio y generador de protocolo) la cual maneja los protocolos de enlace de datos a través del aire y las funciones de control del radio. Esta aplicación permite la transferencia de archivos y mensajes con un grado de calificación adicional, lo cual proveería a nuestro prototipo del medio físico para la transferencia de la documentación calificada y, además, un tercer nivel de seguridad para la información.

El UDT utilizado para HF hace uso de múltiples protocolos tanto para modulación como para control de errores en el enlace los cuales son parte de los estándares militares globales (especificación Std-Mil). La velocidad óptima de transferencia en HF es de hasta 9600 bps mientras que para VHF/UHF puede ser utilizada a velocidades de hasta 32000 bps. Al mirar al UDT RF-6710 como una solución a nuestro problema de enlace con los buques, podemos decir que es una solución probada y viable a mediano plazo.

Fig. A-3

Las pruebas de transferencia de archivos se las realizaron satisfactoriamente entre dos repartos que cuentan con este sistema obteniéndose una tasa de transferencia promedio de 35 Kb/min. en archivos de hasta 2 Mb. Una vez que exista el financiamiento necesario se debe adecuar los equipos de radio existentes e instalar la aplicación indicada.

WG RF-6750W

El software de ruteo inalámbrico RF-6750W permite la conexión directa a una LAN bajo TCP/IP y provee enlace remoto de múltiples servicios (e-mail, FAX, transferencia de archivos, teléfono) para múltiples plataformas (UNIX, Mac y Windows).

Fig. A-4

El RF-6750W contiene un conjunto de terminales de mensajes inalámbricos RF-6710W que permiten ver a la máquina madre como un servidor de red

físico. La aplicación consiste del software que corre bajo Windows NT y una tarjeta de hardware para sincronismo en las comunicaciones.

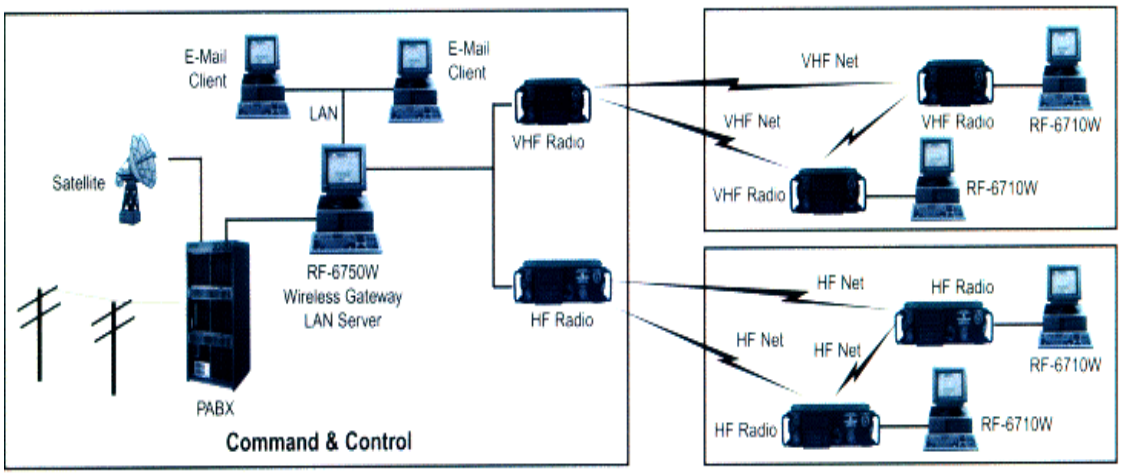


Fig. A-5

La solución tiene un alcance mucho mayor, esto implica obtener mayores recursos económicos para su implementación. Debemos tener presente que implementarla expande el brazo de la Red DIGMAT a lugares distantes y remotos tanto en la mar como en tierra, siendo quizás esta la meta a la que queremos llegar.

Controles Active X

Un control Active X es una extensión del cuadro de herramientas de Visual Basic. Los controles Active X se usan como cualquiera de los controles estándar incorporados.

Este control una vez incorporado pasa a ser parte del entorno de desarrollo y de tiempo de ejecución proporcionando nuevas funcionalidades a la aplicación desarrollada. Dentro de una aplicación podemos utilizar los controles adicionales existentes en Visual Basic, desarrollar controles nuevos o utilizar controles comerciales o gratuitos. El uso de estos controles permite encapsular procedimientos para una aplicación específica, en nuestro caso, hemos utilizado un control Active X *shareware* para proveer mensajes emergentes encriptados a nuestro prototipo.

Equipos biométricos de seguridad

Biometría, palabra derivada del griego bio (vida) y metro (medir), es la técnica automatizada que se utiliza para medir los rasgos físicos y particulares de una persona para fines de verificación de identidad. Estos sistemas básicamente leen la información de determinada parte de nuestro cuerpo y la almacenan en una base de datos para su posterior verificación, han sido desarrollados para una amplia gama de usos y aplicaciones, que varían desde controles de acceso, prevención de fraude, manejo de negocios en línea y mucho más.

En la actualidad existen varias técnicas y aparatos biométricos (miden los rasgos del rostro, las manos, la retina, la voz y la escritura), pero casi todos

actúan de manera similar: la información recopilada por el sensor nunca es almacenada y por lo tanto no puede ser reconstruida, al contrario es convertida en una serie de números o códigos que el programa asociado reconoce y almacena para usarlos únicamente al ser comparados con la huella viva, asegurándose la estricta confiabilidad del individuo. Es aconsejable estudiar detalladamente las opciones de análisis biométrico existentes y, dependiendo de la relación costo/beneficio que presenten, emitir el requerimiento adecuado.

Tarjetas criptográficas

Se debe considerar implementar a mediano plazo el uso de tarjetas criptográficas tanto para el tráfico de mensajes internos como para los externos a la Red. Existen soluciones de codificación por hardware que permiten encriptar desde todo el disco duro hasta un simple mensaje, labor realizada de una manera transparente y continua ya sea usando tarjetas adicionales a las existentes o suplantandolas con nuevas tarjetas que incluyen el chip de criptografía existentes (por ejemplo, las tarjetas de red XP de Intel o 3COM).

