DATOS DEL PROYECTO

TITULO

CRIPTOGRAFIA APLICADA PARA LAS COMUNICACIONES NAVALES

AUTORES

Javier Flores Barahona[1], Carlos Jordán Villamar[2]

[1]Ingeniero en Computación 2001

[2]Ingeniero Eléctrico, BS en Ingeniería Eléctrica y Maestría en Física, Universidad de Tufts, USA, 1975. Profesor de la ESPOL desde 1975.

RESUMEN

El desarrollo de la tesis consiste en la conjugación de herramientas de criptografía existentes con las opciones necesarias para la Armada del Ecuador, buscando proporcionar un sistema seguro y confiable que soporte la transición hacia un nuevo sistema criptográfico para las comunicaciones navales. El sistema 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 seguridad total 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 actualmente en vigencia.

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 podemos explotar la tecnología de la que disponemos.

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 y parte de la segunda 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***, ya que estos son usados en la Armada para otros propósitos, y con algunas adecuaciones podrían ser utilizados para brindar el enlace de comunicaciones requerido.

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:

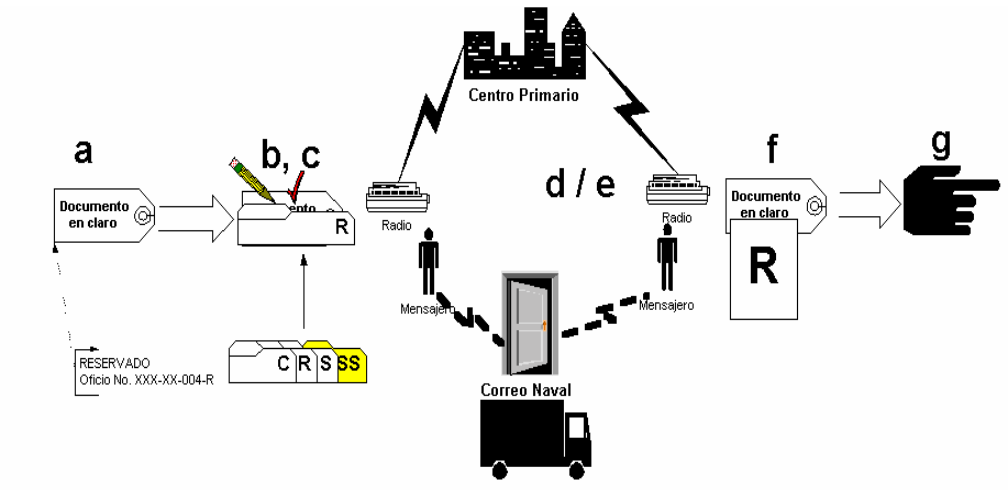

Fig. 1

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.

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.

2.2. 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.

2.2.1. 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.

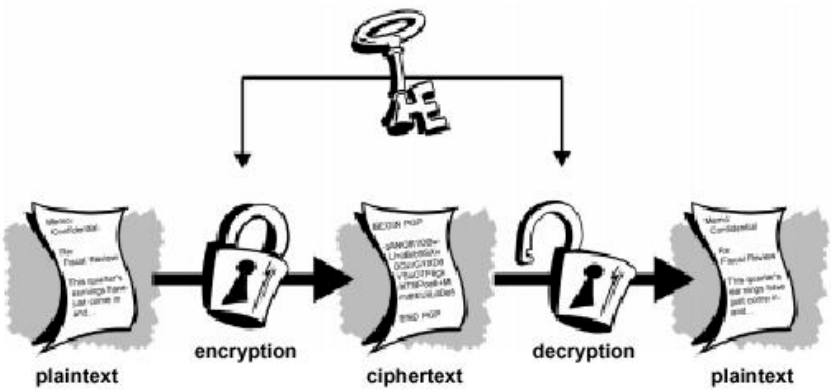

Fig. 2

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:

▪ ***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.

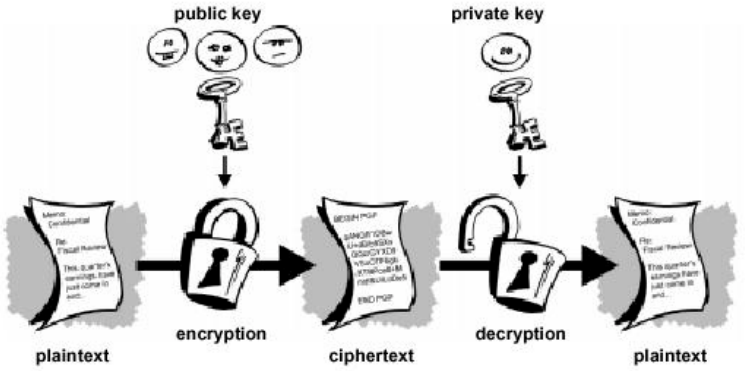

Fig. 3

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.

2.3. 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

2.3.1. 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.

