

ÍNDICE

PRÓLOGO	IX
Capítulo 1. CRIPTOGRAFÍA TEÓRICA	1
1.1 Conceptos básicos	3
1.2 Reglas de Kerckhoffs	7
1.3 Tipos de ataque	8
1.4 Fuente del texto	10
1.5 Secreto perfecto	14
1.6 Equivocación	22
1.7 Redundancia y distancia de unicidad	24
Capítulo 2. CRIPTOGRAFÍA DE CLAVE SECRETA	29
2.1 Transposición, sustitución y producto.....	30
2.1.1 Sustitución monoalfabética.....	32
2.1.1.1 Sustitución de letras.....	32
2.1.1.2 Sustitución de 2-palabras.....	34
2.1.2 Sustitución polialfabética.....	37
2.1.2.1 Cifrado de Vernam.....	37
2.1.2.2 Cifrado Vigenère	38
2.1.2.3 Criptoanálisis.....	39
2.2 Cifrado en bloque, DES	41
2.2.1 Algoritmo DES	42
2.2.1.1 Función f.....	44
2.2.1.2 Cálculo de la clave.....	46
2.2.1.3 Seguridad.....	48
2.3 Cifrado en flujo	51

Capítulo 3. CRIPTOGRAFÍA DE CLAVE PÚBLICA	57
3.1 Sistema RSA	61
3.2 Sistema de Rabin	68
3.3 Sistema de ElGamal	71
3.4 Sistema de Merkle-Hellman.....	73
3.5 Sistema de McEliece	78
3.5.1 Conceptos de teoría de la codificación	78
3.5.2 Descripción y discusión	83
3.6 Sistemas basados en curvas elípticas	85
3.6.1 Conceptos de teoría de las curvas elípticas	85
3.6.2 Descripción y discusión	88
3.7 Sistema probabilístico	92
Capítulo 4. APLICACIONES CRIPTOGRÁFICAS	97
4.1 Autenticación	97
4.1.1 Modelo matemático	98
4.1.2 Métodos	103
4.2 Firma digital	105
4.3 Identificación de usuario	109
4.4 Seguridad en redes	111
4.5 Protocolos criptográficos.....	113
4.5.1 Elecciones	114
4.5.2 Transferencia inconsciente.....	115
4.5.3 Lanzamiento de monedas	116
4.5.4 Esquema umbral	117
4.5.5 Demostración de conocimiento nulo	119
BIBLIOGRAFÍA	121
ÍNDICE ALFABÉTICO	135