ANEXO B

Detalle del código

El lenguaje utilizado en el proyecto es Microsoft Visual Basic 6.0 Edición Empresarial, el prototipo consta de los siguentes formularios:

NOMBRE DEL FORMULARIO	***DESCRIPCION***
frmLogin	Formulario de inicio de sesión. Permite el acceso al sistema por parte de los usuarios o administradores autorizados.
frm Main	Formulario Principal. Permite el manejo total del prototipo desarrollado, en el menú encontramos los enlaces necesarios para la calificación y encriptación de archivos, para el envío de mensajes emergentes, para el manejo de usuarios y para la búsqueda de ayuda.
frmCalCrypt	Subformulario de calificación y encriptación. Con el podemos calificar y descalificar los documentos, llamar a PGP para encriptación o desencriptación, llamar a Exchange para envío o diseminación del archivo codificado y buscar el archivo recibido o enviado.
frmPopup	Subformulario de mensajes emergentes. Nos ayuda a tener un vínculo momentáneo con otro usuario activo de la red. Gracias a un algoritmo lineal brinda una codificación básica previa al envío del texto del mensaje, también podemos codifcarlo con PGP.
frmAdministrador	Subformulario del administrador. Permite manejar los perfiles de usuario locales del prototipo.

frmUsuario	Subformulario del usuario. Permite al usuario cambiar su password de ingreso en caso de existir anomalías en la seguridad interna.
frmBrowser	Subformulario navegador de Web. Abre una pantalla del navegador disponible en la PC, para consultas rápidas en Internet. Contendrá un vínculo al sitio Web del proyecto de Seguridad Naval cuando concluya.
frmAcercade	Subformulario de presentación. Presenta el título de la tesis, su justificativo y el enlace con el autor.

Tabla B-1

frmLogin

- *Defino las variables que enlazan la base de datos de los usuarios*

```
Dim Ruta_base As String
Dim Abre_base As Database
Dim Abre_tabla As Recordset

Option Explicit
```

- *Comando que cierra el formulario y cierra el programa*

```
Private Sub cmdCancel_Click()

    End

End Sub
```

- *Al cargar del formulario debo ejecutar ...*

```
Private Sub Form_Load()
```

- *validación de posibles errores*

```
    On Error GoTo error
    '**************
    Exit Sub
    error:
    MsgBox Err.Description, vbCritical

End Sub
```

- *Acciones a seguir una vez que se ingresó el user y password*

```
Private Sub cmdOK_Click()
```

- *defino una variable para almacenar la consulta a la base*

```
    Dim Glb_Sql As String
```

- *direcciono la base de datos previo a la consulta*

```
    Ruta_base = App.Path
    Ruta_base = Ruta_base + "\datos.mdb"
    Set Abre_base = OpenDatabase(Ruta_base)
```

- *consulto si existe el usuario ingresado*

```
    Glb_Sql = "SELECT usuario,clave FROM usuarios" _
    & " WHERE usuario='" & User_caja.Text & "' and clave='" &
    Pass_caja.Text & "';"
```

- *abro la base para efectuar la comparación*

```
    Set Abre_tabla = Abre_base.OpenRecordset(Glb_Sql,
    dbOpenDynaset)
```

- *si no he llegado al final de la tabla sin resultado, significa que la búsqueda del usuario dio una coinicdencia, presento el formulario principal y oculto el formulario actual*

```
    If Not Abre_tabla.EOF Then
            frmMain.Show
```

```
            Unload frmLogin
        Else
```
- *caso contrario, debo preguntar si desea continuar intentando o no*

```
            If MsgBox("Clave Incorrecta, ¿Desea continuar?", vbQuestion +
            vbYesNo, "SISTEMA DE SEGURIDAD NAVAL") = vbYes Then
                User_caja.Text = ""
                Pass_caja.Text = ""
                User_caja.SetFocus
            Else
                Abre_tabla.Close
                Abre_base.Close
                End
            End If
        End If
```

- *antes de salir, cierro la base*

```
        Abre_tabla.Close

End Sub
```

- *comando que envia la señal al botón Aceptar desde la caja de password con la tecla Enter*

```
Private Sub Pass_caja_KeyPress(KeyAscii As Integer)
If KeyAscii = 13 Then
   cmdOK.SetFocus
   End If
End Sub
```

frmMain

- *Definición automática de la carga y descarga del formulkario MDI*

```
Private Sub MDIForm_Load()
   Me.Left = GetSetting(App.Title, "Settings", "MainLeft", 1000)
   Me.Top = GetSetting(App.Title, "Settings", "MainTop", 1000)
   Me.Width = GetSetting(App.Title, "Settings", "MainWidth", 6500)
   Me.Height = GetSetting(App.Title, "Settings", "MainHeight", 6500)
End Sub

Private Sub MDIForm_Unload(Cancel As Integer)
   If Me.WindowState <> vbMinimized Then
      SaveSetting App.Title, "Settings", "MainLeft", Me.Left
      SaveSetting App.Title, "Settings", "MainTop", Me.Top
      SaveSetting App.Title, "Settings", "MainWidth", Me.Width
      SaveSetting App.Title, "Settings", "MainHeight", Me.Height
   End If
End Sub
```

- *Menú Salir carga la forma correspondiente*

```
Private Sub mnuFileExit_Click()
End
End Sub
```

- *Menú Manejo de Archivos carga la forma correspondiente*

```
Private Sub mnuSegcnaArchivos_Click()
frmCalCrypt.Show
End Sub
```

- *Menú Mensajes emergentes carga la forma correspondiente*

```
Private Sub mnuSegcnaEmergentes_Click()
frmPopup.Show
End Sub
```

- *Menú cuenta de usuario carga la forma correspondiente*

```
Private Sub Usuario_Click()
```

```
frmUsuario.Show
End Sub
```

- *Menú Administrador carga la forma correspondiente*

```
Private Sub Administrador_Click()
frmAdministrador.Show
End Sub
```

- *Menú navegador de Web carga la forma correspondiente*

```
Private Sub mnuHelpNavegadorWeb_Click()
Load frmBrowser
End Sub
```