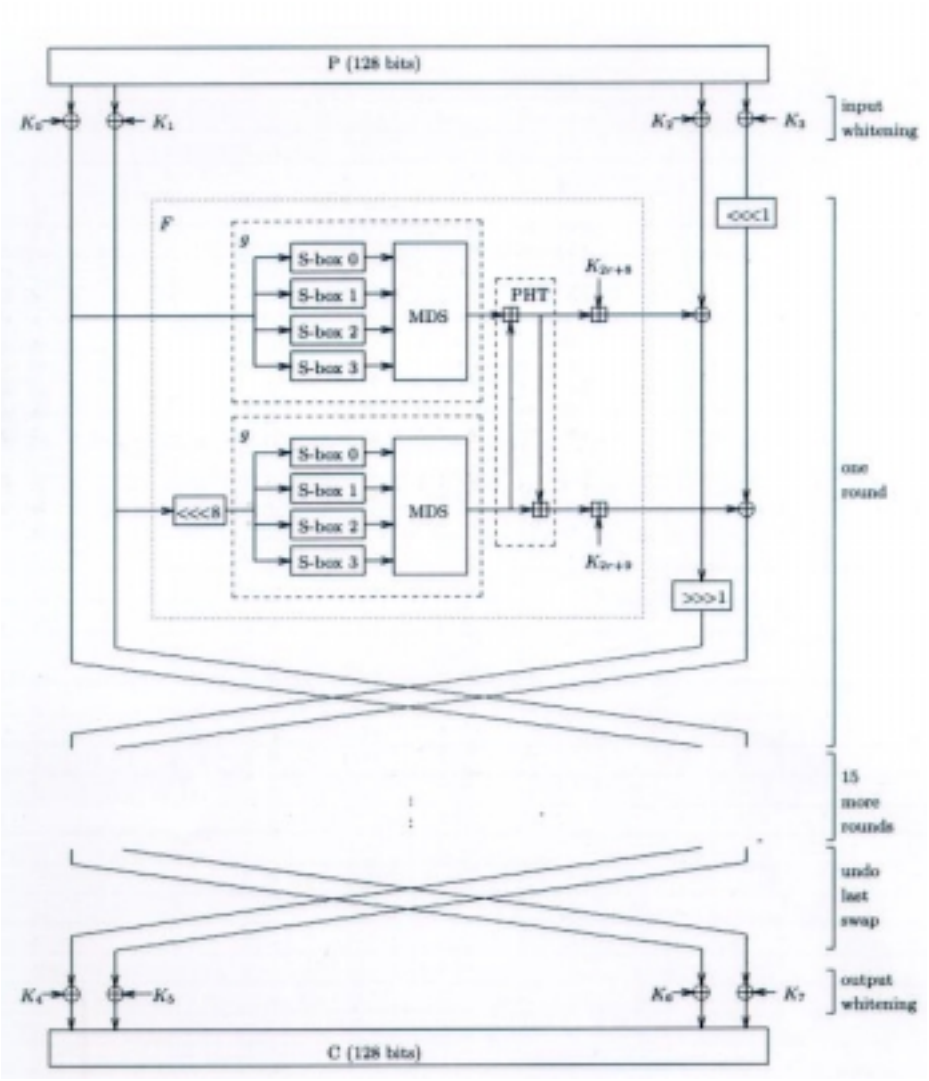

Fig. 4

2.3.2. 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:

2.3.2.1. 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. 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.

2.3.2.2. 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.

2.3.2.3. 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.

2.3.2.4. 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 mod 32

b’ = a + 2b mod 32

2.3.2.5. 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.

2.3.2.6. 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 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.

3.2. 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

Para la construcción del prototipo he usado varios módulos, cada uno con su respectiva función, estos son:

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:

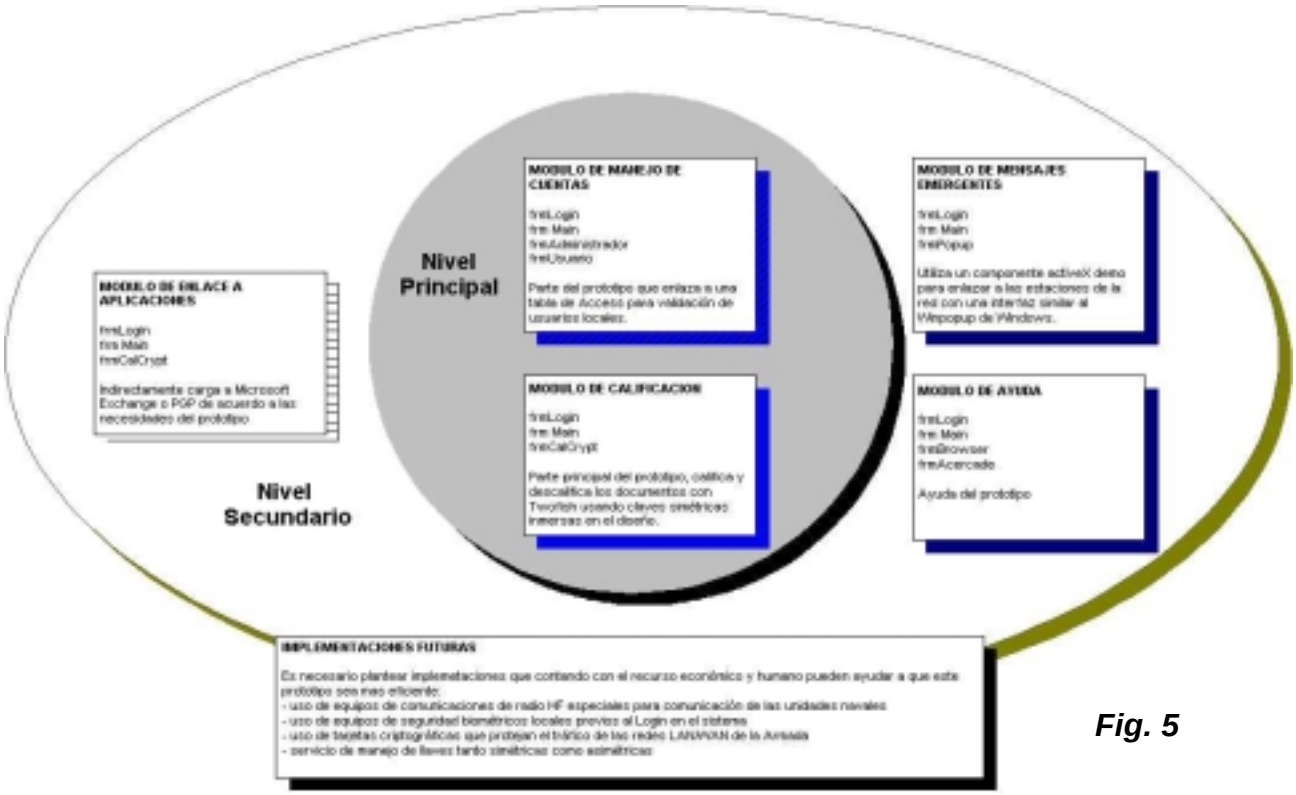

Fig. 5

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).

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:

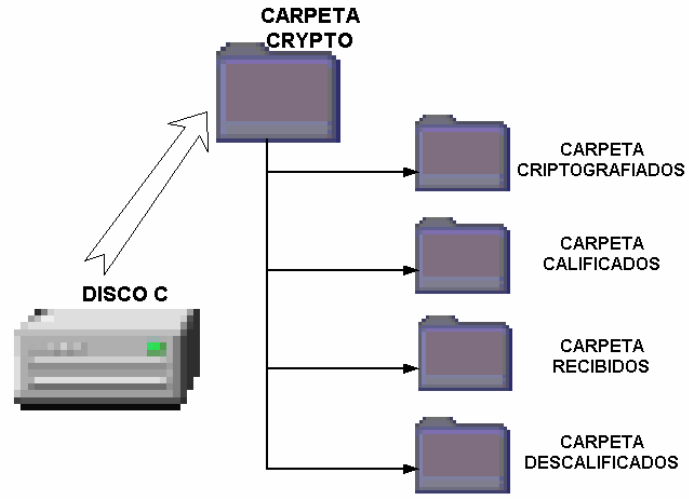

Fig. 6

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. 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.

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.

- **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. código.

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

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 I

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 II

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 III

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

IÐ âô¨²Øy•¥<¤óè +éO¤Jj 6â îæ[ØúñÈ ³&O'É§ßåÝp &ÒßûÁlØ1ÂÜ ©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˜

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 o+Fà- äx>F í:ý@ eü8Ö è±d4 ï E-"ª

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‰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

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.

REFERENCIAS

1. **FLORES BARAHONA JAVIER**, Diseño de un software criptográfico para las comunicacines navales, Tesis de Grado, Facultad de Ingeniería en Electricidad y Computación, ESPOL 2000
2. **LUCENA LOPEZ Manuel José**, Criptografía y Seguridad en Computadores, 2ª Edición, Universidad Politécnica de Jaén - España, Internet: www.kriptópolis.com , septiembre de 1999.
3. **PONS MARTORELL Manuel**, Criptología, Departamento de Telecomunicaciones de la Escuela Universitaria de Mataró – España, Internet: www.kriptópolis.com , marzo del 2000.
4. **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.
5. **STALLINGS William,** Comunicaciones y Redes de Computadoras, Editorial Prentice Hall, 5ª. Edición, 1999.
6. **ROBLING DENNIG Dorothy Elizabeth,** Cryptography and Data Security, Editorial Addison – Wesley USA, enero de 1983
7. **FINCH James, DOUGALL Graham,** Computer Security: a global challenge, Editorial IFIP Canadá, septiembre de 1984.
8. **GRIMSON Jane, KUGLER Hans-Jurgen,** Computer Security: the practical issues in a trouble world, Editorial IFIP Canadá, agosto de 1985.
9. **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
http://www.stealthencrypt.com/index2.html
http://twofish-py.sourceforge.net/
http://www.counterpane.com/twofish_performance.html
http://www.counterpane.com/twofish_hardware.html
http://www.3com.com

Información o archivos relacionados

http://www.counterpane.com/twofish.pdf
http://www.counterpane.com/twofish-keys.pdf
http://www.cam.org/~droujav/pgp/pgplib.zip
http://www.jetico.sci.fi/np_new.htm