UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

TEMA:

"TECNOLOGÍAS DE ENCRIPTACIÓN DE INFORMACIÓN Y PROTOCOLOS SEGUROS"

AUTORES:

- **ARTEAGA ARTEAGA JAIME FRANCISCO**
- **GARCÍA SANTILLÁN IVÁN DANILO**

DIRECTOR:

ING. RODRIGO NARANJO

IBARRA, NOVIEMBRE DEL 2003

CERTIFICACIÓN

Los Señores Egresados Arteaga Arteaga Jaime Francisco y García Santillán Iván Danilo han trabajado en la Investigación y Desarrollo de "TECNOLOGÍAS DE ENCRIPTACIÓN DE INFORMACIÓN Y PROTOCOLOS SEGUROS", previa a la obtención del Título de Ingeniero en Sistemas Computacionales, realizándola con interés profesional, responsabilidad y esfuerzo tesonero, lo cual certifico en honor a la verdad.

Ing. Rodrigo Naranjo
DIRECTOR DE TESIS

AGRADECIMIENTO

El agradecimiento más profundo y sincero a todos y cada uno de los que conforman la Universidad Técnica del Norte, que de una u otra manera aportaron con sus valiosos conocimientos, sugerencias, comentarios y recomendaciones para la correcta culminación del presente trabajo investigativo, en especial al Ing. Rodrigo Naranjo, Director de Tesis, quien en forma desinteresada supo guiarnos hasta el final.

Para todos ellos, con profundo respeto y consideración.

DEDICATORIA

A mis padres; con mucho amor, quienes supieron llevarme por el camino del bien y la verdad.

A mis hermanos y familiares, quienes estuvieron a mi lado en todo momento.

Iván

A Eduardo y Aída Arteaga, mis padres; que en esta larga trayectoria fueron de notable apoyo.

A mi esposa e hijo, fieles testigos de la dedicación y entrega durante estos años de estudio universitario.

Francisco

ÍNDICE

Capítulo I: SEGURIDAD EN LA RED

1.1 Introducción ……..…..... 2

1.2 Problemas de Seguridad ……...…….....…. 3

1.3 Niveles de Seguridad …….…..... 5

1.4 Políticas de Seguridad ……..... 9

1.5 Intrusos en la Red ……..……..... 11

1.6 Aspectos Sociales …….……..……..... 12

Capítulo II: CRIPTOLOGÍA

2.1 Definición ……...…… 15

2.2 Historia e Importancia ……..…..…….…..... 17

2.3 Fundamentos ……...……..... 19

2.3.1 Números Aleatorios …….....…….....….. 19

2.3.2 Números Primos …….…..... 21

2.3.3 Aritmética Modular …….……..... 23

2.3.4 Test de Primalidad……...……..... 29

2.4 Clasificación: Simétrica y Asimétrica ….....…….….... 32

2.5 Aplicaciones: PGP, S/MIME, PEM, EFS ……....…….…..... 37

Capítulo III: CRIPTOGRAFÍA DE CLAVE PRIVADA

2.1 Definición …… 44

2.2 Cifrado por Sustitución ……..... 45

2.3 Cifrado por Transposición ……..... 46

2.3.1 Algoritmo DES (Data Encryption Standard) …..… 47

2.3.2 Algoritmo IDEA (Data Encryption Algorithm) 54

2.4 Criptoanálisis Diferencial y Lineal ……..... 59

Capítulo IV: CRIPTOGRAFÍA DE CLAVE PÚBLICA

4.1 Definición ……..…….....……. 64

4.2 Algoritmo RSA *(Rivest, Shamir, Adleman)* ….....…….... 66

4.3 Algoritmo El Gamal ……..... 69

4.4 Criptosistemas basados en Curvas Elípticas …….…..... 72

4.5 Criptosistemas basados en Logaritmos Discretos 83

Capítulo V: VALIDACIÓN DE IDENTIFICACIÓN

4.1 Protocolos de Validación de Identificación ….……..... 86

4.2 Autentificación de Mensajes ……...…….…..... 99

4.2.1 Algoritmo MD5 *(Message Digest 5)* ……...…….…….100

4.2.2 Algoritmo SHA *(Secure Hash Algorithm)* …….....…...104

4.3 Firmas Digitales …….…..... 107

4.3.1 DSS (Digital Signature Standard) …… 109

4.4 Sistemas de Identificación Biométrica ……...….…..... 115

Capítulo VI: PROTOCOLOS SEGUROS

6.1 SSL *(Secure Sockets Layer)* ……..…….. 120

6.2 TLS *(Transport Layer Security)* …….. 125

6.3 PCT *(Private Communications Technology)* ……...…… 128

6.4 S-HTTP *(Secure HyperText Transfer Protocol)* …..……...…… 130

6.5 IPSEC *(IP Security)* ……..…..... 132

6.6 Conclusión de los Protocolos ……....…... 144

Capítulo VII: AUTORIDADES DE CERTIFICACIÓN

7.1 Introducción …….. 146

7.2 Organismos de Control ……....… 147

7.3 Autoridades de Certificación (CA) …...…….…..... 148

7.4 Requisitos para la formación de una CA ……..... 152
7.5 Deberes y Obligaciones de una CA ……..... 153
7.6 Auditorías a la CA ……..... 154
7.7 Manifestación de Práctica de la CA ……..... 155
7.8 Cese de Actividades por parte de la CA ……..... 155
7.9 Sanciones impuestas a la CA ……..... 156
7.10 Certificados Digitales ……..... 157
7.11 Suspensión y Revocación de Certificados ……..... 160
7.12 Deberes de los Suscriptores ……..... 161
7.13 Responsabilidad de los Suscriptores ……..... 162

C a p í t u l o VIII: VERIFICACIÓN DE LA HIPÓTESIS, CONCLUSIONES Y RECOMENDACIONES

8.1 Verificación de la Hipótesis ……..……..... 164
8.2 Conclusiones ……..... 165
8.3 Recomendaciones ……..... 170

ANEXOS

APÉNDICE A.- Organismos de Estandarización y Control 175
APÉNDICE B.- Ley de Comercio Electrónico 183
APÉNDICE C.- Estándares de Criptografía de Clave Pública 189

GLOSARIO TÉCNICO 193
BIBLIOGRAFÍA 200