- *Menú Acercade carga la forma correspondiente*

```
Private Sub mnuHelpAbout_Click()
frmAcercade.Show
End Sub
```

frmCalCrypt

- *Acciones a seguir al cargar el formulario*

```
Private Sub Form_Load()
On Error GoTo error
Dim i As Integer
Dim Var_Califica As String
```

- *Conexión con Exchange*

```
   MAPISession1.SignOn
   MAPISession1.LogonUI = True
   MAPIMsg1.SessionID = MAPISession1.SessionID
   MAPIMsg1.MsgIndex = -1
```

- A pesar de no existir el servidort de impresión, puedo continuar con la ejecución del programa

```
Sin_Sesion:
   SSTab1.Tab = 0
   Var_Califica = ""
```

- *Añado items de calificación al combo respectivo*

```
   For i = 1 To 5
      Select Case i
         Case 1:
            Var_Califica = "Ordinario"
         Case 2:
            Var_Califica = "Confidencial"
         Case 3:
            Var_Califica = "Reservado"
         Case 4:
            Var_Califica = "Secreto"
         Case 5:
            Var_Califica = "Secretisimo"
      End Select
      Cmb_Calificacion.AddItem Var_Califica
   Next i
Exit Sub
```

- En caso de error

```
error:
If Err.Number = 32003 Then
  MsgBox "No se pudo establecer la conexión con el Servidor ", vbInformation
  GoTo Sin_Sesion
Else
  MsgBox Err.Description, vbInformation
End If

End Sub
```

- *Procedimientos de direccionamiento en las diversas carpetas de la PC para la lengüeta de salientes (1) y para la de entrantes (2)*

```
Private Sub Dir1_Click()
   File1.Path = Dir1.Path
   File1.Refresh
   Text_Arch_seleccionado = ""
End Sub

Private Sub Dir1_Change()
   File1.Path = Dir1.Path
   File1.Refresh
   Text_Arch_seleccionado = ""
End Sub

Private Sub Dir2_Click()
   File2.Path = Dir2.Path
   File2.Refresh
End Sub

Private Sub Dir2_Change()
   File2.Path = Dir2.Path
   File2.Refresh
End Sub

Private Sub Drive1_Change()

On Error GoTo driverror
Dir1.Path = Drive1.Drive
Exit Sub
```

```
driverror:
MsgBox Err.Description, vbInformation, "Manejo de Archivos"
End Sub

Private Sub Drive2_Change()

On Error GoTo driverror
Dir2.Path = Drive2.Drive

Exit Sub
driverror:
MsgBox Err.Description, vbInformation, "Manejo de Archivos"
End Sub

Private Sub File1_Click()
Text_Arch_seleccionado = File1.List(File1.ListIndex)
End Sub

Private Sub File2_Click()
Txt_Arch_Encryp = File2.List(File2.ListIndex)
End Sub
```

- *Procedimientos de llamada a las herramientas de PGP para las opciones de salientes y entrantes*

```
Private Sub pgp_descal_Click()
 On Error Resume Next
       Dim i
       i = Shell("C:\Archivos de programa\Network
Associates\Pgp\PGPTools.exe ", vbNormalFocus) '& Txt_Calificado.Text & "",
vbNormalFocus)
End Sub

Private Sub pgp_cal_Click()
On Error Resume Next
   Dim i
       i = Shell("C:\Archivos de programa\Network
Associates\Pgp\PGPTools.exe ", vbNormalFocus) '& Txt_Calificado.Text & "",
vbNormalFocus)
End Sub
```

- *Procedimientos de llamada al directorio de Exchange para el envío o diseminación de los archivos codificados o en texto claro*

```
Private Sub Exchange_Click()
On Error GoTo error
'llamo a la libreta de direcciones de exchange
MAPIMsg1.Compose
MAPIMsg1.AddressResolveUI = True
MAPIMsg1.Show
'abro pantalla de envio de mensajes
MAPIMsg1.ResolveName
'titulo del mensaje (opcional)
MAPIMsg1.MsgSubject = "Nuevo mensaje"
'mensaje (opcional)
MAPIMsg1.MsgNoteText = "Anexo documento calificado"
MAPIMsg1.Send True
error:
If Err.Number = 0 Then
MsgBox "Operación exitosa"
Else
MsgBox Err.Description, vbInformation, "Salir de Exchange"
End If

End Sub

Private Sub Exchange2_Click()
On Error GoTo error
'llamo a la libreta de direcciones de exchange
MAPIMsg1.Compose
MAPIMsg1.AddressResolveUI = True
MAPIMsg1.Show
'abro pantalla de envio de mensajes
MAPIMsg1.ResolveName
'titulo del mensaje (opcional)
MAPIMsg1.MsgSubject = "Nuevo mensaje"
'mensaje (opcional)
MAPIMsg1.MsgNoteText = "Anexo al presente dignese/sirvase encontrar documento"
MAPIMsg1.Send True
error:
```

```
If Err.Number = 0 Then
MsgBox "Operación exitosa"
Else
MsgBox Err.Description, vbInformation, "Salir de Exchange"
End If
End Sub
```

- *Definición de variables del formulario y del algoritmo Twofish*

```
Dim Ruta_base As String
Dim Abre_base As Database
Dim Abre_tabla As Recordset
Dim sKey As String
Dim Origen, Destino As String
Option Explicit
```

- Enumerador que define la acción a seguir por el algoritmo

```
   Private Enum eActionDef
        Encrypt = 1
        Decrypt = 2
   End Enum

Private Sub voidAction(iAction As eActionDef)
   On Error Resume Next

   Dim bKey() As Byte
   Dim bInput() As Byte
   Dim bOutput() As Byte
   Dim lCount As Long
   Dim oTwofish As New clsTwofish
   ReDim bKey(Len(sKey) / 2 - 1)

   For lCount = 0 To Len(sKey) / 2 - 1
      bKey(lCount) = CByte("&h" & Mid(sKey, lCount * 2 + 1, 2))
   Next

   oTwofish.bKey = bKey
Select Case iAction
      Case eActionDef.Encrypt
         bOutput = oTwofish.bEncrypt(bInput)
      Case eActionDef.Decrypt
         bOutput = oTwofish.bDecrypt(bInput)
   End Select
```

