

CONTENIDO

Prólogo	XIII
Capítulo I	1
I.1. IntrOducc1ón.	1
I.2. MOt1vac1ón.....	3
I.3. Pre11m1nares.....	4
I.4. Contend1O.....	6
Ejercicios.....	7
B1bl1Ograf1a.....	8
Capítulo II	9
II.1. DES.	10
II.2.1 Triple DES.	16
II.2.2 Triple-DES-96.	17
II.3. AES.....	19
II.3.1. Preliminares.....	19
II.3.2. Descripción de alto nivel.	24
II.3.3. Algoritmo de cifrado.	30
II.3.4. Algoritmo de las llaves ronda.	31
II.3.5. Modos de operación.....	34
II.3.5.1. Modo ECB.	34
II.3.5.2. Modo CBC.....	35
II.4. Subst1tut1On Permutat1On NetwOrk.....	35
B1bl1Ograf1a.....	39
Capítulo III	41
III.1. EntrOpía.	41
III.2. COefic1ente de COrrrelaci3n.	43
III.3. Prueba de h1p3tesis estadística.....	45
III.3.1. Prueba de aleatoriedad propuesta.	45
III.4. TransfOrmada D1screta de FOUr1er.....	48
III.5. Distribuciones de probabilidad.....	50

III.6. Distribución uniforme y aleatoriedad.....	51
III.7. Histogramas.	52
III.8. NPCR, UAC1 y AC.	53
Bibliografía.....	57
Capítulo IV.....	59
IV.1. Preliminares.	60
IV.2. Algoritmo para la generación de permutaciones.....	63
IV.3. Medición de la no-linealidad de las cajas.....	68
IV.3.1. Medición de no-linealidad reciente.	73
Bibliografía.....	77
Capítulo V.....	79
V.1. Procedimientos de un solo camino.....	79
V.2. Alta primalidad.	80
V.2.1. Inversos multiplicativos.....	81
V.3. Algoritmo de Euclides.....	82
V.4. Algoritmo de Miller-Rabin.....	85
V.5. Exponenciación.	88
V.6. Teorema Chino del residuo.	91
V.7. El Teorema de Lagrange y el pequeño Fermat.....	95
V.8. Criptosistema RSA.	96
Bibliografía.....	101
Capítulo VI.....	103
VI.1. Cálculo de un elemento generador.	104
VI.2. El problema del logaritmo discreto.....	106
VI.3. El criptosistema asimétrico ElGamal.	107
Bibliografía.....	112
Capítulo VII.....	113
VII.1. La Operación de suma en el conjunto $E(L) \cup \{\infty\}$	115
VII.2. La Curva Elíptica Discreta.....	118
VII.3. Generación de Curvas Elípticas.	124
VII.4. Cifrado de Información con la Curva Elíptica.	127

VII.5. Protocolos para el envío de llaves de sistemas simétricos.	130
B1bl10grafía.....	134
Capítulo VIII.....	135
VIII.1. Ecuaciones de Lorenz.....	136
VIII.2. La ecuación logística.....	142
VIII.3. Las funciones Hash Sha.	143
VIII.4. La función Has Sha 1.....	147
B1bl10grafía.....	152
Capítulo IX.....	153
IX.1. Firma digital utilizando el criptosistema RSA.....	154
IX.2. Firma digital usando el criptosistema ElGamal.....	158
IX.3. Firma digital usando la Curva Elíptica.	161
IX.4. Firma digital basada en reticulados.....	165
IX. 4.1 Criptosistema NTRUEncrypt de llave pública.	168
B1bl10grafía.....	179
Capítulo X.....	181
X.1. Daño en 1mágenes encr1ptadas.....	182
X.1.1. Ruido generado por una variable aleatoria gaussiana.	182
X.1.2. Dominio espacial.	183
X.1.3. Dominio de frecuencias.	183
X.1.4. Ruidos aditivo y multiplicativo.....	184
X.1.5. Ruido de oclusión.	185
X.2. COnstrucción de elementOs.....	186
X.2.1. Filtro de mediana.....	186
X.2.2. Parámetro de similitud.	187
X.3. COnstrucción de s-box 8x8	188
X.3.1. Generación de cajas de alta no-linealidad y dpa menor a 10.188	
X.4. Cr1ptOsistema 1nnOvador de c1fradO usandO númeroS trascendentes.....	190
X.4.1. Cifrado de imágenes usando números trascendentes.....	190
X.4.1.1 Resultados del cifrado con números trascendentes.	193
X.5. Criptosistema innovador de cifrado usando la curva elíptica	197

X.5.1. Cifrado de imágenes utilizando la curva elíptica.....	197
X.5.1.1. Resultados con imágenes sin daño.....	200
X.5.1.2. Resultados de imágenes con daño.....	206
Bibliografía.....	210