Paraninfo

Problemas resueltos de Criptografía

Editorial: Paraninfo
Autor: VICENTE JARA VERA, CARMEN SÁNCHEZ ÁVILA
Clasificación: Universidad > Matemáticas
Tamaño: 17 x 24 cm.
Páginas: 160
ISBN 13: 9788428341820
ISBN 10: 8428341826
Precio sin IVA: $ 100038.00 COP
Precio con IVA: $ 100038.00 COP
Fecha publicacion: 16/04/2019

Sinopsis

Las (mal llamadas) clases de problemas constituyen una herramienta fundamental en cualquier disciplina científica. Tradicionalmente, estas clases cumplen el objetivo de complementar aspectos más o menos difíciles de la disciplina en cuestión. Sin embargo, deberían entenderse más como un entrenamiento que capacite al estudiante para resolver cualquier problema (en sentido amplio) que se le pueda plantear en su vida profesional. Con este espíritu se concibe esta colección de “Problemas resueltos” que Ediciones Paraninfo pone a disposición de profesores y estudiantes de una gran variedad de disciplinas académicas.

***

Estamos ante una original y necesaria publicación. Se trata de una colección de problemas resueltos que cubren desde la Criptografía histórica y clásica de todos los sistemas principales desarrollados hasta el siglo XX antes de la aparición de los sistemas digitales y los ordenadores, hasta la Criptografía moderna, hoy en uso.

En este último caso se han cubierto en esta obra tanto los cifradores de tipo simétrico (DES, T-DES, AES…), de bloque y de flujo, como asimétrico (RSA, Elgamal, Curva Elíptica, Paillier…), vigentes y utilizados en la actualidad. Por otro lado, se han incluido ejercicios sobre funciones hash SHA, el intercambio de clave de Diffie-Hellman, los Generadores Pseudo-aleatorios o la Firma Digital, entre otros temas, necesarios para completar el marco de la seguridad criptológica de uso hoy en día.

Esta colección permite así de manera pedagógica y gradual acceder a la comprensión de los sistemas de seguridad actuales, así como a las bases matemáticas e ingenieriles de la Criptografía y la Seguridad

Informática y de la Telecomunicación.

Vicente Jara Vera. Doctor Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid. Investigador y docente en el área de la Criptografía y Ciberseguridad en la Universidad Politécnica de Madrid ().

Carmen Sánchez Ávila. Doctora en Ciencias Matemáticas por la Universidad Politécnica de Madrid. Catedrática en el área de Matemática Aplicada en la Universidad Politécnica de Madrid. Directora del grupo de investigación en Biometría, Bioseñales, Seguridad y Smart Mobility ().

Indice

Presentación

1. Criptografía clásica

1.1. Cifrado Eskitalé

1.2. Cifrado atbash

1.3. Cifrado Polybios

1.4. Cifrado Julio César y César Augusto

1.5. Cifrado de transposición

1.6. Cifrado de sustitución

1.7. Cifrado afín

1.8. Cifrado polialfabético

1.9. Cifrado poligrámico

1.10. Cifrado homofónico

1.11. Cifrado ADFGVX

1.12. Cifrado Vernam

1.13. Cifrado de máquina ENIGMA

1.14. Cifrados de origen desconocido

2. Criptografía moderna

2.1. Cifrado simétrico y asimétrico: generalidades

2.2. Cifrado en bloques

2.3. Cifrado DES

2.4. Cifrado AES

2.5. Cifrado en ujo

2.6. Cifrado de la mochila

2.7. Cifrado RSA

2.8. Cifrado Paillier

2.9. Test de primalidad

2.10. Intercambio Di e Hellman

2.11. Cifrado ElGamal

2.12. Cifrado de curva elíptica

2.13. Generadores pseudo-aleatorios

2.14. Funciones hash

2.15. Firma digital

Bibliografía

Paraninfo Colombia Calle José Abascal, 56 (Utopicus). Oficina 217. 28003 Madrid (España)
Tel. (+34) 914 463 350 Fax
clientes@paraninfo.co www.paraninfo.mx