- validacion de la calificacion / descalificacion

```
 If iAction = Encrypt Then
      Open "c:\Crypto\Calificados\" & Txt_Calificado.Text For Binary As #1
   Else
      Open Destino For Binary As #1
   End If

   Put #1, , bOutput
   Close #1
End Sub
```

- Calificación del documento con Twofish (Algoritmo simétrico, claves hexadecimales)

```
Private Sub Cmb_Calificacion_Click()
   On Error GoTo error
   Dim Var_Califica As String
   If Trim(Cmb_Calificacion.Text) = "" Then
      Exit Sub
   End If
   Var_Califica = ""
     sKey = ""
   Select Case Cmb_Calificacion.Text
```

- Orden de la clave de hasta O^{64}

```
Case "Ordinario":
         Var_Califica = "O"
         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA45"
```

- Orden de la clave de hasta O^{128}

```
Case "Confidencial":
         Var_Califica = "C"
         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA45"
```

- Orden de la clave de hasta O^{160}

```
Case "Reservado":
```

```
        Var_Califica = "R"
        sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28A
C31DD8AE5DAAAB63182B02D81497EA45"
```

- Orden de la clave de hasta O^{224}

```
Case "Secreto":
        Var_Califica = "S"
        sKey =
"7AFF7A70CA2FF28AC31DD8A7AFF7A70CA2FF28AC31DD8AE5DAAAB6
3182B02D81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D
81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA4
5E5DAAAB63182B02D81497EA45"
```

- Orden de la clave de hasta O^{256}

```
Case "Secretisimo":
        Var_Califica = "SS"
        sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28A
C31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28AC31DD8A
E5DAAAB63182B02D81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB
63182B02D81497EA45"

End Select

   If Text_Arch_seleccionado.Text <> "" Then
      Txt_Calificado.Text = Text_Arch_seleccionado.Text & Var_Califica
      'se procede a grabar el archivo calificado
      Origen = File1.Path & "\" & Text_Arch_seleccionado.Text
      If Mid(Origen, 3, 2) = "\\" Then
         Origen = File1.Path & Text_Arch_seleccionado.Text
      End If
      Destino = "c:\Crypto\Cal_Cryp\" & Txt_Calificado.Text
      If Origen <> "" And Destino <> "" Then

         Me.MousePointer = 11
         Call voidAction(Encrypt)
         Me.MousePointer = 0
      End If
   End If
```

```
  Exit Sub
```

- Descalificación del documento con Twofish (Algoritmo simétrico, claves hexadecimales)

```
Private Sub Command2_Click()
   sKey = ""
   Me.MousePointer = 11

If Txt_Arch_Encryp.Text <> "" Then
      'se procede a obtener el archivo encryptado
      Origen = File2.Path & "\" & Txt_Arch_Encryp.Text
      If Mid(Origen, 3, 2) = "\\" Then
         Origen = File2.Path & Txt_Arch_Encryp.Text
      End If
      'Destino = App.Path & Mid(Txt_Arch_Encryp.Text, 1,
Len(Txt_Arch_Encryp.Text) - 1)
      Destino = "c:\Crypto\Descalificados\" & Mid(Txt_Arch_Encryp.Text, 1,
Len(Txt_Arch_Encryp.Text) - 1)
```

- se usan las mismas claves para descalificar

```
Select Case Mid(Txt_Arch_Encryp.Text, Len(Txt_Arch_Encryp.Text), 1)

Case "O":
         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA45"

Case "C":
         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA45"

Case "R":
         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28A
C31DD8AE5DAAAB63182B02D81497EA45"

Case "S":
         sKey =
"7AFF7A70CA2FF28AC31DD8A7AFF7A70CA2FF28AC31DD8AE5DAAAB6
3182B02D81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D
```

```
81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA4
5E5DAAAB63182B02D81497EA45"

End Select

Select Case Mid(Txt_Arch_Encryp.Text, Len(Txt_Arch_Encryp.Text) - 1, 2)
      Case "SS":
         Destino = "c:\Crypto\Descalificados\" & Mid(Txt_Arch_Encryp.Text, 1,
Len(Txt_Arch_Encryp.Text) - 2)

         sKey =
"7AFF7A70CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70
CA2FF28AC31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28A
C31DD8AE5DAAAB63182B02D81497EA457AFF7A70CA2FF28AC31DD8A
E5DAAAB63182B02D81497EA457AFF7A70CA2FF28AC31DD8AE5DAAAB
63182B02D81497EA45"
   End Select

      If Origen <> "" And Destino <> "" Then
         Call voidAction(Decrypt)
      End If
   End If

   Me.MousePointer = 0
End Sub
```

- Comando salir del formulario

```
Private Sub Cmd_Salir_Click()
   Unload frmCalCrypt
End Sub
```

frmPopup

- *Acciones a seguir al iniciar y cargar el formulario*

```
Public msErrorMsg As String

Private Sub Form_Load()
Call cmdStart_Click
CmdEncrypta.Enabled = True
CmdDecrypta.Enabled = True
End Sub
```

- *Rutinas de manejo del control Winpopup*

  - Envío de la información

```
Private Sub cmdSend_Click()

   WinPopup1.MsgSize = 512
   WinPopup1.Msg = txtSend
   txtComputerName.Refresh
   WinPopup1.UserOrComputerName = txtComputerName
   WinPopup1.SendToComputer
   txtSend.Text = ""
   MsgBox "Mensaje enviado", vbInformation, "Prototipo"
  CmdEncrypta.Enabled = True
End Sub
```

  - Inicio del Winpopup residente del prototipo

```
Private Sub cmdStart_Click()
   msErrorMsg = ""
   ret = WinPopup1.StartPopup

   If ret = 0 Then
      cmdStart.Enabled = False
   Else
      MsgBox (msErrorMsg)
   End If

End Sub
```

