

Índice

AGRADECIMIENTOS.....	11
CAPÍTULO 1. SEGURIDAD DE LA INFORMACIÓN	15
1.1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN	16
1.2 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN	17
1.3 EN BUSCA DE LA SEGURIDAD DE LA INFORMACIÓN	18
1.3.1 Amenazas	19
1.3.2 Vulnerabilidades	21
1.3.3 Medidas de seguridad	21
CAPÍTULO 2. CRIPTOGRAFÍA.....	23
2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA	24
2.1.1 Definiciones	24
2.1.2 Criptosistemas	25
2.1.3 Aplicaciones.....	26
2.1.4 Otras técnicas.....	28
2.2 PERSPECTIVA HISTÓRICA.....	29
2.2.1 Criptografía manual.....	29
2.2.2 Criptografía mecánica.....	31
2.2.3 Criptografía computacional	33
2.3 FUNDAMENTOS TEÓRICOS DE LA CRIPTOGRAFÍA.....	34
2.3.1 Teoría de la información.....	34
2.3.2 Teoría de los números.....	39
2.3.3 Teoría de la complejidad de algoritmos	45
CAPÍTULO 3. CRIPTOGRAFÍA CLÁSICA	51
3.1 TIPOS DE MÉTODOS DE CIFRA CLÁSICOS	52
3.2 PRINCIPALES ALGORITMOS CLÁSICOS DE CIFRADO	53
3.2.1 La escítala.....	53
3.2.2 Polybios.....	54
3.2.3 Cifrado César.....	54
3.2.4 Cifrado Vigenère.....	55
3.2.5 Cifrado Playfair	57
3.2.6 Cifrado Hill	58
3.2.7 Cifrado Vernam	60
3.2.8 Máquina Enigma.....	61

3.3	ATAQUES CRIPTOANALÍTICOS SOBRE MÉTODOS CLÁSICOS DE CIFRADO	62
3.3.1	Ataque Kasiski	62
3.3.2	Ataque Gauss Jordan	64
CAPÍTULO 4. CRIPTOGRAFÍA MODERNA.....		67
4.1	CRIPTO SISTEMAS MODERNOS.....	68
4.2	CIFRADO EN FLUJO VS. CIFRADO EN BLOQUE	68
4.2.1	Cifrado en flujo	68
4.2.2	Cifrado en bloque.....	70
4.3	CIFRA SIMÉTRICA.....	70
4.3.1	Funcionamiento.....	70
4.3.2	Algoritmos	74
4.4	CIFRA ASIMÉTRICA	76
4.4.1	Funcionamiento.....	76
4.4.2	Intercambio de claves.....	77
4.4.3	Algoritmos	79
4.5	CIFRADO SIMÉTRICO VS CIFRADO ASIMÉTRICO. CRIPTOSISTEMAS HÍBRIDOS	83
4.5.1	Comparativa simétrico vs asimétrico.....	83
4.5.2	Sistemas híbridos	84
4.6	EL FUTURO DE LA CRIPTOGRAFÍA: CRIPTOGRAFÍA CUÁNTICA.....	85
4.6.1	Computación cuántica.....	85
4.6.2	Paralelismo cuántico	86
4.6.3	Atacando RSA.....	86
4.6.4	Ideas básicas de criptografía cuántica.....	87
4.6.5	Protocolos más usuales de criptografía cuántica	89
CAPÍTULO 5. MÉTODOS DE AUTENTICACIÓN		93
5.1	AUTENTICACIÓN Y CRIPTOGRAFÍA	94
5.2	FIRMA ELECTRÓNICA.....	94
5.2.1	Definición.....	94
5.2.2	Proceso	96
5.2.3	Validación de una firma electrónica	97
5.2.4	Formatos de firma electrónica	98
5.2.5	Aplicaciones de firma electrónica	99
5.3	FUNCIONES RESUMEN. HASH.....	101
5.3.1	Definición.....	101
5.3.2	Longitud de la signatura.....	102
5.3.3	Estructura	102
5.3.4	Algoritmos	103
5.4	CERTIFICADOS DIGITALES	108
5.4.1	Definición.....	108
5.4.2	Obtención de certificados	108

5.4.3	Renovación de certificados.....	109
5.4.4	Revocación de certificados.....	109
5.5	INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).....	110
5.5.1	Definición.....	110
5.5.2	Elementos de una PKI.....	110
CAPÍTULO 6. CORREO ELECTRÓNICO SEGURO.....		113
6.1	¿POR QUÉ CORREO ELECTRÓNICO SEGURO?.....	114
6.2	PGP.....	115
6.2.1	Introducción e historia de PGP.....	115
6.2.2	Funcionamiento de PGP.....	116
6.2.3	Vulnerabilidades de PGP.....	118
6.3	GPG.....	118
6.4	S/MIME.....	120
6.4.1	Introducción e historia de s/mime.....	120
6.4.2	Funcionamiento de s/mime.....	120
CAPÍTULO 7. COMUNICACIONES SEGURAS.....		123
7.1	INTRODUCCIÓN.....	124
7.2	REDES PRIVADAS VIRTUALES (VPN).....	125
7.2.1	Definición.....	125
7.2.2	Tipos de VPN.....	126
7.2.3	Requerimientos.....	128
7.3	TÚNELES CIFRADOS (TUNNELING).....	129
7.3.1	Funcionamiento.....	129
7.3.2	Tunneling en VPN.....	129
7.3.3	Tipos de túneles.....	130
7.4	PROTOCOLOS DE TÚNEL: PPTP, L2TP E IPSEC.....	130
7.4.1	PPTP.....	130
7.4.2	L2TP.....	132
7.4.3	IPSec.....	134
7.5	PROTOCOLOS SSL, TLS Y SSH.....	138
7.5.1	SSL.....	139
7.5.2	TLS.....	141
7.5.3	SSH.....	144
7.6	SISTEMAS VPN SSL.....	146
7.6.1	Definición.....	146
7.6.2	Tipos de VPN SSL.....	146
7.6.3	VPN SSL vs. VPN IPSec.....	146
7.7	VENTAJAS E INCOVENIENTES DE LAS VPN.....	147

CAPÍTULO 8. PROTOCOLOS DE SEGURIDAD WI-FI	149
8.1 NECESIDAD DE SEGURIDAD EN WI-FI	150
8.2 PROTOCOLO WEP.....	151
8.2.1 Definición y características de WEP	151
8.2.2 Seguridad en WEP	152
8.2.3 Vulnerabilidades de WEP	153
8.2.4 Variantes de WEP.....	154
8.3 PROTOCOLO WPA.....	154
8.3.1 Definición y características de WPA.....	154
8.3.2 Mejoras respecto a WEP.....	155
8.3.3 Modos de funcionamiento de WPA.....	155
8.3.4 Vulnerabilidades de WPA.....	156
8.4 PROTOCOLO WPA2.....	156
8.4.1 Definición de WPA2.....	156
8.4.2 Funcionamiento de WPA2.....	157
REFERENCIAS.....	159
ÍNDICE ALFABÉTICO	161