

INTRODUCCIÓN A LA CRIPTOGRAFÍA

2ª edición actualizada

Autor: Pino Caballero Gil

Editorial: Ra-Ma

Año 2002 –133 páginas

ISBN: 84-7897-520-9

www.ra-ma.es

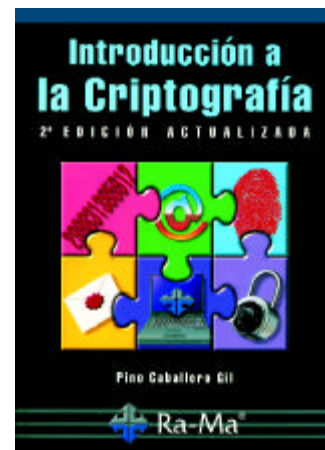
Más de un lustro después, pero conservando el estilo y la estructura de la primera edición, el libro escrito por **Pino Caballero Gil** –una de las más activas y reputadas investigadoras españolas en la materia– pretende realizar una revisión, desde un punto de vista generalista y asequible, de los últimos avances realizados, tanto a nivel internacional como nacional, en lo que la autora ha denominado ‘revolución criptográfica’.

Esta prestigiosa profesora de la Universidad tinerfeña de La Laguna, destaca especialmente el cambio que ha sufrido, durante el final del siglo pasado, la orientación de la investigación, pasando del tema ya clásico de la confidencialidad mediante el cifrado hacia otros más actuales, como son los de la firma digital o los protocolos criptográficos. Dicha variación, según la autora, es una consecuencia del impacto de la informatización en la sociedad, resaltando como acontecimientos más destacados, por un lado, el nacimiento del “nuevo” están-

dar de cifrado en bloque, denominado Rijndael (sustituto del DES), y de otro, la expiración de la patente del algoritmo RSA, lo que facilitó la apertura a las diversas aplicaciones de la criptografía de clave pública.

En resumen, la puesta al día de la obra conserva lo valioso de su antecesora, desecha lo obsoleto y aborda cuestiones actuales de sumo interés, realizando un recorrido introductorio por los aspectos más destacables de cada una de sus facetas, reuniendo la metodología y los fundamentos de la base teórica, y prestando una especial atención a las aplicaciones de mayor relevancia, como por ejemplo, la identificación de usuarios para el control de accesos.

Básicamente, el primer capítulo aborda los conceptos elementales de los sistemas criptográficos y el modelo teórico de Shannon; el segundo se centra en los cifrados simétricos o de clave secreta, en tanto que el tercer capítulo está dedicado al campo de la criptografía asimétrica, describiéndose en él varios de los sistemas de clave pública con mayor relevancia, destacando naturalmente el RSA. Finalmente, en el cuarto se repasan las aplicaciones criptográficas, centrándose principalmente en la autenticación, la firma digital y la identificación de usuarios, y tratando brevemente otras, como la seguridad en las redes y los protocolos criptográficos.



DISAPPEARING CRYPTOGRAPHY

Information Hiding: Steganography & Watermarking

Autor: Peter Wayner

Editorial: Morgan Kaufmann Publishers

Año 2002 –413 páginas

ISBN: 1-55860-769-2

www.mkp.com / www.elsevier.com

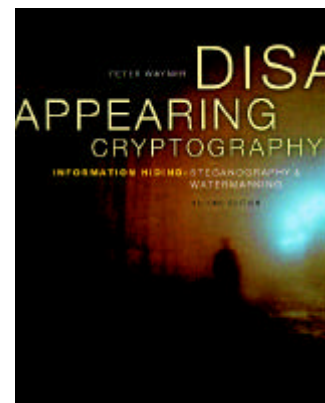
La idea que subyace en la glosa del presente volumen, escrito por **Peter Wayner**, está plasmada en el título con total exactitud: analizar los puntos de vista, los artilugios tecnológicos y las parcelas de investigación relacionadas con la ‘información oculta’ (*information hiding*) en varias áreas de interés, entre ellas, la confidencialidad (esteganografía) y la protección de la propiedad intelectual (marcas de agua digitales).