- Permite el ingreso del nombre de destinatario solo en mayúsculas (necesario para el protocolo UDP de la red de DIGMAT)

```
Private Sub txtComputerName_Change()
txtComputerName.Text = UCase(txtComputerName.Text)
txtComputerName.SelStart = Len(txtComputerName)
End Sub
```

- Permite la recepción del mensaje enviado por otro originador

```
Private Sub WinPopup1_Message(MsgFrom As String, MsgTo As String, Msg As String)
On Error Resume Next

   If Msg <> "" Then
   Text1 = ""
   Text2 = MsgFrom
   Text1 = Msg
  ' Text1 = Text1 & MsgFrom & vbCrLf & Msg & vbCrLf
   CmdDecrypta.Enabled = True
   End If

End Sub
```

- Rutina de error

```
Private Sub WinPopup1_Error(ErrorMsg As String)
   msErrorMsg = ErrorMsg
End Sub
```

- *Rutina de encriptamiento del texto*

```
Private Sub CmdEncrypta_Click()
Call Encripta
End Sub

Private Sub Encripta()
Dim new_word As String

i = 1
new_word = ""
Len_Clave = Len(Trim(txtSend.Text))
```

```
Do While Not i > Len_Clave
   Letra = Mid(txtSend.Text, i, 1)
   'Letra = Chr(Asc(Letra) + Asc("A"))
   Letra = Chr(Asc(Letra) + "10")
   new_word = new_word + Letra
   i = i + 1
Loop

txtSend.Text = new_word
CmdEncrypta.Enabled = False
'Var_Encripto = True
End Sub
```

- *Rutina de desencriptamiento del texto*

```
Private Sub CmdDecrypta_Click()
Call Desencripta
End Sub


Private Sub Desencripta()
If Trim(Text1.Text) <> "" Then
Else
   Exit Sub
End If
i = 1
new_word = ""
Len_Clave = Len(Trim(Text1.Text))

Do While Not i > Len_Clave
   Letra = Mid(Text1.Text, i, 1)
   'Letra = Chr(Asc(Letra) - Asc("A"))
    Letra = Chr(Asc(Letra) - "10")
   new_word = new_word + Letra
   i = i + 1
Loop
Text1.Text = new_word
CmdDecrypta.Enabled = False
'Var_Desincripto = True
End Sub
```

- *Rutina de salida y parada del control Winpopup*

```
Private Sub cmdExit_Click()
   WinPopup1.StopPopup
   Unload Me
End Sub
```

frmAdministardor

- *Inicializa el formulario*

```
Dim Ruta_base As String
Dim Abre_base As Database
Dim Abre_tabla As Recordset

Option Explicit

Private Sub Form_Load()
On Error GoTo error
'*************
Exit Sub
error:
MsgBox Err.Description, vbCritical
End Sub
```

- *Comprobar si quien ingresa es realmente el administrador del sistema*

```
Private Sub Cmd_Entrar_Click()
Dim Glb_Sql As String

Ruta_base = App.Path
Ruta_base = Ruta_base + "\datos.mdb"
Set Abre_base = OpenDatabase(Ruta_base)
Glb_Sql = "SELECT usuario,clave FROM usuarios" _
   & " WHERE usuario='" & TxtUser.Text & "' and clave='" & TxtPass.Text & "'
AND TIPO='ADMIN';"
   Set Abre_tabla = Abre_base.OpenRecordset(Glb_Sql, dbOpenDynaset)

   If Not Abre_tabla.EOF Then
      MsgBox "Bienvenido Administrador", vbInformation, "Mensaje del
Sistema"
```

- abre el formulario y habilita los frames de edicion de usuarios

```
      frmAdministrador.Width = 6480
      Frame_Uno.Enabled = True
      Frame_Dos.Enabled = True
   Else
```

```
        MsgBox "Acceso permitido solo al Administrador", vbCritical, "Mensaje del Sistema"
        frmAdministrador.Width = 1650

        Frame_Uno.Enabled = False
        Frame_Dos.Enabled = False
    End If

Abre_tabla.Close
Abre_base.Close
End Sub
```

- *fin del formulario*

```
Private Sub Command1_Click()
Unload Me
End Sub

Private Sub adminSalir_Click()
Unload Me
End Sub
```

frmUsuario

- *Inicializa el formulario*

```
Dim Ruta_base As String
Dim Abre_base As Database
Dim Abre_tabla As Recordset

Option Explicit

Private Sub Form_Load()
On Error GoTo error
'*************
Exit Sub
error:
MsgBox Err.Description, vbCritical
End Sub
```

- actualización de la clave de usuario

```
Private Sub usuarioActualiza_Click()
Dim Glb_Sql As String
Dim find As Boolean
find = False
```

- validacion de nueva contraseña

```
If Text3.Text <> Text4.Text Then
MsgBox "No coinciden las claves"
Text3.Text = ""
Text4.Text = ""
Else
Ruta_base = App.Path
Ruta_base = Ruta_base + "\datos.mdb"
Set Abre_base = OpenDatabase(Ruta_base)

  Glb_Sql = "SELECT clave FROM usuarios" _
    & " WHERE clave='" & Text2.Text & "';"

Set Abre_tabla = Abre_base.OpenRecordset(Glb_Sql, dbOpenDynaset)
If Not Abre_tabla.EOF Then
      find = True
```

```
Else
     If MsgBox("Clave Incorrecta, ¿Desea continuar?", vbQuestion + vbYesNo,
    "SISTEMA DE SEGURIDAD NAVAL") = vbYes Then
        Text2.Text = ""
        Text2.SetFocus
        Else
        Unload Me
        Abre_tabla.Close
        Abre_base.Close

        End If
    End If
```

- cambia la clave de usuario

```
If find = True Then
    Glb_Sql = "UPDATE usuarios" _
    & " SET clave='" & Text4.Text & "';"
    Abre_base.Execute Glb_Sql
    Unload frmUsuario
    MsgBox "Operacion Exitosa", vbExclamation
Abre_tabla.Close
End If
End If

End Sub
```

