

## Indice alfabético

### A

Acceso múltiple por división de código, 229-233  
 Aleatoriedad, 15-21  
 Aleatorización  
   proceso de, 222  
   en el estándar DVB, 224  
   en el sistema MAC/paquetes, 223  
 Algoritmo  
   Blumer, 191  
   Massey-Berlekamp, de, 67, 181  
   Ziv-Lempel, de, 187  
 ASG, generador, 116  
 Ataques por correlación, 207  
 Autenticación en GSM, proceso de, 219  
 Autocorrelación, función de, 22, 134  
 Autodecimación de secuencias, 83  
 Autodecimadas, generador de secuencias, 109  
 Autodecimadas de Rueppel, secuencias, 110  
 Automatas  
   celulares, generadores basados en, 125  
   deterministas, 175

### B

Básculas, funciones combinadoras con, 79, 98  
 Beth-Piper, generador de, 113  
 Binomial, distribución, 56  
 Blum-Micali, generador de, 51  
 Blumer, algoritmo de, 191  
 Brechas, test de, 151  
 BRM, generador, 108

### C

Campos de Galois, 63  
 Caóticas, generador de secuencias, 44  
 Cascada, control de reloj en, 82

Cascada, generador en, 107  
 Central del límite, teorema, 55  
 Chambers-Gollmann, generador de, 111  
 Chi-cuadrado, test, 141  
 Cifrado  
   computacionalmente seguro, 205  
   de bloque, 198  
   de redes ATM, 217  
   de seguridad incondicional, 204  
   de seguridad probable, 206  
   en comunicaciones móviles GSM, 219  
   en flujo, 195-207  
   en flujo autosincronizante, 202  
   en flujo síncrono, 200  
   prácticamente seguro, 205  
   Vernan, de, 198  
 Clave criptográfica, 50, 196  
 Códigos de Gold, 231-233  
 Coeficientes de correlación, 158  
 Colector de cupones, test, 154  
 Combinadora, función, 72  
 Complejidad  
   lineal, 66, 177  
   máximo orden, de, 189  
   perfil de, 178, 191  
   Ziv-Lempel, de, 186  
   Turing-Kolmogorov-Chaitin, de, 15, 175  
 Confidencialidad de mensajes, 196  
 Congruencias, generador  
   cuadrático, 39  
   lineal, 34  
   lineal aditivo, 38  
   lineal mixto, 36  
   lineal multiplicativo, 34  
 Consistencia lineal, test de, 95, 207  
 Control  
   bilateral, generador de, 115

de reloj, técnicas de, 82, 104  
 de reloj en cascada, 82  
 de reloj con modulación de fase, 105  
 Controlador de marcha y espera, 82, 113  
 Correlación  
 aperiódica (impar) de secuencias, 137  
 cruzada de secuencias, 135, 261  
 propiedades de, 133  
 sucesiva, test de, 158  
 Criptoanálisis, 206  
 Criptografía, fundamentos de, 195  
 Cuerpos finitos, 63

## D

De Bruijn, secuencias de, 86  
 Dispersión de energía, 222-225  
 Distancia  
 de Hamming, 209  
 de Levenshtein, 209  
 euclídea, 155  
 restringida de Levenshtein, 209  
 test de, 155  
 Distribución  
 binomial, 56  
 de claves, 199  
 de claves en Eurocrypt, 216-217  
 de claves en GSM, 221  
 exponencial, 57  
 gaussiana (normal), 54  
 Poisson, de, 58  
 uniforme, 16  
 uniforme no estándar, 54

## E

Entropía por bit  
 definición de, 165  
 test de, 163  
 Espectral, test, 166  
 Euler, función de, 65  
 Eurocrypt, acceso condicional, 211-217  
 Exponencial, distribución, 57

## F

Falsa alarma, probabilidad de, 147, 165  
 Fourier, transformada discreta de, 48, 166, 167  
 Frecuencia, test de, 148  
 Fuente binaria simétrica, 14  
 Función  
 acumulada de probabilidad, 53  
 combinadora, 72