Básicamente, los capítulos que conforman la obra, que son un total de 17, están estructurados de una forma original: una narración alegórica inicia el recorrido a seguir, ilustrando así las ideas plasmadas en cada uno de ellos. La información

contenida en los mismos está graduada según el nivel de dificultad, y además, se incluye al principio y al final un sumario aclaratorio de los conceptos analizados, los detalles técnicos y los puntos discutidos para que de esta forma, según cita el autor, cada lector pueda diseñarse sus propias herramientas tecnológicas.

El contenido de la obra se estructura de la siguiente forma: 1) Información encerrada, 2) Cifrado, 3) Errores de corrección, 4) Partiendo el secreto 5) Compresión 6) Imitación básica, 7) Gramática y plagio, 8) Reverso y anverso, 9) Vida en el ruido, 10) Reenvíos anónimos, 11) Secretos difundidos, 12) Llaves, 13) Ordenando y desordenando, 14) Difundiendo, 15) Mundos sintéticos, 16) Marcas de agua, 17) Esteganoanálisis. También se incluyen cuatro apéndices, en los que se recogen de forma resumida y ordenada algunos de los conceptos y programas analizados en la obra.

Por último, cabe destacar que el autor utiliza un estilo claro y conciso en el análisis de las distintas variables de un tema, *a priori*, tan abstracto. En este sentido, es de agradecer los numerosos ejemplos gráficos (fotografías, esquemas y capturas de pantalla), que ayudan en gran medida a comprender lo que se ha dado en denominar ‘información oculta’.



WINDOWS INTERNET SECURITY

Protecting your Critical Data

Autores: Seth Fogie y Cyrus Peikari

Editorial: Prentice Hall

Año 2002 – 370 páginas

ISBN: 0-13-042831-0

www.personed.es

El libro escrito por **Seth Fogie** y **Cyrus Peikari**, redactado y diseñado para los usuarios finales, trata de transmitir de una forma sencilla, clara y concisa lo que subyace detrás de lo que los autores han denominado ‘seguridad en Internet’, focalizándose completamente en lo que toca a los sistemas operativos de Microsoft, léase Windows 95/98/Me/2000/XP.

Concretamente, el contenido de este volumen está dividido en seis partes repartidas en veinte capítulos estructurados del siguiente modo: **Parte I. Estudiando el campo de batalla** [Temas: 1) Revisión de sistemas operativos y arquitecturas, 2) Comprendiendo la Red, 3) TCP/IP]; **Parte II. Conociendo al enemigo** [Temas: 4) Reconociendo al enemi-

go, 5) Técnicas de *hacking* para accesos no autorizados, 6) Técnicas de *hacking* para el ataque, 7) Seguimiento de un ataque *hacker*]; **Parte III. Planificando la defensa** [Temas: 8) Construyendo la estrategia de defensa, 9) Sistemas de detección de intrusiones y cortafuegos personales, 10) Cómo dejar de compartir tu ordenador, 11) Seguridad en el comercio electrónico, 12) Dominando las herramientas de red, 13) Virus, gusanos y caballos de troya, 14) Códigos maliciosos]; **Parte IV. Movimientos ocultos** [Temas: 15) Confidencialidad y anonimato, 16) El Gran Hermano te vigila]; **Parte V. Amenazas futuras** [Temas: 17) Windows XP: nuevas configuraciones de seguridad, 18) Amenazas de seguridad futuras]; **Parte VI. Temario Avanzado** [Temas: 19) Editando el registro, 20) Recuperación ante desastres]. También se incluye dos anexos, en los que se recogen, de forma resumida, los puertos comunes de acceso para los troyanos y la bibliografía comentada, incluida la que se puede encontrar en Internet.

Por último, cabe destacar que el libro está ilustrado con numerosas capturas de pantalla y diagramas explicativos, así como anotaciones y recomendaciones, que posibilitan la superación con éxito de los ‘obstáculos’ implícitos en los aspectos puramente técnicos tratados en este volumen.