- *fin del formulario*

```
Private Sub usuarioCancela_Click()
Unload Me
End Sub
```

frmBrowser

Código autogenerado por Visual Basic

frmAcercade

Sin código importante

ANEXO C

Manual del usuario

MANEJANDO EL PROTOTIPO PASO A PASO

INICIO DE SESION

Con el inicio del prototipo se llama a la pantalla de validación de usuarios, solamente quienes existan en la base de datos local, ya sea como administradores o como usuarios corrientes, podrán ingresar al sistema; en caso contrario, no lo podrán hacer

Fig. C-1

PANTALLA PRINCIPAL

Dentro de este entorno se albergan las demás pantallas del prototipo. En el Menú dispongo de las siguientes opciones:

Fig. C-2

MENU	SUBMENU	DESCRIPCION
ARCHIVO	SALIR	Comando utilizado para salir del prototipo
OPCIONES	MANEJO DE ARCHIVOS	Comando utilizado para obtener la pantalla que permite calificar y manejar los archivos, llamar al PGP y al Exchange
	MENSAJES EMERGENTES	Comando utilizado para obtener la pantalla que permite enviar y recibir mensajes cortos y encriptados utilizando una utilidad shareware similar al winpopup de Windows
CUENTAS	ADMINISTRADOR	Comando que llama a la pantalla que permite a la persona soporte del sistema administrar los usuarios existentes
	USUARIO	Comando que llama a la pantalla que permite al usuario cambiar su password o contraseña

MENU	SUBMENU	DESCRIPCION
AYUDA	NAVEGADOR DE WEB	Comando que llama al navegador de Web. Posteriormente se diseñará un sitio web de ayuda/sopòrte en línea para este y para otros sistemas de diversa índole.
	ACERCA DE	Comando que llama a la pantalla de información del prototipo y del autor

Tabla C-1

MANEJO DE ARCHIVOS

En esta pantalla tengo dos opciones: manejo de archivos entrantes y manejo de archivos salientes

- En el manejo de archivos salientes puedo seleccionar el archivo de Word, Excel, Power Point o PGP que deseo calificar.
- Selecciono la calificación y el documento resultante se guarda en la carpeta de Calificados.
- Previamente puedo llamar al PGP para encriptar el archivo, también puedo llamar al Exchange para enviar el nuevo documento por la Red DIGMAT.

Fig. C-3

- En la lengüeta de los recibidos en cambio tengo la facilidad de seleccionar el archivo recibido y descalificarlo para que este documento de word, Excel, Power Point o PGP pueda ser editado.

- Puedo llamar al PGP para desencriptarlo si lo requiero o, puedo llamar al Exchange si quiero redistribuir el documento.

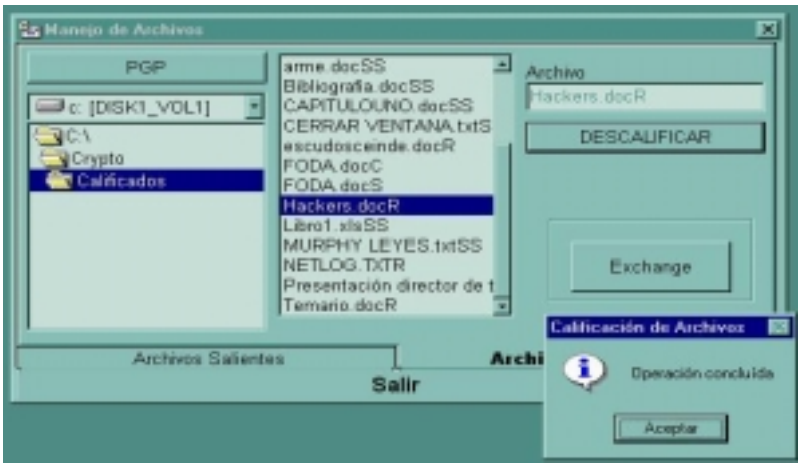


Fig. C-4

MENSAJES EMERGENTES

El envío de los mensajes emergentes se lo realiza con una aplicación shareware obtenida en Internet, similar al Winpopup de Windows y se le ha adaptado una criptografía básica sobre el texto corriente la que se puede o no aplicar antes de enviar el mensaje al usuario seleccionado. Esta aplicación tiene una duración de 10 minutos como limitante de su licencia.

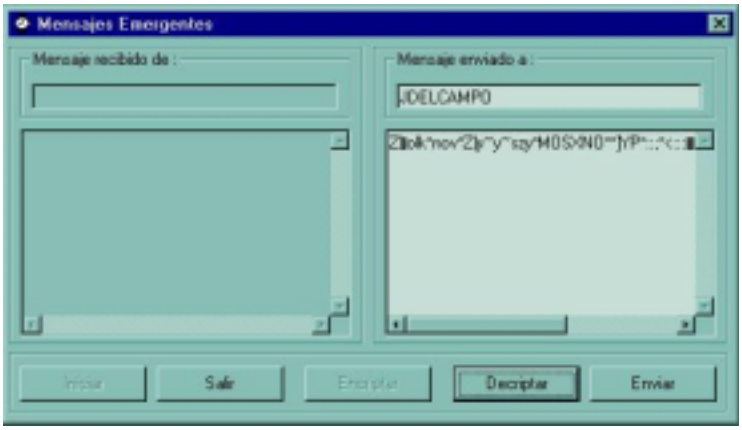


Fig. C-5

CUENTAS

Opción que nos ayudará en la administración local de usuarios y de passwords tanto al administrador del sistema como a los usuarios respectivamente.

Fig. C-6

Fig. C-7

AYUDA

En la opción de ayuda existe un navegador de web propio del prototipo que direccionará al sitio de soporte que se construirá en el CEINDE para todos los proyectos desarrollados, además se incluye la información del prototipo y del autor.

