

LOS CÓDIGOS SECRETOS

El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet

Autor: Simon Singh
Editorial: Debate
2000 - 386 páginas - ISBN: 84-8306-278-X

En este libro se explica el fascinante desarrollo de los códigos secretos y su análisis, desde el espionaje militar en la antigua Grecia a las claves criptográficas y avanzados algoritmos de aplicación en la informática y las comunicaciones modernas, para revelar cómo la criptografía ha cambiado frecuentemente el curso de la Historia, todo ello relatado de forma ágil y aceptable desde el punto de vista literario. Sólo puede aducirse como detalle puntilloso la licencia del autor –que quizá incomode a los exquisitos– al usar en algunas ocasiones los verbos codificar y cifrar como sinónimos.

El nacimiento de las claves secretas con Julio César; la extraña historia de las cifras Beale, que describen el emplazamiento secreto de una fortuna en oro enterrada en algún lugar de Virginia en el siglo XIX y que aún no ha sido encontrada; el descubrimiento y traducción del antiguo idioma egipcio a partir de la Piedra Rosetta (incluida la controversia Young/Champollion en tanto pioneros); la historia de María Estuardo, reina de Escocia, atrapada en su propio código y condenada a muerte por la reina Isabel I de Inglaterra; los esfuerzos monumentales de creación y desciframiento de los códigos que tanto influyeron en el desenlace de la primera y segunda guerras mundiales (máquina Enigma, incluida); o los colosales avances en los algoritmos criptográficos modernos, en los que se basa una parte importante de la información contenida en los sistemas de información y que transita por redes



(Internet, por ejemplo), hacen que este apasionante libro nos ofrezca una nueva lectura de la Historia, de acontecimientos imposibles de comprender sin conocer las claves y los códigos secretos que se utilizaron.

La autoría corresponde a Simon Singh, Doctor en Física por la Universidad de Cambridge. Después de ser productor en la BBC, dirigió y coprodujo *El último teorema de Fermat*, un documental científico que obtuvo el premio BAFTA y que sirvió de base para su libro del mismo título, que fue un éxito de ventas.

La obra sorprende por su calidad y claridad divulgativas, que la hace muy recomendable para todos los públicos, sin renunciar por ello a la exposición del aparato matemático indispensable y justo para captar el interés de los profesionales de las TIC, incluyo aquellos especializados en técnicas de cifra. ■

FACTBOOK TECNOLOGÍAS DE LA INFORMACIÓN

Autoría: Cap Gemini / SAP AG
Editorial: Aranzadi & Thomson
Año 2000. 768 páginas
ISBN: 84-8410-443-5

Esta obra intenta alcanzar el loable objetivo de recoger en sus muchas páginas todo aquello que un directivo superdotado debe conocer sobre Tecnologías de Información, presumiblemente para no caer de forma indocumentada en el tradicional error de reducir en exclusiva los proyectos TI a meras cifras económicas y precios hombre/hora, con ser este último epígrafe tan llamativo como esencial en las economías modernas. En sintonía con lo dicho, el Factbook de referencia ofrece al empresario la oportunidad de estar informado (en ocasiones, esquemáticamente sobreinformado, lo cual se entiende) de las «últimas» técnicas de gestión de las TIC para

planificar las infraestructuras tecnológicas de la empresa, su calidad, la gestión de proyectos y la externalización de recursos, temas los dichos de gran aprovechamiento mercantil para las compañías autoras de la obra: Cap Gemini y SAP, de escasa tradición –dicho sea de paso– en el mercado español en materias de seguridad técnica y protección de la información hasta la fecha.

En el volumen se abordan las siguientes temáticas: Planificación de la infraestructura de las TI, Calidad de las TI, Gestión del Proyecto, Política de compras, Externalización de recursos, Herramientas y Técnicas de TI, Seguridad, Protección de datos, Soporte para las TI, Comercio e y Sistemas de gestión integrados: implantación y evolución. Para completar el Índice se aportan un Glosario y un Anexo de legislación, que incluyen normas sobre protección de datos, propiedad inte-



lectual, firma electrónica y tributación fiscal de comercio electrónico.

Aunque algunos contenidos sean discutibles por ligeramente incompletos (simplista resulta la explicación del cifrado simétrico) en un contexto técnico –es claro que la obra va dirigida a empresarios y directivos–, no por ello resulta menos recomendable su lectura, y con ella la de los productos es que la misma se perpetúa (actualización de temas, *checklist*, boletines...). En líneas generales, y en materia de protección y seguridad, los autores han realizado un buen trabajo recopilatorio en diversos asuntos: Seguridad, Protección de Datos, Soporte de las TI, y Comercio electrónico: Seguridad de las transacciones, y Medios de pago... No obstante lo dicho, en algunos pasajes los recursos bibliográficos y normativas citados están ligeramente apolillados, algo criticable en una obra editada en 2000. ■

LINUX MÁXIMA SEGURIDAD

Autor: Anónimo
Editorial: Prentice Hall/Pearson Educación
2000 - 780 páginas - ISBN: 84-8322-244-2.
Incluye CD ROM
Sitio: www.pearsoned.es

Este libro está enfocado a aquellos administradores de sistemas, gestores y usuarios de Linux interesados en proteger servidores y estaciones de trabajo contra intrusiones no autorizadas y otras amenazas externas que pudieran afectar a la integridad de sus sistemas. Su autor es un *hacker*, apodado «Anónimo» –programador en Linux y Perl–, que ha sido condenado por varios delitos económicos tras desarrollar una técnica para burlar la seguridad del sistema de cajeros automáticos de bancos. En la actualidad dirige una empresa de consultoría de seguridad en Internet con base en California (EE.UU.), además de realizar programación de contratos para

varias empresas de Fortune 500. Su proyecto más reciente es un cortafuegos llave en mano en Linux diseñado expresamente para empresas de técnicos especialistas en contabilidad. Anónimo, es el autor de la controvertida obra *Maximun Security*, cuya edición española ya fue comentada en SIC (Nº 30, junio 1998).

El contenido del volumen, en el que dicho sea de paso se realizan algunas precisiones y se usan vocablos poco afortunados –quizá producto de una traducción discutible–, se estructura en cinco partes: Fundamento de seguridad en Linux (Presentación de Linux, Seguridad física, Instalación, Administración básica del sistema Linux), Seguridad de los usuarios de Linux (Ataques a contraseñas, código dañino), Seguridad de las redes Linux (*Sniffers* y escuchas electrónicas, *Scanners*, *Spoofing*, Protección de datos en tránsito), Seguridad Linux en Internet (Se-



guridad en FTP, Seguridad en el correo, Seguridad Telnet, Seguridad de servidores *Web*, protocolos *web* seguros, desarrollo *web* seguro, Ataques de denegación de servicio, Linux y *firewalls*, *Logs* y auditorías, Detección de intrusiones, Recuperación de desastres) y Apéndices (Guía de comandos de seguridad de Linux, Índice de seguridad de Linux: problemas de seguridad del antiguo Linux, Otras herramientas de seguridad de Linux útiles, Fuentes para obtener información, Glosario e Índice alfabético).

En realidad el libro no tiene desperdicio: los asuntos tratados en el muy complejo Índice está adecuadamente documentados, y las exposiciones son breves, claras, concisas y precisas, lo que le convierte en muy recomendable en particular para los amantes de Linux y, en general, para una gran mayoría de administradores de sistemas de red. ■