de estado no lineal, 68  
 Euler, de, 65

## G

Gausiana, distribución, 54  
 Geffe, generador de, 95  
 Generador  
 ASG, 116  
 autómatas celulares, basado en, 125  
 Beth-Piper, de, 113  
 Blum-Micali, 51  
 BRM, 108  
 cascada, en, 107  
 Chambers-Gollmann, 111  
 congruencias cuadrático, de, 39  
 congruencias lineales, de, 34  
 congruencias lineal aditivo, de, 38  
 congruencias lineal mixto, de, 36  
 congruencias lineal multiplicativo, 34  
 control bilateral, de, 115  
 De Bruijn, de, 86  
 Geffe, de, 95  
 Gold, de, 231-233  
 Gollmann, de, 114  
 Hénon, de, 43  
 Jennings, de, 93, 214-216, 264-275  
 MacLaren-Marsaglia, de, 40, 105  
 marcha y espera, de, 82, 1013-115  
 Massey-Ruepple, de, 118  
 memoria, basado en, 126  
 mochila, de, 51  
 modulación de fase del reloj, de, 105  
 multiplicador de tasa binaria, 108  
 pasos alternados, de, 116  
 permutaciones, de, 40  
 permutación de subsecuencias, de, 122  
 Pless, de, 98  
 producto escalar, de, 106  
 producto interior, de, 119  
 PRN, 33  
 Ruepple, de, 101  
 suma entera, de, 49  
 Tatebayashi, de, 102  
 umbral, de, 97  
 Windmill, de, 120  
 Wolfram, de, 126  
 secuencias autodecimadas, de, 109  
 reloj en cascada, de, 82  
 Gold, códigos de, 231-233  
 Gollmann, generador de, 114  
 Golomb, postulados de, 21-25

GPSS/360, sistema, 32

## H

Hénon, generador de, 43

## I

Impredictibilidad, 66, 173, 177, 203

Inmunidad a la correlación, 73

Irreducible, polinomio, 65, 87

## J

Jennings, generador de, 93, 214-216, 264-275

## K

Kolmogorov-Smirnov, test de, 144

## L

Lineal, complejidad, 66, 177

## M

Maclaren-Marsaglia, algoritmo de, 40

MacLaren-Marsaglia, generador de, 105

Máquina de Turing, 15, 175

Marcha y espera, controlador de, 82, 113-115

Massey-Berlekamp, algoritmo de, 67, 181

Massey-Ruepple, generador de, 118

Máximo orden, complejidad de, 189

Medio del cuadrado, algoritmo de, 31

Memoria, generador basado en, 126

Mersenne, primo de, 65

Método

transformación inversa, de la, 53

síndrome lineal, del, 96, 209

Mochila, generador de, 51

Modulación de fase de reloj, 105

Monte-Carlo, técnica de, 52

Multiplexor, combinación con, 76, 94, 95, 214

Multiplicador de tasa binaria, generador, 108

M-secuencias, 21, 66, 135

## N

Números de Stirling, 153

## P

Parejas, test de, 150

Pasos alternados, generador de, 116

Perfil de complejidad lineal, 178

Periodicidad de secuencias, 134, 258

Permutaciones, generador de, 40

Permutaciones, test de, 156

Permutación de subsecuencias, generador de, 122

Pless, generador de, 98

$PN^2$ , secuencias, 85

Pocker, test de, 152

Poisson, distribución de, 59

Polinomio

característico, 62

irreducible, 65, 87

primitivo, 63, 65, 87

realimentación, de, 62

Windmill, de, 120

Preámbulos, 112

Producto de secuencias pseudoaleatorias, 74

Producto escalar, generador de, 106

Producto interior, generador de, 119

PRN, generador, 33

Pseudoaleatoriedad, 25

## R

Redundancia de clave, 206

Registro de desplazamiento, 61

Ruepple, generador de, 101

## S

Secuencia

aleatoria, 15

autodecimada, 83

$b$ -aria, 17

de De Bruijn, 49, 86

$k$ -distribuida, 17

$m$ -secuencia, 21, 66, 135

G-aleatoria, 21

Gold, de, 231-233

$PN^2$ , 85

pseudoaleatoria, 25

Seguridad, requerimientos de, 203

Semilla, 31

Simulación de procesos, 225-226

Síndrome lineal, método del, 96, 209

*Spread spectrum*, modulación, 226-229

Stirling

números de, 153

triángulo de, 154

Subsecuencias, test de, 157

Sucesivos, tests, 149

Suma, de secuencias pseudoaleatorias, 74

Suma entera, generador de, 49

**T**

Tasa de rechazo, 147, 163

Tatebayashi, generador de, 102

Técnicas

control de reloj, de, 82, 104

modulación de fase de reloj, de, 105

Teorema,

central del límite, 55

Test

brechas, de, 151

chi-cuadrado, 141

colector de cupones, 154

consistencia lineal, de, 95, 207

correlación sucesiva, de, 158

distancia, de, 155

empíricos, 147

entropía por bit, de, 163

espectral, 166

estadísticos, 139

frecuencia, de, 148

hipótesis, de, 139

Kolmogorov-Smirnov, de, 144

parejas, de, 150

permutaciones, de, 156

poker, de, 152

subsecuencias, de, 157

sucesivos, 149

teóricos, 166

transiciones, de, 159

trios, de, 151

Transformación inversa, método de la, 53

Transiciones, test de, 159

Trios, test de, 151

Turing, máquina de, 15

Turing-Kolmogorov-Chaitin, complejidad, 175

**U**

Umbral, generador de, 97

**V**

Variador de velocidad de reloj, 83

**W**

Windmill, generador de, 120

Wolfram, generador de, 126

**Z**

Ziv-Lempel, complejidad de, 186