Fig. C-8

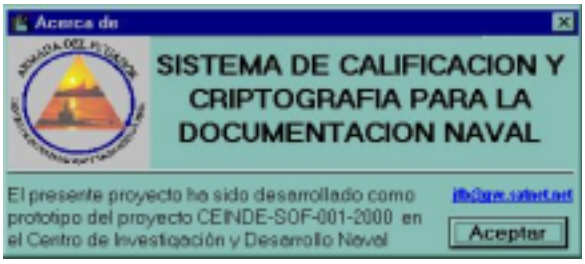
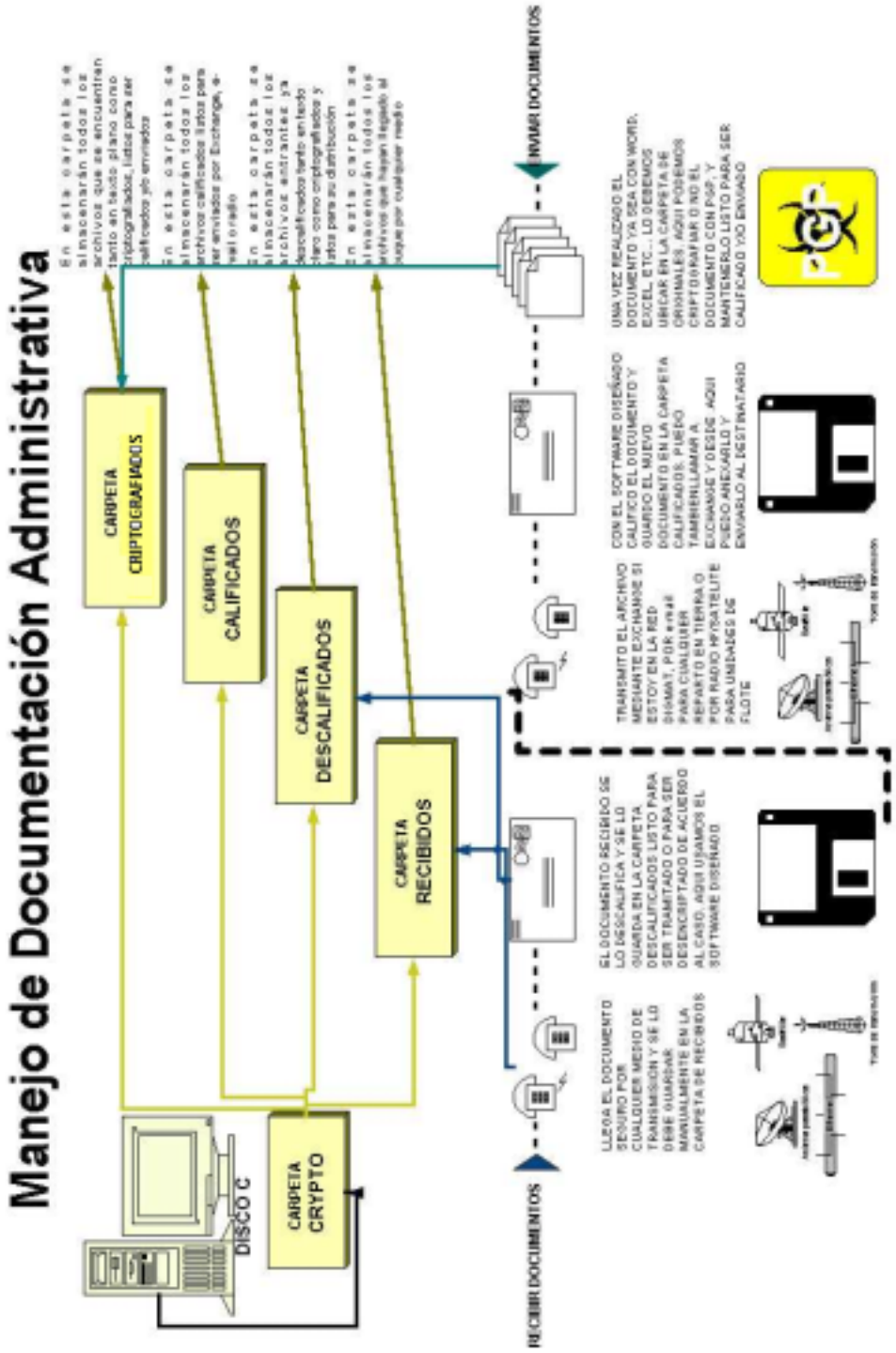


