

ÍNDICE DE CAPÍTULOS

AGRADECIMIENTOS	VII
PRÓLOGO	IX

Parte I

CRIPTOGRAFÍA

1. A Semantically Secure Knapsack Cryptosystem	3
2. Algoritmo para discriminar curvas elípticas con potencias elevadas de 2 ó 3 en su cardinal	13
3. A Note on Secret Sharing Schemes with 3-Homogeneous Access Structure	21
4. Aplicación del doble cifrado a la custodia de claves	33
5. Cifrado de imágenes usando autómatas celulares con memoria	37
6. Efficient and Secure Elliptic Curve Cryptosystem from Point Doubling	45
7. Elliptic Curve Cryptography Applications	55
8. Generador de números pseudoaleatorios de período largo para aplicaciones criptográficas en entornos de PCs	63
9. Generación de secuencias entrelazadas primitivas a partir de un DLFSR	73
10. Hardware vs software: el algoritmo criptográfico IDEA implementado mediante FPGAs	83
11. Los matroides idénticamente autoduales con ocho puntos son representables por códigos autoduales	93
12. On Provably Secure Encryption Schemes Based on Non-Abelian Groups	101
13. Un generador matricial de claves frente a Blum Blum Shub	113
14. Un sistema criptográfico de clave pública a partir de códigos correctores	125
15. Un sistema de cifrado simétrico y algunas consideraciones sobre la seguridad computacional	131
16. Una conjetura acerca de la densidad de primos seguros	139
17. Una revisión de los criptosistemas de clave pública sobre curvas elípticas e hiperelípticas	149

Parte II

CRIPTOANÁLISIS

18. Yet Another Meyer-Müller Like Elliptic Curve Cryptosystem	159
19. On a Gap Implementation of an Attack to the Polly Cracker Cryptosystem	167
20. On the Security of Certain Public Key Cryptosystems Based on Rewriting Problems	175
21. Prediciendo el generador cuadrático	185
22. Reconstrucción de la secuencia de control en generadores con desplazamiento irregular	197
23. Algunas estructuras de acceso multipartitas ideales	205
24. Distributed Key Generation for ID-Based Schemes	215
25. Especificación formal y verificación de requisitos de seguridad	225
26. Modified Paillier Scheme Revisited	235

Parte III

PROTOCOLOS CRIPTOGRÁFICOS Y VALIDACIÓN

27. Abandono de jugadores en esquemas distribuidos de juego de cartas	243
28. Un nuevo esquema RSA híbrido	251
29. Un nuevo esquema umbral para imágenes	259
30. Una aproximación racional a los protocolos criptográficos bipartitos	269
31. Verificabilidad en protocolos de intercambio equitativo	279

Parte IV

SEGURIDAD EN SISTEMAS DE INFORMACIÓN (BD, aplicaciones, etc.)

32. Algunas consideraciones técnicas y de procedimiento para la investigación de delitos informáticos	293
33. Confianza dinámica para la regulación del tráfico en Internet	303
34. Descripción semántica de propiedades y patrones de seguridad en modelos software	311
35. Dispositivos de identificación con verificación biométrica	321
36. El modelo de control de acceso semántico	331
37. Firma de trabajos en la integración de Globus 3 y Globus 2	341
38. Generación de agentes móviles seguros a partir de itinerarios y arquitectura criptográficas	353
39. Hacia una clasificación de métricas de seguridad	363
40. Incorporando seguridad al modelado multidimensional	373
41. Integrando la ingeniería de seguridad en un proceso de ingeniería software	383
42. Propuesta de un modelo de BIOS seguro	393
43. Protegiendo la información de la ruta de los agentes móviles	401
44. Uso de técnicas esteganográficas para la distribución y ocultación de claves en redes corporativas seguras	413

Parte V

SEGURIDAD EN REDES E INTERNET

45. CADAT: Control de acceso basado en tokens y cadenas HASH delegables	425
46. Comunicaciones comerciales no solicitadas y marketing directo: el sistema <i>opt out</i> como excepción (<i>correo electrónico y mensajes SMS con fines publicitarios</i>)	437
47. Desarrollo de un entorno seguro de comunicación en una red ad-hoc	447
48. Detección geométrica basada en anomalías de ataques sobre HTTP	455
49. Detección y prueba de ataques en sistemas de agentes móviles	465
50. Diseño y desarrollo de un sistema colaborativo para la prevención de ataques coordinados	475
51. Extensión de algoritmos de gestión de claves de grupo para redes MANET	495
52. Fast Predictor-Corrector Intrusion Detection System Based on Clustering	507
53. Implementación GnuPG con curvas elípticas	517
54. Mecanismos de protección para agentes itinerantes	527
55. Mejorando servicios de correo electrónico certificado con prontitud temporal y multicasting	537
56. Protocolo asíncrono óptimo para la firma de contratos multiparte	547
57. Un canal de comunicaciones anónimo	557

Parte VI

SERVICIOS DE CERTIFICACIÓN Y NOTARIZACIÓN

58. Diseño e implementación del marco de trabajo de certificados de atributos X509 como plataforma para la delegación de privilegios	571
59. Hacia una caracterización de los servicios de datación digital con respecto a otros servicios de terceros de confianza	581
60. Reducción del overhead de comunicación de un diccionario de revocación offline ..	595
61. Revocación de certificados en la validación de caminos de certificación	605
62. Seguimiento de cadenas de certificados para un sistema de revocación	615
63. Servicio de acceso a la red basado en autorización SAML	625

Parte VII

SEGURIDAD EN DRM

64. Análisis crítico de los sistemas de huella digital para multicast	639
65. ePPV: un sistema de pago por visión sobre Internet	647
66. Identificación de traidores mediante trellises	655
67. PlaPID: una plataforma para la protección de imágenes digitales	665
68. Transmisión progresiva de imágenes marcadas digitalmente	675

Anexos

UNA VISIÓN EMPRESARIAL

A.I. Riesgos y amenazas en la plataforma PC	687
A.II. La importancia de la gestión para un nivel de seguridad efectivo	691
A.III. El panorama de la seguridad de la información en España	693
A.IV. Seguridad en la administración electrónica	695