Fig. C-9

FLUJO DEL DOCUMENTO CODIFICADO



0

FLUJO DEL MENSAJE EMERGENTE

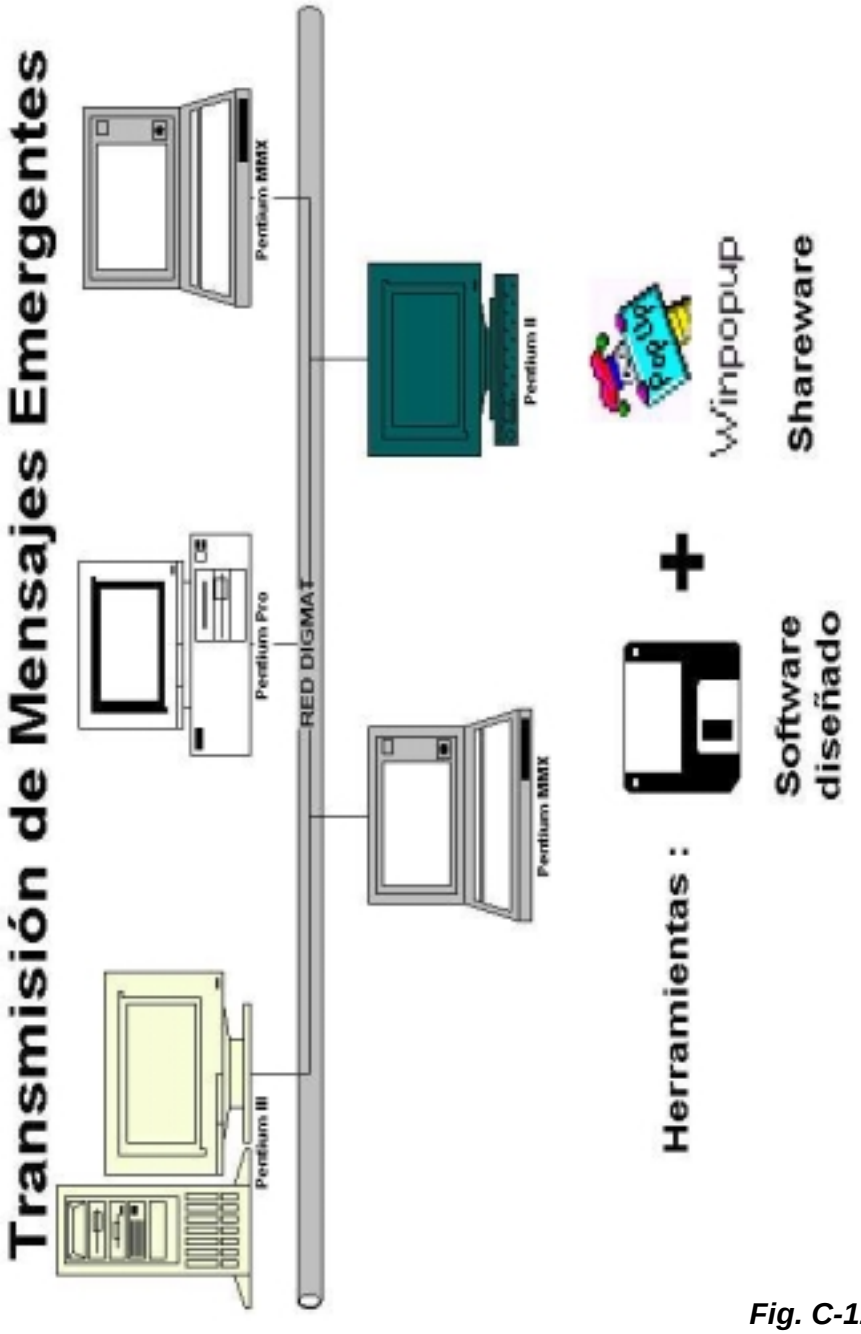


Fig. C-11

ALCANCES DEL PROTOTIPO

Con el presente diseño, el operador puede ser capaz de realizar múltiples actividades de acuerdo a sus necesidades, estas son:

MANEJO DE ARCHIVOS

- Llamar al Exchange para transferir archivos
- Encriptar archivos externamente con PGP
- Calificar archivos internamente con Twofish

MENSAJES EMERGENTES

- Encriptar texto antes de enviarlo
- Desencriptar el texto recibido
- Transferencia de mensajes en la red interna

CUENTAS

- Permite a los usuarios cambio del password de ingreso al sistema
- Permite a la persona soporte de sistema administrar usuarios

NAVEGADOR DE WEB

- Permite consultar via web detalles del proyecto

BIBLIOGRAFIA

- **LUCENA LOPEZ Manuel José**, Criptografía y Seguridad en Computadores, 2ª Edición, Universidad Politécnica de Jaén - España, Internet: www.kriptópolis.com , septiembre de 1999.

- **PONS MARTORELL Manuel**, Criptología, Departamento de Telecomunicaciones de la Escuela Universitaria de Mataró – España, Internet: www.kriptópolis.com , marzo del 2000.

- **PONS MARTORELL Manuel**, Control de accesos, Departamento de Telecomunicaciones de la Escuela Universitaria de Mataró – España, Internet: www.kriptópolis.com , marzo del 2000.

- **SCHNEIER Bruce, KELSEY John, WHITHING Doug, WAGNER David, HALL Chris, FERGUSON Niels,** Twofish: A 128-bit block cipher, Counterpane USA, Internet: www.counterpane.com/twofish.html, junio de 1998.

- **STALLINGS William,** Comunicaciones y Redes de Computadoras, Editorial Prentice Hall, 5ª. Edición, 1999.

- **ROBLING DENNIG Dorothy Elizabeth,** Cryptography and Data Security, Editorial Addison – Wesley USA, enero de 1983

- **FINCH James, DOUGALL Graham,** Computer Security: a global challenge, Editorial IFIP Canadá, septiembre de 1984.

- **GRIMSON Jane, KUGLER Hans-Jurgen,** Computer Security: the practical issues in a trouble world, Editorial IFIP Canadá, agosto de 1985.

- **MICROSOFT CORPORATION,** Visual Basic. Guía de herramientas componentes. Sistema de programación para Windows, USA, 1997.

- **CEBALLOS Francisco Javier,** Enciclopedia de Visual Basic 4, Editorial ALFAOMEGA México, 1997.

- **DIRECCIONES ELECTRONICAS.**

Sitios relacionados

http://www.kriptopolis.com
http://www.kriptopolis.com/criptograma/cg.html
http://www.counterpane.com/index.html
http://www.counterpane.com/twofish.html
http://www.counterpane.com/applied.html
http://www.aba.net.au/solutions/crypto/
http://www.rsa.com
ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code
http://csrc.nist.gov/encryption
http://www.meste.cl
http://www.cryptix.org

http://www.mach5.com/crypto
http://www.freecrypto.org/
http://www.yurisw.com/default.htm
http://guille.costasol.net/indice_nf.htm
http://www.nl.cryptix.org/
http://www.stealthencrypt.com/index2.html
http://www.stealthencrypt.com/twofish.html
http://www.tecapro.com/recursos.html
http://twofish-py.sourceforge.net/
http://www.counterpane.com/twofish_performance.html
http://www.counterpane.com/twofish_hardware.html
http://www.3com.com
http://www.intel.com

Información o archivos relacionados

http://www.counterpane.com/twofish.pdf
http://www.xs4all.nl/~vorpal/pubs/yarrow.zip
http://www.math.utah.edu/pub/tex/bib/index-table.html
http://ourworld.compuserve.com/homepages/crypto/BIB1XX.HTM
http://www.counterpane.com/twofish-keys.pdf
http://www.xs4all.nl/~vorpal/pubs/forget.zip
http://www.xs4all.nl/~vorpal/pubs/twofishTR5.zip
http://www.xs4all.nl/~vorpal/pubs/AESperformance.zip
http://www.cam.org/~droujav/pgp/pgplib.zip
http://www.jetico.sci.fi/np_new.htm